ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2017 ENST 0043

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité « Informatique »

présentée et soutenue publiquement par

Merve ŞAHİN

le 21 septembre 2017

Understanding Telephony Fraud as an Essential Step to Better Fight It

Directeur de thèse : **Aurélien FRANCILLON**

Jury

Olivier FESTOR, Directeur de Recherche, INRIA	Rapporteur
Patrick TRAYNOR, Associate Professor, University of Florida	Rapporteur
Christian BONNET, Professor, EURECOM	Examinateur
Christina POEPPER, Assistant Professor, New York University Abu Dhabi	Examinateur
Christophe SCHOLER, Managing Director, Araxxe	Examinateur
Davide BALZAROTTI, Professor, EURECOM	Examinateur

T H È S E

TELECOM ParisTech
École de l'Institut Télécom - membre de ParisTech

Understanding Telephony Fraud as an Essential Step to Better Fight It

Thesis

Merve ŞAHİN
merve.sahin@eurecom.fr

École Doctorale Informatique, Télécommunication et Électronique, Paris
ED 130

September 21st, 2017

Advisor:
Prof. Dr. Aurélien Francillon
EURECOM, France

Reviewers:
Prof. Dr. Olivier Festor,
INRIA, France

Prof. Dr. Patrick Traynor,
University of Florida, USA

Examiners:
Prof. Dr. Christian Bonnet,
EURECOM, France

Prof. Dr. Christina Poepper,
NYU Abu Dhabi, UAE

Christophe Scholer,
Araxxe, France

Prof. Dr. Davide Balzarotti,
EURECOM, France

Acknowledgements

First and foremost, I would like to thank my advisor Aurélien Francillon for his constant support and guidance during my PhD. I am grateful that he always believed in me, his door was always open for all my questions, and he was always kind and positive, even in difficult times. I would also like to thank Davide Balzarotti, for his invaluable help and advices whenever I needed.

Second, I would like to thank the Government of Monaco for supporting this thesis, and current and former Monaco Telecom employees (in particular Bertrand Petit, Andrea Masnata, Sabine Herine, Benoit Cellario, Jean-Michel Moro and Jeremie Bertrand) for their collaboration and sharing of knowledge. In addition, many thanks to my thesis committee and reviewers for their constructive comments and criticism.

During my projects and experiments, I had several friends and colleagues who helped me to a great extent. Many thanks to Mariano Graziano, Claudio Soriente, Patrick Loiseau, Hugo Venturini, Clementine Maurice, Claudio Marforio, Emre Gozek and Marius Muench for taking care of our (sometimes annoying) phones and helping to conduct the experiments. Thanks as well to Dario Nisi and Federico Barbero for supporting this work with their semester project. Finally, I would like to mention all the telecom professionals I have met in various events. Special thanks to those who answered our questionnaire and shared their valuable knowledge and experiences.

Aside from work, I was so lucky to meet so many great people in such a short amount of time. I want to start by saying thanks to Melek Onen and Leyla Bilge for their friendship and enormous help in adjusting to life in France. Then of course comes the best group of all: Jonas Zaddach, Mariano Graziano, Marius Muench, Fabio Pagani, Emanuele Cozzi, Andrei Costin, Luca Bruno, Davide Canali, Xiao Han, Tom Hayes, Dario Nisi, Samuele Aicardi, Giovanni Camurati and Sebastian Poeplau – I have learned a lot from them, always felt their support, and had a great time together!

I also would like to express my gratitude to my parents and sisters. Thank you for always being there for me!

Last and the most, I want to thank Onur Catakoglu, my partner in life and partner in PhD survival, without whom I would not even start this adventure.

Being a part of Eurecom and the S3 group was a great experience. Thank you all for your friendship, help, support and wisdom!

Abstract

Telephone networks first appeared more than a hundred years ago, forming the oldest large scale network that has grown to touch over 7 billion people. Telephony is now merging many complex technologies and because numerous services enabled by these technologies can be monetized, telephony attracts a lot of fraud. However, there is little academic work on this topic, in part because of the complexity of such networks and their closed nature.

In the first part of this thesis, we aim to systematically explore fraud in telephony networks. We propose a taxonomy that differentiates the root causes, the vulnerabilities, the exploitation techniques, the fraud types and finally the way fraud benefits fraudsters. We present an overview of each of these and use CAller NAMe (CNAM) revenue share fraud as a concrete example to illustrate how our taxonomy helps in better understanding this fraud.

In the second part, we study two different types of fraud that manipulate the wholesale billing process and significantly affect the operators. We start with the *Over-The-Top (OTT) bypass* fraud, which is a recent form of interconnect telecom fraud. In OTT bypass, a normal phone call is diverted over IP to a voice chat application on a smartphone, instead of being terminated over the normal telecom infrastructure. We study the possible techniques to detect and measure this fraud and evaluate its real impact on a small European country, with more than 15,000 test calls and a large-scale user study. Later, we look at the International Revenue Share Fraud (IRSF), one of the most problematic types of wholesale fraud. In IRSF, calls to certain destinations are hijacked by fraudulent operators and diverted to the so-called 'international premium rate services'. To gain a better insight into the IRSF ecosystem, we first analyze the international premium rate test numbers that we collect from several 3rd party premium rate service providers. Using this data, we propose a set of features for the source and destination numbers of a call, which can be used in IRSF detection.

In the last part of the thesis, we switch our focus to the consumer-side telephony fraud, mainly voice spam. We study a recent countermeasure against unwanted phone calls, which involves connecting the phone spammer with a phone bot ("robocallee") that mimics a real persona. *Lenny* is such a bot (a computer program) which plays a set of pre-recorded voice messages to interact with the

spammers. We try to understand the effectiveness of this chatbot, by analyzing the recorded conversations of Lenny with various types of spammers.

While presenting a broad view of telephony fraud, our work also reveals its complex nature and the key challenges in fighting fraud. We hope to stimulate research in this area, in particular, leveraging interdisciplinary approaches to study the diverse effects of telephony fraud.

Contents

Chapter 1

Introduction

Telephony, which is used to be a closed system, has undergone fundamental changes in the past several decades. The introduction of new communications technologies and convergence of telephony with the Internet has added to its complexity. Despite (or because) of having been deployed for virtually hundreds of years, security challenges for telephony are neither well understood nor well addressed.

In this thesis, we focus on the fraud and cybercrime ecosystem surrounding voice telephony (over all three networks - the Public Switched Telephone Network or PSTN, cellular and IP networks). We aim at improving our understanding of the fraud on telephony networks by providing a clear taxonomy of fraud schemes and detaily studying several of them, without ambiguity. We believe this is necessary to fight such frauds, in particular to improve understanding and cooperation between researchers and industry.

A survey of telecom service providers in 2015 estimates the losses due to fraud to 38.1 billion US dollars. This constitutes 1.69% of the estimated global revenue [CFC15]. In addition to the financial losses, fraud aiming at service disruption may have devastating effects, because the telecommunications network is a critical infrastructure with millions of users relying on it both for daily activities, but also for emergency services. On the other hand, consumers are also victims of such fraud, the United States Federal Trade Commission (FTC) receives an average of 400,000 complaints per month [Fed16a].

It is important to note that, in the telephony ecosystem, every actor can be a victim or perpetrator of fraud. Moreover, in some cases there may not be a clear distinction between the two: For instance, an operator that suffers from one fraud scheme can be performing the same (or a different) fraud scheme himself. As there are often no clear laws or regulations that make fraud schemes illegal, fraud usually falls into a gray area of legality and is difficult to address. However, as we will discuss in upcoming chapters, telephony fraud may bring severe consequences (such as degraded call quality, inconsistent and unexpected network behavior) that would affect both the operators and consumers.

Although we focus on telephony fraud, our work has broader implications, especially on online security. For example, a recent work shows how telephony fraud can negatively impact secure creation of online accounts [TIB+14]. Another example is about technical support scam calls, where fraudsters try to install remote administration tools or malware on users' computers [Mic]. Yet another recent incident was the exposure of the recorded telemarketing calls that contain private information (names, addresses, credit card numbers) [Cam17]. Also, several cases were reported, where the fraudsters take over a SIM card by calling operators' customer representatives and later hijack various online accounts which use the mobile phone number as a second factor authentication, including Bitcoin wallets [Hon12, Shi16].

Telephony is often considered to be a trusted medium, but it is not always. A better understanding of telephony vulnerabilities and fraud will therefore help us understand potential Internet attacks as well.

Next, we summarize the contributions of the thesis, together with an overview of the organization.

Contributions and Organization of the Thesis

We start the thesis with a background on the telephony ecosystem, billing methods and call routing (Chapter 2).

Later, in the first part (Part I) of the thesis, we aim to provide a holistic understanding of fraud and clarify the existing ambiguities in fraud terminology. In particular, in Chapter 3.1, we summarize the previous work on the classification of fraud schemes. Then, in Chapter 4, we propose a taxonomy for telephony fraud, which considers the vulnerabilites, the techniques, the fraud schemes and the reasons why fraud may be profitable. Our taxonomy analyzes fraud on these multiple layers, and provides a comprehensive picture of the fraud ecosystem. We then demonstrate the CNAM (Caller NAMe) revenue share fraud within the taxonomy, as a small case study. This chapter is based on a publication in the proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P) in 2017 [SFGA17]. Later in Chapter 5, we give an overview of the state-of-the-art fraud detection and prevention techniques proposed in the academic literature, as well as being used in the industry.

In the second part, we present detailed studies of two fraud schemes commonly experienced by telecom operators. Chapter 6 describes a relatively recent fraud scheme called Over-The-Top (OTT) bypass. We first analyze the inner workings of this fraud scheme and evaluate possible detection and measurement techniques. For a deeper examination of the prevalence and the effects of this fraud on the telephony network and users, we conduct experiments with more than 15,000 test calls and a large scale user study. We show various problems that OTT bypass can cause in a network, and the amplification of these problems when multiple fraud schemes collide with OTT bypass. This chapter includes the work that is published at the ACM Conference on Computer and Communications Security (CCS) in 2016 [SF16]. In Chapter 7, we study the long-standing, yet unsolved problem of International Revenue Share Fraud (IRSF). Similar to the previous chapter, we first describe this fraud scheme in relation to our taxonomy, and explain the challenges in fighting it. Later, we explore the IRSF ecosystem, by analyzing the International Premium Rate Number (IPRN) resellers and their test portals frequently used by the fraudsters: We present our observations on the more than 150,000 international premium rate test numbers that we collect from such test portals. Finally, we propose several phone number features that might be useful in detecting IRSF, by leveraging the information on the test numbers.

In the third part of the thesis, we focus on voice spam, which has been a significant problem for phone users. After a description of the problem and an overview of the honeypot-based studies (Chapter 8), we present "Lenny", a chatbot and a high interaction honeypot, which can be used to defend against various types of spam calls. Using 200 call recordings that were collected at a public deployment of this chatbot, we analyze the effectiveness of the chatbot from an applied conversation analysis perspective. We also present various observations on the different types of spam calls and discuss the challenges in the widespread use of chatbots against voice spam. This chapter (Chapter 9) is based on a publication in the proceedings of the Symposium on Usable Privacy and Security (SOUPS) in 2017 [SRF17].

Finally, we conclude the thesis in Chapter 10, with a discussion of the possible future research directions.

Chapter 2

Background on the Telephony Ecosystem

In this chapter, we provide a high level overview of voice telephony related networks and components that are required to understand fraud in voice telephony.

2.1 Telephony Networks and Components

Today, the global telephony network encompasses many different technologies. While the Public Switched Telephone Network (PSTN) has been the primary medium enabling telephony since the last century, cellular networks and Voice over IP (VoIP) technology were incorporated into it over time, enabling many different services.

Figure 2.1 presents an overview of the current telephony ecosystem. Next, we will explain the key concepts in more detail.

Public Switched Telephone Network (PSTN) The historic core of telephony networks is formed of copper telephone wires that use circuit-switching technology to transmit analog voice signals (also called Plain Old Telephone Service (POTS). Switches in operators' *Central Offices* (PSTN CO) control call establishment by creating a dedicated physical circuit from the caller's phone to the callee's phone. Initially, the same circuit was used for the *in-band* signaling between the callee and the operator (e.g., dial tone and ringing) but also between operators (e.g., billing, call routing).

Integrated Services Digital Network (ISDN) ISDN allows digital transmission over the copper lines. Up to 30 lines can be multiplexed on a physical phone line (T1 or E1 *Primary Rate Interface* (PRI)) for transmitting data or voice. ISDN dedicates a separate channel for signaling (*out-of-band* signaling), which constitutes the user part of the Signaling System 7 (SS7) protocol [DH05]. Digital networks and out-of-band signaling solved some security problems (see Section 4.5.1) and introduced new features to telephony, e.g., voice mail, call forwarding and caller ID display.

Mobile Networks Most of the mobile networks are still using GSM protocols and equipment (2G) but also support more recent protocols (3G and 4G/LTE). Each generation of mobile communication uses some form of encryption (over the wireless channel) and specific equipment to handle the communications and customer identification.

In GSM, Base Stations (BTS) are connected to the Mobile Telephone Switching Office (MTSO), which contains the core network elements. Each MTSO contains at least one Mobile Switching Center (MSC) that is responsible from keeping and updating subscriber information, registration and authentication of subscribers, call routing and billing records. Operator's network also have a Home Location Register (HLR) or a Visitor Location Register (VLR) which is used to keep information about location of the mobile phone.

Mobile phones (except CDMA phones) use a SIM (Subscriber Identity Module) card with an International Mobile Subscriber Identity (IMSI) that uniquely identifies the user on the network. The SIM card contains a cryptographic key which is assigned by the operator and associated with the IMSI.

Voice over IP (VoIP) With the rise of the Internet, transmission of Voice over IP (VoIP) emerged as an alternative to traditional PSTN. Over time, VoIP technology has become a major part of the global telephony network, e.g., it is used for dedicated peering links between operators or to reach VOIP phones with regular, internationally routable, phone numbers. Currently, telephone networks consist of various gateways between PSTN, cellular networks and VoIP telephony.

Over-The-Top services (OTT) are services which work on top of data links and, in general, out of operators' control. Such voice services (e.g., Skype, Viber) are attracting more users and are seen as a threat by the operators [For15].

Private Branch Exchange (PBX) Enterprise customers usually use a PBX to manage their internal and external communication needs. A traditional PBX provides *extensions*, i.e., an internal phone number to reach each user within the enterprise. A PBX also has a connection (called a *trunk*) with an operator to reach the PSTN or mobile networks. The trunk usually supports a certain number of simultaneous communications, which may be different from the total number of phone numbers used by the company. A traditional PBX uses phone cables for all internal lines which is expensive to deploy and manage. On the other hand, an IP-PBX can connect IP phones or soft phones over IP (see Figure 2.1). IP-PBXs can use PRI trunks, SIP trunks or SIM cards (using a SIM gateway, or 'simbox') for external communications. The generalized internet access, powerful CPUs (which allow audio transcoding) and powerful open source software (e.g., Asterisk [Ast]) makes possible to use any computer as an IP-PBX to which interface cards can be added (e.g., to support a PRI trunk or analog phones).

2.2 Telephony Actors

Apart from the end-users, the main actors of the telephone networks are the operators (carrier, telecom service provider) and third party service providers.

Operators The deregulation of the telecommunications markets have resulted in wide variety of service providers and operators. Some of these operators invest in, or own, the network infrastructure and equipment, whereas others only resell the service they buy from other operators (e.g., Mobile Virtual Network Operators (MVNO)). Often, the term 'carrier' is used to refer to the operators providing interconnect services between other operators.

Third Parties Third party service providers and VoIP resellers [Voi] are important actors of the telephony ecosystem. Value added service (e.g., premium rate service) providers deliver content to end-users via phone calls, messaging or data network (e.g., gaming, chat lines or news). VoIP resellers buy communication services from carriers, and resell through VoIP gateways. They provide geographical numbers (numbers with country and area codes), mobile numbers, toll free numbers and premium rate numbers in every country. In recent years, cloud based communication services have appeared (e.g., Twilio [Twi]) and provide access to cheap bulk phone numbers (that are usually recycled), *cloud PBX*, SIP trunks or scripted *Interactive Voice Response* (IVR) systems.

2.3 Billing Systems and Call Routing

Understanding billing mechanisms is key to understand telephony fraud, as most of the fraud schemes aim at financial benefits. Operators keep Call Detail Records (CDR) for each call routed (originated, terminated or transited) over their networks. CDRs are created at the network switches and include various information, such as originating and destination phone numbers, inbound and outbound routes, date, call duration and call type. All CDRs generated at different switches are collected and processed in a central location and sent to the

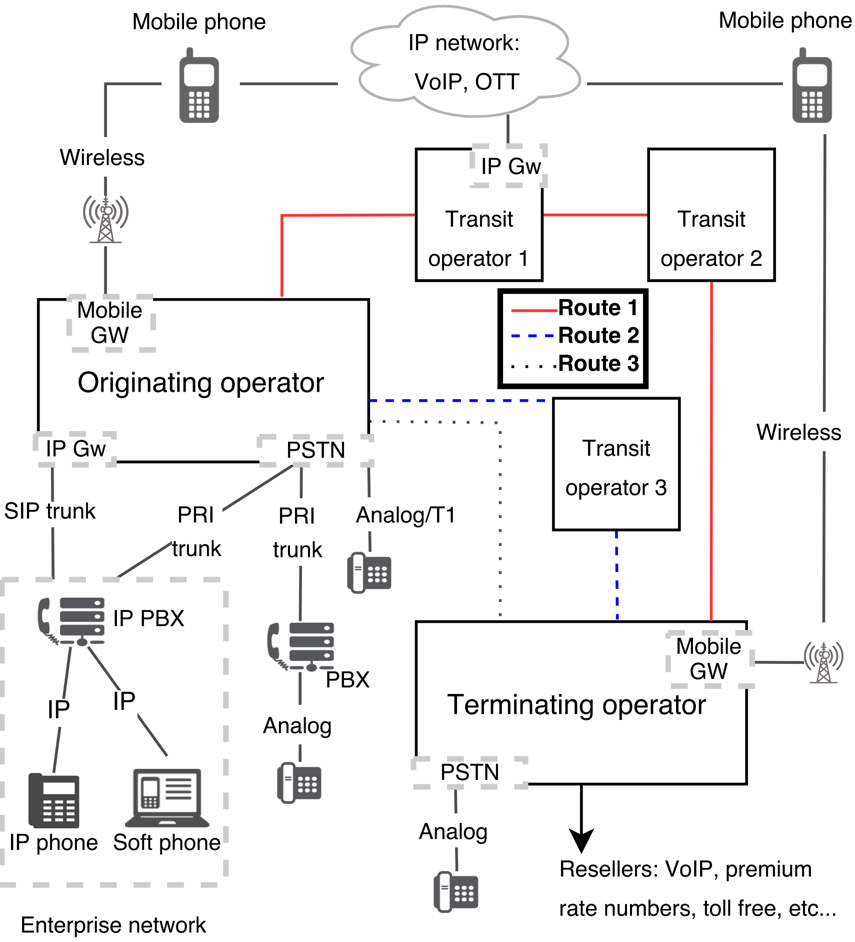


Figure 2.1: Overview of the telephony ecosystem.

billing system to be charged. Operators deal with two types of billing: *retail billing* and *wholesale billing*.

Retail Billing Most services (international or domestic landline, mobile, or data services) are billed to customers at the end of the billing period (*post-paid*). However, mobile services are also often available as *pre-paid*. The post-paid billing process involves the collection of usage reports, validating them, applying the tariff plan and sending the final bill to the customers. To be sure to be paid, operators verify the personal and financial information of their post-pay customers. In the pre-paid billing, customer information check is often less strict, because the customer will only be able to use the service he already paid for. Other variants of pre-paid service are the calling and top-up cards. One technical difficulty with pre-paid billing is that it requires real time tracking of usage records [ETS].

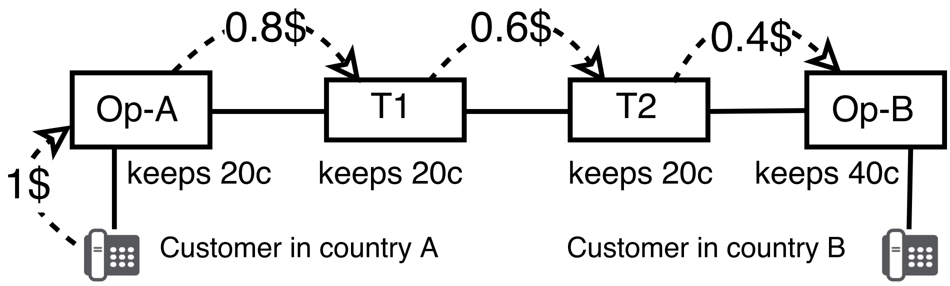


Figure 2.2: Overview of money flows in a call.

Wholesale Billing The wholesale (interconnect) market is mainly for international and long distance calls, as operators need to make *interconnection agreements* and to rely on *transit operators* to be able to provide world-wide coverage. Such interconnect agreements describe the prices for interconnect communications, but also policies and dispute resolution. There are also stock-exchange like platforms where operators can buy and sell minutes directly and even anonymously [Ele03].

An international call originated from a mobile or fixed line, travels over multiple intermediate operators (transit operators) before reaching its destination country and operator. Each of these transit operators get a share from the call revenue for passing over the call, and the local operator in the destination country receives a *call termination fee* for terminating this international call on its network [Big12].

An example of money flow, in an international call, is shown in Figure 2.2. The call is initiated from the originating operator (Op-A) and goes through two transit operators, to finally reach the customer through Op-B. For this call, Op-A will bill his end customer for a *collection charge* of $1. However, the operator will pay 80c for routing the call, and keep 20c, similarly the transit operators each keep a 20c and finally the terminating operator Op-B will keep the termination fee of 40c. In other words, each upstream (originator) network pays to its downstream (terminator) network the cost of terminating the call [Jon06] until the call reaches its final destination. Operators may have multiple routing choices to route a call. They choose the best route depending on the prices and quality of alternative routes.

Quality of service is generally measured with *Average Call Duration* (ACD) and *Answer Seizure Ratio*[1] (ASR). Other aspects such as the transit operator's reputation (prone to fraud) and ability to pay are important too.

The process of checking the quality and reliability of a transit operator before the partnership agreement is called *due diligence*. Unlike in IP networks, the routing of a call is very often opaque. Each operator only knows the next hop of the

[1] The number of answered calls divided by the number of total calls.

upstream and downstream routes as well as the originating[2] and the destination number.

[2]The originating number may be absent or incorrect.

Part I

A Deeper Look into the Fraud Ecosystem

In this part, we aim to provide a comprehensive picture of the current telephony fraud ecosystem. We start by explaining the challenges in understanding fraud, and limitations of the previous work on telephony fraud classification. Then, in Chapter 4, we present our taxonomy that analyzes telephony fraud in several layers. In the last chapter, we give an overview of the existing fraud detection and prevention techniques.

Chapter 3

Obstacles in Understanding Fraud

Having a comprehensive understanding of telephony fraud is a challenging task. For this, one needs to have a good understanding of the telephony ecosystem, its history, underlying technologies, regulations and international agreements. Even the industry experts working in fraud management may have a partial view, because they often specialize on the fraud types which are the most frequently encountered, or detected, in their businesses.

Existing definitions of telecommunications fraud usually focus on obtaining free telecommunications services and gaining financial benefits [GH99,Hoa08]. In this work, we narrow our perspective to voice telephony but we do not limit frauds to financial benefits (a definition will be given in Section 4.1). Perpetrators of voice fraud may be any actor of the telephony ecosystem, such as operators, third party service providers, customers, employees and any other external party with the means and motivation to commit fraud. On the other hand, victims of voice fraud can be the operators, customers and enterprises that use telecom networks.

Perpetrating fraud in telecom networks is relatively easy. Most of the attacks can be performed remotely and they do not require major equipment or high level of technical expertise. Moreover, it is often very easy to obtain a financial benefit from telephony fraud [Hoa98]. Often, fraud is buried in massive volume of traffic and large variety of services. Therefore, it is difficult to identify, detect and prevent.

We list some of the challenges faced in understanding fraud:

- **Ecosystem diversity:** Telecom industry embodies different communities such as operators, regulators and users. Every actor in this ecosystem experiences or approaches fraud in a different way. In addition, fraudsters may have various motivations and skills, and their methods are only limited by their imagination.

- **Inconsistent terminology:** Each community has its own terminology, context and resources regarding fraud which is a major obstacle in understanding fraud. A fraud scheme often has multiple names, e.g., describing a variant, the technical aspect or the user visible part of the iceberg. In other cases, one name is used to describe several different schemes.

- **Restricted access:** Operators and service providers usually share fraud related information (recommendations, best practices) among their partners and various industry associations (e.g., TMForum, i3Forum, GSMA, FIINA, CFCA).[1] Unfortunately, such groups are often restricted to vetted members and do not make their documents publicly available. The point we make in this thesis is the opposite: *we will only be able to fight fraud efficiently if it is well understood and openly discussed*.

- **Incomplete view:** A lot of information about fraud schemes can be found in white papers by companies selling fraud detection systems [Trab, Suba]. However, those often present an incomplete view because of the possible commercial interests.

- **Lack of data:** One reason for the lack of academic work could be the lack of data for conducting experiments. Obtaining real data is difficult because of the privacy constraints and technical limitations.

We next explain the related work from different communities and their limitations.

3.1 Previous Work on Fraud Classification

There is no previous systematic survey of telephony fraud, however, there are resources that handle part of the problem or try to reduce the problem into a single dimension such as actors (fraudster or victim) [Wik], underlying service and technology [Joh12, GH99], attack methodology or attack motivation [BVW10]. However, the fraud ecosystem is too complex to be explained with a binary classification.

[And08] studies the telecom system security, covering many fraud related topics. It concludes that information on phone fraud is scattered and no single resource provides a comprehensive view. Another important work on telecommunications crime [Col99] presents historical information and phreaking techniques, PBX,

[1] www.tmforum.org, i3forum.org, www.gsma.com, www.fiina.org, www.cfca.org

mobile, and premium rate related fraud. However, it does not mention the inter-carrier related fraud and more recent problems such as robocalling.

A first attempt to create a fraud classification system that distinguishes *enabler techniques* and *fraud types* was proposed by the TM Forum [SAE12], an approach that we extend in this work. The aim of TM Forum was to enhance the fraud reporting process, and facilitate fraud monitoring, analysis and benchmarking.

Academic work is rather limited on this topic, because the papers are either too old, covering a small part of the problem, or focusing on fraud detection. In [GSBA15, BGG+16] authors analyze the data from phone honeypots uncovering several fraud schemes affecting end users. [TDZA16a] analyzes voice spam ecosystem and evaluates existing solutions. There are also many books on telecom security related topics such as revenue assurance [Mat05], fraud and quality of service management [Joh12], UC (Unified communications) [CE13] and VoIP network security. However, none of those resources provide a comprehensive view of the fraud ecosystem.

International bodies, such as ITU (an agency of the United Nations) and BEREC (an agency of the European Union), and regulatory bodies, such as the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), are also concerned about some aspects of the fraud (e.g., *number misuse* [Int07], *robocalling* [Fed15a]) but they also do not aim at providing a comprehensive view on the telephony fraud.

Fraud classification in other domains Several taxonomies or systematization of fraud exist in other domains. [BDD15] presents a taxonomy of fraud that are committed against individuals. In [ES12], Edge et. al., present a rule based policy management language for proactive fraud management in financial data streams.

In [Ros15] Ross presents a broad view of fraud schemes, but only quickly discusses fraud in telephony systems. [Ros15] presents the 3 Cs rule for identifying Fraud: Conduct, Circumstances and Consequences. This 3 C rule is useful to recognize a fraud in practice but does not help to understand and systematize it as our approach does. However, the third C "Consequences" is similar to our benefits category (which we will describe in Section 4.6).

Chapter 4

A Taxonomy of Telephony Fraud

In this chapter, we aim to provide a systematization of knowledge relevant to understanding telephony fraud. Our taxonomy allows to classify the techniques and fraud schemes without ambiguity. We believe that a good understanding of telephony fraud will provide insights for future research, increase cooperation between researchers and industry and finally help in fighting such fraud.

A fraud scheme often has multiple names, e.g., describing a variant, the technical aspect or the user visible part of the iceberg. In other cases, one name is used to describe several different schemes. We therefore also aim to clarify the inconsistencies in existing fraud terminology.

Moreover, this study may be beneficial to increase fraud awareness among users and operators that are not members of any industry group. In fact, a survey conducted among the wholesale operators in 2013 [Sub13] shows that around 73% of the operators are not members of any of the industry groups.

4.1 Overview and Systematization Methodology

One common fallacy in previous classifications is that the fraud descriptions are often bundling different problems together. For example, a fraud will be described by the technique it uses. However, techniques used by a given fraud often change, e.g., in reaction to the implementation of new countermeasures. The intricate combination of those concepts makes previous descriptions confusing or narrow.

We propose to analyze the problem in several layers to clarify the cause and effect relations surrounding telephony fraud and explore a part of the problem at each layer. For this purpose, we base our classification on the following definition of fraud:

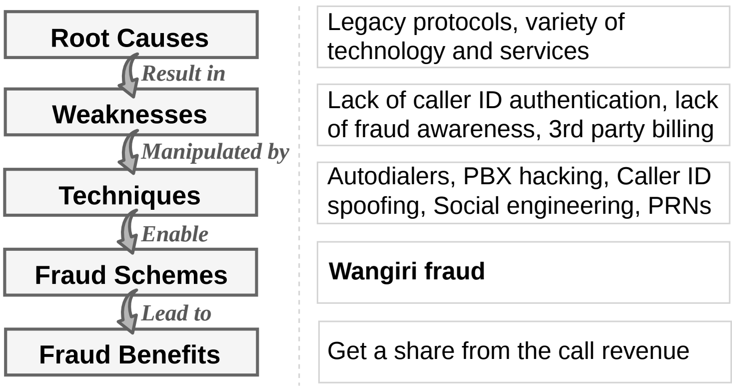


Figure 4.1: Overview of our fraud taxonomy with an example of Wangiri fraud.

> A **fraud scheme** is a way to obtain an illegitimate **benefit** using a **technique**. Such techniques are possible because of **weaknesses** in the system, which are themselves due to **root causes**.

Based on this general definition we further refine these concepts as follows:

- A **root cause** is an inherent characteristic of the telephony networks, standards and ecosystems which can result in weaknesses.
- A **weakness** is a vulnerability or a feature of the system, that can be manipulated in unintended ways.
- A **technique** is a mechanism, or service, which is used to abuse a weakness in a telephony system to commit a fraud. Such techniques may be illegitimate (e.g., compromising a PBX) or may have legitimate uses (e.g., conference calling) that are abused to commit a fraud.
- A **fraud scheme** is a method which is intentionally and knowingly used by a fraudster, relying on one or more techniques, to abuse a user, an entity, or a system with the goal of obtaining an illegitimate benefit.
- **Benefit**: The goal of a fraud scheme is to obtain a benefit, this can be a monetary benefit or not (e.g., competitive advantage, reputation, bypassing regulation).

4.1.1 Applying the Taxonomy on Wangiri Fraud

To present our taxonomy in a concrete way, we analyze Wangiri fraud, which is a well-known voice scam, within this context. Figure 4.1 summarizes this example.

Wangiri ('one ring and cut' in Japanese) fraud is also called *callback* scam, *ping call* or *one-ring* scam. In this scam, the fraudster leaves missing calls on a huge number of (usually randomly chosen) victims' phone numbers. The call only rings once, so that the victim does not have the opportunity to answer. As a result, the curious victim calls back the phone number, which usually turns out to be a premium rate number (PRN) owned by the fraudster. The **fraud benefit** in this scheme is financial: the premium rate service provider pays the fraudster a certain share of the call revenue for each minute of call received by this premium rate number.

To generate the large number of calls, the fraudster can use **multiple techniques**, e.g., autodialers or compromised PBX systems and spoof the originating phone number (caller ID) as the premium rate number. The fraudster can easily set up this scheme using online premium rate service providers or resellers. Such online services even include ready to use IVR systems to keep victims on the phone for a longer duration.

These techniques abuse several **weaknesses** in the telephony ecosystem, which could be related to the underlying technologies (e.g., lack of caller ID authentication), third party services (e.g., abusive PRN resellers) or end users (e.g., users' lack of fraud and security awareness).

Finally, we can identify the **root causes** that result in these weaknesses, such as the presence of legacy protocols, convergence of multiple technologies and variety of service providers. Analyzing the problem at these different layers can help us see the overall picture and anticipate the outcome of possible actions to fight this fraud.

4.1.2 Methodology

Our goal is not to provide an exhaustive list of frauds, but to provide a comprehensive survey of the topic. For this, our first source of information was the literature, books, publications but also white papers from industry groups and fraud management companies. However, this is not enough as information on the topic is scattered and often incomplete.

To make sure we had a good understanding of the ecosystem, we interviewed several experts in the field and participated to industry forums. We also sent a questionnaire to a selected list of experts and well identified mailing lists to obtain feedback on the first version of our taxonomy. We only had 15 answers to this questionnaire (so we don't present statistics) but most were from experts in fraud management or those working in the field. Their feedback and some discussions with the respondents allowed us to refine our taxonomy, to better understand fraud, and to discover new fraud schemes.

Figure 4.2 shows a detailed view of the taxonomy. However, it is not feasible to draw all the relations between each component of the figure in one page. Therefore, we created a dynamic picture showing all the links between

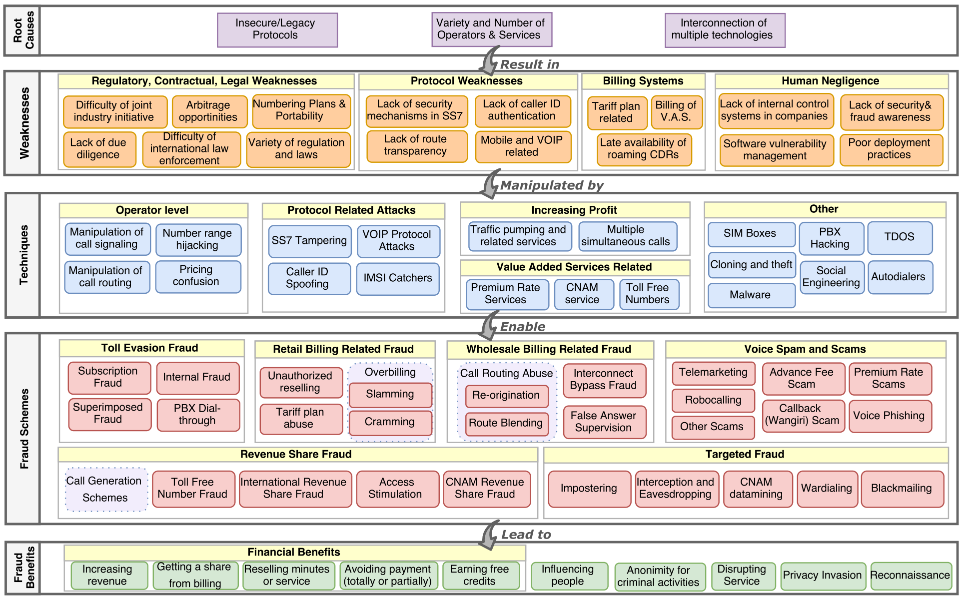


Figure 4.2: Comprehensive picture of voice fraud. A dynamic figure with links can be found at: https://telephony-fraud.github.io/taxonomy/

the components which is available, with a copy of the questionnaire, at: https://telephony-fraud.github.io/taxonomy/.

Finally, our goal with this classification is to help explain each component of telephony fraud without ambiguity. In the next sections, we describe the taxonomy: root causes and weaknesses, techniques, fraud schemes and benefits in more detail.

4.2 Root Causes of Telephony Fraud

Root causes are inherent to the telephony ecosystem and are unlikely to be solved in the near term.

The **legacy systems** that lie in the core of telephony network were not designed with security in mind. This was not an issue when telecom networks were a closed and controlled environment where all the entities were trusted, or at least identifiable (monopolistic operators). However, this can cause various weaknesses in today's environment. Unfortunately, upgrading these legacy systems on a global scale is not feasible in near future, due to high costs.

Telecommunication networks are made of different, **interconnected technologies**, services and products, which are usually obscure and poorly understood [Joh12]. This leads telephony networks to have a large attack surface. All actors in the ecosystem have to adopt themselves to new technologies, while remaining vigilant against possible attacks.

As the telecom market became more liberalized, a **large number and variety of operators** have gotten involved in the market. As a result, it is not possible to make sure that all parties are carrying good intentions. It is also not possible to reduce the number of operators, as this would damage the competition and liberalization, and prevent the growth of new technologies and diversity of services.

4.3 Weaknesses of Telephony Networks

Weaknesses are consequences of the root causes, but they can be addressed or mitigated, if they are properly identified. We classify weaknesses in 4 categories related to **protocol and network**, **regulation**, **billing** and **human factors**.

4.3.1 Protocol and Network Weaknesses

Telecom networks are an interconnection of PSTN, cellular and IP networks, all of which have different weaknesses and vulnerabilities. In particular, the **lack of security mechanisms in SS7 signaling** leads to many problems, SS7 itself does not have any encryption or authentication mechanisms. Therefore, operators using SS7 (or anyone with access to signaling links) can tamper with SS7 messages or interact with SS7 systems [DH05]. The SIGTRAN protocol suite was introduced as a transport layer for SS7 messaging over IP, which can use TLS or IPSec [PTL15]. However, there is no end-to-end security and each transit operator can modify the SS7 messages.

With deregulation and Internet convergence, it became **easy to access SS7 networks**, i.e., access is no more restricted to a small number of trusted operators. Nowadays, operators employ traffic screening mechanisms and filtering rules to discard unwanted incoming signaling messages [DH05]. Indeed, it became easier for external parties to have partial or complete access to signaling through femtocells, SIP/PRI trunks, operator partnerships (e.g., value added services) or by attacking telecom equipment [Lan12]. Legal interception gateways, which operators often have to install to comply with laws, also have direct access to SS7, and have been sources of vulnerabilities [SCCB05, BBB+06].

The SS7 protocol also does not support a mechanism to trace the route of a call. Each switch has its own routing table and select the appropriate outbound link based on the destination phone number, pricing and commercial agreements. Thus, they only have a partial view of the call route which leads to a **lack of route transparency**. VoIP interconnections make it even harder to trace the calls. Similarly, during a phone call, caller ID (identification) information is transmitted between operators through the signaling system of the underlying telecommunication service. However, this information cannot be trusted as

SS7 [DH05] or most of the IP based signaling protocols **lack caller ID authentication**.

Wireless and VoIP networks also often lack proper authentication or encryption, e.g., between a mobile device and a base station, leading to the possibility to use *IMSI Catchers* [JR00]. Most of the problems in mobile network protocols are addressed starting with third generation networks. However, legacy technologies are still widely deployed, opening the possibility of downgrade attacks [Abi]. In addition, cellular and VoIP networks inherit some vulnerabilities from PSTN, as calls still traverse PSTN networks [EC06]. LTE networks involve both VoIP and cellular network related issues, and can be vulnerable to billing, DoS and caller ID spoofing attacks [KKK+15].

4.3.2 Regulatory, Contractual and Legal Weaknesses

Arbitrage, as a concept in economics, is the manipulation of price discrepancies in different markets. In telecommunications, price discrepancies can occur between mobile/PSTN/VoIP originated calls or domestic/international calls. Fraudsters can circumvent the high cost route or terminate a high cost call in a low cost market to profit from the price difference. Countries with high international call termination rates (usually developing countries with heavy regulations [Alt]) are frequently manipulated by fraudsters.

Numbering plans allow to decode phone numbers and find the operator or type of service for a given number. The E.164 standard describes a globally routable phone numbering structure and assigns number ranges (country codes) to countries [E1697]. Each country has its own regulatory body to further assign and control its national number range, but number portability blurs the lines. There is no global numbering plan listing all valid number ranges that are in use, although some databases allow partial lookups[1]. Therefore, an operator may not know for sure, if a phone number in another country is currently in use [PST14]. VoIP protocols use the notion of contacts instead of phone numbers. However, if the call traverses a VoIP/PSTN gateway, a phone number should be associated with the contact [PLCY13]. Many OTT providers use phone numbers to identify and authenticate their users (e.g., Viber, WhatsApp).

Telephony ecosystem embodies a large **variety of regulations and laws**, and the notion of legality can significantly vary depending on the country and the communication medium. For example, some countries ban VoIP usage, e.g., to protect their revenue from international call termination [Gue]. Some countries try to bound OTT providers by the same regulations that operators are subjected to [Was14, OTT15]. In general, the need for regulation may not be perceived before the system is manipulated. Therefore, it can be difficult for regulators to anticipate regulation needs.

[1] www.bsmilano.it, www.numberingplans.com

The **lack of cooperation** is another weakness of telephony ecosystem. Law enforcement authorities have **difficulties in international law enforcement**, which makes identification of fraudsters difficult, even when the fraud is detected [Sub13]. Moreover, despite the presence of international organizations, there is a **lack of joint industry initiative** to fight fraud. Due to the privacy issues and competition, operators are usually not willing to share their pricing terms, routing options or fraud related findings [Ber12]. In addition, not all the operators have the same incentives to fight fraud. Indeed, sometimes the losses due to fraud at one operator can benefit another, innocent, operator in addition to the fraudster. In other cases, fighting small scale fraud can be more expensive than the losses due to the fraud itself.

Having a large number of operators brings the inevitable need for partnerships between them. **Lack of due diligence** in these partnership agreements make call traffic vulnerable to fraud, if one party has fraudulent intentions. Especially the competitive transit operators may ignore route quality and make use of cheap routes to grow their business.

4.3.3 Billing Related Weaknesses

Complexity of billing mechanisms have increased with the introduction of new technologies and services. Any mistake in the billing process (e.g., inaccurate or late billing, errors in pre-paid credit tracking) can be manipulated by fraudsters [Joh12, Mat05]. Most of the time, operators are reluctant to change the legacy billing systems, due to the high cost and backward compatibility problems. Errors in the complicated *tariff plans* are also known to be exploited by fraudsters.

Billing of **value added services** is another weakness, because it adds a third party to the system. Because of their high fees, they can result in significant losses. Operators should be careful in identification of value added service numbers and registration of entities who use these numbers. Unfortunately, fraudsters often abuse complex networks of resellers and service providers and are therefore difficult to identify.

Mobile roaming services also complicate billing. **Roaming CDRs** are not immediately available to the home operator, so detecting and stopping fraud quickly is difficult. To address this issue, Near Real Time Roaming Data Exchange (NRTRDE) systems have been developed. Nevertheless, using NRTRDE, the transmission of CDRs from the visited network to the home network still takes about four hours [All], which is a long enough time window for the fraudsters to make profit.

4.3.4 Human Negligence

Humans interact a lot with telecom networks. This leads to various weaknesses due to their negligence or naivety. Lack of security and fraud awareness is frequently manipulated by fraudsters [Joh12]. On the enterprise level, lack of internal control systems (such as access control), poor deployment practices (weak passwords, neglecting updates) and lack of vulnerability management in software and hardware systems are some other sources of weaknesses [CE13].

4.4 Techniques Used in Fraud Schemes

In this section, we describe the techniques which enable various fraud schemes. Some of these techniques may have legitimate uses as well. We group them by the kind of access they require (e.g., operator level) or their purpose (e.g., increasing profit).

4.4.1 Operator Level Techniques

Number range hijacking occurs when a fraudulent operator advertises very cheap rates for a destination number range and attracts traffic from other operators [i3 12]. For example, in Figure 2.1, there are several possible routes to the terminating operator. Assume that routes 1 and 3 are the usual routes. In the event that the transit operator 3 suddenly advertise a very cheap rate (possibly for a very small range of numbers), the originating operator may select route 2 for delivering the calls. In this case, the calls to the victim number range will be hijacked and routed/terminated fraudulently [Dav08, Dav12]. Lack of due diligence in operator partnership agreements facilitates this technique.

A parallel can be made between phone number range hijack and BGP hijacks [VTD15]. In both cases, a part of the traffic is redirected by a malicious entity that advertises false (or misleading) information. For phone number ranges, this is the price for a destination, while in BGP, this is the prefix advertisements. However, as opposed to the IP networks, call routing is opaque (Section 4.3.1), which makes detection more difficult. Furthermore, there is no mechanism in telephony networks to directly authenticate the owner of a number range or check if an operator really has the connectivity to route the call to that number range. Like with BGP, deploying security mechanisms would face significant practical difficulties [BFMR10].

Manipulation of call routing is possible as the operators have full control over the calls that transit through their networks (either legitimately or because of a hijack). A fraudulent transit operator can divert a call or send it over illegitimate routes to perform different fraud schemes. In case of *call short-stopping*, the transit operator directly terminates the call (e.g., to an IVR) instead of sending the call to the legitimate destination. It can also selectively *short-stop* only some of the calls. Due to the lack of route transparency, the originating operator cannot know if the call was routed normally and has reached the correct destination.

Manipulation of call signaling messages is also easy for the operators. For example, the caller ID can be changed to fake the origin of the call (which may affect billing). Call setup signals can be tampered to answer the call before it is actually answered by the customer (*early answer*) or to not disconnect the call immediately (*late disconnect*) [Meu14]. The call will be longer than it should, which will affect the revenue (False Answer Supervision, see Section 4.5.3).

Pricing confusion is the use of multiple and varying pricing plans to confuse customers about the real market price of a service. Such operators constantly provide new offerings and special introductory discounts, to be competitive [And08], but quickly change the prices once customers are registered.

4.4.2 Techniques For Increasing Profit

Here we present techniques which can be used to make a fraud scheme more efficient, however, many of them have a legitimate use.

Traffic pumping, or artificial inflation of traffic, is the act of generating a high level of call traffic to some phone numbers deliberately. This can be achieved by creating and advertising 3rd party services such as conference calling [Fre], free radio broadcast over phone [Tra13] or adult entertainment. By providing such services for free (or at a very low cost) many users are attracted, which, in turn, generates a high volume of calls. Value added services or arbitrage opportunities can make traffic pumping advantageous in certain fraud schemes (Sections 4.5.4 and 4.5.3).

Initiating **multiple simultaneous calls** allows the fraudster to increase the profit of a fraud scheme in a certain time window. Multiple outgoing calls, or conference calls, can be generated on compromised PBXs [Trab], VoIP accounts [Tra15c], or SIM cards. Up to 6 simultaneous calls can be generated from a single SIM card [Bsw12]. Finally, *call forwarding* can be used to forward all incoming calls to a certain fraudulent phone number.

4.4.3 Value Added Services

Premium Rate Numbers (PRN) are used to provide wide range of services such as gambling, live chat, adult services; through voice call or SMS. To cover the cost of services provided, the cost of calling a premium rate number is much higher than a regular call. In most countries, a fixed number range is allocated for PRNs which allows users to easily distinguish them, however, this is not true everywhere. Users sometimes tend to confuse the number ranges and call PRNs unwittingly. Such premium rate numbers may be abused, e.g., when the promised service is not delivered, the cost of the service is not clearly stated or artificial traffic is created to these numbers [i3 12]. The abusive premium rate services usually manipulate the lack of due diligence between number resellers and numbering plans in which the premium rate number range is not clearly identifiable by users [ECC06]. Many online sites offer premium rate number services, which gives a cash back on calls reaching this premium number.

Such service providers often advertise International Premium Rate Numbers (IPRN)[2]. Such numbers are usually numbers in a destination with an expensive termination rate [Tra15a], rather than being real premium rate numbers, allocated for this purpose.[3]

CNAM (Caller Name) lookup service provides a 15-character long caller name string (associated with caller's phone number), to help users easily identify a caller [Flo15]. In the USA, operators are responsible for making the CNAM lookup (dip) for the calls received by their customers. A CNAM service usually comes as part of the landline package and it is enabled by default. However, there is no centralized CNAM database in North America. Instead, multiple independent CNAM providers allow operators to lookup the CNAM information for a fee [Voi16]. Fraudsters can use a CNAM service to register a false caller name for their phone number, or to abuse the payment mechanism (Section 4.7).

Toll free numbers are phone numbers which do not incur any charges to the caller. Instead, the call is charged to the toll free customer (call recipient), which is usually a call center service. Toll free numbers use a prefix allocated by the regulator. For toll free numbers, charge collection is reversed: The toll free customer pays the toll free number provider (usually the terminating operator) for all incoming calls. Toll free providers keep a part of the profit and passes a share to the originating operator, as the caller does not pay for the call [Trac].

4.4.4 Protocol Related Attacks

SS7 tampering by external parties became possible with easy access to SS7 networks. This can lead to attacks such as locating the phone users, intercepting the calls or denial of service [Eng14, Noh14]. Such attacks were also reported to be performed by intelligence services to locate targets and eavesdrop on communications [McD16]. Moreover, several cases where SS7 attacks

[2] www.purple-numbers.com, www.premiumskytel.com
[3] The international prefix (country code) +979 is an International Premium number range [ITU98] but it does not seem to be commonly used [Tra15a].

were used for intercepting SMS authentication messages have recently been reported [GOO17, Pag16].

VoIP protocol attacks can manipulate the implementation flaws, underlying network platform or the voice application layer [Col04]. Various attacks, such as SIP scanning, registration hijacking, redirection attacks, session tear down, SIP phone reboot and audio insertion are demonstrated in [NSF06, GDK+06, Ker12, EC06]. Billing systems can be manipulated through VoIP attacks as well [ZWYJ07].

IMSI catchers (or *stingray*) [JR00, Abi] are fake GSM base stations that are used to identify phones in proximity (catch their IMSI), intercept calls and communications, or even to send out spam and fraud messages [LWW+17]. IMSI catchers manipulate the lack of authentication from the network to the device in GSM. Such a fake base station can be built using operator grade equipment or open-source software and cheap hardware [BS+08, WFS+08, Ett05]. The phone is deceived to connect to the false base station and usually the mobile device is forced to not use encryption or downgrade to an insecure mode (e.g., 3G to 2G) [Abi]. More recent mobile protocols (like LTE) are using authentication but are not immune to such attacks. First, the authentication keys could be leaked (or seized); second, the IMSI catcher may abuse vulnerabilities in the protocol stacks [SBA+15]. Some discrepancies in the perceived network features can be used to detect IMSI catchers [DPK+14, GSM13, sno, DPW].

Caller ID spoofing requires transmission of fake caller IDs in the signaling system. Even though there are certain legitimate ways of using caller ID spoofing [Cla07], it is definitely a catalyst for voice fraud. PRI and SIP trunks enable transmission of fake caller ID to the SS7 network, as a result of the lack of caller ID authentication [PST14, DH05]. Various online services and mobile applications provide caller ID spoofing, via the service provider's IP-PSTN gateway connections[4]. Spoofing caller ID between two VoIP applications is even easier, because the caller ID can be inserted in SIP requests.

Apart from enabling various fraud schemes, caller ID spoofing can be damaging when used against services (such as banking systems, voice mails or emergency services) where caller ID information is used to authenticate or locate the users [MASX].

STIR (Secure Telephony Identity Revisited) working group [STI] attempts to provide a SIP header authentication mechanism to authenticate the caller ID [Pet15, PT16]. However, operators may be reluctant to deploy this solution due to the implementation overhead [Fed15a]. Moreover, with cloud VoIP services, phone numbers became an extremely cheap commodity and fraudsters could easily obtain bulk phone numbers and change authenticated phone numbers faster than they can be blacklisted.

[4] www.spoofcard.com/caller-id, www.spooftel.com

Researchers also propose caller ID authentication mechanisms for telephony networks. AuthLoop [RBT16] is a TLS-inspired protocol that uses the voice channel to provide end-to-end authentication irrespective of the underlying technology. A subsequent work, AuthentiCall [RBA+17], utilizes a low-bitrate data connection to authenticate the caller ID even before the call is answered. Tu et al. [TDZA16b] proposes a caller ID authentication scheme via the transmission of a pre-computed security indicator over the SS7 network. However, these solutions have their own limitations (e.g., difficulty of deployment, scalability or overhead) and have not yet found extensive, practical use. Another related work includes the use of call audio features to determine the source of the call and the types of traversed networks [BPA+10].

4.4.5 Other Techniques

PBX hacking is a significant threat for enterprises. PBX systems (hardware or software) are often not properly administrated and secured. Attackers can find PBX systems by calling a large range of numbers (e.g., via wardialing, in Section 4.5.5) or through the enterprise's publicly known phone numbers. IP-PBXs can also be identified using SIP scanners [Gau12]. Once a PBX is identified, attackers will typically gain access to maintenance interfaces or voice mail systems (e.g., by abusing weak passwords), or use social engineering [Subb, Mak] to compromise and reconfigure the PBX.

Cellular phones and SIM cards can be abused by techniques like **cloning and theft**. In CDMA networks, phone cloning is done by reprogramming phone's electronic serial number and mobile identification number. In GSM networks, the phones are identified by their IMEI number. Tampering IMEI can be useful in some countries to circumvent state control on phones, or to avoid blacklisting of stolen phones. *SIM swap* is a service provided by operators to the customers to register an existing phone number on a new SIM card. This service can be manipulated by fraudsters to obtain the ownership of the phone line [SIM16]. To this end, the fraudster contacts the operator claiming, e.g., that the SIM card was stolen, and uses social engineering techniques to impersonate the SIM card owner. If the fraudster can convince the operator to register a new SIM card for a particular phone number, he can generate calls that will be billed on someone else's account [Tim15]. SIM swap can also affect two factor authentication mechanisms, including banking [MBSS13].

Simboxes, or *GSM Gateways*, are devices that can act as a gateway to the mobile network (e.g., GSM) and provide a VoIP or PRI trunk. Those devices can be used to provide mobile connectivity to a PBX. The device is essentially composed of one, or more, mobile modems to which SIM cards can be attached, the modem(s) are then controlled by a computer which converts the calls to VoIP or ISDN. Simboxes have legitimate uses (such as providing GSM gateways to enterprise PBX systems) that are permitted by operators and regulators [Ofc05, RSB+15]. However, there are many frauds that rely on simboxes, in particular interconnect bypass (Section 4.5.3) and IRSF (Section 4.5.4) [MZJP, EIS13].

Autodialers are systems that automatically dial telephone numbers, randomly or given a predefined list [Bla13]. Once the call has been answered by the other party, a sophisticated autodialer can analyze the incoming audio stream to predict whether it has been picked by a real human being or an answering machine. Autodialers can either play a recorded message or connect the call to a live person upon the determination of human pickups.

Telephony Denial of Service (TDoS) attacks are performed by sending a very large volume of call traffic to a target number, to deprive the system resources (such as the trunk capacity) and disrupt the telephony service of the targeted customer. There are different ways to initiate a TDoS attack, such as organizing people on social media to call a specific number,using autodialers [CE13], or mobile malware such as baseband rootkits [GME17]. TDoS attacks became easier with the convergence of telephony and internet. The attacker can use a VoIP-PSTN gateway to generate cheap calls, a call generation software and some audio content to stall the target with a realistic scenario [CE13]. The VoIP-PSTN gateway can be a free IP-PBX software (e.g., Asterisk [Ast]) with an access to a SIP trunk. Other methods can be using a compromised PBX, a botnet or an online TDoS service [Sec14].

Social engineering is the process of manipulating people to act in a certain way or to give up confidential information [CE13]. Social engineering attacks exploit individuals' lack of security and fraud awareness. Tricking company employees to give up their passwords or persuading people to call a certain phone number are some examples of social engineering attacks. Telephony has been a preferred channel for social engineering because of the trust people put in the telephone and because impersonation is easier over the phone [And08]. **Malware** infecting smartphones and VoIP phones can steal personal data, e.g., helping in social engineering, but can also initiate calls or send SMS [Apv10, Cas17].

4.5 Fraud Schemes

Abuse of telecommunication infrastructure started in late 50's. Driven by technical curiosity, the *phreakers* (from 'phone freaks') explored the telephone network by reverse engineering the tone patterns in in-band signaling, and by social engineering telecom company's personnel [Gol08]. Detailed information on the history of telephony fraud can be found in [Ros71, Gol08, And08, Lap13].

In this section, we provide an overview and categorization of the modern fraud schemes. We focus on the current fraud ecosystem, but some of the schemes may be applicable or profitable only in some parts of the world. Also, we do not provide legal opinion on the fraud types as it depends on country specific laws.

4.5.1 Toll Evasion Fraud

Toll evasion fraud aims at making calls without the obligation of paying the call charges. Toll evasion is the oldest type of fraud in telephone networks [Col99] and can be categorized in four main categories.

Subscription fraud is the act of using stolen identity credentials, or providing fake information while subscribing for a service, in order to avoid service charges [Joh12], e.g., SIM card subscription for a post-paid account using false information. Researchers have proposed solutions to detect subscription fraud using data mining [FS11] and other classification techniques [HR15].

Similarly, **superimposed fraud** aims to take control over a legitimate customer's account via cellular cloning or theft, and burden call charges on his account [RMN+99a, HS05a, Hil09].

Enterprises are also frequent targets of toll evasion fraud. In **PBX dial-through fraud**, compromised PBXs can be used to make free calls, while the call charges are ascribed to the PBX owner. [GSFG13] demonstrates various attacks aiming at toll evasion fraud, using a IP-PBX honeypot with PSTN connections. **Internal fraud** is usually committed by employees of a telecom company who have access to user accounts, tariff plans and billing system [Joh12]. Fraudulent employees can, for example, deactivate billing for certain accounts, tamper the call records or manipulate the tariff plans to avoid or reduce the call charges [CE13].

4.5.2 Retail Billing Related Fraud

In this section, we analyze the fraud schemes related to retail billing (see Section 2.3). The fraudulent actor may be the customer, the operator, or a 3rd party service.

Due to the complexity of billing systems or confusing pricing policies, tariff plans can be inconsistent or can contain errors. Customers or other operators can exploit the mistakes in tariff plan or campaigns. One example of **tariff plan abuse** occurs when customers gain credits as they receive calls. In this case, customers inflate traffic to their own phone numbers to gain free credits. Another example is the abuse of unlimited or flat-rate calling plans by customers or businesses to call specific destinations, or by wholesale operators to terminate large volumes of traffic.

Over-billing fraud is performed by operators against their customers or partners, to increase operator's revenue illegitimately. *Cramming* is one example of over-billing fraud, where telecom operators or other service providers intentionally place unauthorized charges on client's bill, for providing services such as voice mail [FCC]. Customers may be deceived into accepting these charges while signing promotional materials, or through social engineering techniques like negative option marketing [Ftc09]. Another scheme called *Slamming* occurs when a fraudulent telecom operator switches the local or international service provider of the customer to itself, without the customer's consent and explicit notice [And08]. The operator may additionally charge the customer for high call termination rates.

Unauthorized call reselling scheme involves reselling of fraudulently obtained calls (e.g., obtained via toll evasion fraud) for prices lower than the market rates. Reselling calls over a compromised PBX is also called *call transfer fraud* [Trab].

4.5.3 Wholesale Billing Related Fraud

This section covers the fraud schemes related to the inter-carrier billing processes in the wholesale market.

Call routing abuses are possible due to the lack of route transparency and lack of security mechanisms in call signaling protocols. This fraud usually aims at profiting from the arbitrage opportunities.

Route blending occurs when an operator illegitimately sends part of its transit traffic over a low quality and low cost network, violating its inter-carrier contracts and service level agreements [Sub13].

Re-origination (also known as *re-file*, *hubbing*, *refiling*) uses an intermediate country to decrease the termination charges. The international traffic is first sent to a hub country, which has a more competitive market and more favorable interconnect agreements [He05, Mel00]. The operator in the hub country changes the origin of the call, by modifying the Calling Line Identity (CLI) in SS7 signaling, and sends the call to the destination country. In this way, a cheaper call termination fee is paid to the destination country. Both the originator and intermediate operator profit from this operation; whereas, the operator in destination country loses revenue. This fraud can also be performed by directly manipulating the CLI information in call signaling. For instance, the recent regulation in European Union, which imposes cheaper call termination rates for the calls originated and terminated within the EU, creates an arbitrage opportunity for this type of fraud [PRI17].

Unauthorized International Resale Fraud[5] is a similar scheme that manipulates the price discrepancies by setting up the international call via a third county using a call reversal mechanism such as calling cards. It became popular in 1990s and

[5] Also named 'call back', 'dial back', 'third country calling' [Ret95].

the USA was used as the intermediary country due to the highly competitive market and low international termination rates [Ret95, Alt].

These fraud schemes became less profitable as the pricing anomalies reduced with the increased competition in telephony markets.

Location Routing Number Fraud manipulates weaknesses in number portability lookups. In the US, the location routing number (LRN) is used to provide local number portability for mobile numbers. Each ported number is assigned an LRN, so that the calls can be routed to the correct switch that is serving the ported number [NPA15]. When a call is made to a ported number, the carriers routing the call should query the number portability database, to learn the LRN associated with the ported number [NPA15]. However, some carriers skip this step to avoid database query charges. In this case, a fraudulent operator can provide a fake LRN that belongs to a low cost destination, and pay a small fee for calling a high cost destination [Tra15b].

Call looping is another form of call routing abuse. Call loops may occur due to routing errors or misconfigurations. An operator can abuse such loops to send the same call multiple times over a loop made of several operators. It will then refuse to pay for the call to the downstream operator, saying that the same call was billed multiple times. On the other hand, it will not mention the loop to the operator that sent him back the calls and will be paid for the calls [Sub13].

Interconnect bypass fraud, or gray routing, can be defined as the use of illegitimate gateway exchanges to avoid the legitimate gateways and international termination fees[6]. These routes are sometimes used to coordinate criminal activities, because the calls are more difficult to intercept [Fad13]. Gray route fraud exploits, e.g., the price differences between wholesale and retail markets [ara16] to reduce the cost of an international call. This is achieved by fraudsters establishing a "bypass" in either the destination or an intermediate country.

The bypass mechanism mostly involves the use of a simbox or a PBX [Suba]. A basic form of interconnect bypass occurs when a fraudulent transit operator routes an international call over the IP network and terminates it as a domestic mobile or landline call in the destination country. However, interconnect bypass can take many forms, depending on the arbitrage opportunity. A more recent type of bypass, which we will describe in more details in Chapter 6, is performed by terminating the regular international calls on the Over-The-Top (OTT) applications installed on recipients' smartphones.

Interconnect bypass fraud leads to financial losses for the destination operator as well as the bypassed transit operators who were supposed to get a share of the call revenue.

[6] Because simboxes and PBXs are frequently used to enable these illegitimate routes, this fraud is also named as *Leaky PBX*, *simbox fraud* and *GSM Gateway fraud*.

Commercial approaches to detect interconnect bypass fraud include test call generators and statistical fraud management systems [Suba]. In addition, there exists machine learning [EIS13, MZJP] and call audio analysis [RSB+15] techniques in the literature focusing on the detection of simboxes and blocking of bypassed calls.

False Answer Supervision (FAS) fraud enables (transit) operators to fraudulently increase their revenue from each call, by performing one of the following [Sub13]:

- *False answer*: (also called *short-stopping fraud*) the operator diverts a call (short-stops it) to a recorded message and starts charging, instead of transmitting the call to the real network.
- *Early answer*: the operator increases the duration of the call fraudulently by, e.g., answering the call and playing a fake ringing tone until the callee actually answers [Nex].
- *Late disconnect*: the operator delays the transmission of call disconnection message to the calling party and therefore bills for a longer call.

False Answer Supervision may affect the quality metrics of carrier's network by altering the average call duration and the number of connected calls [Voi12]. For example, the Answer/Seizure Ratio (ASR) may increase due to the high number of (imitated) connected calls, which will have a positive effect on the quality. On the other hand, performing false answer may decrease the Average Call Duration (ACD), because the calls are not properly connected. FAS may also damage the reputation of retail carriers, as they may receive customer complaints about incorrect billing issues. According to a survey conducted in 2013, FAS was the top fraud reported by the wholesale carriers [Sub13].

4.5.4 Revenue Share Fraud

Revenue share fraud occurs when an operator (or third party service provider) makes an agreement with another party which will generate calls to predefined numbers (the *revenue share numbers*). The operator who owns the revenue share numbers, usually advertises these numbers through an online premium rate service reseller (see Section 4.4.3). A fraudster can easily obtain a revenue share number and start generating calls to this number.

Revenue share fraud often involves a combination of multiple fraud schemes. In this section, we will first examine the schemes used for *traffic generation* to the revenue share numbers. Then we will analyze common *fraud agreement* schemes and in particular fraudulent termination.

Traffic Generation Schemes

In general, fraudsters will be attracted to generate calls as long as the revenue share they receive is higher than the cost of generating the calls.

Toll Evasion Fraud (see Section 4.5.1) can be used to create traffic without bearing any charge to the fraudster. Common techniques involve exploiting PBXs, roaming SIM cards, or using *dialer* malware (e.g., smartphone malware which dials revenue share numbers without user's permission [Apv10, NGT11]). Fraudsters may also *abuse unlimited (or low cost) international tariff* plans.

Call generation schemes are often combined with other techniques to maximize profit (Section 4.4.2) of revenue share fraud in a limited time, before the fraud is detected. For instance, PBX dial through fraud can be combined with conference calling, multiple call and call forwarding techniques [Trab]. Moreover, *social engineering and scams* (Section 4.5.6) can be used to deceive people into calling the revenue share numbers. For instance, fraudster can send a phishing SMS or leave voice mail to many phone lines, promising them a profit or service if they call a specific number. Social engineering can also be used to keep the caller on the phone for a long duration.

Fraud Agreement Schemes

Various different fraud agreement schemes are possible. For example, in *domestic revenue share fraud*, parties making the fraud agreement operate in the same country, whereas the *international revenue share fraud* involves international traffic (will be analyzed in Chapter 7 in detail). *CNAM revenue share fraud* is also possible and will be described in more details in Section 4.7.

Access stimulation fraud is a form of domestic revenue share fraud, seen in the USA, which abuses the high termination rates in rural areas. In this fraud, an operator in a rural area makes an agreement with a company that bears high volume of inbound calls [FCC14]. Such companies use various techniques (see Section 4.4.2) to inflate incoming traffic to the number range of the operator in rural area. Finally, the operator shares some of its revenue with the company.

In **toll free number fraud**, the fraudster makes an agreement with an operator (often a competitive local carrier) and uses this operator to initiate a large volume of calls to a toll free number [Trab]. Because of the reverse payment flow used for toll free numbers (Section 4.4.3), the originating operator earns revenue from this call volume, and shares the profit with the fraudster who generated the calls.

This fraud usually targets toll free numbers of big corporations. To remain unnoticed, the fraudster usually makes automated, short-duration calls which will stay in the waiting queue (or IVR system) and avoid connecting to an human operator. Other methods to avoid detection include using caller ID spoofing and calling toll free numbers of many different companies.

4.5.5 Targeted Fraud

Fraud schemes targeting a certain company or individual may not be as common as other types of fraud, but they may have significant consequences, affecting many users or resulting in huge losses. **Impostering** is the act of stealing someone else's identity, and performing operations on his/her behalf. Techniques like caller ID spoofing, mobile malware or social engineering can be used to spoof identity, steal one-time passwords and trick companies (such as banks) to perform unauthorized operations. Another fraud targeting individuals is **call interception and eavesdropping** operations. SS7 access, mobile technologies (IMSI catcher), insecure VoIP systems (compromised PBXs) and legal interception gateways enable eavesdropping on phone calls, SMS messages as well as location tracking [CE13, Eng14, CIB+13, PS07]. Although, it is possible to have end-to-end encrypted VoIP calls and secure VoIP protocols (like SIPS, SRTP) exist, majority of voice communications are still vulnerable to eavesdropping [SS14], and are subject to legal interception. Another form of targeted fraud can be performed by tracking an individual's call records (via phone bills or operator's CDR database) and extracting information from the call metadata (e.g., source and destination numbers, duration) [CE13, HRP+17]. To prevent this kind of attacks, researchers have proposed a call forwarding infrastructure that will obfuscate the metadata by routing the call over a series of telephony relay nodes [HRP+17].

Wardialing is the use of autodialers to scan a phone number range, e.g., to identify modems, fax machines or voice mail accounts. This can be used for reconnaissance purposes targeting a company, and further attacks can be initiated [Tra09]. In **CNAM datamining**, a fraudster calls himself multiple times by spoofing the caller ID of other numbers, to obtain the caller name information for those numbers. While the fraudster's main goal is to illegitimately build a database of caller names, his carrier will be forced to make the CNAM lookups for the spoofed numbers [McC11].

Disruption of service, e.g., using TDoS (see Section 4.4.5), can have devastating effects for an operator, an enterprise or service (such as health or police emergency lines), and is often used in **blackmailing** schemes [McA13, TDO13].

4.5.6 Voice Spam and Scams

Voice spam is one of the most visible types of voice fraud targeting customers. It includes all types of unsolicited and illegitimate calls. Fraudsters can obtain phone number lists from leaked databases, form submissions, or simply by purchasing them online [TDZA16a]. They mostly use autodialers to generate large number of calls and use prerecorded messages (*robocalling*) which may be later forwarded to live call center agents to interact with the victims. Caller ID spoofing and social engineering techniques are frequently used to deceive people to do certain actions or to reveal sensitive information. Due to the low cost and scalability of VoIP based calling systems, scammers can make millions of calls and easily expand the scam ecosystem. A recent work [TDZA16a] describes the challenges that arise in fighting voice spam by comparing it to email spam. It then analyzes existing anti-spam techniques and provides an assessment criteria. Voice spam can take many forms, but we will explain some of the most common schemes (see [TDZA16a] for more examples).

Telemarketing is a method of direct marketing in which a salesperson entices customers to buy products or services over the phone [GSBA15]. Telemarketing can be illegal in certain jurisdiction, e.g., if the telemarketer did not take prior consent from the call recipient [ftc16].

In **voice phishing** (also known as *vishing*), the caller imitates a legitimate organization, person or entity and tries to gain access to private, personal and financial information using social engineering [LaC14, CE13]. Caller ID spoofing is often used by scammers to hide their real identity and makes it difficult to block the spam calls or to take legal actions against fraudsters [TDZA16a].

Many other types of scams can make use of telephony. For example, in the **tech support scam**, fraudsters try to convince people that their computer is infected with malware (mostly by tricking them into installing remote access tools) and request a payment to solve the so-called problem [Mic, MSN17]. In **advance fee fraud** (419 scam), the victim is being tricked into making some up-front payment to be able to receive a larger sum of money, such as a bogus lottery prize [ITC+13]. A similar scam is the **free cruise scam**, where fraudsters advertise a free cruise opportunity, but later on require additional payments [Ask].

4.6 Benefits

Benefits are central to the fraud, and without the benefits, there would be no fraud. Most of the fraud schemes on telephony networks target financial benefits, but financial aspects are not the only motivation. For example, a goal may be to learn individuals' opinions about a political election, through voice spam [TDZA16a].

It is important to make a separation between fraud schemes and benefits, as different fraud schemes can target the same benefit. One example of problem when failing to separate fraud scheme from the benefit is the use of *toll fraud* term for various fraud schemes such as subscription fraud, International Revenue Share Fraud (IRSF) and PBX dial through fraud [CE13, Tol15, New13]. Here, "toll fraud" indicates that the fraud will have financial benefits. However, these fraud schemes are very different from each other and lead to different types of financial benefits. A fraud scheme may also generate multiple benefits. For example, telemarketing can involve *increase of company revenue* through sales, *influencing people* through advertisement, and *getting a share of revenue* through CNAM revenue share [Dav, CNA]. Hence, separating fraud schemes and benefits provides a clear view of fraud, and solves common terminology problems.

4.7 Case Study: CNAM Revenue Share Fraud

CNAM revenue share is not a very well known fraud mechanism, this scheme was probably made possible because of the obscure and deregulated nature of the CNAM service. As we mentioned in Section 4.4.3, many CNAM (Caller NAMe) lookup (*dip*) service providers exist. Operators rely on them to provide caller name information to their customers. When a call is received by the terminating phone company, it performs a *dip* for a fee (*CNAM dip fee*). This compensation happens for every call where the calling party name is displayed to the called party, even if the call is not answered.

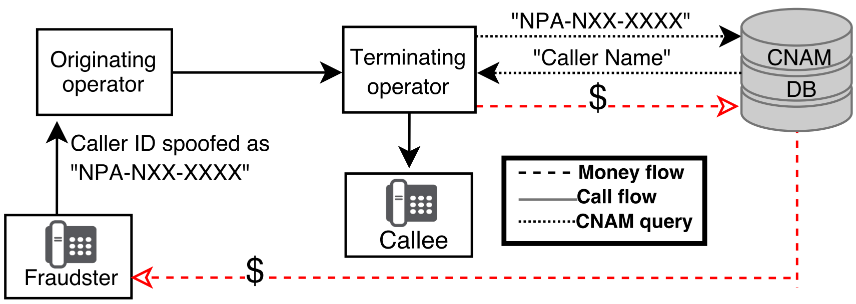


Figure 4.3: CNAM revenue share fraud.

CNAM revenue share fraud is similar to other revenue share fraud schemes where a fraudster generates call traffic to a partner service provider, who will share part of his revenue with the fraudster. However, the fraudster needs to 'originate' calls from the revenue share numbers (instead of 'terminating'). This is because the CNAM lookup service uses the looked up caller ID to identify the revenue share partner. Moreover, call generation is cheap for the fraudster because the calls are generally not answered.

On the other hand, the CNAM dip fee is usually very small and to make a significant profit, the fraudster has to generate a large number of calls from the revenue share number. As it is not practical to generate thousands of calls from a single phone, the fraudster usually spoofs his caller ID and uses multiple autodialers to generate the calls (Figure 4.3).

For telecom customers, the visible effect of this fraud will be a large number of missed calls on their landline phones. These calls are most likely to be incorrectly treated as *voice spam* (or *ping calls*) by customers. In fact, CNAM services

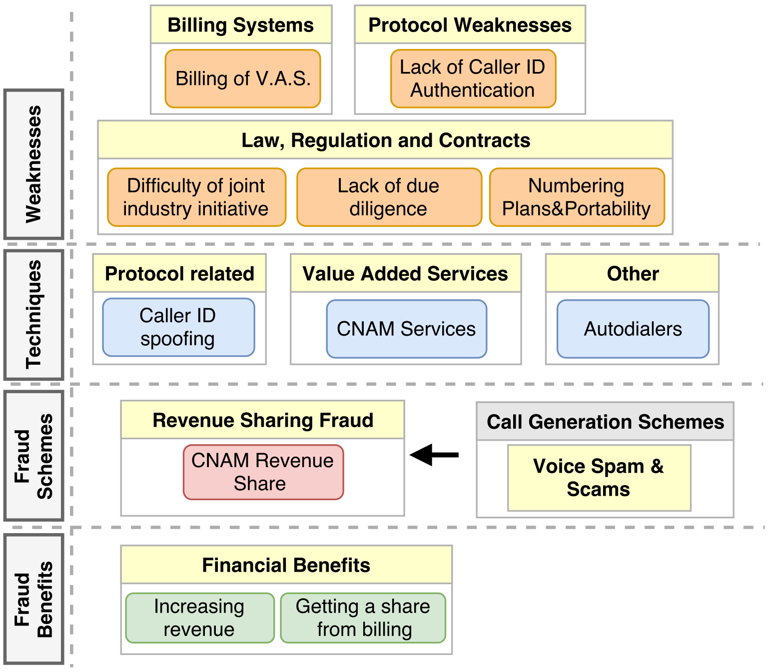


Figure 4.4: Taxonomy for CNAM revenue share fraud.

are also often used by telemarketers to get some additional revenue from their calls [The13], which could explain why it is uncommon for telemarketers to randomly spoof their caller IDs [Luc13].

CNAM fraud advertisement in India In [Dav], a CNAM provider offers a revenue share deal to a call center in India. In this example, 34 million calls were generated over a period of 10 months with 39% of the calls leading to a CNAM dip reaching the CNAM provider. The average revenue share was of $1.15 per thousand CNAM lookups (dips), generating a total revenue of $15,372. While it is difficult to fully trust this advertisement, it nevertheless provides an interesting view on the scale of this fraud. Another source confirms the order of magnitude by advertising a revenue of 50c to $1 per 1000 calls [CNA].

Honeypot findings We also study the data from the telephony honeypot presented by Gupta et al. in [GSBA15]. (More information on telephony honeypots will be given later in Chapter 5.) This data was collected during the course of 2.5 months from 17th July 2014 to 30th September 2014. The 275K phone numbers linked to the honeypot received 2.3 million calls from 285K sources. In addition to the numerous fraudulent calling patterns, e.g., telemarketing and robocalls [GSBA15], we also noticed traces of CNAM revenue share fraud. Table 4.1 shows the call volume from the number block which was used by the attacker. A total of 39K calls hit the honeypot from this pool of 10 source num-

Table 4.1: CNAM revenue share fraud case study on the telephony honeypot.

Source Number	# calls	Source Number	# calls
141XXXX2353	13040	141XXXX2807	1681
141XXXX2328	7118	141XXXX2801	1389
141XXXX2538	6678	141XXXX2335	1334
141XXXX2368	3503	141XXXX2322	684
141XXXX2362	2918	141XXXX2710	597

bers. The intuition that this was CNAM revenue share fraud was confirmed by a fraud management expert from a Tier 1 operator, who recognized the pattern and numbers used.

Fighting CNAM fraud Figure 4.4 shows CNAM fraud in our taxonomy, we see that there are several ways CNAM fraud could be mitigated: by addressing the call generation schemes (regulating telemarketing, or autodialers), the protocol weaknesses (Caller ID authentication), or the financial benefits (for example by regulating cash back schemes). None of them are likely to completely solve the problem but the taxonomy provides a clear view of the CNAM ecosystem and the points at which the CNAM revenue share fraud can be addressed.

4.8 Conclusion

Telephony fraud has constantly evolved throughout history. Starting with curiosity of people and simple tricks to make free calls, it became a huge fraud ecosystem involving various actors, technologies, applications and networks. In this chapter, we systematically studied the fraud in voice telephony. For this, we proposed a taxonomy that provides a holistic framework to better understand and analyze such frauds. Our work provides a comprehensive view of the causes, weaknesses, techniques, schemes and benefits obtained by fraudsters. Based on a clear fraud definition, new fraud schemes can be easily inserted in our taxonomy to extend it. This will help to analyze their relations and interactions with other fraud schemes and techniques, and finally pinpoint their root causes. Without such a holistic view of fraud schemes, they may be misunderstood. E.g., CNAM fraud can be easily misinterpreted as *ping calls* but it may not be addressed the same way because the revenue share mechanism is not the same.

Throughout the thesis, we will use this taxonomy to analyze the three fraud schemes that we study in more detail: Over-The-Top bypass, International Revenue Share Fraud (IRSF), and voice spam. However, we will first make an overview of the existing fraud detection and prevention mechanisms in the next chapter.

Chapter 5

Overview of Fraud Detection and Prevention Techniques

Although our primary focus is to understand telephony fraud, we also give an overview of the existing fraud detection and prevention techniques, both proposed in the academic literature, and being used in the industry (by telecom operators or vendors selling anti-fraud products). Note that some of these techniques are already mentioned in the previous chapter, however, this chapter aims to summarize the common approaches.

Detecting the fraudsters in telephony networks is a challenging problem. Individual operators can deploy monitoring systems to trace calls within their network, but can not monitor calls once they are routed through another network, which is typical for international calls. As the SS7 protocol [DH05] does not provide a mechanism for tracing the complete call route, this information can only be recovered when different operators collaborate. However, this is often difficult because of the variety and number of operators, fierce market competition and non disclosure agreements. Inevitably, operators lack the complete view of the network and fraudsters are difficult to identify. The difficulty of monitoring very large data streams in real time and differentiating between malicious and normal behavior is another major challenge in detecting fraud. In some cases, fighting fraud can be more expensive than the visible (or estimated) cost of fraud, decreasing the incentives for operators to invest in fraud management. Fraudsters can easily hide their identity (e.g., by spoofing the caller ID) and launch attacks remotely. Moreover, the variety of laws and regulations, lack of cooperation between operators and legal authorities, and the difficulties in international law enforcement make it hard to take action against fraudsters, even if they are identified. Thus, prevention is usually more difficult than detection.

The main types of data sources that can used by an operator for fraud detection are the Call Detail Records (CDR), network and signaling data and information related to customers (such as service plan, credit score, payment history) [Wei05, BVW10]. Note that the available data sources can vary depending on the service given by the operator (e.g., wholesale transit or retail). In addition, call audio has also been used in several studies and applications [BPA+10, RSB+15] Next, we will analyze the techniques that make use of these data sources.

5.1 Rule Based Approaches

Rule based fraud detection schemes often require fraud analysts to prepare a set of rules to either find anomalies in the data, or detect fraudulent behavior based on previous observations.

In the threshold-based approach, certain data features (such as call duration or the number of calls within a specific time window) are monitored and an alert is triggered if the fixed threshold is violated [BVW10]. However, determining the threshold values is often difficult, as different users have different needs and behavior. Usually, the threshold is set to a high value, which allows the fraudsters to stay under the radar by, e.g., making short duration calls in parallel (Section 4.4.2).

In pattern matching approach, the call logs and other related data is compared against a set of known fraud patterns. This approach has several drawbacks, such as the difficulty of determining the patterns, scaling the rules to all types of fraud, and continuously adjusting them to adapt to emerging fraud schemes [RMN+99b].

In [RMN+99b], authors discuss the problems with rules discovery and propose a two step process: First, a set of candidate rules are generated, and second, the actual rules are selected depending on both their individual performance, and the incremental performance they bring into the existing rule set. [KLJ00] discusses the similarities between intrusion detection systems and rule based fraud management, and proposes to combine these two approaches. In addition, Lahmadi et. al. propose a rule-based approach to automatically prevent SIP attacks, which may lead to TDoS attacks or billing abuses [LF12].

5.2 Profiling User Behavior

User profiling aims to leverage the past behavior of a user to build a model of his typical, expected behavior [HS05b]. Usage characteristics (such as the average call duration, number of daily international calls) and other customer-related information (credit score, tariff plan) can be used to create a behavior profile, which will be monitored for deviations and abnormal behavior [RMN+99b, HS05b] This approach can be used to detect fraudulent behavior of retail customers (e.g., subscription and superimposed fraud). Compared to the rule based approaches, user profiling has the advantage of treating each user individually, instead of imposing the same set of fraud rules to all users.

Hilas et. al. [HM08] evaluates the efficiency of different user profiling methods to detect fraudulent user behavior on 2500 days of CDR data collected from a PBX with 6000 users. Each user's call data is first modeled based on five different user profiling methods. As the authors have pre-labeled data on fraudulent accounts, they compared the accuracy of user profiling techniques, by employing both supervised and unsupervised learning methods. They find that profiling based on the accumulated weekly behavior gives the best results.

User behavior can be leveraged to detect voice spam as well. Studies propose various behavior features for the caller (such as the ratio of inbound/outbound calls, diversity of the call destinations, rejected call count) that can be used for spam detection. More information can be found in [TDZA16a].

In addition, simboxes also display specific behavior patterns (e.g., they do not move, always make outbound calls, never send or receive SMS), which can be used by operators for simbox detection. To avoid such detection mechanisms, fraudsters often use virtual SIM cards, and advanced simboxes that can simulate human behavior.

5.3 Machine Learning Based Approaches

Data mining and machine learning techniques have been frequently used for fraud detection in different domains, including telecommunications [KLSH04, PLSMG10]. In fact, telecommunications was one of the first industries that adopted machine learning technologies due to the huge amount of high-quality data they store [Wei05].

In general, machine learning approaches use certain behavior patterns as features of the machine learning algorithm. Most of the academic work in this field focus on applying machine learning on CDRs to detect subscription and superimposed fraud (Section 4.5.1), as well as simboxes (Section 4.5.3).

For instance, in [EIS13], a supervised learning algorithm based on Artificial Neural Networks (ANN) is used to detect simbox fraud. The dataset is gathered from a mobile operator and it includes CDR data from both legitimate subscribers and subscribers belonging to a fraudulent simbox. All the CDRs come from one cell of the network and 234K CDRs gathered in 2 months are analyzed. The features used in the classifier include the subscriber ID, total incoming and outgoing calls per day, total duration of calls per day and similar statistics about the calls during night. The classifier has 98.7% accuracy in identifying the SIM cards that are used in the simbox device.

A similar study is conducted in [MZJP], with a much larger dataset and different set of features used for classification. In this work, CDRs gathered from 500 fraudulent simbox devices and 93000 legitimate accounts in one and a half years period are analyzed. The aim of the study is to differentiate legitimate and fraudulent devices (IMEIs) using a classification algorithm. The average duration and total number of incoming and outgoing calls per IMEI (with corresponding origination and destinations), account age, the number of SIM cards (IMSIs) per IMEI and the number of base stations that an IMEI connected to within one week are some of the features used. The analysis shows that simboxes are usually static, they connect to a few base stations, they are associated with many IMSIs and they initiate a significant number of calls. Due to the huge amount of data, authors perform some preprocessing steps to eliminate obviously legitimate accounts. The proposed classification methodology gives 99.9% accuracy.

5.4 Graph analysis

Representing CDR data as a voice call graph is another approach to visualize the connections between callers and callees, and detect fraudulent patterns. Source and destination numbers can represent the set of nodes, and the calls become the directed edges. The weight of an edge can be the number of calls, or the total call duration between the nodes [HR15].

In [JJS+12], authors use two year CDR data from a Tier-1 cellular network operator in the US. The CDRs include calls from domestic numbers to international numbers. First, a voice call graph is constructed and the very large connected components are decomposed to identify community structures, where a set of source numbers make calls to a set of destination numbers. Such structures are then analyzed for fraudulent activity. Authors classify the detected fraud activities as types of voice spam and international revenue share fraud (Chapter 7), by correlating the data with online user complaints.

[BAP07] uses the notion of social networks to represent the call history as the previously formed links (previous communications) between the caller and callee. This information is combined with data on call durations to identify the spammers and prevent them from calling legitimate users.

5.5 Test Call Generation Platforms

Test Call Generation (TCG) platforms provide call origination points worldwide (from various networks in various countries) to enable the operators to generate traffic from remote points to their own networks. Virtual SIM cards, calling cards or VoIP technology can be used to generate calls from different networks.

The commercial TCG platforms[1] often provide automated periodic testing and web interfaces to schedule and manage the test calls. They are often used by the operators for testing the accuracy of billing systems and QoS, as well as for fraud detection. For instance, monitoring the call start time, end time and duration can help to detect FAS fraud (Section 4.5.3). Moreover, monitoring the received caller ID of a call, and comparing it with the actual caller ID may allow to detect simbox and PBX based interconnect bypass fraud, as these fraud schemes are likely to alter the caller ID.

5.6 Audio Based Approaches

Call audio features can be used to detect packet losses (that often occur in VoIP networks) and identify the audio codecs applied to a call, which can be used to detect the types of networks a call is initiated from and has traversed over [BPA+10]. This information helps to detect VoIP based phishing attacks and other suspicious calls.

A recent study in [RSB+15] aims to detect simboxes by analyzing the audio signals for each individual call at a cell tower serving to a simbox. The idea is to detect the audio degradation caused by a VoIP-to-GSM gateway, by observing the frame losses in the GSM-encoded audio. The proposed method achieves 87% accuracy in detecting the calls bypassed over a real simbox.

A disadvantage of audio based fraud detection approaches is the difficulty of accessing the call audio streams, and real-time processing of this huge volume of data.

Call audio can also be used as a channel to transfer data between the caller and the callee. For instance, the AuthLoop protocol [RBT16] uses the audio channel to provide a TLS-like authentication method to verify the caller ID information. The advantage of this approach is that it works independently of the underlying call technology.

5.7 Honeypots

Similar to other domains [CB13, Pro04], honeypots have been used to collect information on telephony threats, and to observe and better understand the fraud landscape.

[1] E.g., Araxxe, Sigos, Revector

Honeypots analyzing VoIP attacks

Several honeypot architectures are proposed [NNSE07, NSF07, DCNF11] to collect and analyze the attacks targeting IP-PBX (IP based Private Branch Exchange, e.g., Asterisk[2]) servers, SIP proxies (e.g., Kamalio[3]) and soft phones. These honeypots can be used to detect malicious call signaling messages, DoS attacks, SPIT (Spam over Internet Telephony) calls and voice phishing attempts targeting enterprise phone systems.

Gruber et al. [GSF+13] deploys a IP-PBX server with vulnerable user accounts (e.g., accounts with weak passwords) and an uplink to PSTN, which enables outgoing calls. Authors capture several 'toll fraud' attacks (which refers to PBX dial-through 4.5.1) and find that all the calls initiated by the fraudsters target international destinations or premium rate numbers.

Telephony honeypots

Telephony honeypots aim to collect data on the incoming phone calls received by a set of phone numbers. The phone numbers are usually directed to an IP-PBX that uses a set of phone lines to receive calls and allows to process them (e.g., answer, record, forward).

The phone numbers that will be assigned to a telephony honeypot can be chosen in different ways, depending on the purpose of the honeypot. For instance, a honeypot that aims to collect data on voice spam will better use a set of numbers that have been returned by users who receive too much spam ('dirty' numbers), instead of using 'new' numbers (previously not assigned to anyone). It is also possible to 'seed' (i.e., advertise) the phone numbers in various platforms (e.g., online social networks, questionable websites [GAC+14]) to attract more calls from fraudsters.

A telephony honeypot can be interactive (responding to the call and interacting with the caller) or low interaction (not responding to the calls, or passive response). In the previous work [GAC+14, GSBA15], researchers propose the following types of interactions for telephony honeypots:

- **No interaction (CDR only):** The calls are either immediately terminated e.g., with a busy tone or "not in service" message. The honeypot records the call metadata.
- **Low interaction:** The calls are allowed to ring for some time before the hangup, or they are answered with silence or some background noise.

[2] Asterisk Open Source Communications Software. www.asterisk.org
[3] Kamailio - The Open Source SIP Server. https://www.kamailio.org

- **High interaction:** The calls are answered and the honeypot interacts with the caller via a voicemail message, an automated voice response mechanism (such as playing pre-recorded or text-to-speech messages), or a live agent talking to the caller.

For the low and high interaction honeypots, call audio can also be recorded in addition to the metadata, depending on the legal restrictions on call recording. Note that deploying high interaction honeypots are much more challenging, as they require to engage in a meaningful interaction with the caller. We will study high interaction honeypots in more detail in Chapter 9.

Part II

Examining Fraud on Operators' Side

Telephony networks carry a huge volume of call, messaging and data traffic every day. This is a complex and opaque ecosystem, which combines multiple technologies and involves various types of service providers and customers.

Because calls can be expensive, and can be used to monetize third party services, telephony becomes a very profitable environment for many fraud schemes.

In this part, we will examine two fraud schemes that are frequently experienced by telecom operators. The first one, Over-The-Top (OTT) bypass, is a relatively recent fraud scheme (started around 2014), whereas the second one, International Revenue Share Fraud (IRSF), has been around for several years, but despite many efforts by industry, it is still present and leads to significant losses. Although these fraud schemes also have implications for consumers, in this part we focus on the operator side of the fraud, as we had the opportunity to collaborate with telecom operators on these topics.

Chapter 6

OTT Bypass: A Recent Fraud Scheme

The so-called *Over-The-Top* (OTT) services (e.g., WhatsApp, Skype) use IP networks to implement a service without involving telecom operators (i.e., passing "over the top" of them). Because of their global presence, through smartphone application markets, OTT providers attract more customers than most telecom operators. Indeed, studies forecast 2 billion users of OTT messaging by 2018 [eMa15]. OTT applications often provide voice communication services, but they are normally not a part of the global telephony network. However, interconnection between OTT and global telephony network is possible through some gateways, which we will explain in Section 6.1.2.

In this chapter, we present and analyze a recent type of telephony fraud, called *OTT bypass* or *OTT hijack*, which arises from a new kind of interconnection between telephony networks and OTT applications. Indeed, in an OTT bypass the OTT provider partners with a transit operator to hijack regular calls (i.e., calls originated from a mobile or landline phone to a mobile number) to terminate them over the OTT application. The large user base of OTT applications, and the high termination fee of some international destinations, make this practice very profitable for the OTT provider and partnering operators. Indeed, OTT bypass has been reported to cause losses to telecom operators in the order of tens of millions of Dollars [OTT16]. Moreover, users and other operators are affected in many ways, as we will study throughout this chapter. We will present an extensive analysis of OTT bypass fraud, with the following contributions:

- We present the first comprehensive study of OTT bypass and position it in the current fraud ecosystem.
- We measure the importance and effects of OTT bypass fraud on a case

study of a small European country[1]: technically, with experiments with more than 15,000 test calls over 8 months, and from the user perspective, with a large-scale user survey.

- We show various implementation flaws, as well as more fundamental problems that OTT bypass can cause in a network. We show that sometimes multiple fraud schemes collide, intensifying the degradation in service quality.

- Finally, we present evaluation criteria for multiple detection and measurement techniques and compare them.

6.1 Background

6.1.1 OTT communication services

Compared to the traditional messaging (SMS/MMS) services and phone calls, OTT applications offer many additional features (e.g., group chat, video calling, photo, file or location sharing). Moreover, OTT services are usually free, whereas the traditional telephony services can be expensive.

On the other hand, due to the high competition in OTT market, it is challenging for OTT service providers to monetize their products: Users are usually not willing to pay for applications and they do not like advertisements. As a result, OTTs need to find other ways to make profit, such as the in-app purchases (e.g., for stickers and games [eMa15]), and paid services that allow interconnection with the telephony network [Cro13].

6.1.2 Telephony and OTT interconnections

To enable connectivity from the OTT service to the global telephony network, OTT providers partner with telecom operators[2] and use gateways between the OTT network and the PSTN. In this way, a call initiated from the OTT network can be terminated on the telephony network and vice versa. We will name these services as regular OTT *-in* and *-out* services.

The -out service allows to reach the telephony network from the OTT application, by terminating calls locally on callee's operator (Figure 6.1-(b)). This service is generally paid by the OTT user to cover the cost of the local call termination on the PSTN or mobile network.

[1]Because of legal concerns, we do not mention any operator names, the name of the bypassed country/operator or of the OTT application.

[2]They may also officially become operators themselves.

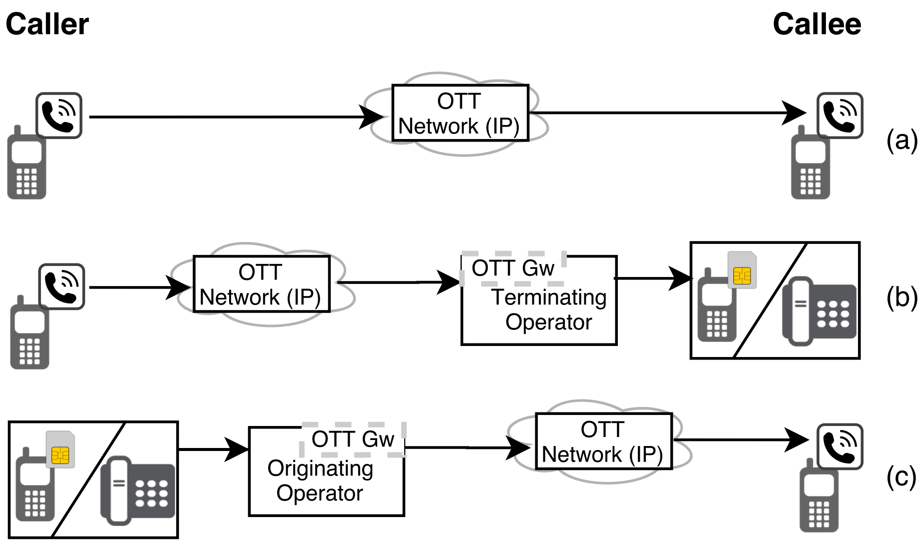


Figure 6.1: Types of OTT involved calls. a) Normal OTT usage, b) OTT-out, c) regular OTT-in.

The -in service (depicted in Figure 6.1-(c)) allows the OTT application to be reachable from any phone on the telephony network, by attributing a phone number to the OTT user. This phone number is often allocated for this kind of service, either by the telecom regulator, or indirectly through another service provider. All calls to this phone number are legitimately terminated over the application, by the OTT network. In this way, the caller can make a cheap local call and the OTT user can receive the call from anywhere in the world through the application. A common example of regular OTT-in service is provided by Skype. A user can purchase a *Skype number*, so that he can answer with Skype the calls initiated to this phone number.

These OTT services are challenging the traditional telephony as they compete directly with telecom operator business. However, they legitimately use the telecom infrastructure and the attributed number ranges. They are also seen as a sign of healthy innovation and are generally accepted by users, even if some countries try to block or regulate them [Was14, Gue].

In this chapter, we address a different kind of service, which is called *OTT bypass*. We claim that OTT bypass is a fraud, because the bypassing parties earn non-legitimate benefits from it, while bringing revenue losses on operators and decreasing the service quality and stability for users.

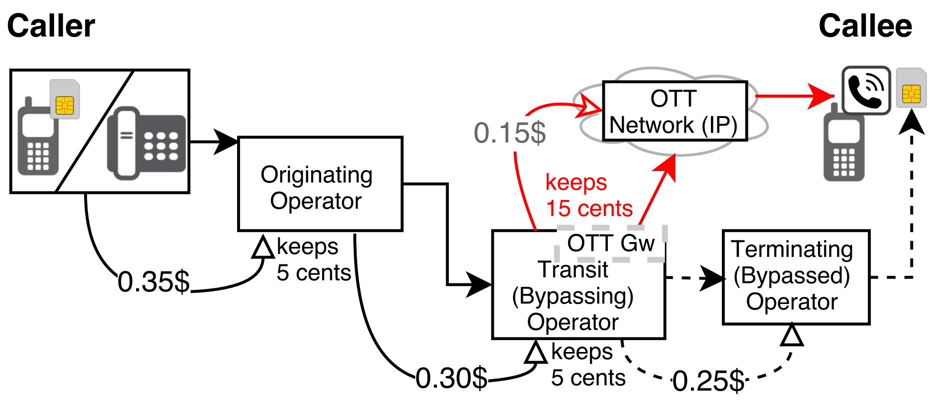


Figure 6.2: A normal call between 2 mobile phones in black and OTT bypass in red.

6.1.3 Telephony and OTT regulation

In order to protect customers, promote competition, and prevent market abuses, telecommunications industries are often subject to strict government regulation [Fis11]. OTT providers are not subject to these regulations, even though they provide similar services. There are efforts to regulate OTTs and VoIP services in some countries [BM15, Was14, Mna15], but this remain a challenge. A common argument is that OTTs are fundamentally different from operators and any regulation on OTT will be against the nature of the Internet. The opposing view argues that OTTs should have the same regulatory obligations as operators (such as taxes, licensing, emergency services and lawful interception) or that they should be paying operators to use their networks [OTT15].

6.1.4 OTT from users' perspective

While users enjoy the free communication services provided by OTT applications, they may also suffer from several security and privacy threats, as their personal data (such as contact lists, photos) is easily shared with these applications [GGAK15].

One issue that should concern all OTT users is the terms of service and end user agreements imposed by OTTs. A study shows that almost 70% of participants never pay attention to the terms of agreements and privacy policies while installing applications on their phones [CFSW12]. Moreover, it is impractical for users to read and understand the terms of service agreements of all the applications they are using [FB14]. As a result, OTT users may unknowingly accept terms of use that come with the end user agreements or default application settings.

6.1.5 Revisiting the Interconnect Bypass Fraud

Interconnect bypass fraud aims to offer cheaper prices for international calls, by routing the calls fraudulently (*gray routes*). Examples of interconnect bypass include the abuse of simboxes [RSB+15] and compromised Private Branch Exchanges (PBX) [GSFG]. Simbox bypass often uses stolen SIM cards (or abuses SIM cards with cheap voice plans) inside a simbox (gateway between VoIP and GSM), which is used to inject international calls into the local telephony network, bypassing the international termination fee. PBX based bypass often abuses a compromised PBX for terminating international calls as national calls.

A fraudulent operator can attract international call traffic by advertising low call termination rates (See "number range hijacking" in Section 4.4.1.) and then terminate this traffic over such *gray routes*. Despite constant fight against interconnect bypass, it is still an unsolved problem in telephony networks, with an estimated annual revenue loss of $5.97 Billion [CFC15]. As we will show next, OTT bypass makes this problem even more challenging.

6.2 OTT bypass

OTT bypass requires agreements between telecom operators and OTT service providers to "bypass" calls. Such calls may originate from a landline or from a mobile number and are supposed to terminate on a mobile number. When a transit operator sees a call for a destination for which a bypass agreement exists, he will check with the OTT provider if the mobile number is registered and online on the OTT network. Many OTT smartphone applications use the mobile phone number as user ID, this greatly simplifies detection of phone calls which can be bypassed. The call will be redirected over the OTT service without the knowledge of the caller or acknowledgment of the callee[3] (or of their operators). OTT bypass is very profitable when the destination of the call has a high termination fee (often in developing countries). The price difference between the normal termination fee, and the negligible cost of OTT call received on a smartphone application becomes a source of revenue for the bypassing operator and the OTT service provider [Col08].

Unlike with other types of OTT-telephony interconnections, this does not benefit the end users, as the caller receives no cost reduction, the callee may pay to receive the call and, as we will show in this study, the service quality is often seriously impaired.

Figure 6.2 shows a fictional example of a regular call from Country A to Country B, where the customer pays 35 cents per minute, operators carrying the call keep 5 cents each and the terminating operator collects 25 cents to terminate

[3] As we will discuss later, the callee can opt-out from this default option.

the call. In this way, the OTT provider proposes an agreement to the transit operator to terminate its calls for 15 cents/min. The transit operator keeps 15 cents per minute instead of 5 cents. Moreover, the OTT provider earns 15 cents per minute by taking over a call which is not intended to be sent over IP. On the other hand, the operator in Country B sees a reduction of its incoming international call traffic, and incurs financial losses due to the termination fees that are not perceived.

Throughout the chapter, we call the operator who performs the bypass (the transit operator in Figure 6.2) the *bypassing operator*. In fact, the bypassing operator could be any of the transit operators on the route, or even the originating operator. All the subsequent operators are bypassed but we will call *the bypassed operator* the operator who is the main target of the bypass.

We will further call bypassed incoming calls *incoming bypass*, i.e., the bypass from the view point of the terminating operator in Figure 6.2. Conversely, we will call *outgoing bypass* the bypass of outgoing calls, i.e., from the view point of originating operator in Figure 6.2.

To the best of our knowledge, the first trials to terminate traditional calls on OTT networks started in 2013 [Cro13] and a patent was issued in 2014 describing this mechanism [Bar14]. This patent also mentions that the OTT service provider may reject some bypass attempts. In this case, the bypassing operator can choose to route the call over another operator. This mechanism is very similar to the *crankback* functionality that is employed in some call routing protocols [MR07]. *Crankback* returns a call to the previous switch, so that it can choose another route (e.g., in case of congestion). The patent mentions transmitting the call twice, via the OTT provider and the traditional operator. The recipient's phone line and OTT application will ring simultaneously and the one that is not answered will be canceled. We show in Section 6.5 that this causes many problems for the users.

OTT bypass: A fraud or not?

It is often delicate to tell if some action is legal or not, especially when telecom operations are international and are subject to very diverse laws. We do not claim that OTT bypass is illegal (a lawsuit may be needed for this), but we claim that OTT bypass is fraudulent for the following reasons. First, a call to a certain phone number has to be routed to the operator to which the phone number was allocated by International Telecommunication Union (ITU) or national regulators [E1697]. This is violated by the entities involved in OTT bypass, because the call is routed to the OTT provider instead. Moreover, most countries impose regulatory fees and taxes for incoming international calls. These are paid by the caller, but hijacked by the bypassing operator. Service level agreements between operators are also violated when an operator pays for a premium quality

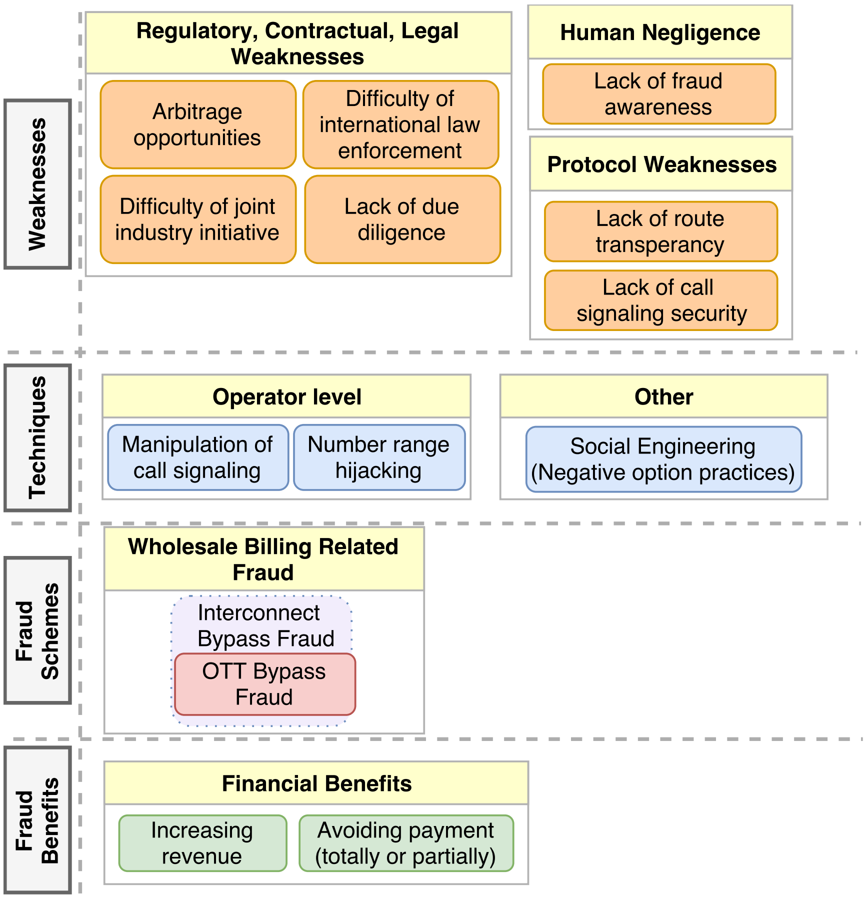


Figure 6.3: OTT bypass fraud in our taxonomy.

call route, but its calls are bypassed over the OTT network. Unlike many OTT services, OTT bypass has no clear benefit for the users. In practice, OTT bypass is similar (in its effects) to other types of interconnect bypass fraud, such as simbox bypass [RSB+15]. As summarized in Figure 6.3, it manipulates many weaknesses in regulatory and legal frameworks, as well as the call signaling protocols. Recently, ITU created a working group to study OTT Bypass, where OTT bypass is clearly reported as a fraud [ITU16].

6.2.1 Possible consequences of OTT bypass

Users may suffer from several problems when a call is bypassed over OTT. First, the call is going over the public internet, without any guarantees of call quality and with poor mobility management (moving away from a Wi-Fi area to mobile data network leads to an interruption of the call). The callee will also be unable to use voicemail, call forwarding or call blocking services provided by his operator.

The caller will pay the same fee for the bypassed call as he would pay for a normal call. However, the callee may be charged for data traffic while call reception is normally free, in most of the world, and may sometimes miss calls.

Effects of OTT bypass on bypassed operators can be more severe. All bypassed operators will suffer from a decrease in call volume. However, the terminating operator is likely to incur the highest revenue loss.

In the short term, OTT bypass is profitable to the bypassing operator. However, as the OTT provider expands its agreement coverage, it may be bypassed itself, as more traffic is terminated on OTT networks. Thus, OTT bypass and its effects should be considered globally, rather than individually by operators.

OTT bypass may also facilitate call hijacking: The registration verification is performed with a code sent over a regular text message. If an attacker is able to intercept such a message[4], he could register this account (phone number) on another phone. Using this technique, we were able to receive OTT bypassed calls on a phone that never had the corresponding SIM card. Finally, OTT bypassed calls may also evade lawful interception platforms.

6.3 Detection and Measurement of OTT bypass

Detecting the existence of OTT bypass and measuring its scale is important for bypassed operators to estimate losses, inform their customers and collect evidence for legal cases or in communication with regulators and bypassing operators. The main difficulty for a bypassed operator is to measure the traffic that is not flowing through his network anymore. We present possible techniques for detection and measurement of OTT bypass and we use the criteria presented in Table 6.1 to evaluate them (Table 6.2). While we focused on detection, most prevention techniques have to rely on detection first. In practice, multiple techniques can be combined to fight OTT bypass.

6.3.1 CDR volume analysis

Operators can observe the decrease in their incoming call traffic and generated revenue from the Call Detail Records (CDR). While this is an indicator, it does not provide a reliable measurement. Indeed, there may be other reasons for this decrease, such as regular OTT calls (other than OTT bypass) or changes of habits. Additionally, this technique can only measure effects of incoming bypass, but it is easy to implement and it does not interfere with the network and users' privacy (as long as CDRs are handled with care).

[4] E.g., through temporary access to the phone, a malicious application, or account hijacking [SFK+12].

Table 6.1: OTT bypass measurement techniques evaluation criteria.

Bypass direction	Detects either incoming or outgoing bypass
No collaboration requirements	Does not require collaboration of users, other operators or regulators
Easy deployment	Cheap and easy deployment, maintenance, no big changes to infrastructure
Scalable	Scalable to millions of users, applicable to different OTT vendors
Accurate	Does not detect legitimate traffic as bypassed traffic (no false positives)
Passive measurement	Measurements do not need intrusive setup, can be performed on past, logged data
Ethical and privacy preserving	Ethically feasible, respects users privacy
Complete	Detects all OTT bypass traffic (no false negatives or traffic which cannot be monitored)
Definitive	Not a cat-and-mouse game between operators and OTT providers
No privileged access required	Does not require access to some sensitive data or systems (e.g., CDR, network access)
Representative measurement	Gives a representative view of the bypass affecting the real call traffic
Technically easy	No potential obstacles foreseen in the deployment or implementation of the technique
Likely to succeed	Technique has been demonstrated work, or is very likely to work

Table 6.2: Measurement techniques with their advantages and drawbacks (✓yes, ✗no, ~partially, **?**unclear).

	Incoming bypass	Outgoing bypass	No collaboration req.	Easy deployment	Scalable	Accurate	Passive measurement	Ethical/privacy	Complete	Definitive	No privilege req.	Representative measurmt.	Technically easy	Likely to succeed
Indirect evaluation (CDR analysis)	✓	✗	✓	✓	✓	✗	✓	~	✓	~	✗	~	~	~
Test calls for incoming and outgoing routes	✓	✓	✓	✗	✓	~	✓	✓	✓	~	✓	✗	✓	✓
CDR comparison with users' OTT online status	✓	✗	✓	~	~	~	✗	✗	✗	~	✗	✓	✗	~
Pinpointing bypassing operators	✓	✓	✗	~	✓	✓	✗	✓	✓	✓	~	✗	✗	~
IP traffic analysis	✓	✗	✓	~	✓	✓	✓	~	✗	✗	✗	✓	✗	~
Audio fingerprinting (operator side)	✗	✓	✓	✗	~	**?**	✓	✗	✓	~	✗	✓	✗	~
Audio fingerprinting (caller side)	n/a	✓	✓	✓	✓	✓	**?**	✓	~	✓	~	✓	✗	~

6.3.2 Tracking the OTT users' online status

OTT applications often automatically discover preexisting contacts on the network by using the address book (the so-called *address book matching* technique). This can be used to crawl registered phone numbers on an OTT network [CYJ+13] and was also used for targetted attacks [GGAK15]. Similarly, contacts' online status displayed on the application can be monitored as well. Correlating this with the decrease of international calls for a large set of phone numbers could allow to estimate the amount of bypassed calls on the network.

We partially validated this approach by collecting online status of a test phone from the instrumented desktop application of the bypassing OTT provider. This allowed us to keep track of the online/offline status of the phone with 90% accuracy when compared to the actual online/offline status of the phone[5]. Furthermore, we tracked the online/offline status of 19 users (with legal advice and their written permission) for 6 months. However, the number of international calls they receive was not large enough to give significant results. On the other hand, we could not perform a larger scale tracking of real users, due to the legal and privacy issues with this approach.

6.3.3 Test Calls

A more precise measurement is possible using test calls. Using a TCG platform, a bypassed operator can generate calls to its own network from various operators in the world. The bypassed operator needs to register some phone numbers to the OTT application and observe if the calls generated by the TCG platform terminate on the regular network or on the OTT application.

Unfortunately, these platforms can be expensive, and often offer inflexible packaged services. Moreover, most of the TCG platforms can only show the bypass on incoming routes. Checking for bypass on outgoing routes would require several phones deployed worldwide and with the OTT service installed (or abusing registration mechanism as mentioned previously).

Test calls shows bypass on tested routes but do not provide the bypass rate on the real traffic. The knowledge of the volume of calls on each particular route (before the bypass) and the market share of the OTT application is needed to estimate the actual bypass volume. However, routes can change quickly and it might be difficult to compute a good estimation of the actual amount of calls on each route.

6.3.4 Pinpointing bypassing operators

A major problem with OTT bypass is the opacity of the call routing. Because of this, discovering the bypassing operator is difficult. Some test call generation platforms provide information about the outbound route taken by a call. If a

[5]This experiment was conducted in a lab environment, with a rooted Android phone and a steady WiFi network.

test call can be performed from the next hop indicated by the TCG platform, then this is one step closer to the bypassing operator. Iterating the tests in this fashion may allow to find who is performing the OTT bypass. However, this approach has multiple limitations, some of which we explain on a case study in the next section.

6.3.5 Network traffic analysis

As the OTT traffic is transmitted over the IP network, the operator may attempt to detect it in the data traffic [BMM+07, KD12, FZS08, EP06]. The main issue with this approach is that it will only allow to evaluate the OTT traffic from users who use OTT over the mobile data network, but not over other data networks from other operators (e.g., Wi-Fi/ADSL).

6.3.6 Audio fingerprinting

Like for simbox fraud [RSB+15], the OTT bypass may incur some distortion on the audio channel which would allow to build fingerprints that could be used for detection. The caller or his operator could use audio fingerprinting to detect OTT bypass on outgoing calls. However, it seems difficult (in terms of resources) for an operator to fingerprint all audio communications. We could imagine to perform this detection from an application on caller's smartphone, but the call audio in smartphones is handled by the baseband processor and usually not available to the applications. Moreover, the incentives for the caller and originating operator to detect OTT bypass are not clear. In addition to this, the callee does not need detection, as he can see how he receives the call. Finally, the callee's operator can not fingerprint the calls because he can not access the audio stream of the bypassed calls.

6.4 Case Study: OTT bypass In A Small European Country

In this section, we present a case study of OTT bypass performed on a mobile operator in a small European country. We mainly focus on test calls in our analysis, as the other techniques either have drawbacks (e.g., ethically questionable, unpredictable results) or would require a complete study on their own.

We next present results from two different test call campaigns in which 15,872 test calls were performed over a period of 8 months (summarized in Table 6.3). The first campaign was performed with a generic commercial TCG platform, with a very broad network coverage. In the second campaign, we performed

Table 6.3: Test calls performed during 8 months of experiments.

Origin	Number of calls	Duration	Date
Worldwide	1016	7 days	November '15
UK	134	3 days	March '16
Germany	260; 2876	4; 68 days	March; April-June '16
Netherlands	1220	55 days	May-June '16
Italy	3201	68 days	April-June '16
Switzerland	3635	67 days	April-June '16
Spain	1392	37 days	May-June '16
Austria	49; 2006	3; 37 days	April; May-June '16
Turkey	83	3 days	April '16
Total	15,872	352 test days	8 months

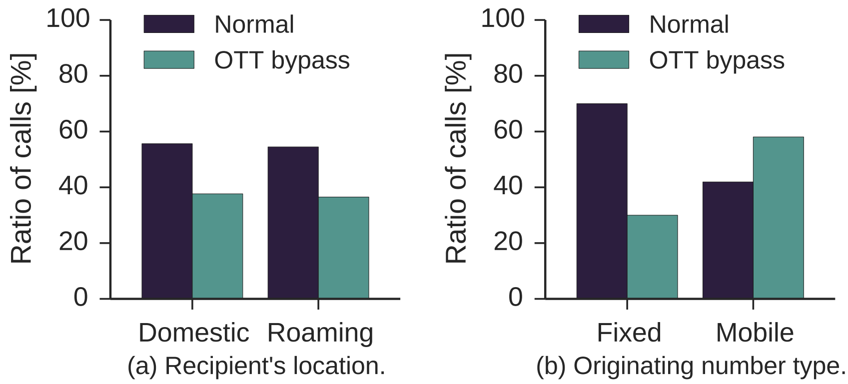


Figure 6.4: Bypass rate depending on callee's roaming status and the type of originating call.

more fine grained analysis using a smaller and dedicated test call platform that we built for this purpose.

6.4.1 Global tests with TCG platform

The TCG platform handles the generation of calls from various landline and mobile numbers that belong to different operators in different countries. For each call, the platform provides a call log including the originating country and network, call start time and call end time. At the receiver end, we use 4 different SIM cards that belong to the bypassed operator and that are registered to the OTT application. We collect the type of call termination from the recipient phones. We do not answer the calls, but only let them ring.

Measuring the prevalence of OTT bypass

1016 test calls were performed with the TCG platform, originating from 148 different networks (operators) in 50 different countries. OTT bypass occurred on calls originating from 90% of these countries and from 62% of the networks. In total, 40% of the test calls were bypassed. This shows that OTT bypass towards this destination is very frequent.

During those tests, the SIM cards were first in the home network (3 days) and then roaming in another country (4 days). The OTT bypass rates seem to stay the same whether the user is roaming or not, as shown in Figure 6.4-(a). With 95% confidence [LB10], bypass rates for domestic and roaming phones are 37% $\pm 4.14\%$ and 36% $\pm 4.26\%$ respectively. We also make a chi-square test to our hypothesis that the OTT bypass rate is independent of phone's roaming status. For the significance level of 0.05, p-value of the test is 0.713, which means that these variables are independent. This is consistent with the fact that the OTT bypass generally occurs before the call reaches the home operator and that a call to a roaming phone generally goes through the home operator first.

In Figure 6.4-(b), we analyze the effect of originating number type[6] on the bypass rate. With 95% confidence, landline numbers were bypassed with a ratio of 17% ± 4.57% and mobile numbers were bypassed with a ratio of 25% ± 4.12% [7]. The bypassing operator may be processing all the calls in the same way, regardless of the originating number type. We note that, the reception of calls from a landline on the OTT application may be surprising for a callee who is not aware of how OTT bypass works.

Identifying bypassing operators

For some of the calls (usually the calls that are originated from landline numbers), the TCG platform also provides the name of the outbound operator. Moreover, for a non-bypassed call, the mobile operator sees the inbound operator from which the call is arriving. We obtain this information from the ISUP logs of the mobile operator.

Figure 6.5 shows the result of combining those logs to build a partial map of routes for the calls originating from 7 different operators in UK. We see that all calls initiated from operators A2, A3 and A4 are bypassed. Those operators may be using a fraudulent route, or they may be the bypassing operators themselves. For operator A1, we are able to see the first level of transit operators (B1, B2, B3, B4). A1 suffers from bypass, every time it selects the operators B2 or B4 for routing the calls. Moreover, operator B1 should have at least one bypassing operator among its immediate or subsequent partners. This is also valid for

[6] Determined using a numbering plan database [bsm].
[7] Using the test calls for which we have the originating number (74% of the test calls).

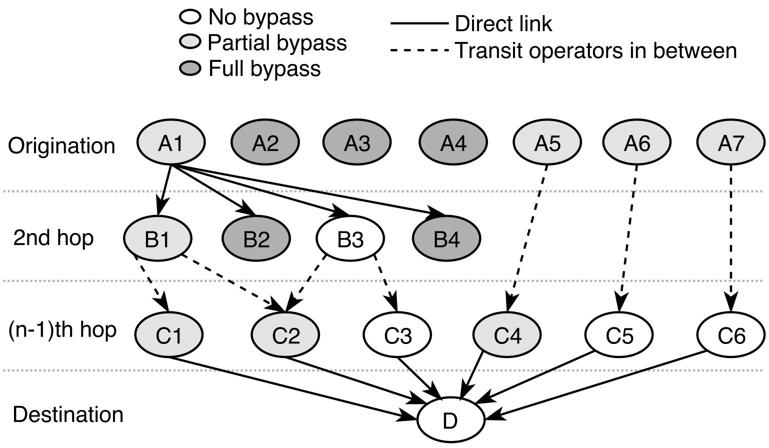


Figure 6.5: Partial map of operators involved in test calls originating from UK.

operators A5, A6 and A7. With this information, we could already start to identify problematic routes and potential bypassing operators.

Pinpointing the exact bypassing operator on a route would be possible by iterating over the route (for example make test calls from B1, on all its possible routes to artificially "trace" a call) to identify the next hops and which of them perform a bypass, until the home operator is reached (as described in Section 6.3.4). This approach would require that (1) the calls will follow the same route when bypassed or not (until the bypass), (2) that a call will be routed similarly when traversing and when originated by a network (3) routes are stable over time and (4) we obtain the next hop for each operator on the route.

However, assumptions (1) and (3) do not always hold because route selection can be very dynamic, depending on the contractual agreements and routing algorithms. We also found cases where operators show different bypass behavior when they are in transit or originating positions. For example, all calls originated from operators C1 and C2 were bypassed even though they have transit agreements with the home operator. Finally, assumption (4) may not hold as the TCG platform may not always provide the next hop information.

Due to these limitations and the high cost of the TCG platform, we were not able to perform such iterative test calls to reveal a larger map of operators.

6.4.2 Fine grained experiments with our custom test platform

In order to run long-term, customized tests, we used a small test call generation platform that we built from scratch. Our platform is built on Android phones that we control remotely via SSH on a Wi-Fi connection. We generate calls from one Android phone (caller) to another (callee). For each test call, we

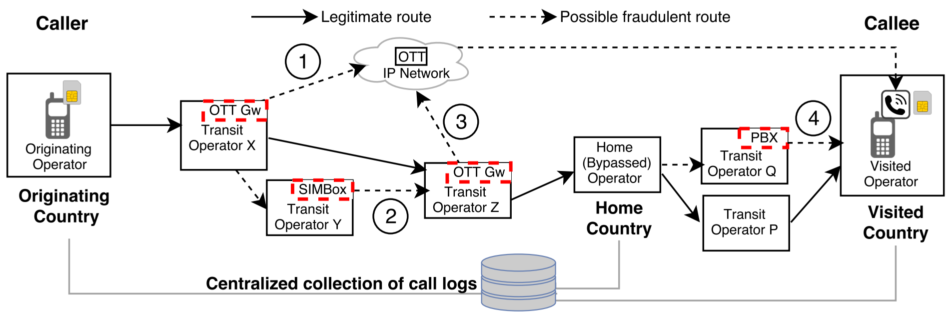


Figure 6.6: Experimental setup and summary of fraudulent routes.

collect information from both phones. For normally terminated calls, we also obtain the Call Data Records (CDR) from the home operator (Figure 6.6). All events are timestamped and phones are synchronized with NTP. With this setup, measurements have an accuracy of 20 milliseconds or better. Again, we do not answer any calls, but let them ring for one minute.

To generate test calls, we placed one phone per country, in 8 European countries. Even though we could test only one originating operator per country, all of them were major operators, with a total of more than 100 million customers. For each generated test call, we collect the network name, call start time, ringing time and call end time from the caller. Because the network conditions may change during the day, we initiate the test calls at every hour of the day, from each of the operators.

On the receiving side, we use 3 smartphones each with a SIM card from the bypassed operator. Two of them are registered on the OTT network and one of them was never registered. One of the registered SIM cards is used with changing configurations such as connectivity on/off and OTT bypass option[8] enabled/disabled. We collect the incoming call logs from the relevant database files in Android and the OTT application. Using these logs, we obtain the incoming call time, call termination type and the received caller ID. Moreover, the recipient phones are roaming in another European country (visited country), outside of their home country, as depicted in Figure 6.6.

Bypass rates and colliding fraud schemes

During the course of the experiments (from April'16 to June'16), we generated calls everyday on an hourly basis, from each of the origination phones to each of the recipient phones. Overall, we observed OTT bypass from 6 out of 8 countries, with bypass rates ranging from 42% to 83% (Figure 6.7-(b)). Moreover, we noticed that multiple fraud schemes may collide: In a few cases, we detected

[8] The application setting that allows OTT bypass

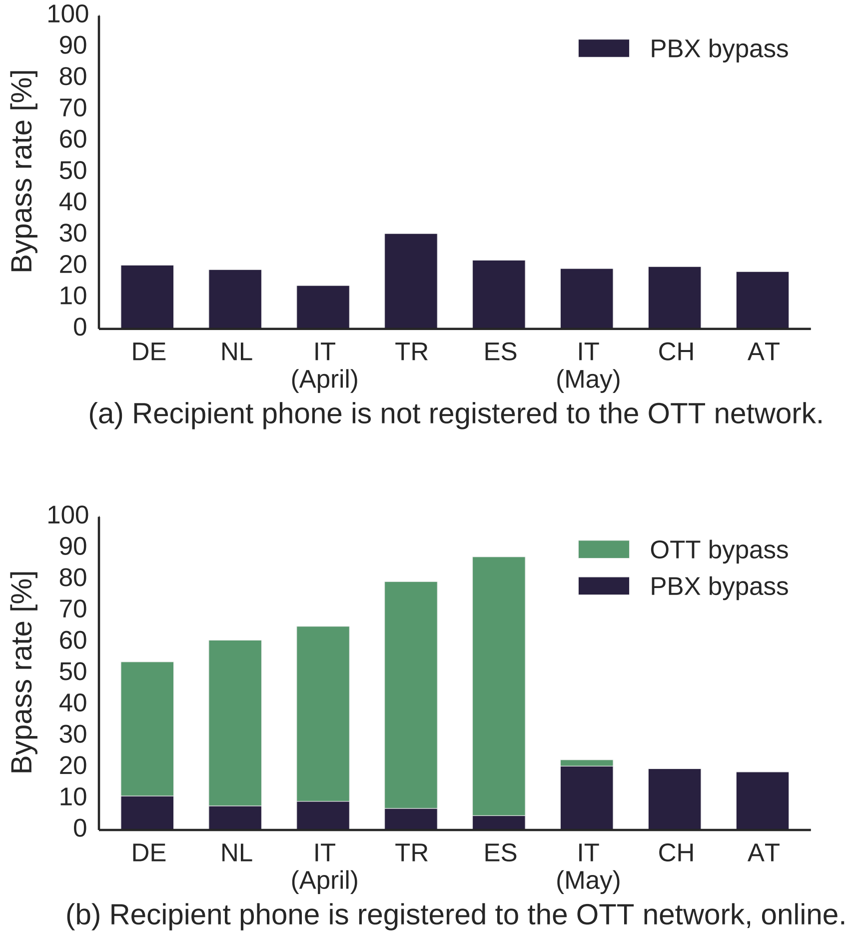


Figure 6.7: OTT and PBX bypass rates depending on the phone status.

other types of interconnect bypass (via simbox and PBX) in addition to OTT bypass (Figure 6.6) and a possible case of *false answer supervision fraud* which we will explain later.

We detect the simbox and PBX bypass frauds by comparing the real caller ID and the received caller ID. An incorrect caller ID often means that the call went over an illegitimate gateway, which modified the caller ID.

If the Caller ID corresponds to a mobile phone number range, we assume the call was bypassed with a simbox. On the other hand, if the number belongs to a fixed range we assume this is a PBX bypass (we also check how the number was allocated). In fact, a PBX may allow to spoof a caller ID, but this is not possible with simboxes, as they essentially use an IP-GSM gateway. Thus, caller ID inconsistencies remains a good indicator of interconnect bypass. In particular, we expect false negatives (forged caller ID) but no false positives. We

Table 6.4: Simbox and OTT bypass combined.

	OTT Not Registered	OTT Registered, Online
Normal calls	38%	22%
Simbox bypass	62%	17%
OTT bypass	-	35%
Simbox + OTT bypass	-	26%

now describe these interesting observations on the test calls.

Simbox and OTT bypass collision The test calls performed from UK in March had a ratio of 61% of OTT bypass. Some of the calls were also bypassed over a simbox, that uses SIM cards from a mobile operator from another country. Table 6.4 shows the bypass rates for two different recipient phone numbers, one is registered to the OTT application and the other is not. The overall simbox bypass rate is 43% if the number is registered on the OTT network and 62% otherwise. We have collected 34 unique simbox numbers, belonging to the same operator.

We observe that 26% of the calls to the OTT registered phone number were bypassed first over the simbox (② in Fig. 6.6) and then over the OTT network (③ in Fig. 6.6). In other words, the operator on which the simbox bypass occurred routed the call over a route which is subject to OTT bypass. However, not all the OTT bypassed calls had simbox caller IDs. Thus, there should be another operator performing OTT bypass on a different route, or before the simbox bypass (such as ① in Fig. 6.6). We also confirm this when we make calls while the phone is offline (has no Wi-Fi or data network connectivity). For example, we make a call to an offline phone but the phone does not receive the call (does not ring). Then we turn on the connectivity and get 2 different missed call notifications on the OTT application: one with a correct caller ID, and one with a simbox caller ID. In other words, each time there is an attempt to send the call over OTT network, the OTT application receives a missed call notification.

PBX bypass on roaming part of the call We observed another interconnect bypass fraud, through possibly compromised cloud IP-PBXs[9]. In this case, a test call arrives with a caller ID belonging to a fixed phone number, with a geographic area code from the visited country. However, we never observe an OTT bypassed call with a PBX caller ID. Also, the call data records from the bypassed operator show the correct caller ID. This PBX bypass therefore occurred between the bypassed operator and the visited operator (④ in Fig. 6.6). As a result, a call bypassed over the OTT network has a correct caller ID, but a call terminated

[9] The phone numbers were allocated by the regulator to this cloud PBX service provider, this interpretation was also confirmed by an operator who was aware of this bypass case.

normally may have an incorrect caller ID. Figure 6.7 summarizes the bypass rates for two different recipient phone numbers, one is not registered on the OTT application (only experiences PBX bypass) and the other is registered and online on the OTT network (experiences both PBX and OTT bypass). We can see that, among the countries that experience OTT bypass, PBX bypass rates are relatively lower for OTT registered phones because most of the call volume is terminated over the OTT network.

False Answer Supervision (FAS) fraud Among the 8 countries from which we generated test calls , Spain has the highest percentage of fraudulent calls: 88% of calls were subject to either OTT or PBX bypass. From Spain, we detect many other problems: 17% of normal call terminations have an empty caller ID and 30% of the calls did not reach their destination (counted as failed calls). Moreover, we were charged for 23% of the calls in the first 10 days of the experiment, even though we do not answer any of the test calls. In addition, half of the calls that were illegitimately billed, were actually failed calls. These issues probably stem from a fraudulent gateway on the call route, which employs False Answer Supervision (FAS) fraud. As we describe in Section 4.5.3, a fraudulent transit operator may start billing the call while the call is ringing, but not yet answered ('early answer'). The transit operator may also short-stop the call to a fake ringing tone or network message and bill the call as if it was answered, without routing it to the legitimate destination ('false answer') [Nex].

PDD analysis and ringing anomalies

The Post Dial Delay (PDD) is the interval of time between the press of the call button (or the last digit of the phone number) and the ringing tone, if the call establishment is successful, or any other network message indicating the call outcome [ITU99, MLMD12]. The PDD covers the connection establishment process in which multiple switches and gateways are involved in setting up an international call. It is one of the main QoS metric in telecommunication networks [RD88] because it affects caller's perception of the state of the call setup and, e.g., her decision to abandon the call [MLMD12, LFS88]. The International Telecommunication Union (ITU) specifies a recommended mean PDD value of 8 seconds for international PSTN calls and 16.5 seconds for international mobile calls [ITU99, ITU96].

VoIP to PSTN gateways generally increase the complexity of call setup process and they often introduce additional performance problems [Col08, ES00]. Thus, we expected the bypassed calls to have higher PDDs (i.e., *PDD (bypass)* in Figure 6.8) would be larger than *PDD (normal)*).

Surprisingly, we found that values for OTT bypassed calls are very similar to those for normal calls (Figure 6.9). Moreover, for 2 countries, Germany and

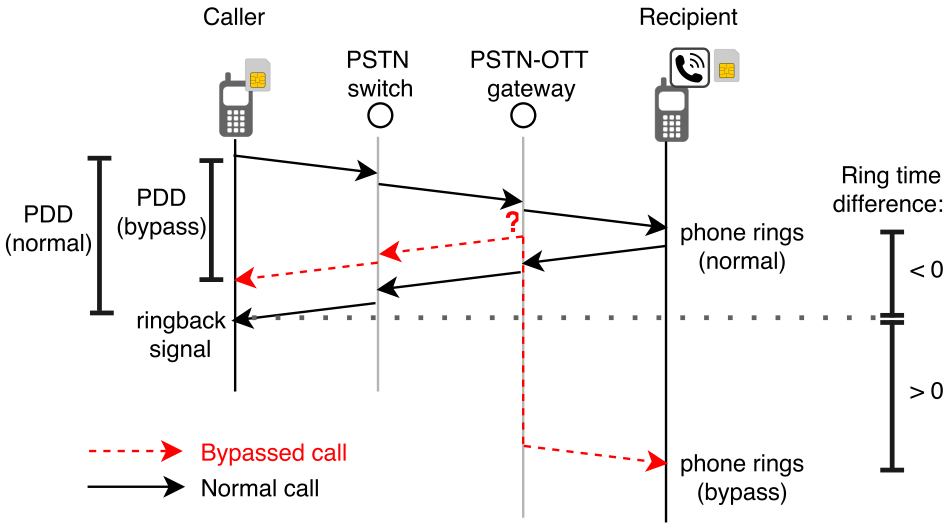


Figure 6.8: Post Dial Delay (PDD) in a normal phone call and in a OTT bypassed phone call.

Turkey, the mean PDD values for OTT bypassed calls are even smaller than for normal calls.

We therefore also measured the time difference between the recipient phone ringing and the caller hearing the ringing tone. We call this the *ring time difference*. As can be seen on Figure 6.8, if the callee's phone starts ringing first, and the caller hears the ringing tone later, ring time difference becomes a negative value. On the other hand, if caller hears the ringing tone first and the callee's phone starts ringing later, this value will be positive. Ideally, the ring time difference should be close to 0, so that the caller and callee are be notified simultaneously. While a small ring time difference is normal, we found that it is much higher for OTT bypassed calls than normal calls (Figure 6.10). This seems to indicate that the OTT provider sends a false ringing tone to the caller, before the recipient's phone actually starts ringing. In other words, during the 30-40 seconds of ring time difference interval, the caller will think that the recipient's phone is ringing, but the recipient will not be notified about this call. As a result, caller may drop the call before the callee is aware of the call or has time to answer. This practice should not be confused with false answer supervision fraud, because here even if the caller hears an early ringing tone, the calls do not start to be charged.

Implementation related problems

OTT bypass requires a good synchronization between the bypassing operator and the OTT provider. Implementation or configuration mistakes may lead to

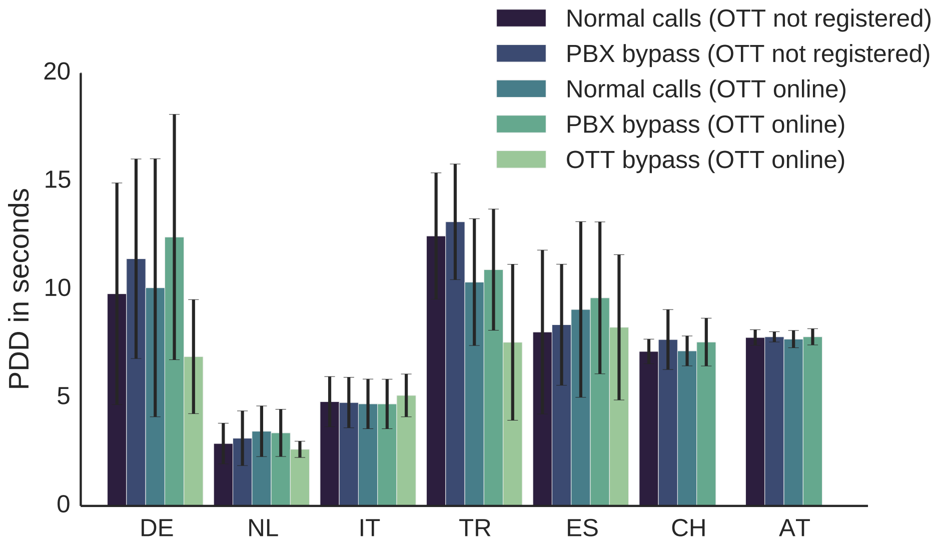


Figure 6.9: Mean PDD and standard deviation, for each country in function of the bypass type (no OTT bypass for 2 countries).

unexpected problems.

The OTT provider needs to check if the user is online and has a proper Internet connection before bypassing a call. This can be done in several ways such as using periodic data probes or using historic data from past calls and locations. Failing to do this accurately can lead to two problems. First, when a user receives a call but recently went offline on the IP network, the OTT provider may still try to bypass the call. Because the user is offline, he will miss the call, even if his phone was in fact able to receive it as a regular call. When he is back online, he will receive a missed call notification from the OTT network. Secondly, when the phone is currently offline and unreachable from the cellular network, e.g., in airplane mode, the calls may still be bypassed. I.e., the caller may hear a ringing tone, instead of getting a network message (or voicemail) indicating that the callee is unreachable.

It is possible that the parallel calling feature (described in Section 6.2) was introduced to hide such problems. With this feature, the bypassing operator notifies the OTT provider and another transit operator at the same time. Thus, even if the OTT provider is not able to terminate the call, the transit operator will try another route to terminate it. As a consequence of this, the user may get a missed call notification on the OTT application even when a call was received normally.

We highlight these problems by conducting a dedicated experiment where we turn off the Internet connectivity off and on and then we switch the phone off and on, waiting for 5 minutes between each step. During the 5 minutes period,

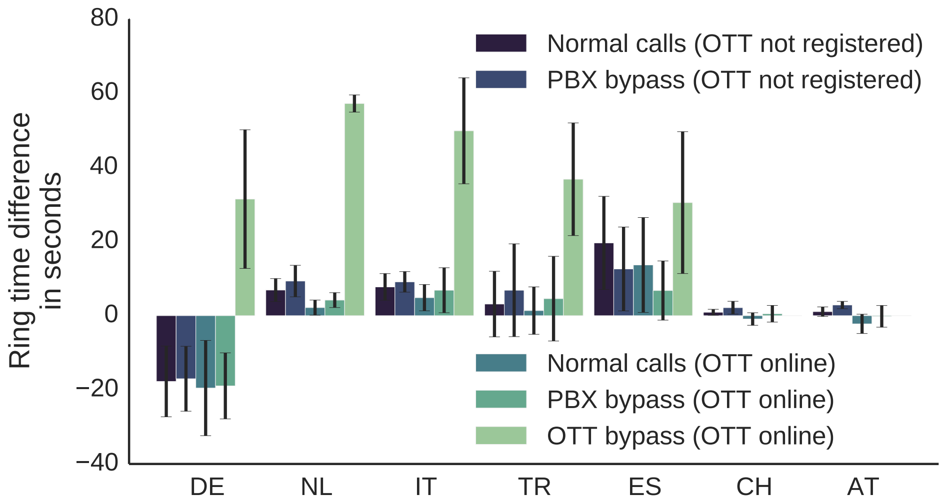


Figure 6.10: Mean ring time difference and standard deviation, for each country in function of the bypass type (no OTT bypass from 2 countries).

we initiated 5 calls to this phone, one call per minute. We do this several times (60 calls in total). We found that 60% of the calls were terminated normally, but left a missed call notification on the OTT application while the Internet connectivity was off. Moreover, the caller heard a ringing tone in 20% of the calls even though the recipient phone was turned off. These problems are also mentioned by the users (Section 6.5.1).

Discussion

Our experiments show that telephony networks are subject to a high amount of fraud, which deteriorates call establishment quality. It seems that OTT bypass often collides with other forms of bypass. This may be due to a "race to the bottom" on the price of call minutes. For example, when an operator receives an artificially low price for a destination due to the presence of OTT bypass, then it might make good offers to its customers for that destination. These low offers may in turn be abused by simbox fraudsters.

Even though the OTT provider seems to conceal some of the effects of OTT bypass, those effects further degrade the quality of call establishment.

Note that, we did not measure audio quality in our test calls, because OTT bypass does not necessarily deteriorate it. Instead, we have focused on other aspects of QoS, which are fundamentally harder to solve in an OTT bypass scheme. Moreover, as we mentioned in Section 6.3.6, call audio is not easily accessible on smartphones and it would be costly to answer the test calls.

6.5 Case Study: User study

In this section we present a user survey conducted on 8,243 customers of the bypassed operator which we studied in the previous section.

Understanding users' perception and experience on OTT applications can provide insights on how to address the issues with OTT bypass. We therefore performed a large-scale survey where we first aim to measure the *perceived QoS* [GJS03] (customers' experience of using the OTT services). Then we measure the *assessed QoS* (i.e., customer's decision on whether to continue using the service). Thus, in this survey we measure:

- OTT usage frequency, experience and habits (perceived QoS),
- the awareness about OTT bypass option,
- the tendency to opt-out from OTT bypass option, after informing users about its effects (assessed QoS).

6.5.1 Organization of the survey

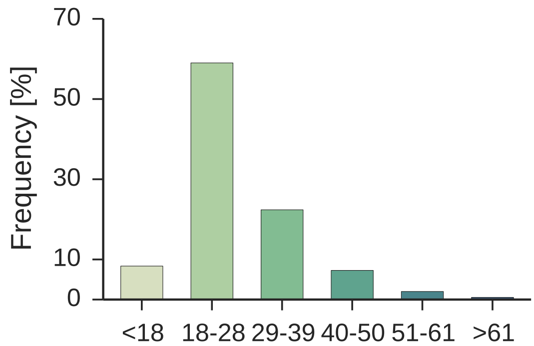
The survey consists of 12 questions. We prepared the survey to be short, easy to answer, and to be as neutral as possible. It was mainly advertised for users of the bypassing OTT provider, via the mobile operator's social media pages and call center. As an incentive, a bundle of 2 GB of free mobile data for 3 months was offered to 10 randomly selected participants. This attracted many responses, but also helped to ensure that only real customers answered the survey as the phone number had to be provided to obtain the prize. The survey received 8,739 answers, out of which 7,617 were left after removing the duplicates [10] and answers from people who claimed they do not use the bypassing OTT application. The questions were written in English and then translated to the local language. A 5-level Likert scale [Lik32] is used in most of the questions. The rest of the questions are either yes/no or open ended questions. (The complete questionnaire and raw data for the answers can be found in Appendix B.)

6.5.2 Results on general OTT usage

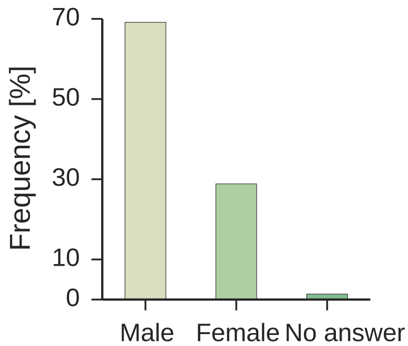
The first five questions of the survey address the general OTT and smartphone usage. Figure 6.11 shows that the majority of the participants are young adults and 70% of participants are male.

Figure 6.12-(a) and (b) show that OTT applications are very popular for both calling and messaging. This can also indicate that a significant percentage of

[10] Only the first answer for each customer (phone number) was kept.



(a) Age distribution.



(b) Gender distribution.

Figure 6.11: Age and gender distribution for participants.

voice and messaging traffic is carried by OTTs. Moreover, 72% of OTT users are using it for international or both international and domestic calls.

Another point we analyze is the frequency of use of Wi-Fi and mobile data networks. Figure 6.12-(d) shows that both Wi-Fi and data use is very common, yet the Wi-Fi usage is slightly more frequent. This is an important observation, because when the Wi-Fi network is used, the operator will not see the OTT bypass IP traffic at all. Moreover, the fact that OTT users stay online most of the time increase their chances to be a victim of OTT bypass.

In figure 6.12-(d), we can see that people frequently experience call quality problems (such as distorted audio, incorrect caller ID and call failures) with OTT applications. 70% of participants experience problems, 'Sometimes' or more often.

6.5.3 Results on the usage of the OTT service

After analyzing overall OTT usage, we ask 5 questions only related to the by-passing OTT provider.

We first remark that this OTT provider has a $OTT\text{-}out$ service, which is a regular OTT service as we described in Figure6.1-(b). The $OTT\text{-}out$ feature is advertised a lot, whereas the OTT bypass option is only shown in the application's settings and in the terms of service, e.g., even the OTT provider's web page does not mention it. Moreover, OTT bypass option is enabled by default and users can opt-out from it inside the application settings.

Awareness about OTT bypass option

We compare the user awareness about the prominent OTT-out feature and the buried but active by default OTT bypass option. Figure 6.13-(a) shows that

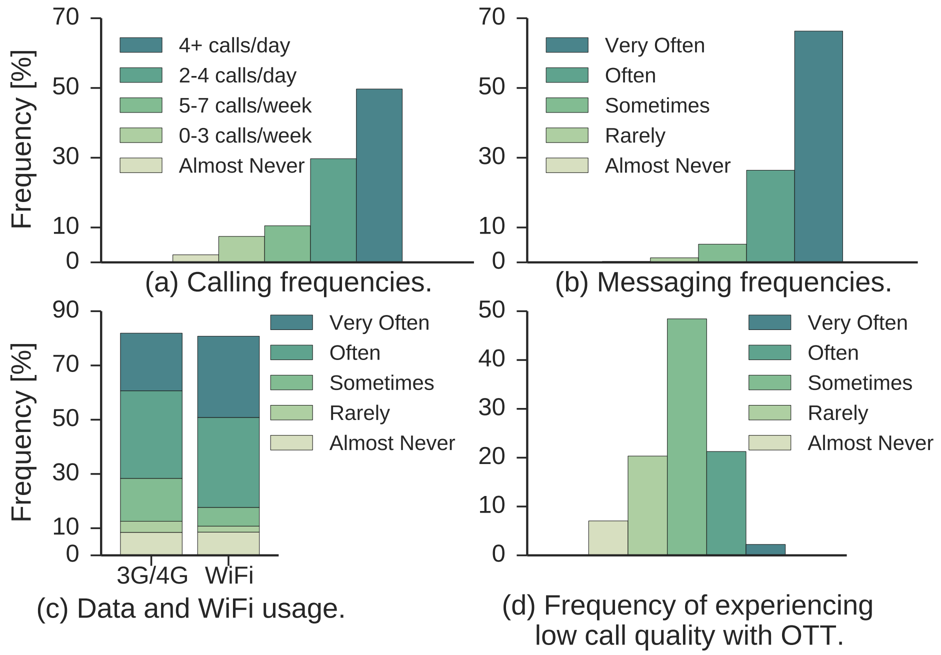


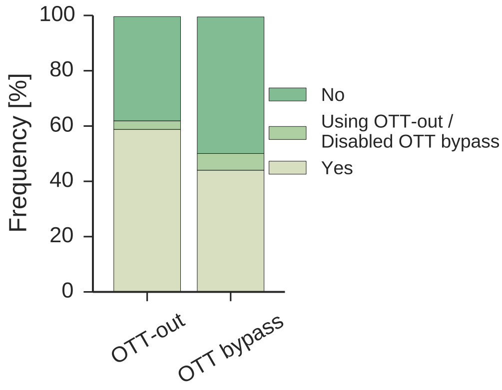
Figure 6.12: Statistics on the usage of OTT applications.

awareness of the OTT bypass option (50%) is lower than the awareness of the OTT-out feature (62%). However, number of people who have deactivated OTT bypass is higher than the number of people who are using OTT-out: Among the people who are aware of OTT-out, 5% are actually using it, but among the people who are aware of OTT bypass, 12% have deactivated it. Apparently, OTT-out feature is not very popular among the participants.

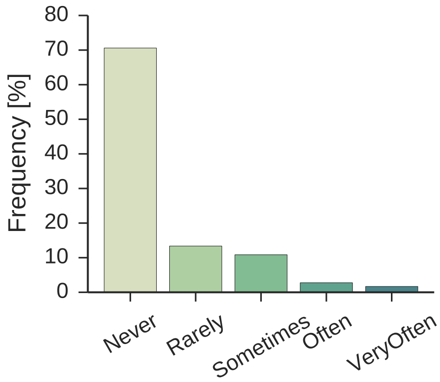
One explanation might be that OTT-out users as more advanced users, who may check the settings and who can better understand the meaning and consequences of the OTT bypass option. Among them, 73% were aware of the OTT bypass option, and 20% have deactivated it. Thus, it is likely that knowing and understanding more about the OTT bypass option increases the deactivation rate.

Bypass detection

Another goal of this survey is to understand participants' experience with OTT bypass. Figure 6.13-(b) shows that, 30% of people think that they have received at least one bypassed call. Among the people who frequently receive bypassed calls (often or very often), 28% were previously not aware of the disable option, 64% were aware and 8% have already disabled. Quite a high proportion of users was aware of the OTT bypass option, but did not opt out. There are two possible



(a) Awareness.



(b) Bypass detection.

Figure 6.13: Awareness on different application options and bypass detection rates.

reasons for not disabling the OTT bypass option. First, it is possible that people do not actually understand the effects of this option. Second, people may not be experiencing any problems with it, so they leave the option as default [LH06]. Then, we ask, in an open ended question, if participants detect any calling anomalies with the bypassing OTT application. 53% of people answer No to this question while 0.6% answer Yes and 1% enter a long answer with additional comments. Some of these comments are not related to our discussion, such as problems with video calls or registration issues. However, some of the answers highlight important issues and confirm the problems we found in Section 6.4:

- The application does not ring during an incoming call, but shows notification afterwards
- Users appear online on the application, even when they do not have Internet connectivity
- Caller hears ringing tone, even when recipient is not online
- Multiple call notifications are received for a single call
- Poor quality or interrupted calls (delays, noise)
- Receiving an international call from a landline on the OTT application

Opt-out analysis

Finally, after we inform the participants about the effects of OTT bypass option, 45% of participants stated that they consider opting out on this option. Among the people who frequently detect bypassed calls and who were previously aware of the OTT bypass option, 39% consider opting out. This shows that, incoming OTT bypass can be reduced by increasing customers' awareness about the effects of the bypass.

6.5.4 Discussion

This survey demonstrates the dependence of users on OTT applications, despite the quality problems they experience. Most people are likely to use OTT applications as a cheaper alternative to traditional communications. However, users rarely pay attention to the details of the terms of use [the14]. The fact that OTT bypass option was known by 50% of people, but it was disabled by only 12% leads to think that this option was not carefully reviewed by most of the people or is not well understood. Therefore, operators can work on increasing customers' awareness on OTT bypass fraud and informing application users about the deactivation option.

6.6 Related Work

Various solutions are proposed to detect and prevent interconnect bypass fraud in the literature.

In [EIS13], a supervised learning algorithm is used to detect simbox fraud. The dataset is gathered from a mobile operator and it includes CDRs from both legitimate subscribers and a fraudulent simbox. The proposed classifier has 98.7% accuracy in identifying the SIM cards that are used in the simbox device. A similar study is conducted in [MZJP], with a much larger dataset and different set of features used for classification. This analysis shows that simboxes are usually static, they connect to a few base stations and they initiate a significant number of calls. These solutions are not applicable to OTT bypass, because (i) there is no single hardware that performs bypass, (ii) detection of OTT application itself is useless, (iii) the bypassed calls may never go over the terminating party's operator and no CDRs will be available for bypassed calls. Audio fingerprinting can be used to determine call provenance [BPA+10]. A more recent study analyzes the degradation in call audio caused by the VoIP-GSM gateways, to detect simboxes [RSB+15]. This technique may be applied to detect outgoing OTT bypass calls on caller's operator or phone, as discussed in Section 6.3.

Identifying OTT traffic in the network is challenging, as the applications are usually obfuscated, communicating over encrypted channels and use proprietary protocols. Various studies try to detect and classify Skype traffic flows using pattern detection, machine learning and protocol identification techniques [BMM+07, KD12, FZS08]. Similar approaches can identify other OTT applications, but only provide a partial solution to the OTT bypass problem.

6.6.1 Commercial solutions

While OTT bypass is a recent form of telecom fraud, there are already commercial offers for detection and blocking of OTT bypass[11]. Public documents do not clearly distinguish between detection and prevention, more information is only available under NDA. Those offers seem to focus on bypass detection using test calls, and then, possibly, use DPI (Deep Packet Inspection) probes to block OTT IP traffic. It is unclear if the DPI probes are able to block the OTT bypass IP traffic only or if all OTT traffic is blocked (which could raise serious network neutrality problems). OTT bypass traffic could be impossible to distinguish from plain OTT traffic, but in practice some differences may be exploited.

6.7 Conclusion

OTT bypass aims at terminating traditional calls on OTT network, while being seamless to both the caller and the callee. In this study, we show that OTT bypass is far from being seamless: communication quality is affected in various ways and users experience problems with it. While we focused on detection and measurement, more research is needed for the prevention of OTT bypass fraud, without disrupting regular OTT communications and violating network neutrality.

Fighting OTT bypass fraud requires a cooperative effort between the different parties that are affected. We have shown that informing users about the consequences of OTT bypass may be the first step to reducing it. Thus, increasing awareness and collaboration between operators, regulators, and users can help to work towards a definitive solution.

In the next chapter we study another common fraud which belongs to the revenue share fraud category.

[11] http://www.revector.com/, http://www.sigos.com/, http://purgefraud.com, http://www.araxxe.com

Chapter 7

IRSF: A Long-standing Problem

In our analysis on revenue share fraud in Section 4.5.4, we distinguish between the 'fraud agreement' and 'traffic generation' schemes. A fraud agreement scheme usually involves multiple parties who collect and share the call revenue and often combined with the traffic generation schemes to generate calls without payment. Value added services (e.g., premium rate services) are often manipulated for revenue share fraud. In this chapter, we focus on **International Revenue Share Fraud (IRSF)**, which abuses international destinations for operating the so-called *International Premium Rate Services (IPRS)*.

In international revenue share fraud, a fraudulent operator, or third party service provider, advertises a range of phone numbers as *International Premium Rate Numbers* (IPRN) in various parts of the world [Int07, ECC06]. This victim number range often belongs to a small, developing country, or to a satellite operator with a high interconnect termination fee. In general, IPRNs are not actually part of a real premium range in the target country.

A fraudster can obtain one of these 'pseudo' international premium rate numbers from various websites[1] that offer revenue in exchange for traffic generation to these numbers [Traa, Tra15a].Those websites provide various cash back methods and tariff plans[2] for the fraudsters who are willing to generate traffic. According to [Yat13], the number of such reseller websites increased by 400% between 2009 and 2013.

Depending on the revenue share mechanism and fraud agreement, the owner of the victim number range may or may not be aware that its numbers are used for IRSF [ECC06, Int07], in particular we can distinguish the three following cases:

[1] e.g., www.mediatel.com, www.premiumtlc.com, www.purple-numbers.com, www.premiumskytel.com

[2] e.g., http://www.globalbilling.com/our-service/tariff-list

- *Terminating operator as part of the scheme:* The owner of the victim number range makes an agreement with a fraudster, and terminates the illegitimate traffic on its own network. The revenue of traffic is shared between the fraudster, who is generating the calls, and the terminating operator. In this case, the legitimate terminating operator is part of the fraud.

- *Transit operator is terminating the calls illegitimately:* A transit operator on the normal route (consider the 'Transit operator 2' in Fig. 2.1) makes an agreement with a fraudster who will generate calls to a victim number range. Then, the fraudulent transit operator short-stops the calls to the victim number range, keeps the termination fee, and shares it with the fraudster. In this case, the owner of the victim number range may not be aware of the fraud scheme performed using its numbers [NF12].

- *Hijacking number range:* Similar to the previous scheme, but this time the transit operator hijacks a number range (e.g., by advertising cheap rates to manipulate the least cost routing mechanisms, Section 4.4.1), which he then short-stops. Therefore, in such a scheme the operator who owns the range is a victim of the revenue share fraud.

For instance, in Figure 7.1, the transit operator T2 hijacks and short-stops the calls to the victim number range, keeps the termination fee, and shares it with the fraudster who generates the calls. In this case, the owner of the number range may only become aware of the fraud because he may become unreachable from some originations [NF12].

7.1 Analyzing IRSF Within The Taxonomy

To demonstrate how our systematization helps in understanding of IRSF, we demonstrate all the relations of mentioned techniques with the manipulated weaknesses and relevant root causes in Figure 7.2. As it can be seen in the picture, IRSF is mainly a result of the legal, regulatory and contractual weaknesses.

One important weakness (leading to 2 techniques) seems to be the lack of due diligence, i.e., operators omit the proper verification of their partners. According to a survey conducted in 2013, lack of due diligence is the second biggest reason for the increase of fraud among wholesale carriers [Sub13].

Another weakness is the fact that the originating operator does not know how its call is routed [Bsw12], i.e., lack of route transparency in Figure 7.2. Even if there are efforts in industry to provide route transparency through collaboration [Ber12], this is not an easy process due to the variety and number of operators and inherent signaling protocol characteristics.

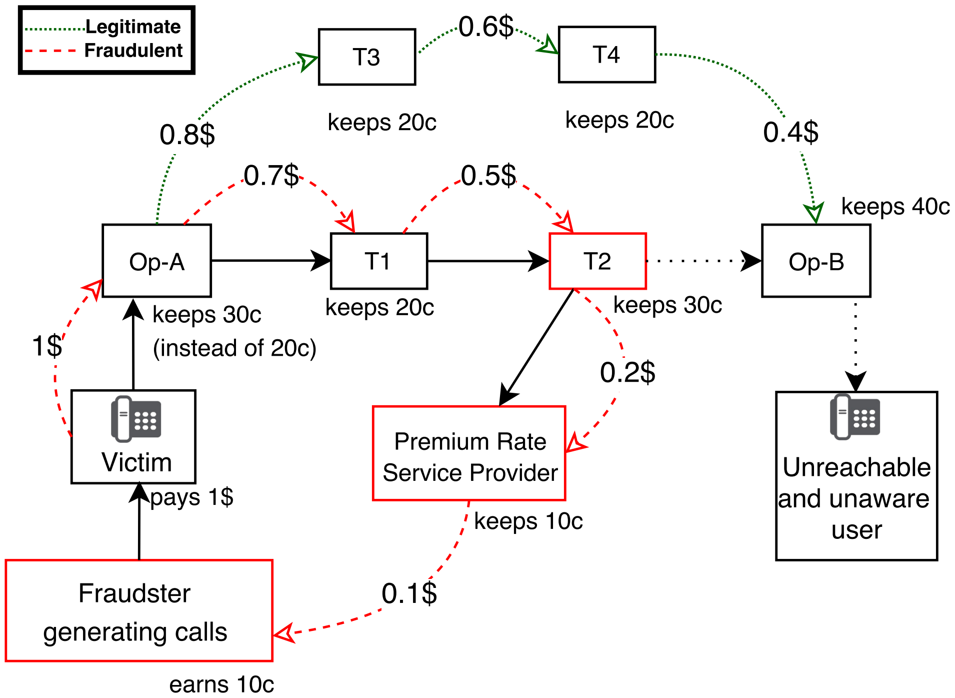


Figure 7.1: Example of IRSF performed through short stopping calls to a hijacked number range.

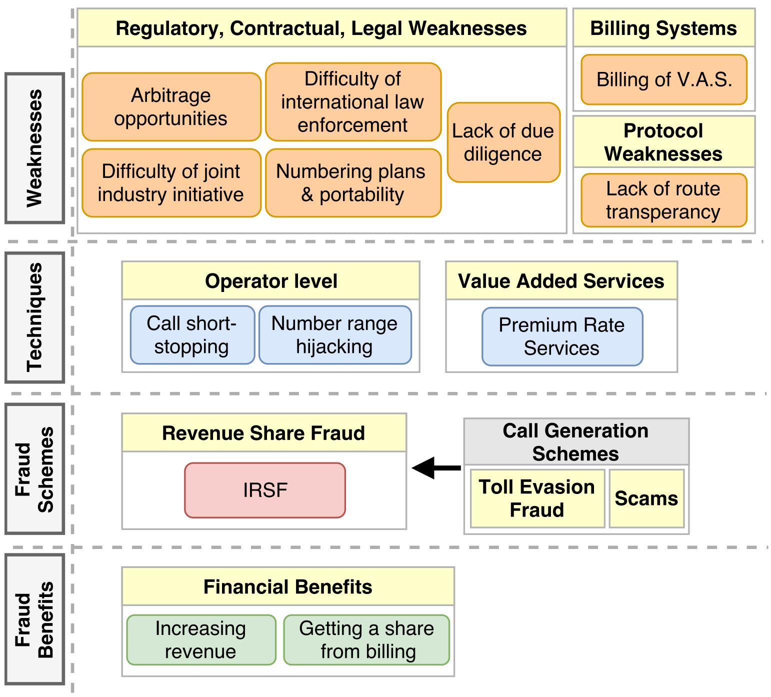


Figure 7.2: Taxonomy for International Revenue Share Fraud (IRSF).

The profitability of IRSF mainly comes from the high interconnect termination rates of victim number ranges. This is a result of the evolution of telecom networks, from a monopolistic ecosystem to a highly competitive and dynamic one. The profit mechanism is hard to track, due to the difficulty of international law enforcement and joint industry collaboration. Moreover, creating regulations for victim number range in the country of origin and country of termination will not be a solution, because (i) victim number ranges frequently change and they look like regular geographical numbers in the country of origin and (ii) calls may not actually reach the country of termination [ECC06]. Due to number portability and number plan misuse issues, originating country may not know if a number is authorized or not [ECC06].

A past example of International Revenue Share Fraud was the hijacking of number ranges belonging to the Pacific Islands, starting in 2005 [Bsw12, Dav12]. The originating operators, who incurred losses due to this fraud, started to block all the calls to the Pacific Islands to avoid fraud and protect their customers [San]. As a result, Pacific Islands were not reachable anymore from certain parts of the world, and their revenue from incoming call traffic significantly dropped. Their reputation was damaged while they were not responsible for the fraud nor they were able to do anything against it [Bsw12].

IRSF was initially performed by using stolen SIM cards in roaming to generate the call traffic [Bsw12, Bsw11]. In an attempt to stop such fraud, NRTRDE (Section 4.3.3) was introduced [Hen11, Gsm07]. However, looking at IRSF within our taxonomy (Figure 7.2), we can see that this only partially mitigates one form of toll evasion, but does not deal with the real causes behind IRSF. Fraudsters can easily shift between the call generation techniques (e.g., mobile malware [Apv10, Fse12]), depending on their profitability and ease to implementation (Section 4.5.4). Although NRTRDE allows to limit the impact of fraud via stolen SIM cards, it is alone not sufficient to address IRSF. In fact, the estimated loss due to IRSF was $10.76 Billion in 2015 [CFC15].

7.2 Exploring IRSF via IPRN providers

In this section, we present our observations on IRSF ecosystem using the data we collected from online IPRN providers. Although it is challenging to identify the exact relationship between the IPRN providers and the telecom operators who collaborate with them, it is possible that these two are in fact the same entity. It is also possible that there is a chain of IPRN resellers, so the IPRN provider is not directly connected to the operator owning/hijacking the number range.

A simple online search for *international premium rate numbers* reveals many websites advertising them, and promising fast, easy money pay-back guarantee for the call traffic generated to these numbers. Some of the websites also provide easy setup for ready-to-use IVRs (such as audio books, weather services) that can be used for the premium rate service.

In addition, such websites often provide web interfaces for testing purposes: they publish a set of 'test numbers', so that the fraudsters can check if the calls they generate are actually routed through the involved fraudulent transit operator (consider the 'Transit operator T2' in Figure 7.1), as routing through another route will not generate revenue. Such test numbers may actually belong to an unallocated or unused number range. Otherwise, if the call does not go through the fraudulent operator (i.e., if a legitimate route is taken instead of the fraudulent route), test calls may ring the phones of genuine users. Such test panels also keep the CDR logs for the calls that are initiated to the test numbers. Fraudsters can view the call records in real time, to check if the current call they are making has reached the premium rate provider. These test calls are usually initiated from a phone system that will soon become a victim of IRSF (e.g., a compromised PBX, a stolen mobile phone).

In a whitepaper from TransNexus, authors contact 121 premium rate number providers and gather information on the advertised number ranges (countries), payout rates and location of the company. [Tra15a] Note that, they do not look into the test numbers, but only analyze the most frequently advertised countries and compare the payout rates. To the best of our knowledge, there is no study that analyzes the test numbers and test call logs available on IPRN providers' websites. Thus, our first aim is to shed more light on this data.

7.2.1 Data Collection

By making online searches for IPRN providers, we identified 45 such websites. For 15 of these websites, we also identified their test portals. It is likely that such websites require login and passwords to avoid being crawled by search engines and phone numbers to be easily found. On the other hand, the login credentials are advertised online (social media or online forums) for fraudsters to easily test those services.

We aimed at collecting data from those test panels, however, for some of them automated data extraction was difficult, or not allowed. Nevertheless, we were able to collect test numbers from 6 of the websites, and collect test call logs from 4 of them. Overall, we collected 157,256 unique IPRN test numbers (from January'16 to April'17) and 91,440 call logs. Moreover, using a commercial numbering plan database, we extracted further information on the test numbers and the source and destination numbers of call logs. Table 7.1 summarizes the type of data we extract from the numbering plan database.

We also extract this data for the source numbers of the test call logs. Note that, some websites obfuscate the source numbers, e.g., by removing the last few digits. However, as long as the country code, national destination code and/or

Table 7.1: Type of data extracted from the numbering plan database.

Data field	Explanation
Country Name	Name of the country that the number range is allocated to.
Country Code (CC)	International country prefix as specified in ITU-T E.164 Recommendation [E1697].
National Destination Code (NDC)	A number prefix that identifies a geographic area or a service. (Some number allocations do not contain NDC, but only SN.)
Subscriber Number (SN)	Initial digits of the subscriber number that is used to distinguish between different areas prefixed by the same NDC. (Some number allocations do not contain SN, but only NDC.)
Subscriber Number Length (SNL)	Valid length (in terms of the number of digits) of the subscriber number. (Some number allocations do no specify the SNL.)
Number type	The type of the international CC-NDC-SN sequence (e.g., Mobile, Fixed, Special Service)
Network and operator name	Name of the operator holding the number range. (Not available for all number allocations.)
Number range validity	- Invalid CC: The number does not match any CC (No such instances in our dataset). - Unallocated number range: The number matches a CC, but does not match any allocated NDC-SN sequence inside the country code. - Valid number range: The number matches with an allocated CC-NDC-SN sequence.
Number length validity	- Valid length: The number has a valid length according to its matching number range. Note that for the unallocated number ranges (i.e., numbers matching only a CC), number length can still be valid. Also, if SNL is not specified for a number, we count it as valid length. - Invalid length: The number has an invalid length according to its matching number range.

Table 7.2: Validity of IPRN test numbers

	Valid number length	Invalid number length	Total
Valid number range	75%	11%	86%
Unallocated number range	3%	11%	14%
Total	78%	22%	100%

subscriber number are available, we can extract data about those numbers using the numbering plan database.

7.2.2 Analyzing the test numbers

Our dataset includes test numbers from 198 countries and 458 operators. This shows that IRSF can target a large variety of countries, with varying call termination costs. Indeed, the whitepaper by TransNexus [Tra15a] analyzes payout rates from 193 countries and mentions that the fraudster's benefit can be as low as $0.00013 per minute. Another observation is that, none of the test numbers belong to the legitimate *Universal International Premium Rate Number* range (+979) specified by the ITU [Int17].

In Table 7.2, we present the validity of the test numbers, classified by the validity of the number range and number length. Number range validity checks if the number belongs to an allocated CC-NDC-SN sequence defined in the numbering plan database[3]. Overall, 75% of the numbers belong to a valid number range and have a valid length according to the numbering plan database we use. The remaining 25% either have an invalid length, or belong to an unallocated number range, or both.

Next, we look at the number type information for these test numbers. Our numbering plan database specifies a number type for each allocated number range (CC-NDC-SN sequence). However, for the 14% of the test numbers which do not match an allocated number range, number type information is not available. As we show in Table A.3, mobile number ranges are the most frequently abused. A possible explanation could be that it is easier to check if a mobile number range is currently in use (assigned to someone) or not, by performing HLR lookups on the SS7 network. Another possible explanation is that the mobile number ranges are often more expensive, and thus allows for a better gain.

In fact, the use of regular international numbers as IRPNs is reported as a misuse by the ITU. In particular, the ITU guideline E.156 [Int07] states that:

[3]Note that, even though we use an up-to-date numbering plan database, our database may not be 100% complete. For example, some recent number range allocations might be missing. However, such commercial databases are the most detailed data available to us, and to most of the operators.

Table 7.3: Types of IPRN test numbers.

Number Type	%
Mobile	56
Fixed	15
Supplementary Services	14
Unallocated number range	14
Satellite	1

> [International country] codes are not designed to be used as charging band indicators for calls that are *terminated short* of the designated country. Furthermore *separate provision* is made within ITU-T Recommendations for designating International Premium Rate and Shared Cost Service.

Figure 7.3 shows a histogram of the number of unique test numbers by country. We can see that, approximately two-thirds of countries have less than 500 advertised test numbers, whereas a few countries have more than 5000.

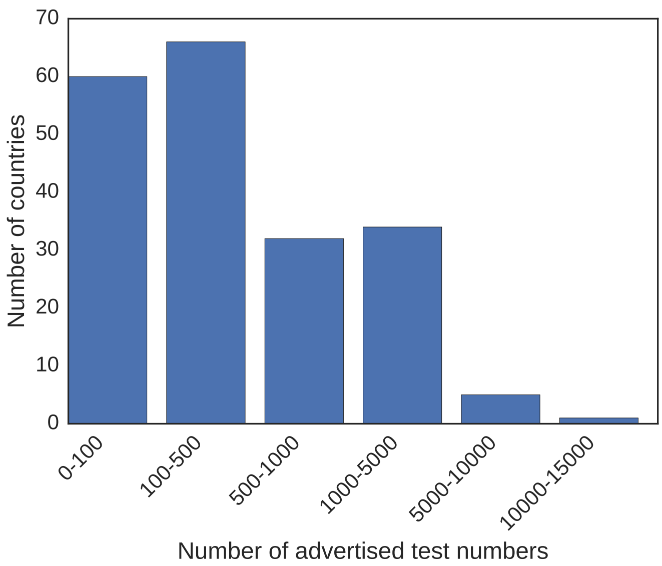


Figure 7.3: Histogram of the number of advertised test numbers by country.

It is likely that the numbers which are advertised as IPRNs are hijacked as part of a whole block of numbers. For example, a block of ten numbers could be represented as +33xxxxxxxxy, where the digits represented by an 'x' are fixed, and digits represented by a 'y' vary inside this range. Similarly a range of hundred numbers can be represented as +33xxxxxxxyy. In our dataset, grouping the numbers in blocks of 10 (ignoring the last 1 digit) results in 98K number ranges, whereas grouping in blocks of 100 results in 73K ranges.

For the top 10 countries with the largest number of advertised test numbers, Figure 7.4 shows the number of collected test numbers, and unique number ranges when the last 1 and 2 digits are ignored. As we can see from this figure, the amount of test numbers are not always an indication of the *dispersion* of abused number ranges in that country. For instance, although Latvia has the highest count of test numbers, these numbers belong to a smaller set of number ranges, especially when compared to the countries like Cuba, Zimbabwe or Guinea.

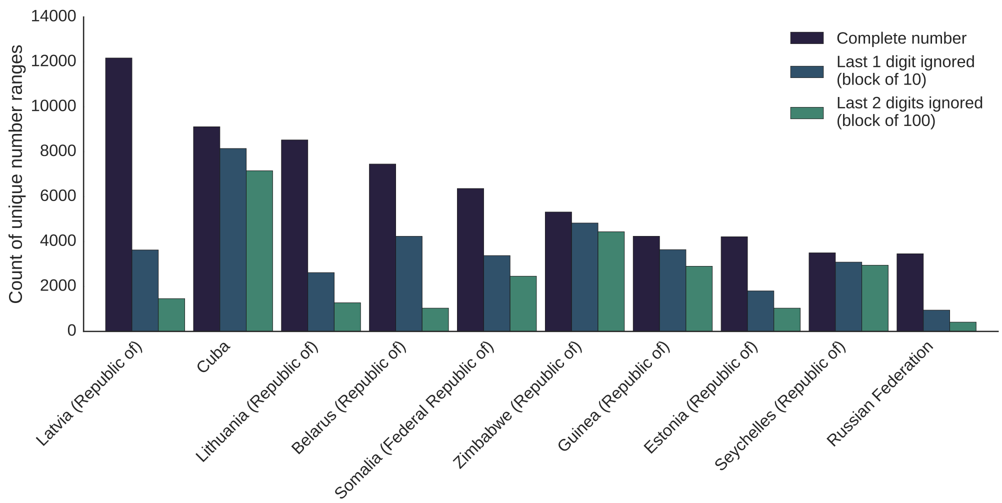


Figure 7.4: Top 10 countries having IPRN numbers advertised.

Rate of operators being involved in IPRNs

For the mobile test numbers, our dataset often contains the name of the mobile network and the operator. Moreover, from the numbering plan database, we can obtain the complete list of mobile network operators in a country. By combining these two sources, for each country, we can compute the ratio of mobile networks whose number ranges were involved in IPRNs. Note that, the operators may or may not be a part of the fraud scheme, but for simplicity, we will call them the victim operators.

We find that, in 61% of countries, all mobile networks are victims of number range hijacking. In 80% of countries, at least half of the mobile networks are hijacked. (These statistics cover 130 countries for which our dataset includes mobile test numbers.) The average number of victim operators per country is 2. This observation is also in line with the data we present in Table 7.4, where we group the countries according to the total number of mobile networks per country.

Table 7.4: Ratio of victim operators per group of country. (Groups are based on the total number of mobile network operators per country.)

	Number of such countries in dataset	Ratio of victim operators (avg.)
Num. of operators <3	71	92%
3 <= Num. of operators <6	40	76%
Num. of operators >=6	19	32%

A closer look into the certain countries reveals that the fraudsters use different strategies to select the IPRNs different countries. For instance in Latvia, 1406 of the mobile test numbers include number ranges from all of the 9 operators. Moreover, 99% of the numbers have a valid length. On the other hand, in Cuba, all 3816 mobile test numbers belong to the number range of a single operator, but 98% of the numbers have an invalid length (which is 1 digit less than the valid length). In this case, as the fraudulent operator is hijacking the invalid-length number ranges, he does not need to check if the numbers are assigned to genuine users or not.

In conclusion, our analysis shows that there is a large variety of number ranges that can potentially be used for IRSF: Both fixed and mobile numbers, invalid length numbers, unallocated number ranges, and number ranges of multiple operators can be abused as IPRNs.

7.2.3 Analyzing the test call logs

The 91,440 test call logs we collect contain calls from 245 origination countries to 129 destination countries. Among these calls, 6445 of them have invalid or anonymized caller IDs. The rest of the calls include 41,891 unique originating numbers. Table 7.5 presents types of originating and destination numbers. A large number of test calls seem to be originated from mobile numbers, which possibly belong to stolen or abused SIM cards. Note that, we cannot completely trust the caller ID, as it can be spoofed by the fraudster (e.g., from a PABX) or during routing by an operator. On the other hand, calls that originate from mobile networks are less likely to be spoofed, as the caller ID cannot be easily modified by the caller (unlike the calls from a PABX with a SIP trunk), and the SIM cards are authenticated.

We also observe that many of the test calls were repeated more than once. To analyze the actual number of fraud cases per country, we remove the recurring calls and only consider the unique source and destination phone number pairs. This leaves us with 53,386 call logs. In Figure 7.5, we present the histogram for the number of unique test calls by the number of countries. From most of the countries, less than unique 100 test calls were originated. However, for a few

Table 7.5: Types of originating and destination phone numbers observed in test calls.

Number Type	Originating Numbers	Destination Numbers
Mobile	71%	54.8%
Fixed	17%	32.9%
Supplementary Services	4%	4.7%
Unallocated number range	8%	7.5%
Satellite	-	0.1%

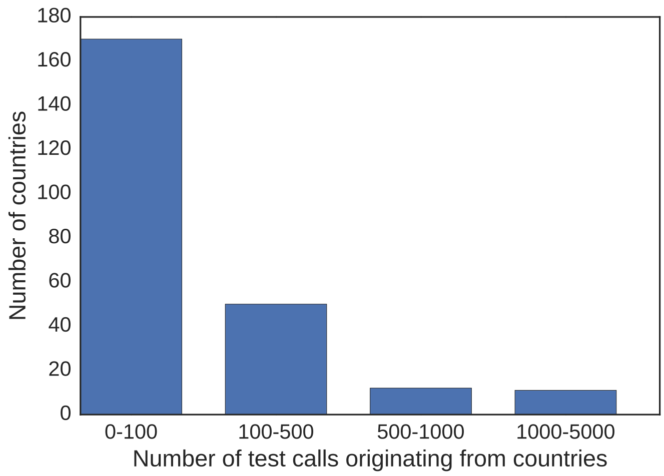


Figure 7.5: Histogram of the number of test calls by country.

countries, more than 1000 originating numbers are observed. In Figure 7.6, we take a more closer look into those countries which are frequent IRSF originations. An interesting point is that, for most of these countries, our dataset includes very few (or even no) test numbers. In particular, the US and India each have 1, Nigeria has 161, Saudi Arabia has 38, Sudan has 41, Germany has 0 test numbers advertised. This might show that the fraudsters are likely to manipulate separate sets of countries for originating and terminating the fraudulent calls.

On the other hand, the most frequent IRSF destinations observed from the test calls (Figure 7.7) are in line with the most frequently advertised countries for test numbers (Figure 7.4).

7.3 Leveraging the dataset for IRSF detection

A naive approach to prevent IRSF is to block all the calls to frequent IRSF destinations, or number ranges. However, this type of extensive interference may lead to unreachability of genuine users in the destination country, and may

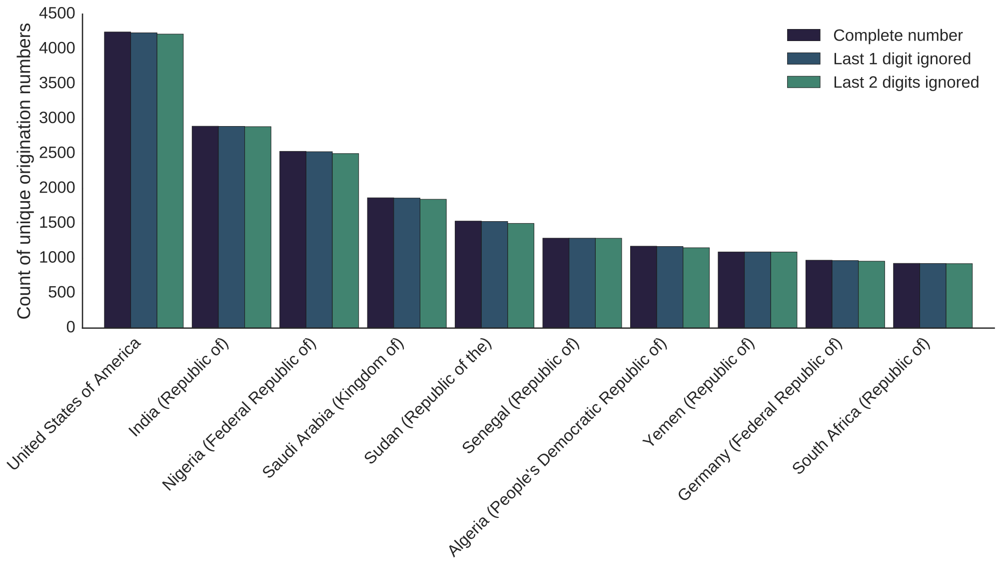


Figure 7.6: Top 10 countries IRSF calls originate from.

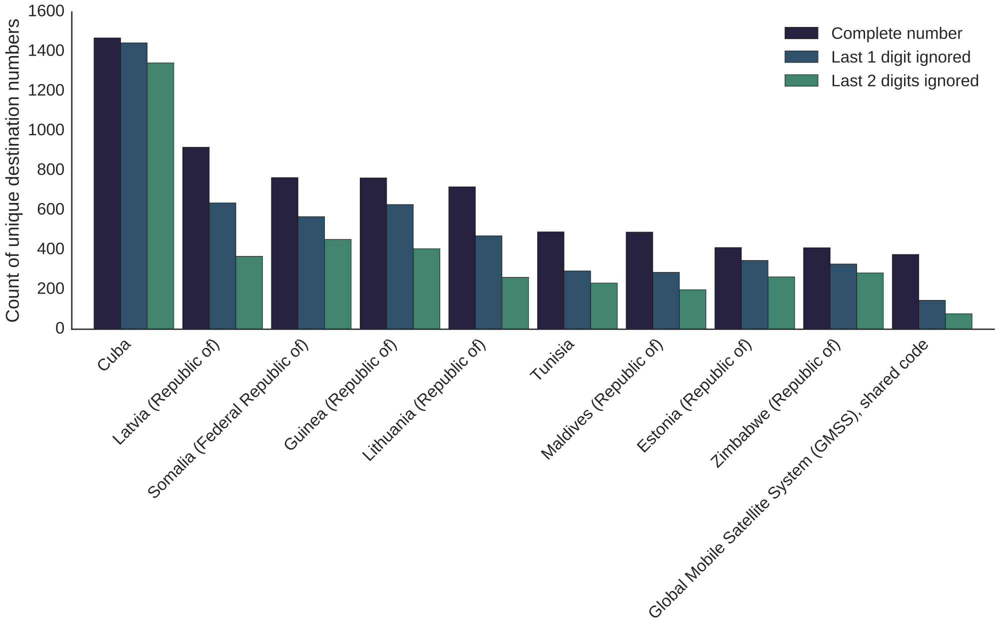


Figure 7.7: Top 10 IRSF destinations in the test call logs.

result in a lot of customer complaints. Moreover, as we show in the previous section, IPRNs may belong to a large variety of countries and operators, which would make it difficult to block all suspicious number ranges.

Another approach is to use phone number blacklists or hotlists that keep a list of previously identified IPRNs. Organizations like GSMA and CFCA share such lists with their members [cfc17, Wil]. However, our analysis show that the phone number space that can be abused is quite large: Fraudsters can easily circulate or renew the IPRNs, which will make the lists outdated.

On the other hand, leveraging the test numbers as an early detection mechanism for IRSF might be a more effective way. Indeed, a few commercial databases of test numbers are being advertised as early detectors of IRSF [ccm17, fra16]. However, this approach only takes advantage of the individual test numbers, and its efficiency relies on the test number list being up-to-date: When the fraudsters start to abuse a different number range, or a new IPRN provider enters into the market, the test number database should be immediately updated.

As an improvement on these existing methods, in Table 7.6, we propose several features that can be used to detect potential IRSF calls. These features aim to leverage the data we collected from IPRN providers, by linking this data to the source and destination numbers of a call.

Our features do not rely on any completed CDRs, so they can be used to detect IRSF or to identify suspicious calls, before the calls go through. Yet, these features can also be combined with behavioral patterns (such as multiple simultaneous calls, calls on non-business hours, long duration calls, no call history related to the destination number) that can be extracted from CDRs after the calls are completed. As an additional feature, for mobile destination numbers, real time HLR lookups can be used to check if the number is assigned to a real user, and currently in use.

Our next aim would be to validate the effectiveness of these features by incorporating them into a machine learning model. This would allow us to see the significance of the features, and optimize them. However, this would require a real-world, pre-labeled CDR dataset that we can use as a ground truth. On the other hand, telecom operators treat CDRs as sensitive data, which makes it difficult to obtain such a dataset. Anonymizing the dataset would not solve this problem, as our features depend on the analysis of the actual source and destination numbers. Thus, we leave the validation of this approach as a future work.

Table 7.6: Features that can be used for detecting IRSF calls.

Feature	Description
Destination number: Proximity to test IPRNs	This feature computes the proximity of the destination number to one of the known test IPRNs. For instance, the number can match an exact test IPRN, or can be in the same number range, with a few digits of difference. Higher proximity makes the call more suspicious.
Destination number: Validity of number range	This feature checks if the destination number belongs to an allocated number range (CC-NDC-SN sequence).
Destination number: Validity of number length	This feature checks if the destination number has a valid length.
Destination country: Likelihood of being IRSF destination	This feature relates to the ranking of the destination country among the countries advertised as IRSF destinations. The number of test IPRNs and test calls which the country appears in can be used as metrics. For instance, on a voice call graph of the test calls, this metric would be the number of incoming edges to this country.
Destination country: Dispersion of the test numbers	This feature aims to take advantage of the fact that, in some countries IPRNs may belong to a limited set of number ranges, or a limited set of operators. For example, If the test numbers in our dataset are widely dispersed over the number range allocation of the country, we would have less confidence in labeling a phone number as suspicious if it is close to a known test number. In other words, this feature computes a 'spreading factor' based on how spread the test numbers are in the country's numbering plan.
Destination country: Pay-out rate	Pay-out rate (i.e., the amount of cash back) advertised by the IPRN providers for this particular destination.
Destination operator: Likelihood of being IRSF destination	This feature computes the ratio of operator's test numbers among all the test numbers in that country. If this ratio is small, this operator would be less suspicious.
Originating country: Likelihood of being IRSF origination	This feature relates to the ranking of the originating country among the IRSF origination countries observed in the test call logs. (Note that the incoming caller IDs might be spoofed.)
Originating operator: Likelihood of being IRSF origination	This feature relates to the ranking of the originating operator among the operators in this country observed in the test call logs.(Note that the incoming caller IDs might be spoofed.)
Previous successful test calls between countries/operators	The test call logs can be used to check previous successful test calls between countries, which is an indication that IRSF calls can occur on these routes.
Price difference btw. standard and premium routes	The difference between the average price of a premium (high quality) route and a standard (often low quality) route from the originating/transiting country/operator to the destination country/operator.

Part III

Examining Fraud from Consumers' Perspective

In this part we focus on voice spam, one of the most prevalent types of telephony fraud from consumers' perspective. We first analyze voice spam within our taxonomy, and then describe the previous work on honeypot based voice spam analysis. Next, we present several findings from a small telephony honeypot that we deployed to observe voice spam in Europe. In the final chapter, we analyze the public data from a high interaction telephony honeypot, which is enabled by a chatbot. We present several measurements on the effectiveness of this chatbot, and try to understand why it is effective, by analyzing its conversations with the phone spammers.

Chapter 8

Voice Spam and Honeypots

Voice spam includes all types of unwanted and abusive phone calls. Such unwanted calls have been a major burden on the users of telephony networks. They are often not legitimate (e.g., generated without the consent of the callee) and can be very disturbing for users as they require immediate attention.

The interconnection of IP and telephony networks facilitates voice spam, as it significantly reduces the cost of calls. Voice spam can be performed in many ways, but a common way is to use an auto-dialer equipment to generate vast number of calls to a given (or randomly chosen) list of phone numbers. Once a call is answered, either a pre-recorded message is played (which is called a *robocall*), or the callee is assigned to a live human agent for further interaction. More intelligent auto-dialer equipment (e.g., predictive dialers) can increase efficiency of call-agent scheduling and also check if the call is answered by a person or an answering machine (such as voicemail) [pre16]. The spam campaigns are often performed by call centers that may belong to legitimate companies, as well as illegitimate organizations.

Fighting voice spam is challenging for various reasons. Fraudsters may spoof or block the caller identification (caller ID) information, which makes their identification more difficult. Overseas fraudsters make law enforcement even harder. Moreover, the operators are not always motivated to stop such spam calls, as some of them may earn revenue thanks to these calls. In addition, users' lack of fraud awareness makes it easier for the fraudsters to perform social engineering attacks over the telephony medium. In fact, in 2015, 75% of generic fraud-related complaints reported telephone as the initial method of contact, which raised from 20% in 2010 [Fed15b]. We summarize the weaknesses and techniques related to voice spam in Figure 8.1. Note that, a spam call might have various purposes: to obtain a financial benefit (e.g., selling a product or scams), to collect personal information about the user for future calls (e.g., targeted marketing), or to influence/learn the users' opinion on a subject (e.g., political calls).

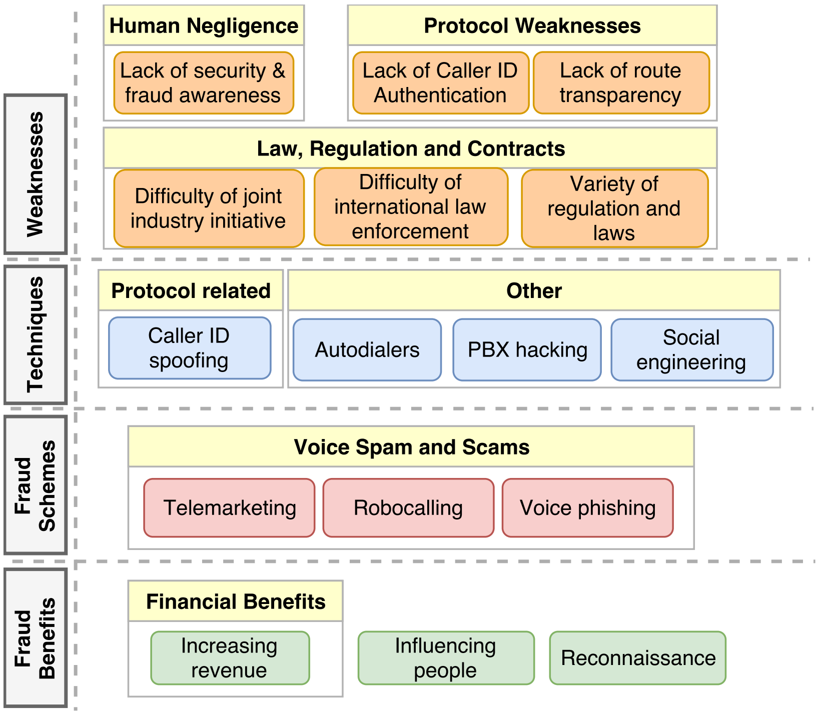


Figure 8.1: Voice spam in our taxonomy.

Although many efforts have been made to prevent voice spam, these efforts are not always effective. For instance, in many countries regulators suggest consumers to register the *Do Not Call (DNC) lists* to reduce the number of unwanted calls. However, efficiency of these lists are questionable, as the illegitimate parties do not follow these lists anyway. For instance, the do not call registry in the USA has received over 5 million complaints about such unwanted or fraudulent calls in 2016 [Fed16a]. Moreover, a recent survey shows that 82% of participants did not notice a significant decrease in number of calls after registering to the national do not call list [BC17]. In fact, some forms of calls (such as calls from charities and political organizations) may be exempt from abiding by the do not call lists [Fed16b]. In addition, suing telemarketers can be time consuming and costly [sui07]. Even though important progress has been made on identifying and blocking robocalls (such as mobile applications [nom17, Bur16], call audio analysis technologies [pin17], government efforts [Fed15c, Fed15a]), voice spam remains an open problem.

8.1 Honeypot Based Voice Spam Analysis

As we discussed in Chapter 5, a telephony honeypot with a set of phone numbers can be used to receive spam calls with an automated system (e.g., a VoIP

PABX such as Asterisk). As opposed to the spam call complaints reported by consumers, telephony honeypots provide complete data with high accuracy on the time and metadata of the call [GSBA15]. In this section, we will summarize the related work on the use of honeypots for voice spam. Then, next section will talk about our observations from a small, no interaction honeypot that we deployed in Europe.

Gupta et al. uses a no interaction honeypot located in the US, which received 1.3 million calls from 250K source numbers to 39K honeypot numbers over 7 weeks [GSBA15]. The calls are not answered, but directly terminated with a busy tone. As the honeypot uses 'dirty' numbers, seeding of the numbers is not required. By correlating the source numbers with other complaint datasets, authors identify and analyze calling patterns of different spam types. They also find that the number blocks that have been allocated for a longer duration receive more spam calls compared to the newly allocated blocks.

In [MKDP16], authors analyze data from a low interaction honeypot that answer robocalls with silence, and record the incoming audio. The recordings are then transcribed and the transcriptions are clustered to find out the type of the spam call. Moreover, by using certain audio features [BPA+10], authors shows that it is possible to identify the infrastructure and the distinct actors behind spam campaigns. It was found that 51% of robocalls were initiated from 38 different infrastructures [Mar16].

Another work [BGG+16] uses a mobile phone honeypot that received hundreds of fraudulent SMS and phone calls over 7 months. The honeypot is located in China and uses 8 mobile phone numbers from various operators. The numbers are seeded in different ways (via publishing them on social networks, using them with the phones that installed mobile malware known to leak data, and calling phone numbers that are known to be abusive) to compare the effiency of seeding techniques. The source numbers are again correlated with a complaint dataset, and various types of abusive calls and SMS are shown. This work can also be considered as a first attempt to a high interaction honeypot, as the calls are answered with a set of pre-recorded messages (e.g., 'Hello?', 'Do you hear me?') that are played to engage the caller. Later the call recordings are transcribed to check if the call is fraudulent or not. However, the paper does not mention any details about how fraudsters interact with these pre-recorded messages, and how efficient the approach was.

8.2 Observing Europe's voice spam ecosystem

In this section, we explain our initial attempt to observe the voice spam ecosystem in Europe. For this purpose, we deploy a no interaction honeypot with 800 phone numbers from 8 European countries. The phone numbers were provided by Voxbone[1] via a SIP trunk. Each country has a consecutive range of 100 numbers, which are all fixed, geographical phone numbers. In our dialplan, incoming calls from this trunk are first ringed for 12 seconds, and then a busy signal is emitted for 10 seconds, before the call is terminated. Note that, all the honeypot numbers were new, i.e., they were not assigned to any other user previously. We did not advertise (seed) the phone numbers in any way. However, for 7 of the 8 countries (except Luxembourg), we registered 10 randomly chosen phone numbers to the Do Not Call (DNC) lists of the corresponding countries, to see if the DNC lists are abused by the fraudsters.

From January 2015 to July 2017, our honeypot received 2200 calls to 800 numbers. However, some of these calls were misdials, as observed in [GSBA15, BGG+16]. We assume that the calls generated from a single source to a single destination on the same day, with a few minutes of time interval in between, are likely to be misdials. Eliminating these calls leaves us with 1493 calls. 49 calls had anonymized caller IDs. As seen in Table 8.1, our honeypot was not able to collect a large number of spam calls, probably because the honeypot numbers have never been used before. However, we still observe two interesting cases as follows.

Table 8.1: Number of calls received by the honeypot per country.

Country	# of calls received
Germany	3
Italy	10
Netherlands	17
France	30
Luxembourg	39
Belgium	84
United Kingdom	205
Spain	1105

8.2.1 Ping calls in Spain

The calls we received from Spain were initiated from 116 distinct source numbers to 94 honeypot numbers. However, most of the source numbers (81) actually generated less than 10 calls. On the other hand, 2 phone numbers were responsible from the 20% of the calls. These are fixed numbers from Balearic Islands and belong to the same number range except the last 2 digits. Moreover, our honeypot has been observing calling activity from these numbers for more than two years (since June 2015).

The voice call graph of these two source numbers (Figure 8.2) shows that most of their target destinations were in common. Note that, we did not detect any

[1] www.voxbone.com

sequential pattern on the destination numbers, and we find that some honeypot numbers are called multiple times, but with a large time interval in between the calls (from 6 months to 2 years).

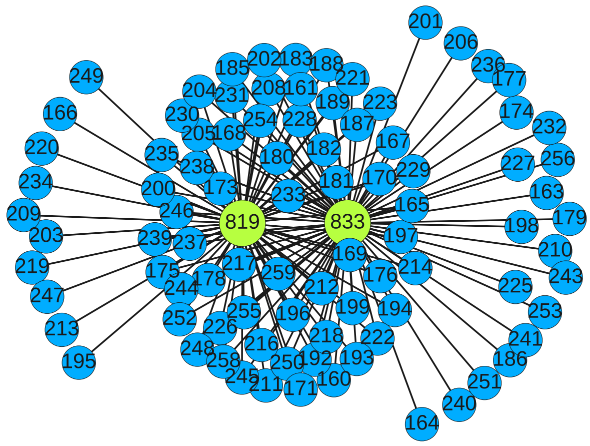


Figure 8.2: Voice call graph of a spam campaign observed in Spain. The two green nodes represent the source numbers, blue nodes represent the honeypot numbers. Node labels represent the last 3 digits of the corresponding phone number.

As another interesting finding, all the calls were terminated either on the 6th or the 7th second of the 12-second ringing period. By looking up the numbers on the online complaint websites[2], we found many fraud complaints, which indeed mention one-ring calls and silent calls.

Due to the fact that the originating numbers are domestic, and not in the range of premium rate, these calls are not likely to aim for revenue share fraud. However, they might be calls that aim to scan number ranges and identify the phone numbers that are currently in use, and vice versa. This information can, for example, be used to create target lists for spam calls, or to determine which domestic number ranges can be abused for IRSF.

8.2.2 Effect of Do Not Call list in the UK

In the UK, we registered 10 randomly chosen honeypot numbers to the Do Not Call list (named *Telephone Preference Service*[3]) on January 16th, 2015. Approximately 2,5 years later (on July 7, 2017), we observed sequential calls to

[2] such as http://stopting.es, www.responderono.es, www.guiatelefonicainversa.es
[3] http://www.tpsonline.org.uk

these numbers, in the same order that we registered the numbers, in a half an hour period. Note that, except single calls to 2 of the phone numbers, these numbers did not receive any calls previously. Moreover, during this half-hour period, there was no other call to the rest of the 90 numbers.

As shown in Table 8.2, all the calls were ringed for maximum 2 seconds. Similar to the previous case, the calls are likely to aim at finding out if the phone numbers are assigned to any user. Again, we found several online complaints[4] about these originating numbers, reporting missed calls and silent calls, especially in the early morning hours. In fact, some users were no able to make sense of these calls, for instance, one user states the following[5]:

> "Has called a few times at 5am, but why, I'm not going to buy anything at that time, is it a faked Caller ID who hasn't bothered to check the actual time in the UK?"

Such ping calls are very difficult evade, because the fraudsters can generate large number of calls using autodialers, without any call cost. Moreover, they can spoof the caller ID to avoid blocking.

Table 8.2: Sequential calls received by the honeypot numbers that were registered to the Do Not Call list.

Date	Caller ID	Honeypot number	Ring duration	# of previous calls
07/07/2017 07:19:35	44124XX29132	441138680563	2	-
07/07/2017 07:23:02	44162XX70017	441138680576	0	1 (01/2017)
07/07/2017 07:26:26	44190XX90242	441138680581	0	-
07/07/2017 07:29:59	44161XX80876	441138680589	2	-
07/07/2017 07:33:13	44120XX65019	441138680601	1	1 (08/2016)
07/07/2017 07:36:43	44208XX91314	441138680613	1	-
07/07/2017 07:40:29	44208XX91314	441138680623	0	-
07/07/2017 07:43:58	44208XX91314	441138680637	0	-
07/07/2017 07:47:10	44124XX29132	441138680645	1	-
07/07/2017 07:50:30	44124XX29132	441138680654	1	-

Although our DNC list registrations only yield interesting results in the UK, it still provides a first, anectodal evidence for the abuse of such lists, likely for fraud. In fact, from a fraudster's point of view DNC list numbers are interesting, as users may not expect to be a victim of fraud, or may be less accustomed to it, and they may have a higher chance to call back. We believe that repeating this experiment on a larger scale might be an interesting future work.

[4] From websites such as www.tellows.co.uk, http://findwhocallsyou.com, www.shouldianswer.co.uk.

[5] Comment collected from digcaller.co.uk.

8.3 High interaction honeypots

As opposed to low interaction honeypots, deploying a high interaction honeypot would allow to collect more information such as fraudsters' strategies, actions, identity and the real purpose of the spam call. However, this requires to engage in an automated, real-time audio conversation with the spammer. Moreover, the conversation should be realistic, so that the spammer will not get suspicious and hang up the call. Another difficulty for setting up a high interaction honeypot is that in many countries recording the call requires both caller and callee agreement, otherwise the recording could be considered as illegal wiretapping. Asking for permission would however change the caller's behavior, raise suspicion, and bias the study.

In Chapter 9, we will study a high interaction telephony honeypot that overcomes these challenges by employing a chatbot to interact with spammers, and doing this in a location where it is legal to record the calls without caller's authorization. We will analyze the effectiveness of this honeypot, and discuss the large scale use of such bots against spam.

Chapter 9

Use of Chatbots Against Voice Spam: A Case Study on '*L*enny'

A spam call is usually initiated with an auto-dialer, and then transferred to a live call center agent, or an Interactive Voice Response (IVR) system that interacts with the callee via pre-recorded messages [TDZA16a]. In case of a "robocall", a pre-recorded audio message is played to the callee. As a second step, the callee might be requested to call back the spammers' phone number, or connect with a human agent after a confirming action, e.g., by pressing a button.

While the robocalls can be very cheap and very easily disseminated, employing call center agents is often a more costly operation. A 1-minute robocall costs around 4 cents per dial[1], whereas servicing a customer at a call center can cost around 50 cents to $1 per minute [Val12, cal17a]. It is also common to utilize overseas call centers (e.g., call centers in India or Philippines [Inf14]), to take advantage of cheap labor. Such call centers still cost around 15-20 cents per minute for outgoing calls [cal17b]. On the other hand, interaction with a live human agent is likely to make the spam campaigns more efficient. In fact, among the 5 million complaints received by the FTC in the US, 64% were recorded calls (robocalls) [Fed16a], which means the remaining 36% involved human agents. Usually, the number of call center agents are much lower than the number of calls that can be generated by the auto-dialer equipments. As a result, human agents may not have time to answer all the connected calls. Thus, human agents become a limiting factor for fraudsters, whereas the actual cost of generating the call is nearly negligible.

As the ongoing efforts to prevent unsolicited calls come short of solving the problem, individuals have been developing their own methods to fight these

[1] http://www.robocent.com/, http://www.robodial.org/instantpricequote/

calls. Many videos where the people are teasing with or scamming back telemarketers and other phone scammers can be found online [Pra]. Moreover, there exists various recommendations on how to annoy telemarketers and waste their time [no_a, Gal17]. Due to the cost of human labor, wasting time of one telemarketer leads to a waste of money for the call center, and also saves other people from falling victims to voice spam. For telemarketers, time is money, because each new call they make increases their chance to reach another customer and make profit [Jos11, no_b]. However, these individual efforts to stall telemarketers require the callee to waste his time talking to the telemarketer as well.

In this chapter, we study an automated way of wasting fraudsters' time and resources (while, at the same time, annoying them). This method employs a chatbot which will act like a legitimate callee and interact with the fraudsters. $Lenny$, to the best of our knowledge, was the first chatbot to become popular for this purpose. It consists of a set of pre-recorded sound files that are played in a specific order to engage in a conversation with a phone spammer.

Although there is no indisputable evidence of this chatbot's origins, some information can be found online. Lenny has been reported to be a recording performed for a specific company who wanted to answer telemarketing calls politely [Red16]. Later, the recordings were modified to suit residential calls [Bos15]. Moreover, Lenny was inspired from $AstyCrapper$ [ast08], which was an earlier version of such chatbots, but has not found extensive use. Note that Lenny was not recorded by a professional actor; the voice and age patterns were acted (faked) by a person using his own local accent [Red16].

Lenny is interesting to study, because it is incredibly realistic and is able to trick many people even without any artificial intelligence or speech recognition mechanism involved. We claim that this success relies on the conversational quality of the recordings. In this study, we will examine how Lenny is able to stall fraudsters (even up to 1 hour [one16]) and discuss the effectiveness of such chatbots to fight voice spam.

Currently, Lenny is provided as a free and open service that allows people to transfer their incoming unwanted calls, using a $warm\ transfer$ or call forwarding.

An important aspect of such chatbots is the usability of the call transfer methods from phone user's perspective (we briefly discuss this in Section 9.5). However, in this study, we instead treat the chatbot as a human computer interface and we study the usability of the chatbot in the specific, sequential context of spam calls. Because Lenny's turns fit very well into the conversation, despite being scripted recordings, Lenny has good "usability" as a conversation partner in spam calls. The better its usability, the longer time the caller will waste on the phone, consequently damaging the spam campaign and protecting real users.

We rely our analysis on the call recordings that are available at the public Youtube channel [len17]. We select 200 videos from this channel (corresponding to 2,000 minutes of calls) and examine the transcriptions of these calls. We also analyze more than 19,000 call data records (including call date, time and duration) collected by this phone system in the last 1.5 years. Our aim is to shed light on various types of spam calls, different strategies employed by spammers, and also to analyze the conversational properties of these calls to better understand the effect and efficiency of this chatbot.

In summary, in this chapter, we make the following contributions:

- We make the first study analyzing a chatbot, which also acts like a high interaction honeypot, to fight voice spam. We observe the different types of spam calls, and evaluate spammers' strategies and interactions with this chatbot.
- We explore the reasons behind the success of this chatbot from an applied conversation analysis perspective.
- Finally, we discuss the challenges in the widespread use of such chatbots and a series of research and design issues.

9.1 Related work

In this section we review related work, first on voice spam, then on chatbots and finally on conversation analysis.

9.1.1 Voice Spam

In addition to the honeypot based studies mentioned in the previous chapter, there are many solutions proposed for voice spam in the academic literature. Tu et al. [TDZA16a] surveys the existing unwanted call prevention techniques and presents an evaluation criteria to assess these. In fact [TDZA16a] shows that none of the techniques are perfect. While the use of chatbots may not be considered as a real spam prevention method, it might be useful to reduce unwanted calls, as it would damage the financial benefits of spammers (Chapter 4).

Miramirkhani et al. [MSN17] takes a different approach and tries to gain a better understanding of technical support scams. Authors identify websites advertising scam phone numbers and call 60 of these numbers to interact with the real scammers. They also analyze scammer demeanor (finding that they are usually polite) and the social engineering techniques used by scammers (such as showing various warnings to convince a computer is compromised). Another approach studied in [Tab16] is to look at the linguistic properties of IRS scam calls posted online. This study aims to understand how forensic linguistics may help in the identification of social engineering attempts.

9.1.2 Chatbots

Bots have been built as personas (an artificial but realistic identity) who produce a recognizable type of conduct from the members of such categories (for ex. an "old guy"). Since ELIZA [Wei66], chat bots associate a recognizable identity with a specific ability to produce some linguistic contribution (for instance, turns at talk).

Today, advanced artificial intelligence techniques enable intelligent chatbots, used as personal assistants on smartphones (e.g., Cortana, Siri), application communications (e.g., banking [Arm17]), even as a friend [Wan16]. There are industry efforts to build better and more intelligent chatbots [Lev16, cha]. While such advanced chatbots are generally not publicly available, they often have a synthetic voice which is distinguishable from a real human voice. However, it can be expected that such chatbots will keep on improving.

Lenny is not the only chatbot used to fight telemarketers. JollyRoger [Jol17] is another similar, but paid, service that hosts multiple chatbots with different personas. However, to the best of our knowledge, Lenny was the first freely available chatbot with a significantly large and public dataset.

9.1.3 Background on Conversation Analysis

Conversation Analysis (CA) is a sociological perspective that aims to study the organization of natural talk in an interactional order [Gar67]. It focuses on the analysis of recorded conversations, and tries to understand how the participants of a conversation deal with the organizational issues and orient themselves to the conversational exchange. Some of the main organizational problems that may arise in a conversation can be listed as follows.

The first issue is the management of speaking and hearing between the participants of a conversation. Sacks et al. [SSJ74] proposes the *turn-taking* model, which is used to study the methods used for minimizing gaps and overlaps during the talk exchange. The second model is the *trouble management*, which aims to explain how speakers repair any trouble in hearing, understanding, or speaking [SJS77].

Another issue is the *sequential organization of actions in talk exchanges*, which we will frequently refer to along this study. Conversationalists assemble their turns at talk in sequences of actions, which allows them to "accomplish and coordinate an interactional activity" [Maz06]. Some of the common type of sequences (also called adjacency pairs [Sch68, SS73] are:

- Question → answer
- Greetings exchange

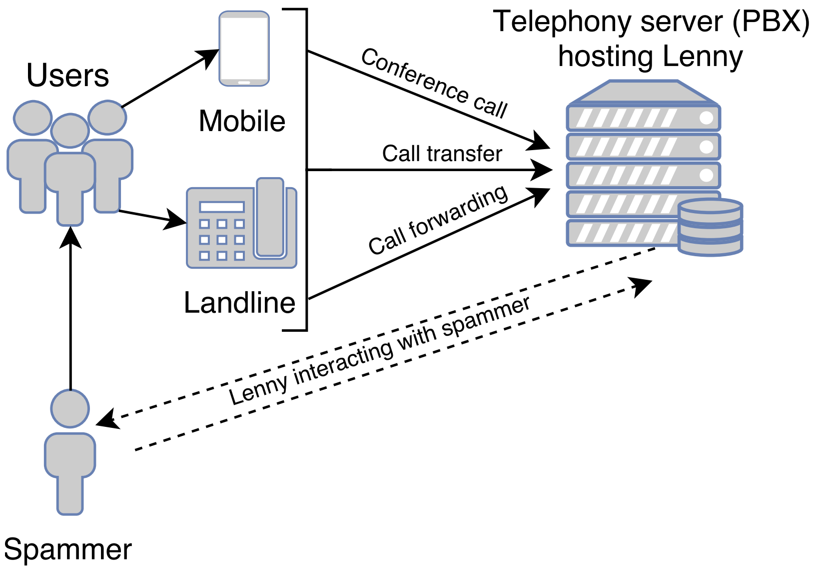


Figure 9.1: Deployment setup and usage.

- Offers → acceptance/rejection
- Request → acceptance/rejection

These sequences consist of two utterances, a first part and a second part (the order), produced by different speakers with an adjacent (contiguous) positioning [SS73]. Note that the form and content of the second part depends on the type of the first part. Once a first pair part is uttered, the other participant should produce a relevant second pair part. In other words, adjacency pairs point to the ways in which we order turns at talk as pairs.

The fourth model aims at *clarifying how speakers use membership categories during talk exchanges*. [Sac72] and [Sac92] discussed how conversationalists use categories to recognize, identify, describe or infer about people. For example, identities, such as "elderly", can be displayed through the sequential organization of talk, without being explicitly referred to.

9.2 Data Collection & Methodology

9.2.1 Lenny's Interactive Voice Response (IVR) System

Lenny's voice recordings are publicly available, and our study focuses on one particular deployment which made audio recordings available and attracted a significant amount of interest [Tao15, Bol16].

In Lenny's particular implementation (Figure 9.1), incoming phone calls are answered and the set of audio recordings are played one after another, to interact with the caller. There is no speech recognition or artificial intelligence to select or modify Lenny's answers, the same set of prompts is always used in the same order. This is controlled by an Interactive Voice Response (IVR) script which allows simple scripting and detection of silences.

The script starts with a simple "Hello, this is Lenny." and will wait for the caller to take his turn. If he does not respond within 7 seconds, the server switches to a set of "Hello?" playbacks until the caller takes his turn. However, if the caller speaks, the IVR script waits until he finishes his turn. The script detects the end of the caller's turn by detecting a 1.55 second long silence period, at this point it will play the next recording. When the 16 distinct turns that are available have been played, it returns to the 5th turn (the 4 first prompts are supposed to be introductory adjacency pairs) and continues playing those 12 turns sequentially, forever.

The PBX server hosting Lenny is reachable both via a SIP URI and via a landline number. Some common methods to transfer a call to Lenny are (Figure 9.1):

- When a phone user identifies a spam call, he asks the spammer to hold on for a second, then either transfers the call to the phone number of the PBX server or creates a 3-way conference call, and lets Lenny interact with the spammer.[2] In this case, the caller ID logged on the PBX server will belong to the phone user.

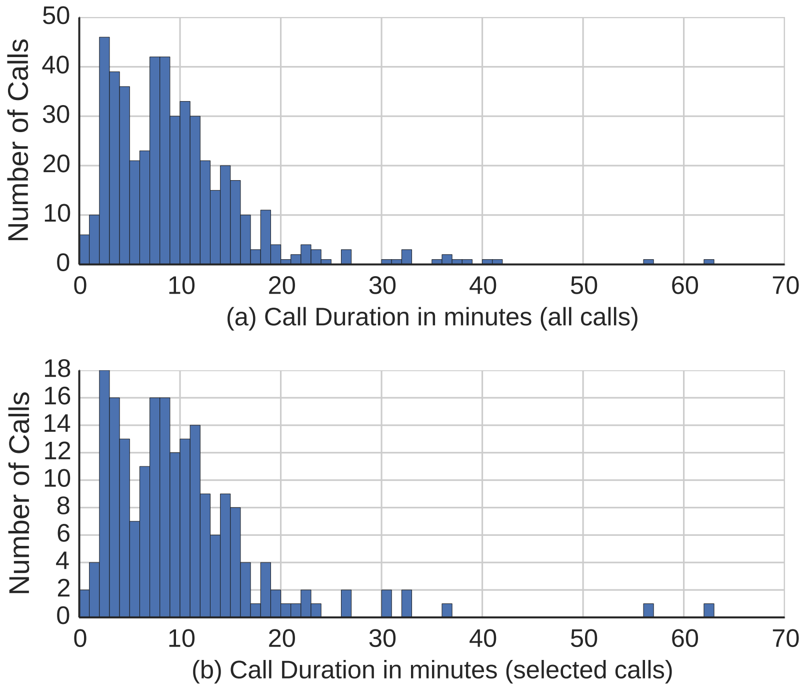
- A user can directly forward previously known (blacklisted) spam numbers to Lenny. In this case, Lenny will be the first respondent of the call, and the PBX server will log the spammer's caller ID.

It is estimated that around 500 users are using this service, as the calls are targeted to real users they sometimes contain private data, such private data is curated before the calls are made public.

9.2.2 Public Dataset and Selection

We use data collected by a popular deployment of Lenny for which a set of call recordings are available online on Youtube [Tao]. Note that the recordings we used in this study were all conducted in a country and under conditions which make those recordings legal.[3]

[2] In a conference call, the user can mute his phone and does not need to interact.
[3] We omit details to preserve the anonymity of the PBX maintainer.



(a) Call Duration in minutes (all calls)

(b) Call Duration in minutes (selected calls)

Figure 9.2: Histogram of call durations uploaded on Youtube channel, (a) all calls as of November 14th, (b) calls selected for being transcribed.

As of November 14th, 2016, the Youtube channel contains 487 unsolicited calls answered by Lenny, with an average call duration of 09:43 minutes. In addition to this, we obtained the PBX server call logs (call date, time and duration) for 19,402 spam calls sent to Lenny over 18 months (from 06/17/2015 to 12/17/2017).

Among the 487 public call logs, we select 200 calls randomly, but preserving the call durations distribution (Figure 9.2). We also include some interesting outliers, like a 1-hour call.

We then used a commercial transcription service to facilitate the analysis of the call recordings.[4] Over 2000 minutes of Lenny calls were transcribed with verbatim transcription and timing of each turn of the conversation. (We provide two examples of the transcribed calls at Appendices C and D.) We chose a professional transcription service over a speech recognition tool (like in [MKDP16]) in order to obtain the high transcription accuracy required for conversation analysis. Finally, we converted selected fragments of transcripts to the Jeffersonian transcription notation [Jef84] required for very fine grained analysis.

[4] gotranscript.com

9.2.3 Limitations of the Dataset

While this dataset is relatively large and instructive on the discussions between abusive telemarketers and Lenny, it comes with a few limitations.

First, the audio recordings publicly available on Youtube were selected by the owner of the PBX server subjectively, with a changing criteria over 3 years.

Second, the call recordings are not always complete, they only contain the part of the call that is handled by Lenny (after it has been transferred) and some parts have been edited to remove personal information.

Finally, the IP-PBX does not always receive the caller ID information of the spammer, but the caller ID of the user transferring the call. As a result, it is not possible to precisely know the spammers' caller IDs and to use this in our analysis. Moreover, a user may arbitrarily transfer only a subset of the spam calls he receives, so the coverage is limited compared to the other honeypots which do not require a human to transfer the call [GSBA15, MKDP16].

Nevertheless, this dataset is very interesting to understand and analyze the audio conversations between a telemarketer and an automated system.

9.3 Analyzing the Spam Landscape

In this section we will analyze the voice spam landscape, comparing our observations with previous work. We will also analyze how call agents behave and how their behavior vary according to the type of the spam call.

9.3.1 Observations on Call Logs

We observe several trends on the spam calls, using the 18-months dataset of 19,402 calls. Figure 9.3 shows how the calls are distributed over the days of a week and hours of a day. Majority of the calls were made on weekdays and business hours, which is in line with the findings in [GSBA15].

Figure 9.4 shows the distribution of the call durations (in minutes). In particular, 78% of the calls were less than 2-minutes long. On closer inspection, many of those short duration calls were due to call forwarding problems. In other, more frequent cases "abandoned" calls were dialed by a predictive dialer, but were not transferred to a human agent afterwards, or dropped by the caller. Unfortunately, we did not have access to all recordings of such calls and we therefore do not have detailed measurements on this aspect. We assume that the calls longer than 2 minutes contain real conversations of spammers with Lenny. Considering the 4094 calls that are longer than 2 minutes, we find that Lenny stalled spammers

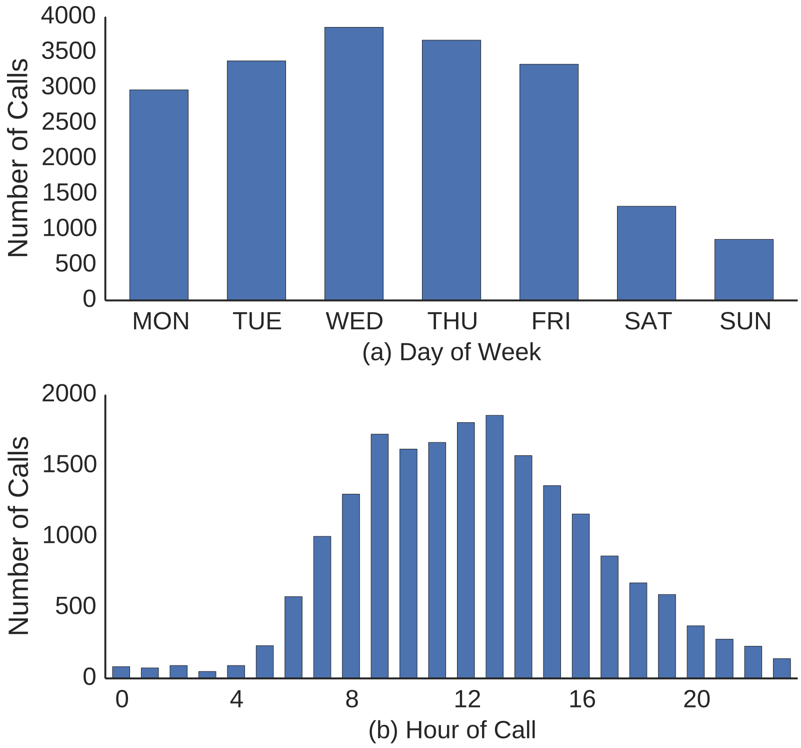


Figure 9.3: Histogram of calls by (a) days of a week and (b) hours of a day. Note that time zone of callee might be different from time zone of the PBX server in some cases.

for more than 385 hours in 18 months, with an average call duration of 5.6 minutes.

Due to privacy concerns, the PBX logs we obtain do not contain any caller IDs. Moreover, as explained in Section 9.2.1, caller IDs received by the PBX may belong to the spammers, and may be spoofed. Therefore, we cannot present statistics on the increase or decrease of spam calls experienced by individual users over time. However, we present the monthly distribution of calls in Figure 9.5. Note that the increase in calls may result from the increase in the popularity of the PBX server among the online community.

9.3.2 Analysis of Call Recordings

Transcriptions of call recordings provide valuable insights on different types of unsolicited calls the customers experience, and the strategies frequently used by fraudsters to convince customers.

Initially, we isolate the spammers' turns in each transcript, tokenize the words and use k-means clustering algorithm (with k=15) to cluster the spam calls.

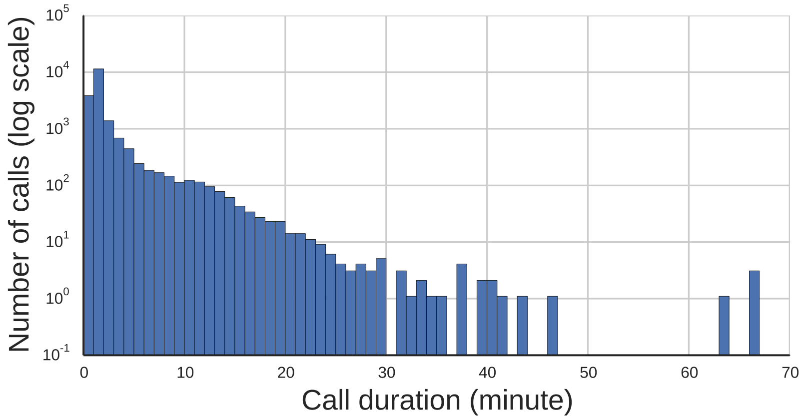


Figure 9.4: Histogram of call durations covering 18 months.

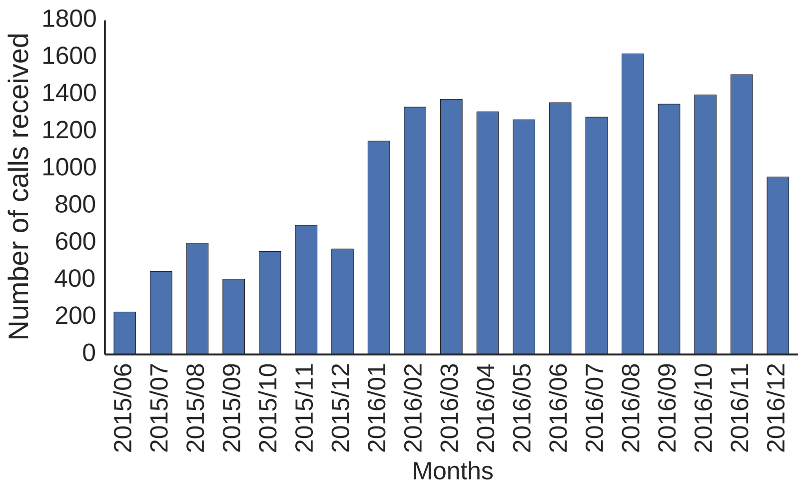


Figure 9.5: Number of calls received by the PBX server each month.

Then, we manually examine the results and end up with 22 clusters. Upon further examination, we create a broader classification of spam types: fundraising, telemarketing (targeting home owners, business owners or personal) and scam calls. Table 9.1 presents the descriptions of different spam calls in each category.

In general, fundraising calls aim to collect donation for political organizations and charities. Telemarketing calls either try to identify potential customers for a business (referred to as ‘lead generation’ calls in telemarketing terminology [Ban]) or try to sell a product. On the other hand, scam calls include all sorts of calls trying to deceive people into making a payment or revealing sensitive information to gain illegitimate benefits.

We observe that a spam call usually starts with a composition of the following turns from the caller (see [Sch86] for an extensive analysis of informal call beginnings):

- Greeting (e.g., 'Hello')
- Self identification (Name of the call agent)
- Company identification (Name of the business)
- Warm up talk (e.g., 'How are you today?')
- Statement of the reason of the call
- Callee identity check (callee's name and attribute)

While identifying the company, spammers often use phrases assuring the legitimacy of the business. While the telemarketers use phrases like "licensed, bonded, insured company", scammers are likely to use a illegitimate or fake company name referring to a well-known institution (e.g., 'Windows service center' or 'US Grants and Treasury Department'). However, here we do not judge the legitimacy of the involved businesses in telemarketing and fundraising calls. Nevertheless, these calls are unwanted (as the user transferred them to Lenny) and often aimed to manipulate customers.

Callee identity check usually aims to verify that the callee is the 'decision maker' (e.g., the owner of the house or business) or he is in need of a certain opportunity (such as lowering interest rates for credit card debt).

To better convince the customers, spammers make several promises throughout the call, such as they will give a free estimate with no obligation, cancellation is easy or free, the price is all inclusive or there will be a lifetime warranty. Another strategy is to pressure the customer for a quick decision. For example, some scams start by congratulating the person to make him believe that he won something and this is a limited time offer (e.g., "valid only for today"). On the other hand, some calls start with a threatening scenario such as "your computer is getting infected", "your air duct system is badly contaminated" or "there are 8,000 home invasions everyday in the US".

During the call, spammers ask several questions, some of which are summarized in Table 9.1. We believe that even if the customer does not qualify or does not accept the offer for the moment, this information is collected to broaden and verify information on customers, which can be used for more efficient advertisement in the future [Sob15].

The final purpose of the spammer is often to convince the customer to make a payment (e.g., by giving credit card information or home address for the bill), or to get an appointment for further interaction. We frequently observe that the spammer does not give the customer an option to decline. Instead, he asks to choose between two different products or services. For instance:

- Donation for a political party: spammer asks if the customer wants to donate $625 or $500, later in the call $425 or $375, and later, $250 or $100.
- Appointment for home improvement technician: spammer asks if the customers prefers 2:30pm or 4pm.
- Medical equipment: spammer asks if the customer needs a knee brace or a back brace.

Interaction with Lenny

Before we analyze Lenny's conversational properties, we would like to present some statistics on how spammers interact with Lenny. In our dataset consisting of 200 calls, spammers on average spend 10:13 minutes talking to Lenny. These conversations include an average of approximately 58 turns (an exact calculation is difficult due to overlapping speeches). Moreover, 72% of calls contain Lenny's set of scripts repeated more than once. On average, a caller hears 27 turns of Lenny, which corresponds to repeating the whole script 1.7 times. These results show that Lenny is a quite successful chatbot in continuing the conversation.

Surprisingly, in only 11 calls (5% of all calls), the caller realizes and states that he is talking to a recording or an automated system. Additionally, 5 of them notice the repetitions in Lenny's turns and state that "something is wrong" with Lenny. 7 spammers think that Lenny has dementia or alzheimer and/or try to contact his nurse, whereas 4 other ones ask Lenny if he is playing a prank on them. 2 of the spammers who realize Lenny is a recording say that they are still getting paid for the call, one even threatens him to be calling every morning at 8:30 am [thr16]. Moreover, several spammers aggresively try to interrupt Lenny by shouting phrases like "sir please stop" or "listen to me", or even by clapping hands.

In Figure 9.6, we analyze how spammers' behavior vary in relation to the different type of spam calls. The *hang up rate* shows what ratio of the spammers hang up the call on Lenny, without a proper closing turn. Even though Lenny's never-ending turns make it hard to leave the conversation, some spammers try to politely end the conversation by pretending that they are not able to hear Lenny or they have to leave for a meeting, and saying that they will call back at a later time. The *cursing rate* shows the ratio of spammers from each category that use bad language and swear words. Finally, we present the average call duration for each category as well.

Table 9.1: Categorization and description of spam types.

Category	*Descriptions of spam types*	*Requested personal information*
Fundraising *(14 calls)*	**Political** calls to collect donations for political parties or organizations **Charity** calls to solicit contributions for charities	- Political affiliation - Credit card information - Email
Telemarketing targeting home owners *(93 calls)*	**Home improvement** calls offering discounts and free price estimates on various work needed around the house, like **window&door replacements** **Furnace and air duct** cleaning/upgrade promotions **Solar energy** calls offering free installation of solar panels to provide lower rates on electricity bills **Security alarm system** companies offering installation of a free (or discounted) alarm system (but requiring a monthly monitoring fee) **Energy providers** offering discounted, flat rate utility bills **Communication providers** offering phone/TV/Internet bundles	- Age of the house - Age of furnace or air conditioning - If the callee is married or single - Recent electricity bill, current energy provider - Recent Internet bill, current provider - TV count in the house - Home address
Telemarketing targeting business owners *(12 calls)*	**Office supply** company offering discounts and free shipping on orders **Business directories** offering premium business listing	- Business name - Location
Other consumer centric telemarketing *(22 calls)*	Medication or medical equipment offers, extended car warranty, newspaper and magazine subscriptions	- Medical history, pain problems - Car mileage - Credit card or check address
Scams *(59 calls)*	**Technical support scams** offer a fake tech support service and request money **Vacation scams** offer a free vacation, but the customer needs to pay for government/port taxes **Credit card scam** offers lower interest rates on credit card debt, but the customer gets no real benefits **Advance-fee and cash advance scams** promise a sum of money, or funding for businesses, but the customer needs to pay up-front fees **SEO scam** offers guaranteed rankings on search engines (claiming relation to a well known company)	- Full name, email - Credit card information - Credit card balance - Current bank interest rate - Business profit - Business name, website

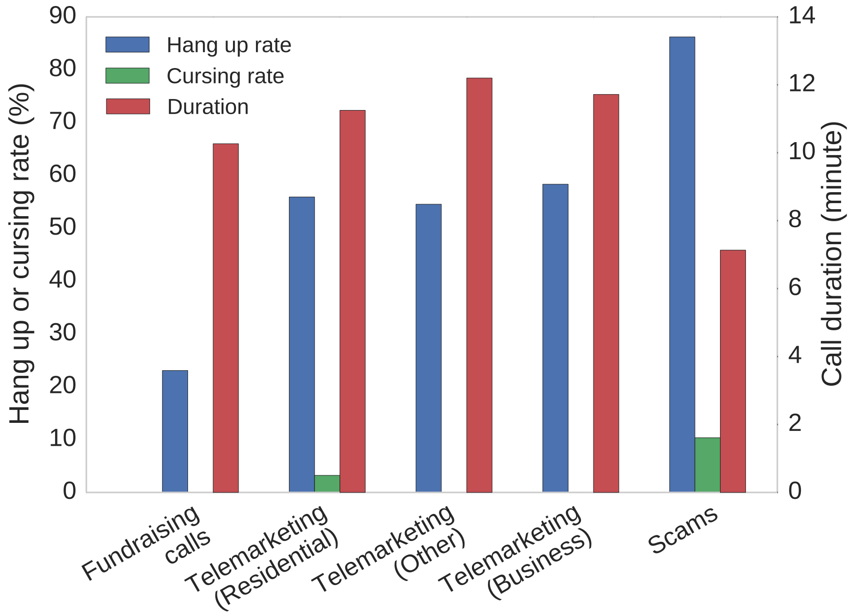


Figure 9.6: Interaction of different type of spammers with Lenny.

Looking at Figure 9.6, we can say that fundraising calls are more polite than others. Such calls often come from charities and political organizations, who usually care about their reputations and impressions they make. Telemarketing calls show similar characteristics, regardless of the call target. On the other hand, scammers are the rudest callers with 89% hang up rate and use of swear words in 10% of the calls.

We also apply Chi-squared and Fisher's exact tests on hang up rates and observe a statistically significant relation between the hangup rate and spam category (telemarketing, fundraising, scam): for the significance level of 0.05, p-values are less than 0.0001.

As opposed to the polite demeanor observed in [MSN17], we find tech support scammers to be particularly rude against Lenny, with 100% hang up rate and 20% cursing rate, probably because Lenny does not comply with their instructions.

Scam calls also have a noticeably shorter average call duration compared to other spam types. Applying a two sample T-test (p=0.05) for each pair of the three categories shows that the duration of scam calls are indeed significantly different from both fundraising and telemarketing calls. Again, a possible reason is that the scammers do not want to waste time with Lenny, once they realize that Lenny will not answer their questions or do what they ask. However, fundraising and telemarketing calls do not have a significant difference between them.

1. L: hello: eh eh this is lenny!
2. L: hi uh uh ss- sorry, I'b- (0.3) I can barely hear you there?
3. L: °ye-° ye:s yes yes
4. L: oh good >yes, yes, yes<.
5. L: uh yes, yes. uh: uh uh, someone, someone did (.) did ss- say
   last week (abou-) someone did call last week about
   the same (.) thing, .h wa- was that was that you?

Figure 9.7: CA transcript of the first pre-recorded Lenny's "turns" (formatted with [Jef84]).

9.4 Usability of Lenny as a conversation partner: An applied CA approach

Lenny's efficiency is closely related to how the pre-recorded, pre-defined turns are able to deal with the four levels of the organization of talk (Section 9.1.3).[5]

9.4.1 The Structure of Lenny's Turns

Figure 9.7 shows the first five turns of Lenny (T1 to T5). After a direct, informal reception of the call in which he gives his first name (T1), Lenny introduces a hearing issue (T2), then produces a first "yes" turn (T3), followed by a more enthusiastic one (T4), and a last "yes" turn which has a second part, a verification question about a past event (T5).

Each turn is supposed to play a specific role in the construction of the conversation. Some turns become parts of a two-unit sequence (adjacency pair). While T1 and T2 are designed as first pair parts, T3 and T4 become second pair parts (i.e., they are supposed to follow a question, a proposal, request, etc.).

Moreover, the beginning of T4 adds two other components: "oh" is a turn-initiated particle that can be analyzed as a prefaced response [Her98] and a sign of assessment (in particular when it is followed by "good") [Her02].[6] It is followed by the three enthusiastic "yes" which end the turn. As a result, this turn shows relation to the previous turn, and engages well with several different types of first pair parts.

T5 sounds as a verification question and presupposes that the reason for the call has been previously introduced by the caller. It has been built to occupy a more specific sequential position in the call (the position after the reason for the call).

[5] A more detailed CA approach can be found in our paper [SRF17].
[6] "oh" is the "second most common turn-initial object in English conversation" [Her16, Nor09]

Another feature of Lenny's turns is that they are designed to display "repair" related features, such as repeats, cut-offs or "uh" types. It has been suggested that a high frequency of "disfluencies" in talk features the class of age of the speaker [HSS10]. Along with the pitch of his voice, such disfluencies facilitate the recognition of Lenny as an "old man" and bring an easy explanation for some other understanding troubles which might occur.

Inspecting Lenny's turns in isolation is not sufficient enough to understand how Lenny can be so efficient in so many different calls. This efficiency is locally built in each call development. Once embedded into a real call, Lenny's turns display an understanding of prior turn and brings new material to be understood by his co-participant.

9.4.2 An analytic insight on the opening section of Lenny's turns

On one hand, most telemarketers use very detailed scripts while talking to a prospect. For this reason, the call trajectories might seem to be even more routinely organized than the informal talk on the phone. On the other hand, the Lenny corpus displays different types of calls (See Table 9.1) and several different caller objectives. In the limited scope of this study, we will only examine the beginning section, because it is often a strategic place in which the trajectory of calls is prepared and launched. The beginning section will refer to the talk which has been produced before the production of the reason for the call.

Calls with minimal beginning section

Some calls do not display any beginning section: the reason for the call is given in the first possible position in the call, just after Lenny's first turn.

In a very few calls, this is done without any self identification of the caller (Fragments 1, 2) or with a minimal identification (Fragment 3).

In turn 2 of Fragment 1, the caller directly goes to the point, without a greeting, self identification, or any other item. The caller addresses the callee with the first name he has given in his first turn. Then the business of the talk is addressed with no more preparation, but it refers to a previous action which the caller has been accomplished on the phone ("pressing one"). The aim of this turn is to focus the attention of the callee to bring an answer in the next turn and to attend to the call. In this sense, this turn drives callee's attention right to the business of the call. It also embodies a preference for a "yes" answer, which will give the floor back to the caller. However, Lenny's second turn (T4) initiates a repair sequence, which is answered by a partial repetition of the caller's first turn. Then, because Lenny's next turn is precisely designed as a "yes" answer, it conforms with the caller's preferred answer, and the caller can ask the next question.

Fragment 1.

1. Lenny: hell<u>o</u>: eh eh this is lenny!
2. Adam: yeah mister lenny, you have been chosen to get a lower interest rate, so (I believe) you have pressed one to get a lower interest rate right?
3. (0,6)
4. Lenny: hi uh uh ss- sorry, I'b- (0,3) I can barely hear you there?
5. Adam: I'm saying so I believe you have pressed one to get a lower interest rate, right?
6. (0,6)
7. Lenny: °ye-° <u>ye:s</u> yes yes.

Fragment 2.

1. Lenny: hell<u>o</u>: eh eh this is lenny!
2. Caller: injured, retired and elderly fop members, as well as create and maintain a state memorial for officers tragically killed in the line of duty. now sir when you receive your pledge kit, can the pennsylvania fraternal order of police foundation count on you for a fully tax deductible donation?
3. (0,6)
4. Lenny: hi uh uh ss- sorry, I'b- (0,3) I can barely hear you there?
5. (1)
6. Caller: oh I was just saying the goal of the drive is to help provide assistance to families in local lodges when fop members are killed in the line of duty. assist injured, retired and elderly fop members, as well as create and maintain a state memorial for officers tragically killed in the line of duty. now sir when you receive your pledge kit, can the pennsylvania fraternal order of police foundation count on you for a fully tax deductible donation?
7. (0,6)
8. Lenny: °ye-° <u>ye:s</u> yes yes.

In the donation call (Fragment 2), the caller again rushes into presenting the reason for the call, but in a somewhat different way. Though this long turn is finished with a yes/no question and then orients to a third turn for the caller, the donation proposal has been prefaced by a long attempt to emotionally engage the callee into a supportive action for police officers and their families who are in difficulty. Thus, it aims to trigger a yes answer. Lenny's turn fit very well into this second beginning as well.

Fragment 3.

1. Lenny: hello: eh eh this is lenny!
2. Caller: oh hi I'm calling at HVAC heating and air we're
   going to be in the area during the maintenance
   for thirtynine dollars if you haven't done this yet as
   a as a promotion we're doing for the next month ok
   but it does include air duct cleaning and under filter
   and a safety inspection for the furnace,
3. (0,6)
4. Lenny: hi uh uh ss- sorry, I'b- (0.3) I can barely hear you
   there?
5. Caller: ho. uh ha- have- have you had a maintenance done
   on your furnace this winter ?
6. (0,6)
7. Lenny: °ye-° ye:s yes yes.
8. Caller: ok we are offering it for a half price right now.

In Fragment 3, the caller quickly identifies the firm he is calling from, to announce the reason for the call, a promotional offer. Note that after the repair initiation of Lenny (T4 here), the caller does not repeat the promotional offer but converts it to a verification question, which gives him the control of the conversation to re-introduce the offer in the following turn (after Lenny's "Yes" turn).

Calls with beginning section: a progressive entry into the business of the call

In most calls, however, the caller does not introduce the reason for the call directly in the first turn. He first greets Lenny back, adds a self identification and/or a "how are you" question.

Fragment 4.

1. Lenny: hello: eh eh this is lenny!
2. Caller: hi sir good afternoon this is michelle with cool duct
air-conditioning and heating how are you
today ?
3. Lenny: hi uh uh ss- sorry, I'b- (0.3) I can barely hear you
there?
4. Caller: ow okay. hu this is michelle with cool ducted air-
conditioning and heating. (.) Is that bett[er ?
5. lenny: [°ye-° ye:s yes yes.
6. Caller: okay, uhm : I was calling about the summer
maintenance for your central air conditioning,
7. (0,6)
8. Lenny: oh good >yes, yes, yes<.
9. Caller: ok we're running a special right now it is more than
fifty percent off and we do a 50-point tune-up on
your unit now with our service we replace your
filter with a free reusable filter and we talked off
the refrigerant up to a pound at no charge ok it's
automatically a hundred dollars savings ok now
uhm the technicians going to also do a complete
mold and mildew inspection flushing vacuum out
the drain line to get rid of the build-up and then
treat it without the side tablets ok so on it will
prevent the build-up of mold and mildew and kill
bacteria so you're getting better quality air in your
home he'll also check your ducts to make sure
there's no tears or separations anywhere that you're
losing energy ok we wanted you should save up to
twenty percent on your monthly electric bill ok
now he'll also check your air handler, calibrate the
thermostat make sure it's accurate the voltage and
the amperage on the motors the starting capabilities

to make sure the A/C is turning on and off when it's supposed to fill sanitizer evaporation oil and oil and lubricate all the moving parts. ok now more importantly you'll get the state certified report to validate your warranty cap that's your proper documentation. okay and our special right now is only forty-four dollars not a penny more that includes the taxes you're 50 point tune up your free filter free refrigerant along with a hurricane safety inspection also free and there is no trip charge or we could take care of you tomorrow.

In the opening of Fragment 4, the caller introduces a greeting, a self identification, and an identification of the firm she is calling for, before adding a "how are you" question. After Lenny initiates the "hearing" repair in the next turn, the caller again partially repeats her turn, except the "how are you" question. Michelle completes this turn as a hearing check, with a yes/no question. Then Lenny's first "Yes" turn fits well to display a confirmation. In turn 6, Michelle makes a first attempt to introduce the "reason for the call". In this sequential context, Lenny's second enthusiastic "Yes" turn (T.8) sounds as an authorization to expand the previous announcement.

Fragment 5.

1. Lenny: hello: eh eh this is lenny!
2. Brianna: I need to speak to the person that handles the clp electric bill, is that you?
3. Lenny: hi uh uh ss- sorry, I'b- (0.3) I can barely hear you there?
4. Brianna: I need to speak to the person that handles the clp bill - electric bill - is that you?
5. Lenny: °ye-° ye:s yes yes.
6. Brianna: hello, my name is brianna, I'm calling on behalf of spark energy in regards to the connecticut electric choice program. do you recall receiving that information, sir?

In Fragment 5, an identification question is introduced before the reason for the call. This identification check aims at finding the right person who is responsible for some task (here the electric bill). Brianna repeats the same question after the hearing trouble question from Lenny. In this sequential context, the "Yes" turn displays a positive answer to the identification question. This understanding is embedded in how Brianna is pursuing the call with the reason for the call. No doubt that Lenny is the right addressee.

Fragment 6.

1. Lenny: hello: eh eh this is lenny!
2. Brian: hi lenny this is brian security specialist how are you today.
3. Lenny: hi uh uh ss- sorry, I'b- (0.3) I can barely hear you there?
4. Brian: my name is brian it's a pleasure to make your acquaintance lenny how'r yu
5. Lenny: °ye-° ye:s yes yes.
6. Brian: have you ever had a security system for yourself.
7. Lenny: oh good yes yes yes.
8. Brian: do you have a security system ?
9. Lenny: uh yes, yes, uh::uh, someone, someone did say last week or some- one did call last week about the same (.) thing, wa-was that, was that, you?
10. Brian: it wasn't me it might have been someone else to my company or something, .hh but do you need do you have a security system.

In such a sequential structure, the identity check or other verification questions ("Are you in front of your computer?", "Do you have a security system?") can be built as pre-sequences, which will sometimes freeze the introduction of the reason for the call.

In Fragment 6, after the presentation and the "how are you" turn (T.2, 4), the caller introduces a verification question which is supposed to preface the offer. The telemarketer tries to ask Lenny whether he has a security system (T.6), but does not accept Lenny's the second enthusiastic "yes" turn (T.7) as a proper answer. Then, the telemarketer repeats the question (T.8). The next Lenny's turn, which begins with a "yes", could have been a second possible acceptable answer to the question, but the telemarketer keeps repeating the question (T.10). The several repeats of the same question indicate that there is an incoming issue in the conversation which has been noticed by the caller.

Nevertheless, in most cases, Lenny does the job and the reason for the call can be introduced. The first five turns adjust to the various different openings and get different senses from their positions in these sequential environments.

9.5 Discussion

As we have shown in the previous section, Lenny's effectiveness does not only come from the design of Lenny's turns, but also from the orientation that the caller display towards Lenny. A conversation analytic perspective reveals Lenny's ability to contribute to the sequential development of various types of spam conversations. To a certain extent, it does not matter that Lenny’s turns are fixed, pre-recorded items, as long as this feature is not discovered by the caller himself during the conversation.

For the future work, a broader analysis of other sections of the calls (the core parts and the conversational treatment of the looping mode) would be interesting. However, in the meanwhile, we would like to focus on the complexity of Lenny’s character, which makes it difficult to replicate, while keeping its “botness” less visible for the caller.

9.5.1 Lenny the subtle bot

Like other professional phone talk settings, unsolicited spam calls are script-guided and goal-oriented [DH92]. As Mazeland [Maz04] has pointed out in one of the very few conversation analysis studies on telemarketing, the operators try to take control over the interaction with “initiatory actions” (i.e., first pair parts).

Rather than being interested in Lenny’s social categories (e.g., grandfather, elderly), callers want to check if Lenny is their specific target for this call (e.g., business owner). They are also not interested in ordinary topics that people usually bring into the daily conversations.

Lenny’s talk displays some features which foster callers: he is ready to talk; he displays some positive alignment in the beginning of the call; he provides some confirmation of the requested identity. On the other hand, the callers have to deal with various aspects of Lenny’s conduct: the repeat queries, verification questions and long, family-centered narratives. These aspects allow Lenny to take control of the turn management, and make it difficult for the callers to come back to their business script. Lenny leads the callers to adjust their own talk to the specificities of Lenny’s turns, while maintaining a continuous, positive orientation to the business of the call. Its brilliant design lies in the subtle equilibrium it preserves between control and alignment.[7]

9.5.2 Usability of Transferring Calls to Lenny

In this work, we did not study the user aspect of transferring calls to Lenny. In fact, we have limited control and data on this aspect of the deployment, but in general the usability of the call transfer is quite poor. Requesting a user to perform multiple steps to transfer the call is not likely to scale well with the general public. On an enterprise desk phone where buttons can be configured to automatically transfer calls to a given phone number, the operation can be

[7] More Conversation Analysis work will be necessary to gain a proper understanding of the skilled Lenny.

straightforward. On the other hand, such tasks are difficult to automate on mobile phones: call control APIs are very limited and the audio of a call is in general directly handled by the mobile baseband chip. As a consequence the audio stream is not easily accessible by applications on unmodified smartphones. Thus, automating the use of such chatbots with a smartphone application, without the involvement of the phone manufacturer or of an operator, is currently very difficult to achieve. Despite the call transfer limitations, the number of people using Lenny have been increasing as its popularity increases among the online community.

9.5.3 Comparing Lenny with Existing Voice Spam Countermeasures

Chatbots like Lenny does not necessarily prevent voice spam, in fact, using Lenny may increase the number of unwanted calls one receives, due to getting marked as a potential customer. In this respect, Lenny does not really compare with the other voice spam countermeasures that often aim to detect and block spam calls [TDZA16a]. In fact, the recipient will still be disturbed with the call, and will need to make a decision on the call type (spam or not) to transfer the call. Moreover, the usability issues with call transfer and the possible need for a third party system reduces the scalability of such chatbots.

9.5.4 Effects on the Economics of Voice Spam

Lenny provides an opportunity to stall fraudsters and slow down economics of voice spam, by directly and indirectly increasing the cost of a failed telemarketing or scam call.

To spend 15 minutes or more of a working time with a Lenny-like bot represents a direct cost for spammers. More importantly, it also results in an opportunity cost, because the spammer will not be able to target other legitimate customers during this time. This increases the call costs until reaching a valid customer and decreases the volume of calls a single spammer can generate in a certain time period [Tal15]. On the other hand, victims could save time by using the chatbot instead of declining the proposal or dropping the call.

Depending on the expected monetary benefit of a spam scheme and the rate of use of chatbots, a spam campaign may become less profitable, or even not be economically viable. However, this would require a large number of chatbot users. In fact, a recent survey shows that more than 90% of participants do not listen to telemarketing proposals until the end; they either politely decline or hang up the call [BC17]. Another benefit of the generalization of such a service would be to reduce the economic damage of voice spam on society, both due to the direct monetary losses [Kok17], and due to the reduced productivity [Bro14].

A possible consequence is that the spammers will get acquainted with the chatbots and be able to quickly recognize and avoid them. Thus, a generic framework could be useful to simplify the creation of personal chatbots, e.g., providing guidelines on script preparation.

9.6 Conclusion

Voice spam is a prevalent, yet unsolved problem affecting telephone users. In this work, we study a particular anti-spam chatbot, $Lenny$, which was created to fight such spam calls with a set of pre-recorded voice messages.

We first present several statistics showing that despite its simplicity, Lenny is very effective in dealing with phone spammers. Then, we propose to investigate the usability of Lenny from the perspective of applied Conversation Analysis. We highlight the complexities of Lenny which are "seen but unnoticed" [Gar67] by his co-conversationalists. Despite the apparent simplicity of this 16 pre-recorded turns chatbot, we show that its success relies on a sophisticated equilibrium between contrastive features: These features give it the necessary flexibility to fit into several sequential organizations, while keeping sufficient control over the interaction.

Our study also reveals various insights on the voice spam landscape and common strategies of phone spammers. Finally, we discuss several factors on the usability of chatbots against voice spam and possible effects on spam economics. We believe that widespread adoption of diverse chatbots can be effective in decreasing financial incentives of spam campaigns.

Chapter 10

Conclusion and Perspectives

This work was motivated by the idea that a better understanding of fraud mechanisms is essential to effectively address telephony fraud. In particular, clearly identifying the weaknesses fraudsters manipulate, the techniques they use, and the benefits they pursue would provide us better directions and context in exploring defense mechanisms.

To this aim, in the first part of the thesis, we presented a comprehensive taxonomy of the current telephony fraud ecosystem. We examined the problem in different layers, ranging from the inherent flaws of the telephony systems to the final goals of the fraudster.

The two fraud schemes we studied in the second part further demonstrates the complexity of fraud ecosystem. In particular, while studying the OTT bypass fraud, we observed the collision of several fraud schemes and their combined effects on the network, call establishment quality and user experience. We also showed that fraud schemes like OTT bypass can be very challenging to detect (and even more challenging to prevent), due to the opaqueness of telephone networks. Later we studied IRSF, a fraud scheme that may take various forms, depending on the fraud agreement, collaborating parties and the traffic generation schemes. The complexity of IRSF increases even further with the third party providers operating online. We first analyzed the data we collected from such online providers, to understand how they operate. By taking advantage of this information, we then proposed a set of features that can be used to detect IRSF calls.

In the last part, we look into voice spam, which have been widely studied in the literature, unlike the two previous fraud schemes. However, instead of focusing on the conventional spam detection and prevention techniques (such as blacklists, caller reputation or behaviour analysis [TDZA16a]), we concentrated on the use of chatbots as a way to decrease fraudsters' financial incentives. As we consider the 'benefits' as a fundamental part of our fraud definition, we believe that chatbots can be combined with the existing fraud detection and prevention mechanisms, as a supplementary way of slowing down voice spam campaigns.

10.1 Future research perspectives

This thesis is only a first contribution in the under-explored academic research on telephony fraud. We believe that there many things to explore in this domain. Here, we list a few immediate followups of the work presented in this thesis, as well as other interesting directions to follow.

Fraud taxonomy and weaknesses

A first idea for the future work would be to present the fraud taxonomy in a more formalized way. In particular, a domain specific language can be defined to formally express the relationships between the components at each layer of the taxonomy. With this, it would be possible to present information in a more concrete way: for instance, the relationship between a fraud scheme and a technique might be definite/explicit, or conditional/implicit. Moreover, the state of the art defense techniques at each layer (weaknesses, techniques and fraud schemes) can be incorporated with this formal model.

The second step would be to address the weaknesses we listed in the taxonomy. In fact, some of the weaknesses such as lack of caller ID authentication has been studied in recent years [RBT16, TDZA16b, Pet15], however the proposed solutions are not widely deployed due to the practical and technical challenges, but also due to the lack of incentives for deployment. For instance, solutions manipulating the audio channel can be difficult to adopt for end user devices, although they can be used on the operator side, or by call centers (e.g., banks).

Another weakness to address would be the drawbacks of decentralized numbering plan databases. Although the operators are able to know the allocated number ranges, they cannot be sure if a phone number is currently assigned and active (in use). Number portability complicates things even further. One solution could be to provide a DNS-like mechanism where the operators can register information about their phone numbers, and securely update and lookup such information. A similar system, called ENUM ('E.164 Number to URI Mapping' [BCF11]), specifies how to link VoIP accounts and E.164 phone numbers. However, ENUM-like services are often used by operators internally. Although it is difficult to deploy such system globally and with participation of all the operators, it can be of interest to the honest parties whose numbers are manipulated by fraudsters.

Finally, more measurements on users' fraud related knowledge and experience would be interesting, especially for consumer protection. For instance, usability studies on the existing voice spam countermeasures can be a starting point.

Another interesting topic would be to study if users' awareness really decrease their chances of being a fraud victim, and which factors are effective in this. For instance, in our user survey in Section 6.5, we find that only a small number of people disable the OTT bypass option in their application, even if they are aware of it. The reasons behind such cases can be studied, possibly in collaboration with social science researchers.

Measuring the real impact of fraud

Measuring the actual impact of telephony fraud is very challenging, even if we only focus on the financial impacts (ignoring the social and psychological effects). The estimates on the financial loss may not be reliable, as the loss for one operator may be benefit to the other. For instance, fraudulent international calls often follow a complex route involving multiple transit operators. In this respect, fraud loss can be only perceived as a loss for the originating operator who, for example, has to pay its succeeding operator, but will not be get paid by the customer. However, some transit operators on the call route might be legitimately benefiting from those calls, as they just provide regular transits. Therefore, one should consider that global fraud loss reports usually do not take into account the benefit that some operators may gain from fraudulent calls. In fact, fraud loss may be shared among the fraudsters, and other legitimate operators who does not do anything wrong, but also may not have strong incentives to fight fraud. Thus, it would be useful to create a more accurate model that will take into account the different aspects of the financial impacts of fraud.

Another topic to study would be the 'acceptable level' of fraud loss for operators: When do they start investing in fraud prevention/detection solutions, what are their decision mechanisms, what is the amount of undetected fraud loss? While the large operators can make significant investments in fraud prevention, small size operators usually cannot. Therefore, studying the optimal fraud management policies could be useful. For this, a game theoretic approach might be utilized.

Mobile malware and fraud relation

Although there are many studies that classify and analyze mobile malware [ZDYZ14, LNW+14], it is not always clear what type of tricks are employed by malware to perform fraud schemes, or how mobile malware facilitates telephony fraud. Several papers and blog posts mention the use of malware, e.g. to initiate calls to premium rate numbers, or to steal personal information [LNW+14, BCI+15, Apv10]. However, it could be interesting to study the actual techniques and the potential weaknesses of smart phones that might be exploited to commit fraud. A recent study [GME17] that explores the possible use of baseband rootkits for anonymized emergency service DoS attacks is a good example of this domain.

Fraud on data networks

With the rise of embedded devices and the future 5G technology, fraud in data networks is likely to become more significant. Currently, machine-to-machine SIM cards and roaming services can be interesting to study.

10.2 Concluding thoughts

Despite the advances in fighting telephony fraud, it will likely continue to be an important topic in the foreseeable future. A good understanding of the problem is required to continue the fight against fraud. We hope that our work will foster more academic research on this topic and in particular help to understand effectiveness and implications of new countermeasures.

Appendix A

Résumé en Français

Les réseaux téléphoniques sont apparus il y a plus de cent ans, formant le plus ancien réseau à grande échelle qui touche aujourd'hui plus de 7 milliards de personnes. La téléphonie fusionne maintenant de nombreuses technologies complexes et comme les services liés à ces technologies peuvent être monétisés, la téléphonie attire beaucoup de fraudes. Pourtant, il existe peu de travaux académiques sur ce sujet, en partie en raison de la complexité de ces réseaux et de leur nature fermée.

Dans la première partie de cette thèse, nous visons à explorer la fraude systématiquement dans réseaux de téléphonie. Nous proposons une taxonomie qui différencie les causes profondes, les vulnérabilités, les techniques d'exploitation, les types de fraude et enfin, la façon dont la fraude profite aux fraudeurs. Dans la deuxième partie, nous étudions deux types de fraude qui manipulent le marché de gros. Nous commençons avec la fraude de contournement "Over-The-Top" et nous mesurons son impact sur un petit opérateur mobile, avec plus de 15,000 appels de test et une étude utilisateur à grande échelle. Puis, nous examinons l'écosystème de la fraude "International Revenue Share Fraud", en analysant plusieurs fournisseurs de services de tarifs premium en ligne. En utilisant cette analyse, nous proposons un ensemble de facteurs utilisables pour détecter l'IRSF avec des techniques d'apprentissage automatique . Dans la dernière partie, nous étudions une récente contre-mesure contre le spam vocal, qui implique l'utilisation d'un robot conversationnel ("chatbot") pour interagir avec les spammeurs. Nous essayons de comprendre l'efficacité de ce chatbot, en analysant ses conversations avec différents types de spammeurs.

Tout en présentant une vision large de la fraude téléphonique, notre travail révèle également la nature complexe et les principaux défis dans la lutte contre la fraude. Nous espérons stimuler la recherche dans ce domaine, en particulier tirant parti des approches interdisciplinaires pour étudier les divers effets de la fraude téléphonique.

Introduction

La téléphonie, qui est un système fermé, a subi des changements fondamentaux au cours des dernières décennies. L'introduction de nouvelles technologies de communications et la convergence de la téléphonie avec Internet a ajouté à complexité. Malgré (ou a cause) d'avoir été déployé depuis des centaines des années, les défis de sécurité pour la téléphonie ne sont ni bien compris ni bien traités.

Dans cette thèse, nous nous concentrons sur l'écosystème de la fraude et de la cybercriminalité autour de la téléphonie vocale (sur les trois réseaux - le réseau téléphonique commuté ou RTC, les réseaux cellulaires et IP). Nous visons à améliorer notre compréhension de la fraude sur les réseaux de téléphonie en fournissant une taxonomie claire des schémas de fraude détaillés, sans ambiguïté. Nous croyons que c'est nécessaire pour lutter contre ces fraudes, en particulier pour améliorer la compréhension de la coopération entre les chercheurs et l'industrie.

Une enquête auprès des fournisseurs de services de télécommunications en 2015 estime les pertes dues à la fraude à 38,1 milliards de dollars américains. Cela représente 1,69% du coût global estimé revenus du secteur [CFC15]. En plus des pertes financières, la fraude visant à perturber le service peut avoir des effets dévastateurs, car le réseau de télécommunications est une infrastructure critique avec des millions d'utilisateurs qui en dépendent à la fois pour leurs activités quotidiennes, mais aussi pour les services d'urgence. D'autre part, les consommateurs sont également victimes d'une telle fraude, aux États-Unis d'Amérique la Federal Trade Commission (FTC) reçoit en moyenne 400 000 plaintes par mois [Fed16a].

Il est important de noter que, dans l'écosystème de la téléphonie, chaque acteur peut être un victime ou l'auteur de la fraude. De plus, dans certains cas, il peut ne pas y avoir de distinction entre les deux: Par exemple, un opérateur qui est victime d'une fraude peut lui-même abuser du même mécanisme. Il n'y a souvent pas de lois ou de règlements clairs qui rendent une fraude illégale, la fraude tombe habituellement dans une zone grise de la légalité et est difficile à résoudre. Cependant, comme nous le verrons dans les prochains chapitres, la fraude à la téléphonie a des conséquences graves (telles qu'une qualité d'appel dégradée, ou un comportement du réseau incohérent ou inattendu) qui affecterait à la fois les opérateurs et les consommateurs.

Bien que nous nous concentrions sur la fraude téléphonique, notre travail a des implications plus larges, en particulier sur la sécurité en ligne. Par exemple, un travail récent montre comment la téléphonie la fraude peut avoir un impact négatif sur la création sécurisée de comptes [TIB+14]. Un autre exemple concerne la fraude aux appels provenant de faux services de support technique, où les fraudeurs font installer par les victimes des outils d'administration à distance ou des logiciels malicieux sur les ordinateurs des utilisateurs [Mic]. Un autre incident récent est lié a l'exposition des appels de télé marketing enregistrés qui contiennent des informations (noms, adresses, numéros de cartes de crédit) [Cam17]. En outre, plusieurs cas ont été signalés, où les fraudeurs prennent le contrôle d'un numéro de téléphone en appelant le service client des opérateurs (pour obtenir une nouvelle carte SIM qu'ils interceptent), puis détournent divers services en ligne utilisant le ce numéro de téléphone mobile comme second facteur d'authentification, y compris les portefeuilles Bitcoin [Hon12, Shi16].

La téléphonie est souvent considérée comme un média de confiance, mais ce n'est pas toujours le cas. Une meilleure compréhension des vulnérabilités de la téléphonie et de la fraude aidera donc nous comprenons également les attaques Internet potentielles.

Obstacles à la compréhension de la fraude

Avoir une compréhension globale de la fraude téléphonique est une tâche difficile. Pour cela, il faut bien comprendre l'écosystème de la téléphonie, son l'histoire, les technologies sous-jacentes, la réglementation et les accords internationaux. Même les experts de l'industrie travaillant dans la gestion de la fraude peuvent avoir une vue partielle, parce qu'ils se spécialisent souvent sur les types de fraude qui sont le plus souvent rencontré, ou détecté, dans leurs entreprises.

Les définitions existantes de la fraude aux télécommunications se concentrent généralement sur services de télécommunication et d'obtenir des avantages financiers [GH99, Hoa08]. Dans ce travail, nous limitons notre perspective à la téléphonie vocale mais nous ne limitons pas les fraudes aux avantages financiers.

Perpétrer la fraude dans les réseaux de télécommunications est relativement facile: la plupart des attaques peuvent être effectuées à distance et ne nécessitent pas d'équipement majeur ou un haut niveau d'expertise technique. De plus, il est souvent très facile d'obtenir un bénéfice financier en grâce a la fraude téléphonique [Hoa98]. Souvent, la fraude est cachée dans la masse volume de trafic et grande variété de services. Par conséquent, elle est difficile à identifier, détecter et prévenir.

Nous énumérons certains des défis rencontrés dans la compréhension de la fraude:

- **Diversité de l'écosystème:** L'industrie des télécommunications est composée de différentes communautés telles que les opérateurs, les régulateurs et les utilisateurs. Chaque acteur de cet écosystème subit ou approche la fraude d'une manière différente. En outre, les fraudeurs peuvent avoir diverses motivations et compétences, et leurs méthodes sont seulement limitées par leur imagination.

- **Terminologie incohérente:** Chaque communauté a sa propre la terminologie, le contexte et les ressources concernant la fraude qui est un obstacle à la compréhension de la fraude. Une fraude a souvent plusieurs noms, par exemple, décrivant une variante, l'aspect technique ou la partie visible par l'utilisateur de l'iceberg. Dans d'autres cas, un nom est utilisé pour décrire plusieurs schémas différents.

- **Accès restreint:** Opérateurs et fournisseurs de services partagent habituellement des informations liées à la fraude (recommandations, meilleures pratiques) leurs partenaires et diverses associations de l'industrie (par exemple, TMForum, i3Forum, GSMA, FIINA, CFCA).[1] Malheureusement, les groupes sont souvent limités aux membres approuvés et ne font pas leur documents accessibles au public. Une des motivations principales de cette thèse en est le contraire: *nous ne pourrons lutter efficacement contre la fraude que si elle est bien comprise et ouvertement discutée*.

- **Vue incomplète:** Beaucoup d'informations sur les systèmes de fraude peuvent être trouvées dans les livres blancs d'entreprises vendant des outils de détection de fraude [Trab,Suba]. Cependant, ceux-ci présentent souvent une vue incomplète car ces vendeurs ne sont pas indépendants et leur but est de vendre leurs solutions.

- **Manque de données:** Une autre raison du peu de travaux académiques est probablement le manque de données pour mener des expériences. L'obtention de données réelles est difficile en raison des contraintes de confidentialité et de limites techniques.

Dans les sections suivantes, nous résumons les contributions de la thèse, et nous fournissons un aperçu de son organisation.

Contributions de la Thèse

Nous commençons la thèse avec un état de l'art sur l'écosystème de la téléphonie, la facturation méthodes et l'acheminement des appels (Chapitre 2).

Puis, dans la première partie (Part I) de la thèse, nous visons à fournir une compréhension holistique de la fraude et clarifier les ambiguïtés existantes dans la terminologie de la fraude. En particulier, dans le Chapitre 3.1, nous résumons les travaux antérieurs sur la classification des systèmes de fraude. Puis dans Chapitre 4, nous proposons une taxonomie pour la fraude téléphonique, qui tient compte des vulnérabilités, des techniques, des schémas de fraude et des raisons pour lesquelles la fraude peut être rentable. Notre taxonomie analyse la

[1] www.tmforum.org, i3forum.org, www.gsma.com, www.fiina.org, www.cfca.org

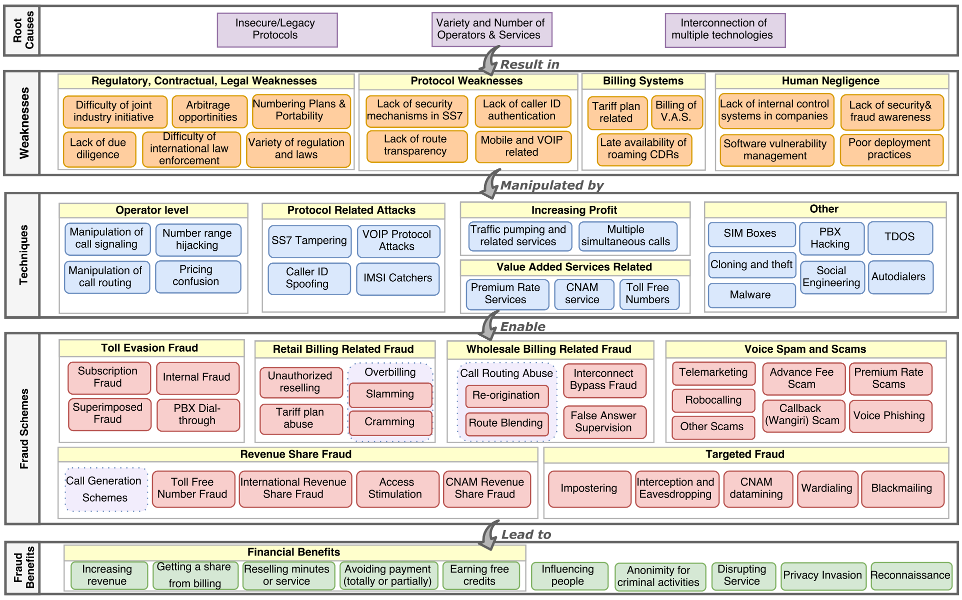


Figure A.1: Image complète de la fraude vocale.

fraude sur ces plusieurs couches, et fournit une image complète de l'écosystème de la fraude (La Figure A.1 montre une vue détaillée de la taxonomie). Nous avons ensuite étudié la fraude au partage des revenus "CNAM" (Caller NAMe) qui dans le cadre de la taxonomie, en tant que petite étude de cas. Ce chapitre est basé sur une publication a l'"IEEE European Symposium on Security and Privacy (EuroS&P)" 2017 [SFGA17]. Cette partie de la thèse se termine par le Chapitre 5 où nous donnons un état de l'art des techniques de détection et de prévention de la fraude, a la fois dans le monde académique, ainsi que du monde industriel.

Dans la deuxième partie, nous présentons une étude détaillée de deux schémas de fraude communément expérimenté par les opérateurs de télécommunications.

Chapitre 6 décrit une fraude relativement récente nommée $Over\text{-}The\text{-}Top\ (OTT)\ bypass$ (La Figure A.2). Nous analysons d'abord les rouages internes de cette fraude et évaluons les techniques de détection et de mesure. Pour un examen plus approfondi de la prévalence et les effets de cette fraude sur le réseau de téléphonie et les utilisateurs, nous effectuons des expériences avec plus de 15000 appels de test ainsi qu'un utilisateur à grande échelle (Le Tableau A.1).

Nous montrons divers problèmes que l'$OTT\ bypass$ peut causer dans un réseau. En particulier, tout en étudiant l'$OTT\ Bypass$, nous avons observé la collision de plusieurs autres fraudes (Le Tableau A.2) et l'effet qu'a leur combinaison sur la qualité de l'établissement de l'appel et l'expérience utilisateur.

Pour cela, nous avons mesuré la différence de temps entre le téléphone destinataire sonnerie et l'appelant d'entendre la sonnerie. La figure A.3 montre si

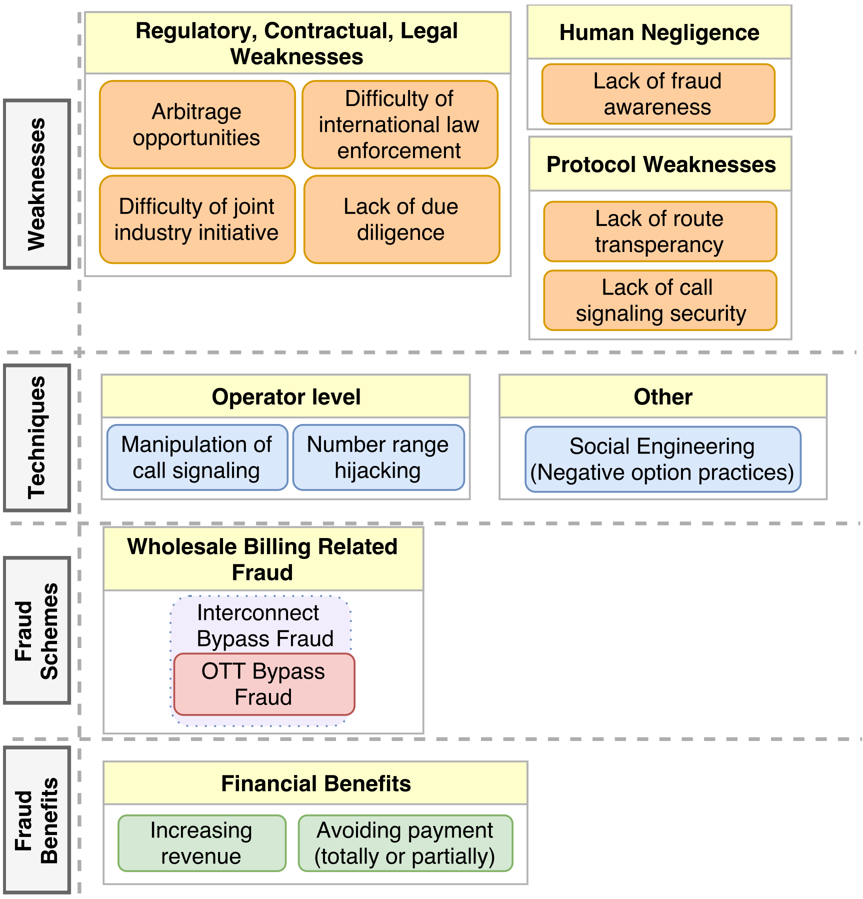


Figure A.2: OTT bypass dans notre taxonomie.

le téléphone de l'appelé commence à sonner d'abord, et l'appelant entend la sonnerie plus tard, la différence de temps de sonnerie devient un valeur négative. D'un autre côté, si l'appelant entend la sonnerie d'abord et Le téléphone de l'appelé commence à sonner plus tard, cette valeur sera positive. Idéalement, cela devrait être proche de 0, de sorte que l'appelant et l'appelé soient informés simultanément. Nous avons trouvé que c'est beaucoup plus élevé pour les appels OTT contournés que les appels normaux (La Figure A.4). Cela semble pour indiquer que le fournisseur OTT envoie une fausse sonnerie à l'appelant, avant le téléphone du destinataire commence à sonner. En d'autres termes, pendant la période 30-40 secondes de l'intervalle de différence de temps de sonnerie, l'appelant pense que le destinataire le téléphone sonne, mais le destinataire ne sera pas averti de cet appel. Comme un résultat, l'appelant peut laisser tomber l'appel avant que l'appelé soit au courant de l'appel ou ait le temps répondre. Cette pratique ne doit pas être confondue avec la supervision de fausses réponses fraude, car ici, même si l'appelant entend une sonnerie précoce, les appels ne

Table A.1: Tester les appels effectués pendant 8 mois d'expériences.

Origine	Nombre d'appels	Durée	Date
Mondial	1016	7 jours	Novembre '15
UK	134	3 jous	Mars '16
Germany	260; 2876	4; 68 days	Mars; Avril-Juin '16
Netherlands	1220	55 jours	Mai-Juin '16
Italy	3201	68 jours	Avril-Juin '16
Switzerland	3635	67 jours	Avril-Juin '16
Spain	1392	37 jours	Mai-Juin '16
Austria	49; 2006	3; 37 jours	Avril; Mai-Juin '16
Turkey	83	3 jours	Avril '16
Total	15,872	352 Jours d'expérience	8 mois

Table A.2: Combinaison de Simbox et OTT bypass.

	OTT Pas enregistré	OTT enregistré, En ligne
Appels normaux	38%	22%
Simbox bypass	62%	17%
OTT bypass	-	35%
Simbox + OTT bypass	-	26%

pas commencer à être chargé.

Nous avons aussi a montré que les schémas de fraude comme l'"OTT bypass" peuvent être très difficiles à détecter (et encore plus difficiles à prévenir), en raison de l'opacité des réseaux téléphoniques. Ce chapitre comprend le travail publié à la "ACM Conference on Computer and Communications Security (CCS)" en 2016 [SF16].

Dans le Chapitre 7, nous étudions le problème de longue date mais non résolu: "International Revenue Share Fraud (IRSF)". Ce système de fraude peut prendre plusieurs formes, en fonction de variantes de la fraude, des parties impliquées et les techniques de génération de trafic utilisées (La Figure A.5).

Similaire au chapitre précédent, nous décrire d'abord ce schéma de fraude en relation avec notre taxonomie, et expliquer défis pour le combattre. Plus tard, nous explorons l'écosystème de l'IRSF, en analysant les revendeurs de *numéros surtaxés internationaux* IPRN (International Premium Rate Number) et leurs portails de test fréquemment utilisé par les fraudeurs. Nous présentons nos observations sur plus de 150.000 numéros de tests de de numéros surtaxés que nous recueillons à partir de ces portails de tests. Notre ensemble de données comprend des numéros de tests de 198 pays et 458 opérateurs. Il montre que l'IRSF peut cibler une grande variété de pays, avec des coûts de terminaison d'appel variables. Une autre observation est que, aucun des numéros de test appartiennent à la légitime *Universal International Premium Rate Number (+979)* spécifié par l'ITU [Int17]. Ensuite, nous regardons les informations de

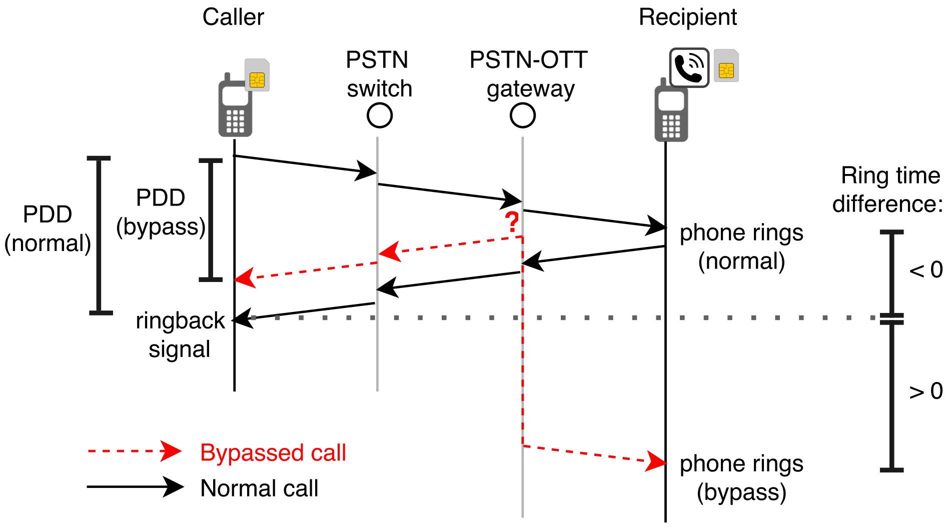


Figure A.3: Post Dial Delay (PDD) in a normal phone call and in a OTT bypassed phone call.

type pour ces numéros de test. Comme nous montrons dans le Tableau ??, les plages de numéros mobiles sont les plus fréquemment abusé. Enfin, nous proposons plusieurs fonctionnalités de numéros de téléphone qui pourraient être utiles détecter IRSF, en tirant parti des informations sur les numéros de test.

Table A.3: Types de numéros de test IPRN.

Type de numéro	%
Mobile	56
Fixé	15
Service supplémentaire	14
Pas alloué	14
Satellite	1

Dans la troisième partie de la thèse, nous nous concentrons sur le spam vocal, qui est un problème important pour les utilisateurs de téléphone.

Après une description du problème et un aperçu des études basées sur les honeypot (Chapitre 8), nous présentons “Lenny”, un chatbot et un honeypot à haute interaction, qui peut être utilisé pour se défendre contre divers types d'appels de spam. En utilisant 200 enregistrements d'appels ont été collectés lors d'un déploiement public de ce chatbot, nous analysons l'efficacité du chatbot avec une perspective d'analyse conversationnelle. Nous présentons également diverses observations sur les différents types d'appels de spam et discuter des défis dans l'utilisation généralisée des chatbots contre le spam vocal. Ce chapitre (Chapitre 9) est basé sur une publication dans le “Symposium on Usable Privacy

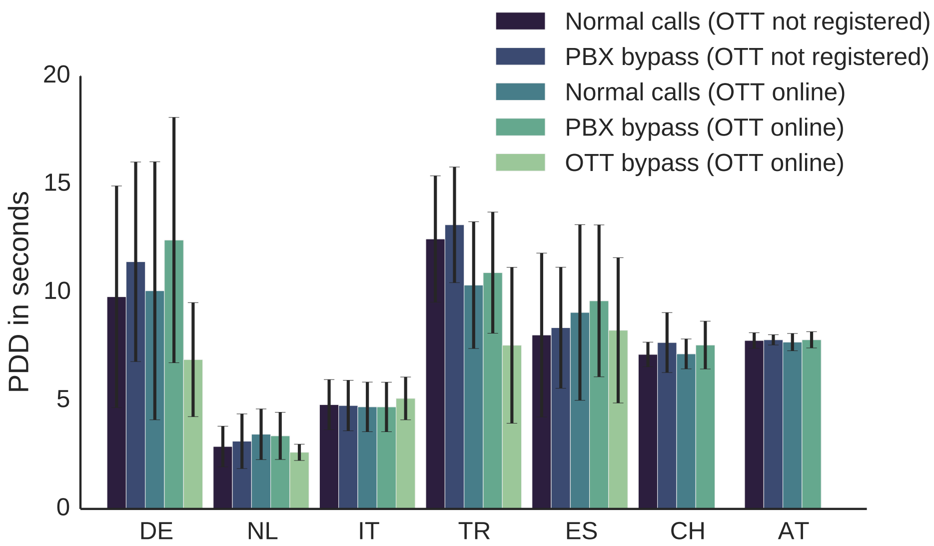


Figure A.4: PDD (avec Stdev), pour chaque pays fonction du type de bypass.

and Security (SOUPS)" 2017 [SRF17].

Dans la dernière partie, nous examinons le spam vocal, qui a été largement étudié dans la littérature, contrairement aux deux précédentes fraudes. Cependant, au lieu de se concentrer sur les techniques classiques de détection et de prévention du spam (telles que les listes noires, la réputation de l'appelant ou l'analyse du comportement [TDZA16a]), nous nous sommes concentrés sur l'utilisation des chatbots pour réduire les incitations financières des fraudeurs. Comme nous considérons les 'avantages' comme une partie fondamentale de notre définition de la fraude, nous croyons que les chatbots peuvent être combinés avec des mécanismes existants de détection et de prévention de la fraude, comme un moyen supplémentaire de ralentir le spam vocal.

Enfin, le Chapitre 10 conclut la thèse, avec une discussion des futures orientations de recherche possibles.

Conclusions

Cette thèse n'est qu'une première contribution à la recherche académique sous-explorée sur la fraude téléphonique. Nous croyons qu'il y a beaucoup de choses à explorer dans ce domaine. Ici, nous énumérons quelques suivis immédiats du travail présenté dans cette thèse, comme ainsi que d'autres directions intéressantes à suivre.

Une première idée pour le travail à venir serait de présenter la taxonomie de la fraude dans un manière plus formalisée. En particulier, un langage spécifique

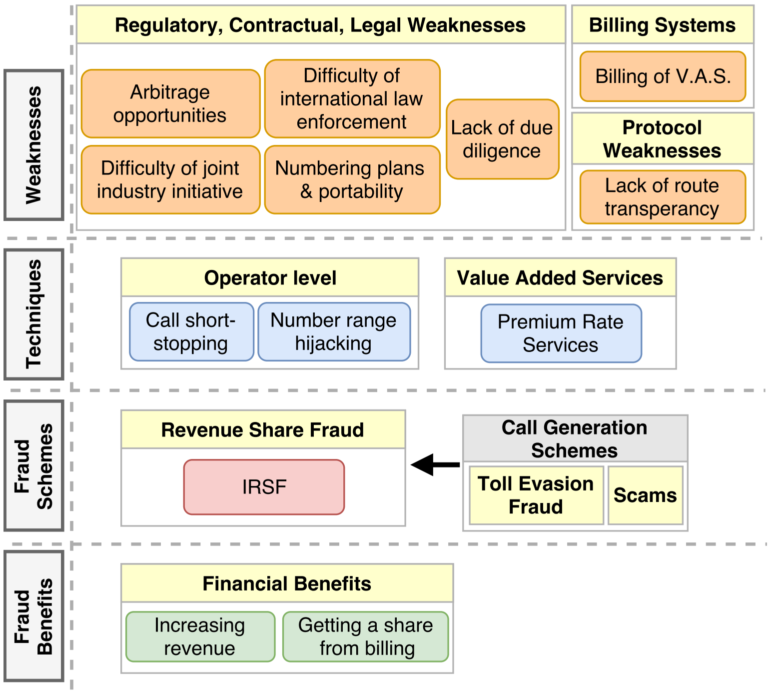


Figure A.5: IRSF dans notre taxonomie.

au domaine peut être défini pour exprimer formellement les relations entre les composants à chaque couche de la taxonomie. Avec cela, il serait possible de présenter l'information de façon crète: par exemple, la relation entre un schéma de fraude et une technique pourrait être défini/explicite, ou conditionnel/implicite. De plus, l'état de l'art techniques de défense à chaque niveau (faiblesses, techniques et schémas de fraude) peut être incorporé avec ce modèle formel.

La deuxième étape consisterait à remédier aux faiblesses que nous avons énumérées dans la taxonomie. En fait, certaines des faiblesses telles que l'absence d'identification de l'appelant ont été étudiée ces dernières années, mais le les solutions ne sont pas largement déployées en raison des défis pratiques et techniques, mais aussi en raison du manque d'incitations au déploiement. Par exemple, des solutions manipuler le canal audio peut être difficile à adopter pour les appareils de l'utilisateur final, bien qu'ils puissent être utilisés du côté de l'opérateur, ou par des centres d'appels (par exemple, des banques).

Un autre sujet à étudier serait le "niveau acceptable" de perte de fraude pour les opérateurs: Quand commencent-ils à investir dans des solutions de prévention / détection de la fraude? Quels sont leurs mécanismes de décision, quel est le montant de la perte de fraude non détectée? Tandis que les grands opérateurs peuvent faire des investissements importants dans la prévention de la fraude, petite Les opérateurs de taille ne peuvent généralement pas. Par conséquent, étudier la gestion optimale des fraudes Les politiques de développement pourraient être utiles. Pour cela, une approche de théorie des jeux pourrait être utilisé.

Avec la montée des dispositifs embarqués et la future technologie 5G, la fraude dans les données réseaux est susceptible de devenir plus important. Actuellement, "machine-to-machine SIM cards" et les services d'itinérance peuvent être intéressants à étudier.

Nous espérons que notre travail favorisera plus de travaux académique sur ce sujet et une fournira une aide précieuse pour comprendre l'efficacité et les implications des nouvelles contre-mesures.

Appendix B

Complete questionnaire and answers for the OTT bypass user study

User Experience on Communication Applications

How often do you use these applications for messaging (texting)?							
Answer Options	**Almost Never**	**Rarely**	**Sometimes**	**Often**	**Very Often**	**Rating Average**	**Response Count**
	52	133	481	2260	5565	4.55	8491
						answered question	**8491**
						skipped question	**54**

How often do you use these applications to make or receive calls?							
Answer Options	**Almost never**	**0-3 calls a week**	**5-7 calls a week**	**2-4 calls a day**	**More than 4 calls a day**	**Rating Average**	**Response Count**
	286	682	893	2533	4092	4.12	8486
						answered question	**8486**
						skipped question	**59**

For which of the following reasons do you use the communication applications most?		
Answer Options	**Response Percent**	**Response Count**
To communicate with people (friends/family/colleagues) in my country	71.6%	6076
To communicate with people (friends/family/colleagues) abroad	73.6%	6252
Other (please specify)	5.4%	455
	answered question	**8491**
	skipped question	**54**

Which network do you use most for internet connectivity on your smart phone?							
Answer Options	**Almost Never**	**Rarely**	**Sometimes**	**Often**	**Very Often**	**Rating Average**	**Response Count**
Data network (3G/4G)	775	339	1334	2749	1749	3.63	6946
Wi-Fi	768	196	586	2819	2473	3.88	6842
						answered question	**8500**
						skipped question	**45**

How often do you experience low call quality (such as distorted audio, latency, dropped calls, missing or wrong caller ID information) on those communication applications?							
Answer Options	**Almost Never**	**Rarely**	**Sometimes**	**Often**	**Very Often**	**Rating Average**	**Response Count**
	645	1767	4076	1775	208	2.90	8471
						answered question	**8471**
						skipped question	**74**

Note: As we do not mention the name of the bypassing OTT application, we will call it AppX.

If you use the AppX application, you can buy "AppX-out" credits to be able to call mobile and landline phone numbers from AppX. Did you know this "AppX-out" feature?		
Answer Options	**Response Percent**	**Response Count**
Yes	57.9%	4912
Yes, and I am using it	3.1%	266
No	37.2%	3157
I do not use the AppX application	1.8%	153
	answered question	**8488**
	skipped question	**57**

The AppX application also has an "AppX-bypass" option, which is enabled by default (this option can be found via the menu Settings->Calls and messages). Did you know this "AppX-bypass” option?		
Answer Options	**Response Percent**	**Response Count**
Yes	43.6%	3696
Yes, and I deactivated it	6.3%	532
No	48.3%	4096
I do not use the AppX application	1.9%	157
	answered question	**8481**
	skipped question	**64**

If "AppX-bypass" is enabled, you may receive regular incoming phone calls over AppX. Such calls are not initiated from the AppX application, but from a normal phone (mobile or landline).							
Answer Options	**Never**	**Rarely**	**Sometimes**	**Often**	**Very Often**	**Rating Average**	**Response Count**
Do you detect such Calls?	6017	1128	936	230	139	1.50	8450
						answered question	**8450**
						skipped question	**95**

Did you detect any calling anomalies with the AppX application?	
Answer Options	**Response Count**
	6245
answered question	**6245**
skipped question	**2300**

AppX-bypass option has the following consequences: - Quality of your calls may decrease - You may pay for data usage for incoming calls - AppX profits from your incoming calls, whereas your operator (and your country) incurs financial losses. Do you consider opting-out from AppX-bypass option?		
Answer Options	**Response Percent**	**Response Count**
Yes	46.5%	3850
No	53.5%	4428
	answered question	**8278**
	skipped question	**267**

What is your age?		
Answer Options	**Response Percent**	**Response Count**
Less than 18 years old	9.4%	794
18 to 28 years old	58.2%	4930
29 to 39 years old	22.3%	1890
40 to 50 years old	7.5%	639
51 to 61 years old	2.1%	180
Over 61 years old	0.5%	44
	answered question	**8477**
	skipped question	**68**

What is your gender?		
Answer Options	**Response Percent**	**Response Count**
Male	70.3%	5944
Female	28.3%	2394
I prefer not to answer	1.4%	117
	answered question	**8455**
	skipped question	**90**

Appendix C

Rough transcript of a telemarketing call

```
[00:00:00] Lenny: hello: thi- this is Lenny!
[00:00:03] Telemarketer: lenny, i'm looking for mr.
   [00:00:04 sound cut]
[00:00:06] Lenny: uh-- sso- sorry, I'b- I can barely
   hear you there?
[00:00:13] Telemarketer: homeowner.
[00:00:15] Lenny: ye- yes yes yes.
[00:00:19] Telemarketer: mr. [00:00:19 sound cut] we're
    giving free estimates for any work you need on your
    house. were you thinking about having any projects?
    a little craning driveway, roof work, anything you
   need done. we'll give you a free estimate.
[00:00:31] Lenny: oh good, yes, yes, yes.
[00:00:34] Telemarketer: what would you like to have
   done? what were you thinking about? anything around
   the house?
[00:00:39] Lenny: uh yes, yes, uh::uh, someone, someone
    did- did say last week or some- one did call last
   week about the same (.) thing, wa-was that, was that
   , you?
[00:00:50] Telemarketer: no, sir. i've might have been
   in another company. what was it that you were doing?
[00:00:55] Lenny: ye-yes. ss- sorry, what- wa- what was
    your name again?
[00:01:00] Telemarketer: yes. what were you thinking
   about having done?
[00:01:04] Lenny: well, it- it it's funny that you
```

should call, because, my third eldest larissa, uhh, she, she was talking about this. (.) u:h #just this last week and .hh you you know, sh– she is–, she is very smart, I would– I would give her that, because, you know she was the first in the family, to go to the university, and she passed with distinctions, you know we're– we're all quite proud of her yes yes, so uhh:: yes she was saying that I should, look, you know, get into the, look into this sort of thing. uhh so, what more can you tell me about it?

[00:01:14] Telemarketer: #mm-hmm. okay. alright. well, good, good. [inaudible 00:01:33] so you're very proud. okay.# well, we are full-service construction company. we do everything from the roof to the foundation. we've been in business for over 32 years. we're licensed, bonded, and insured, and we have plenty plenty of references if you need them. where you thinking about doing any work inside or outside?

[00:02:05] Lenny: I: I am sorry, I, I (.) couldn't quite catch you th–, catch you there. wha–what was that again?

[00:02:12] Telemarketer: where you thinking about doing work inside or outside?

[00:02:17] Lenny: uh. ( ) the: (.) ss sorry, aw again?

[00:02:23] Telemarketer: [laughs] where you going to do work inside or outside?

[00:02:28] Lenny: cou–could you say that again– again please?

[00:02:32] Telemarketer: i tell you what, i'm going to send one of my guys over to your place. you're at six [00:02:37 sound cut]. he can sit down with you. he'll discuss everything about our services. he'll give you our coupon. it's up to 50% off. i'll have him there, let's see it's 12:30, i can get him over there by 2:30. are you and your wife be home at 2:30? we'll come by, show show you all our stuff and you can let us know what you wanna do then. okay.

[00:02:59] Lenny: yes, yes, yes...

[00:03:01] Telemarketer: that makes sense?

[00:03:03] Lenny: sorry uhh, which company did you say you were calling from again?

[00:03:08] Telemarketer: wise. w–i–s–e. it'd be very wise for you to use our services. that's our commercial.

[00:03:15] Lenny: well, you know. here's– here's the thing because the last time that I—that someone called up, uh #and spoke to me on the phone, I got in quite a bit of trouble from—with the people here because I went for something that I shouldn't have. uh, I probably shouldn't be–be telling you that. but um, yes, I–I think m–my– my eldest Rachel, she–she uh, uh would–wouldn't speak to me for a week, now, you know that— that happens, you know but uh it bit—that really hurt and–and–and sometimes in the family you know these–these things are quite important you know. they're more important than uh—uh any, you know, job or–or— Phone call or–or—what– wha— whatever it is.
[00:03:22] Telemarketer: #mm–hmm. umm–hmm. umm–hmm. that's okay? mm–hmm. oh boy she got mad at you?# of course, family is always important. now let me asked you. uh, is three o'clock going to be good for you and your wife?
[00:04:11] Lenny: well yeah, since—since you–you put it that way, I mean you–you've been quite friendly and straightforward with me here. #um, h–hello?
[00:04:20] Telemarketer: #great. very good.# yes, i'm here. thank you.
[00:04:25] Lenny: hello? #are you there?
[00:04:25] Telemarketer: #i'm just saying, thank you.# yes sir, i'm here.
[00:04:30] Lenny: #oh yes— s–sorry. Is–is—I have a—have a bit of a—bit of a problem with this phone——and–and my hearing is not so good. um, yes,# uh, w–wha– sorry, wha–what were you saying again?
[00:04:30] Telemarketer: #hello? that's okay. that's okay. no problem.# i just saying that it was a pleasure speaking with you as well and we're going to have my guy come out and talk to you and your wife about three o'clock. i just wanna be able to let him know what it is that you guys were thinking about doing on the house. was it painting or kitchen, bathroom remodeling? what was it that you guys wanted to have look at?
[00:05:05] Lenny: well, you know with–with the world finances the way they are I know you know we're not–we're not allowed to spend as much as–as what we were. [stammering] how–how:: how–how–how is this

going to uhh h–how is this going to work?
[00:05:23] Telemarketer: well, we'll have to come out and see what the job is first before we could talk about any form of uh, money but, uh, you won't have to worry about that until we see what it is that you need done.
[00:05:36] Lenny: #well,that–that–that does sound good. I mean, you–you have been very patient with an old man here and uh [laugh] Bt–it's uh— yeah I mean, uh, it's–it's something that–that I've been told that I should be looking at— uh–, my third eldest laris– larissa, she uh, I think I mentioned larissa before (.) yes–yes she uh— she says th–that I should be going for the—something like this but uh, it's just a matter of what, you know, what–what is most appropriate for—for uhh th–the time and I guess what not. sorry could you— just hang on# for one second here? hang on. [ducks quacking in the background]
[00:05:36] Telemarketer: #what it is that you are thinking of doing? oh, no problem , that's— that's our job. i mean your purpose so. yes what was she said— she told you to have done? mm–hmm— i got you .#
[00:06:32] Lenny: yeah. so–sorry #about that. uh— s– sorry# wha–what were you saying there again?
[00:06:33] Telemarketer: #yes, sir. that's okay.# i was asking what work that you need done?
[00:06:43] Lenny: uh yes, yes, uh::uh, someone, someone did– did say last week or some– one did call last week about the same (.) thing, wa–was that, was that, you?
[00:06:54] Telemarketer: no sir. that may have been another company.
[00:06:58] Lenny: ye–yes. ss– sorry, what– wa– what was your name again?
[00:07:03] Telemarketer: my name is michael.
[00:07:06] Lenny: well, it– it it's funny that you should call, because, my third eldest larissa, #uhh, she, she was talking about this. (.) u:h just this last week and .hh you you know, sh– she is–, she is very smart, I would– I would give her that, because, you know she was the first in the family, to go to the university, and she passed with distinctions,

you know we're— we're all quite proud of her yes yes , so uhh:: yes she was saying that I should, look, you know, get into the, look into this sort of thing . uhh so, what more# can you tell me about it ?
[00:07:12] Telemarketer: #mm-hmm, mm-hmm— what was she talking about? right. what was she talking about? what was she talking about? what was she talking about? what were she talking about mr. [00:07:32 sound cut]? looking to what sort of thing mr. [00:07:43 sound cut] ?# what would she like to have done mr.[00:07:49 sound cut]?
[00:07:51] Lenny: I: I am sorry, I, I (.) couldn't quite catch you th–, catch you there. wha–what was that again?
[00:07:57] Telemarketer: what do you want done?
[00:08:00] Lenny: uh. ( ) the: (.) ss sorry, aw again?
[00:08:06] Telemarketer: well, i guess we'll gonna be here a while. what did she want done?
[00:08:11] Lenny: cou–could you #say that again– again please?
[00:08:12] Telemarketer: #i mean bathrooms.# so do you need your bathroom redone?
[00:08:19] Lenny: #yes, yes, yes...#
[00:08:19] Telemarketer: #maybe your kitchen# how about the drive way? maybe even the garage? have you done any work on your roof?
[00:08:27] Lenny : sorry uhh, which company did you say you were calling from again?
[00:08:32] Telemarketer: i didn't say, uh, the thing is we were tying to see what did you need done.
[00:08:39] Lenny: #well, you know. here's– here's the thing because the last time that I—that someone called up, uh and spoke to me on the phone, I got in quite a bit of trouble from—with the people here because I went for something that I shouldn't have. uh, I probably shouldn't be–be telling you that. but um, yes, I–I think m-my– my eldest Rachel, she–she uh, uh would–wouldn't speak to me for a week, now, you know that— that happens, you know but uh it bit —that really hurt and–and–and sometimes in the family you know these–these things are quite important you know. they're more important than uh— uh any, you know, job or–or— Phone call or–or— what– wha— whatever it is.#

[00:08:39] Telemarketer: #although i love having this conversation. i get paid by the hours, so the longer i sit, the longer i talk with you, the better um, yeah, right. um, um, how often do you do this? [laughs] this is so much fun. i— i've never seen anybody have their own routine over the phone. this is quite cool since both of us are going to talk. now i'm thinking this is maybe recording because you can't hear anything that i'm saying to you at this point. so we might as well just go ahead and do this over.# so now you're gonna ask me, "what did i say? i didn't hear you. would you repeat that?"
[00:09:31] Lenny: well yeah, since—since you–you put it that way, I mean you–you've been quite friendly and straightforward with me here. um, h–hello?
[00:09:45] Lenny: hello? are you there? oh yes— s–sorry. Is–is—I have a— have a bit of a—bit of a problem with this phone— —and–and my hearing is not so good. um—#um, yes, uh, w–wha– sorry, wha–what were you saying again?
[00:09:59] Telemarketer: #i ran into a building, that's not—# did you hear them?
[00:10:15] Lenny : well, you know with–with the world finances the way they are I know you know we're not–we're not allowed to spend as much as–as what #we were. [stammering] how–how:: how–how–how is this going to uhh h–how is this going to work?
[00:10:29] Telemarketer: #[laughs] this is great.#
[00:10:30] Lenny: h–how is this going to work? hello? are you there?uh yes— s–sorry wha–what were you saying there again?
[00:11:16] [END OF AUDIO]

Appendix D

Rough transcript of a scam call

```
[00:00:00] Lenny: hello: thi– this is Lenny!
[00:00:04] Adam: yeah mr. lenny, you have been chosen
   to get a lower interest rate, so i believe you have
   pressed one to get a lower interest rate right?
[00:00:13] Lenny: uh–– sso– sorry, I'b– I can barely
   hear you there?
[00:00:17] Adam: i'm saying so i believe you have
   pressed one to get a lower interest rate, right?
[00:00:24] Lenny: ye– yes yes yes
[00:00:26] Adam: okay, the interest you're paying at
   the moment is 19.9, right?
[00:00:32] Lenny: oh good, yes, yes, yes.
[00:00:34] Adam: and we are going to drop that down to
   less than 10% on this same call okay?
[00:00:40] Lenny: uh yes, yes, uh::uh, someone, someone
    did– did say last week or some– one did call last
   week about the same (.) thing, wa–was that, was that
   , you?
[00:00:50] Adam: oh okay, and did they provide you the
   low interest?
[00:00:56] Lenny: ye–yes. ss– sorry, what– wa– what was
    your name again?
[00:01:01] Adam: sir i'm saying my name is adam, adam
   chaw and i'm saying did they provide you the lower
   interest?
[00:01:09] Lenny: well, it– it it's funny that you
   should call, because, my third eldest larissa, uhh,
```

she, she was talking about this. (.) u:h just this last week and .hh you you know, sh– she is–, she is very smart, I would– I would give her that, because, you know she was the first in the family, to go to the university, #and she passed with distinctions, you know we're– we're all quite proud of her yes yes, so uhh:: yes she was saying that I should, look, you know, get into the, look into this sort of thing. uhh so, what more can you tell me about it?

[00:01:29] Adam: #yeah# so as you know today you are getting this call from low interest rate department working for the head office of visa and mastercard and you have been chosen only because of your good payment history. for the past six to seven months, you have been making your payments on time, right? you always try to make more the minimum payments right?

[00:02:10] Lenny: I: I am sorry, I, I (.) couldn't quite catch you th–, catch you# there. wha–what was that again?

[00:02:13] Adam: #you always try to make more than # the minimum payments, right?

[00:02:18] Lenny: uh. ( ) the: (.) ss sorry, aw again?

[00:02:23] Adam: you always try to make more than the minimum payments, correct sir?

[00:02:28] Lenny: cou–could you say that again– again please?

[00:02:31] Adam: sir, i'm asking you, you always try to make your payments on time, right?

[00:02:37] Lenny: yes, yes, yes...

[00:02:39] Adam: okay, and today that's the reason you're getting this call and that's the reason we are going to provide to lo—lower interest rate because of your good payment history, okay.

[00:02:50] Lenny: sorry uh, which company did you say you were calling from again?

[00:02:54] Adam: sir, we are working for the head office of visa and mastercard, working with the head office of visa and mastercard and that's the reason we are going to provide you the low interest, okay. so grab your card on hand and verify me the membership number starting from five.

[00:03:09] Lenny: well, you know. here's– here's the thing because the last time that I—that someone called up, uh and spoke to me on the phone, I got in quite a bit of trouble from—with the people here because I went for something that I shouldn't have. uh, I probably shouldn't be–be telling you that. but um, yes, I–I think m–my– my eldest Rachel, she–she uh, uh would–wouldn't speak to me for a week, now, you know that— that happens, you know# but uh it bit—that really hurt and–and–and sometimes in the family you know these–these things are quite important you know. they're more important #than uh —uh any, you know, job or–or— Phone call or–or— what– wha— whatever it is.

[00:03:40] Adam: #you tell me your eldest—the daughter's name for some correction, yeah mr. lenny i understand that, i understand mr. lenny, that today we are going to provide you the lower interest # on this same call, so i need you to grab your mastercard on hand and verify me the membership number starting from five, can you do that?

[00:04:07] Lenny: well yeah, since–#–since you–you put it that way, I mean you–you've been quite friendly and straightforward with me here. um, #h–hello?

[00:04:08] Adam: #can you grab you card and verify me the membership number? # yes, yeah sir.

[00:04:20] Lenny: hello? are you there?

[00:04:24] Adam: yes sir, i'm here. grab #your card and verify me the membership number starting from five.

[00:04:26] Lenny: #oh yes— s–sorry. Is–is—I have a— have a bit of a—bit of a problem with this phone— —and–and my hearing is not so good. #um, yes, uh, w–wha– sorry, wha–what were you saying again?

[00:04:34] Adam: #[laugh] no problem, no problem.# grab your card sir, your mastercard and verify me the membership number starting from five.

[00:04:47] Lenny: well, you know with–with the world finances the way they are I know you know we're not–we're not allowed to spend as much as–as what we were. #[stammering] how–how:: how–how–how is this going to uhh h–how is this going to work?

[00:04:56] Adam: #yeah sir, i understand, i understand that completely and that's the reason i want to provide you the lower interest on your mastercard. # sir can you grab your mastercard?

[00:05:07] Lenny: well, that–that–that does sound good.

I mean, you–you have been very patient with an old man here and uh [laugh] it–it's uh— yeah I mean, uh, it's–it's something that–that I've been told that I should be looking at— #uh–, my third eldest laris–larissa, #she uh, I think I mentioned larissa before (.) yes–yes she uh— she says th–that I should be going for the—something like this but uh, it's just a matter of what, you know, what–what is most appropriate for—for uhh th–the time and I guess what not. sorry could you— just hang on for one second here? hang on. [ducks quacking in the background]

[00:05:19] Adam: #okay, okay yeah so are you grabbing you card sir or should i hang up?#

[00:05:34] [END OF AUDIO]

List of Figures

List of Tables

List of Publications 2014—2017

Conference Publications

1. M. Sahin, A. Francillon, P. Gupta, and M. Ahamad. SOK: Fraud in telephony networks. In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroSP'17)*.
2. M. Sahin and A. Francillon. Over-The-Top bypass: Study of a recent telephony fraud. In *Proceedings of the 23rd ACM conference on Computer and communications security (CCS'16)*.
3. M. Sahin, M. Relieu, A. Francillon. Using chatbots against voice spam: Analyzing Lenny's effectiveness. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS'17)*.

Invited Presentations

1. Participation to the OTT Bypass Panel at RAG (Risk & Assurance Group) meeting, 2017
2. Invited talk at TROOPERS Telco Security Day, 2017
3. Presentations at M3AAWG Voice and Telephony Abuse SIG Workshops, 2014, 2015 & 2016

Teaching

1. Guest lecture as part of Aurélien Francillon's course *"System Security"*: *Fraud in telephony networks*, EURECOM, 2016.

Bibliography

[Abi] Ability, *3G-Cat, Smallest & Smartest 3G IMSI/IMEI/TMSI Catcher*, Official page: http://www.interceptors.com/intercept-solutions/detects-parameters-3G-networks.html Wikileaks document: https://www.wikileaks.org/spyfiles/files/0/80_ABILITY-GSM_3G_Intercept.pdf. 24, 29

[All] Allround, *NRTRDE - Near Real Time Roaming Data Exchange Buyer's Guide*, whitepaper available at http://www.allround.net/images/stories/pdf/NRTRDE%20Buyers%20guide.pdf. 25

[Alt] *Alternative calling procedures: Background and trends*, ITU, World Radiocommunication Conference, 2012. 24, 34

[And08] Ross J. Anderson, *Security engineering: A guide to building dependable distributed systems*, 2 ed., Wiley Publishing, 2008. 16, 27, 31, 33

[Apv10] Axelle Apvrille, *WinCE/Terdial or Impunity for Dialers*, Fortinet blog, May 2010. 31, 36, 86, 135

[ara16] *Insight into new sim box types*, white paper, april 2016. 34

[Arm17] Keith Armstrong, *Conversational banking will transform the financial services industry*, available at: https://thefinancialbrand.com/63772/conversational-banking-chatbots-bots-ai-messaging/, February 2017. 112

[Ask] Dan Askin, *The free cruise offer: Scam or legit?*, http://www.cruisecritic.com/articles.cfm?ID=1185Cruis. 38

[Ast] *Asterisk*, http://www.asterisk.org/. 7, 31

[ast08] *Astycrapper v.03*, available at: http://web.archive.org/web/20081030013832/http://www.linuxsystems.com.au:80/astycrapper/, October 2008. 110

[Ban] Amanda Banach, *Outbound telemarketing strategies*, available at: http://smallbusiness.chron.com/outbound-telemarketing-strategies-24269.html. 118

[BAP07] Vijay Balasubramaniyan, Mustaque Ahamad, and Haesun Park, *Callrank: Combating SPIT using call duration, social networks and global reputation.*, 4th Conference on Email and Anti-Spam, CEAS 2007, 01 2007. 46

[Bar14] Matan Barth, *M. barth, call termination on ott network, patent wo 2014087269 a4*, Patent WO 2014087269 A4, 2014, Patent WO 2014087269 A4. 60

[BBB+06] Steven Michael Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson, and John Treichler, *Security implications of applying the communications assistance to law enforcement act to voice over IP*. 23

[BC17] Cyril Brosset and Gregory Caret, *Le demarchage telephonique et vous*, available at: https://www.quechoisir.org, January 2017. 102, 131

[BCF11] S. Bradner, L. Conroy, and K. Fujiwara, *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, RFC 6116, 2011. 134

[BCI+15] Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna, *What the App is That? Deception and Countermeasures in the Android User Interface*, Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2015. 135

[BDD15] Michaela Beals, Marguerite DeLiema, and Martha Deevy, *Framework for a taxonomy of fraud*, Stanford Center on Longevity, July 2015, http://fraudresearchcenter.org/wp-content/uploads/2015/07/FFRC_Taxonomy_FullReport_7-22-15.pdf. 17

[Ber12] *Article 28(2) Universal Service Directive: A harmonised BEREC cooperation process - Consultation paper*, Body of European Regulators of Electronic Communications, September 2012. 25, 84

[BFMR10] K. Butler, T. Farley, P. Mcdaniel, and J. Rexford, *A survey of BGP security issues and solutions*, Proceedings of the IEEE (2010). 26

[BGG+16] Marco Balduzzi, Payas Gupta, Lion Gu, Debin Gao, and Mustaque Ahamad, *Mobipot: Understanding mobile telephony threats with honeycards*, Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ASIA CCS '16, ACM, 2016. 17, 103, 104

[Big12] Chris Bignell, *The different frauds: Interconnect bypass*, Revector, Fraud for thought blog, August 2012. 9

[Bla13] Simon Blackburn, *The top 10 types of phone dialer and automated dialing technology*, May 2013. 31

[BM15] Mahanagar Doorsanchar Bhawan and Jawahar Lal Nehru Marg, *Consultation paper on regulatory framework for over-the-top (OTT) services*, Telecom Regulatory Authority of India, March 2015. 58

[BMM+07] Dario Bonfiglio, Marco Mellia, Michela Meo, Dario Rossi, and Paolo Tofanelli, *Revealing skype traffic: When randomness plays with you*, SIGCOMM (2007). 65, 80

[Bol16] Doug Bolton, *Meet Lenny - the Internet's favourite telemarketer-tricking robot*, The Independent, Thursday 14 January 2016 http://www.independent.co.uk/life-style/gadgets-and-tech/news/lenny-telemarketer-bot-robot-prank-a6813081.html, 2016. 113

[Bos15] Robert Bostelaar, *Lenny the call-bot tortures telemarketers: just ask the woman calling on behalf of Pierre Poilievre*, available at: http://news.nationalpost.com/, August 2015. 110

[BPA+10] Vijay A. Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael T. Hunter, and Patrick Traynor, *Pindr0p: Using single-ended audio features to determine call provenance*, CCS '10, ACM, 2010, pp. 109–120. 30, 44, 47, 80, 103

[Bro14] Eileen Brown, *Spam phone calls cost US small businesses half a billion dollars in lost productivity*, available at: http://www.zdnet.com, February 2014. 131

[BS+08] David A Burgess, Harvind S Samra, et al., *The OpenBTS Project*, 2008, http://openbts.org. 29

[bsm] *BSMilano, Worldwide National Numbering Plans Collection*, http://bsmilano.it/. 67

[Bsw11] *Roaming fraud: The importance of real-time data exchange and analysis*, http://bswan.org/roaming_fraud.asp, September 2011. 86

[Bsw12] *International revenue share fraud: Are we winning the battle against telecom pirates?*, Black Swan Telecom Journal, November 2012. 27, 84, 86

[Bur16] Alexandra Burlacu, *AT&T starts robocalls crackdown with Call Protect service to block spam phone calls: How it works*, available at: http://www.techtimes.com, December 2016. 102

[BVW10] Richard A. Becker, Chris Volinsky, and Allan R. Wilks, *Fraud detection in telecommunications: History and lessons learned*, Technometrics **52** (2010), no. 1, 20–33. 16, 44

[cal17a] *Call center pricing*, available at: https://www.worldwidecallcenters.com/call-center-pricing/, 2017. 109

[cal17b] *Outsource2india's call center pricing*, available at: https://www.outsource2india.com/callcenter/pricing.asp, 2017. 109

[Cam17] Dell Cameron, *Major leak exposes 400k recorded telemarketing calls, thousands of credit card numbers*, available at: http://www.dailydot.com/layer8/telemarking-breach-calls-leaked-vici-marketing-kromtech/?tw=share, January 2017. 2, 139

[Cas17] Carlos Castillo, *Trojanized photo app on Google Play signs up users for premium services*, McAfee Labs, January 2017. 31

[CB13] Davide Canali and Davide Balzarotti, *Behind the scenes of online attacks: an analysis of exploitation behaviors on the web*, NDSS 2013, 20th Annual Network and Distributed System Security Symposium, February 24-27, 2013, San Diego, CA, United States, 02 2013. 47

[ccm17] *International and fraud databases*, http://www.ccmi.com/international-tariff-databases, 2017. 95

[CE13] M. Collier and D. Endler, *Hacking exposed unified communications & voip security secrets & solutions, second edition*, Hacking Exposed, McGraw-Hill Education, 2013. 17, 26, 31, 32, 37, 38

[CFC15] *2015 Global Fraud Loss Survey*, http://cfca.org/fraudlosssurvey, September 2015. 1, 59, 86, 138

[cfc17] *CFCA International Revenue Fraud Number Database*, www.cfca.org, 2017. 95

[CFSW12] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner, *Measuring user confidence in smartphone security and privacy*, SOUPS '12, 2012. 58

[cha] *Chatbot conference*, https://chatbotconf.com/. 112

[CIB+13] Andrei Costin, Jelena Isachenkova, Marco Balduzzi, Aurelien Francillon, and Davide Balzarotti, *The role of phone numbers in understanding cyber-crime schemes*, PST, July 2013. 37

[Cla07] Richard Clayton, *Can {CLI} be trusted?*, Information Security Technical Report (2007). 29

[CNA] *CNAM partner revenue sharing FAQ*, Stratics Networks, http://straticsnetworks.com/cnam-partner-revenue-sharing/. 39, 40

[Col99] Michael Collins, *Telecommunications crime - part 1*, Comput. Secur. (1999), no. 7, 577–586. 16, 32

[Col04] Mark D. Collier, *Enterprise telecom security threats*, SecureLogix Whitepaper, 2004. 29

[Col08] E. Coll, *Telecom 101: Third edition*, Teracom Training Institute, 2008. 59, 72

[Cro13] Jordan Crook, *Viber is testing new revenue models, value-add features by integrating with traditional telephony*, TechCrunch, July 2013, http://techcrunch.com. 56, 60

[CYJ+13] Yao Cheng, Lingyun Ying, Sibei Jiao, Purui Su, and Dengguo Feng, *Bind your phone number with caution: Automated user profiling through address book matching on smartphone*, AsiaCCS'13, 2013. 64

[Dav] Kevin Davis, *CNAM revenue sharing - caller ID management*, http://www.callcentersindia.com/showall-orig.php?value1=85430_CNAM_Revenue_Sharing_-_Caller_ID_Management. 39, 40

[Dav08] Stuart Davies, *Report on number hijacking*, APT Report, July 2008. 26

[Dav12] ———, *Numbering misuse and fraud*, ITU Seminar, May 2012. 26, 86

[DCNF11] Rodrigo Do Carmo, Mohamed Nassar, and Olivier Festor, *Artemisa: An open-source honeypot back-end to support security in voip domains*, Integrated Network Management (IM), 2011

IFIP/IEEE International Symposium on, IEEE, 2011, pp. 361–368. 48

[DH92] Paul Drew and John Heritage, Talk at work: interaction in institutional settings, Cambridge University Press, 1992. 130

[DH05] Lee Dryburgh and Jeff Hewett, *Signaling system no. 7 (ss7/c7): protocol, architecture, and services*, Cisco press, 2005. 6, 23, 24, 29, 43

[DPK+14] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl, *IMSI-catch me if you can: IMSI-catcher-catchers*, ACSAC, 2014. 29

[DPW] Adrian Dabrowski, Georg Petzl, and Edgar Weippl, *The messenger shoots back: Network operator based IMSI catcher detection*, RAID'16. 29

[E1697] *The international public telecommunications numbering plan*, ITU-T Recommendation E.164, 1997. 24, 60, 88

[EC06] D. Endler and M. Collier, *Hacking exposed voip: Voice over ip security secrets & solutions*, 2006. 24, 29

[ECC06] *Consumer abuses and fraud issues relating to high tariff services*, Electronic Communications Committee (ECC) report 86, 2006. 28, 83, 86

[EIS13] AbdikarimHussein Elmi, Subariah Ibrahim, and Roselina Sallehuddin, *Detecting SIM box fraud using neural network*, IT Convergence and Security, 2013. 31, 35, 45, 80

[Ele03] Electronic Communications Committee, *ECC report 28: Accounting rates and settlements evolution*, March 2003. 9

[eMa15] eMarketer, *Digital content and advertising key revenue generators for messaging apps*, emarketer, November 2015, http://www.emarketer.com. 55, 56

[Eng14] Tobias Engel, *SS7: Locate. Track. Manipulate.*, Talk at 31st Chaos Communication Congress, December 2014. 28, 37

[EP06] Sven Ehlert and Sandrine Petgang, *Analysis and signature of skype voip session traffic*, 2006. 65

[ES00] Tony Eyers and Henning Schulzrinne, *Predicting internet telephony call setup delay*, First IP Telephony Workshop, 2000. 72

[ES12] Michael E. Edge and Pedro R. Falcone Sampaio, *The design of ffml: A rule-based policy modelling language for proactive fraud management in financial data streams*, Expert Systems with Applications (2012). 17

[ETS] ETSI/3GPP, *Digital cellular telecommunications system (phase 2+); universal mobile telecommunications system (umts); customised applications for mobile network enhanced logic (camel) phase x; camel application part (cap) specification (3gpp ts 29.078 version 12.0.0 release 12)*. 8

[Ett05] Matt Ettus, *USRP User's and Developer's Guide*, Ettus Research LLC (2005). 29

[Fad13] Firdaus Fadzil, *Illegal bypass for international calls: Industry position*, http://www.slideshare.net/firdausf1/sim-box-issue, 2013. 34

[FB14] Casey Fiesler and Amy Bruckman, *Copyright terms in online creative communities*, CHI, 2014. 58

[FCC] *Cramming-unauthorized charges on your phone bill*, Federal Communications Commission (FCC). 33

[FCC14] *Traffic pumping*, Federal Communications Commission Encyclopedia, September 2014. 36

[Fed15a] Federal Communications Commission, *FCC robocall and caller ID spoofing workshop*, Sept 2015, Video recording available at https://www.fcc.gov/events/workshop-focus-robocall-blocking-and-caller-id-spoofing. 17, 29, 102

[Fed15b] Federal Trade Commission, *Consumer Sentinel Network Reports*, available at: https://www.ftc.gov/enforcement/consumer-sentinel-network/reports, 2008 to 2015. 101

[Fed15c] ______, *Robocalls: Humanity strikes back*, 2015, Available at https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back. 102

[Fed16a] ______, *National Do Not Call Registry Data Book FY 2016*, December 2016. 1, 102, 109, 138

[Fed16b] ______, *Q&A for Telemarketers and Sellers About DNC Provisions in TSR*, August 2016. 102

[Fis11] Fisher Investments, *Fisher investments on telecom*, Wiley, 2011. 58

[Flo15] Flowroute Inc., *What is CNAM and how can it work for your business?*, December 2015. 28

[For15] Simon Forge, *The future of global telecommunications in view of the growth of OTT services: expected impacts on usage and prices*, ITU/BDT Regional Economic and Financial Forum of Telecommunications/ICTs for Latin America and the Caribbean, April 2015, https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0421-BS-Economic/1_1.pdf. 6

[fra16] *Fraudstrike data sheet*, http://www.fraudstrike.com/New_FraudStrike_Data_Sheet_v3_1_.pdf, 2016. 95

[Fre] *Conference for free anywhere, anytime!*, https://www.freeconferencecall.com/. 27

[FS11] Hamid Farvaresh and Mohammad Mehdi Sepehri, *A data mining framework for detecting subscription fraud in telecommunication*, Eng. Appl. Artif. Intell. **24** (2011), no. 1, 182–194. 32

[Fse12] *You will be billed $90,000 for this call 3: F-secure discloses mobile app virus attacks*, Privacy-PC.com news, March 2012. 86

[Ftc09] *Negative option marketing workshop report*, Federal Trade Commission, January 2009. 33

[ftc16] *Complying with the telemarketing sales rule*, FTC Tips and advice, June 2016. 38

[FZS08] E. P. Freire, A. Ziviani, and R. M. Salles, *Detecting skype flows in web traffic*, NOMS 2008, April 2008. 65, 80

[GAC+14] Payas Gupta, Mustaque Ahamad, Jonathan Curtis, Vijay Balasubramaniyan, and Alex Bobotek, *M3AAWG Telephony Honeypots: Benefits and Deployment Options*, 2014. 48

[Gal17] SEAN Gallagher, *"You took so much time to joke me"-two hours trolling a Windows support scammer*, available at: https://arstechnica.com, January 2017. 110

[Gar67] Harold Garfinkel, *Studies in ethnomethodology*, Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1967. 112, 132

[Gau12] S Gauci, *Sipvicious, tools for auditing SIP based VoIP systems*, Apr 2012. 30

[GDK+06] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, K. S. Ehlert, and D. Sisalem, *Survey of security vulnerabilities in session initiation protocol*, Commun. Surveys Tuts. **8** (2006), no. 3, 68–81. 29

[GGAK15] Srishti Gupta, Payas Gupta, Mustaque Ahamad, and Ponnurangam Kumaraguru, *Abusing phone numbers and cross-application features for crafting targeted attacks*, CoRR **abs/1512.07330** (2015). 58, 64

[GH99] Phil Gosset and Mark Hyland, *Classification, detection and prosecution of fraud on mobile networks*, ACTS Mobile Summit, 1999. 15, 16, 139

[GJS03] J. Gozdecki, A. Jajszczyk, and R. Stankiewicz, *Quality of service terminology in IP networks*, IEEE Communications Magazine (2003). 76

[GME17] Mordechai Guri, Yisroel Mirsky, and Yuval Elovici, *9-1-1 ddos: Attacks, analysis and mitigation*, Security and Privacy (EuroS&P), 2017 IEEE European Symposium on, IEEE, 2017, pp. 218–232. 31, 135

[Gol08] Emmanuel Goldstein, *The best of 2600: A hacker odyssey*, Wiley Publishing, Inc., 2008. 31

[GOO17] DAN GOODIN, *Thieves drain 2fa-protected bank accounts by abusing SS7 routing protocol*, arstechnica.com, March 2017. 29

[GSBA15] Payas Gupta, Bharath Srinivasan, Vijay Balasubramaniyan, and Mustaque Ahamad, *Phoneypot: Data-driven understanding of telephony threats*, 22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2014, 2015. 17, 38, 40, 48, 103, 104, 116

[GSF+13] Markus Gruber, Christian Schanes, Florian Fankhauser, Martin Moutran, and Thomas Grechenig, *Architecture for trapping toll fraud attacks using a voip honeynet approach*, Network and System Security - 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013. Proceedings, 2013, pp. 628–634. 48

[GSFG] Martin Gruber, Christian Schanes, Florian Fankhauser, and Thomas Grechenig, *Voice calls for free: How the black market establishes free phone calls - trapped and uncovered by a voip honeynet*, IEEE Privacy, Security and Trust (PST) 2013. 59

[GSFG13] Markus Gruber, Christian Schanes, Florian Fankhauser, and Thomas Grechenig, *Voice calls for free: How the black market establishes free phone calls - trapped and uncovered by a VoIP honeynet*, PST, 2013. 32

[Gsm07] *GSMA speeds up the transfer of roaming call records*, http://www.gsma.com/newsroom/press-release/gsma-speeds-up-the-transfer-of-roaming-call-records/, August 2007. 86

[GSM13] GSMK, *GSMK introduces new groundbreaking secure mobile phone*, March 2013. 29

[Gue] Saad Guerraoui, *Morocco banned skype, viber, whatsapp and facebook messenger. it didn't go down well*, middleeasteye.net, 9/3/2016. 24, 57

[He05] Daniel Sheldon Hamilton and Joseph P. Quinlan (eds), *Deep integration: How transatlantic markets are leading globalization*, Center for Transatlantic Relations/Centre for European Policy Studies, 2005. 33

[Hen11] Eugene Bergen Henegouwen, *Roaming fraud - arresting fraud*, Syniverse Technologies, November 2011. 86

[Her98] John Heritage, *Oh-prefaced responses to inquiry*, Language in Society **27** (1998), 291–334. 123

[Her02] ______, *Oh-prefaced responses to assessments: A method of modifying agreement/disagreement*, The Language of Turn and Sequence (Cecilia E. Ford, Barbara A. Fox, and Sandra A. Thompson, eds.), Oxford, 2002, pp. 196–224. 123

[Her16] ______, *Commentary: On the diversity of 'changes of state' and their indices*, Journal of Pragmatics **104** (2016), 207–210. 123

[Hil09] Constantinos S. Hilas, *Designing an expert system for fraud detection in private telecommunications networks*, Expert Systems with Applications **36** (2009), no. 9, 11559 – 11569. 32

[HM08] Constantinos S. Hilas and Paris As. Mastorocostas, *An application of supervised and unsupervised learning approaches to telecommunications fraud detection*, Know.-Based Syst. **21** (2008), no. 7, 721–726. 45

[Hoa98] Peter Hoath, *Telecoms fraud, the gory details*, Computer Fraud & Security (1998). 15, 139

[Hoa08] ———, *Fraud overview*, TAF Regional Seminar, January 2008. 15, 139

[Hon12] Mat Honan, *How apple and amazon security flaws led to my epic hacking*, Wired magazine, June 2012. 2, 139

[HR15] Wilko Henecka and Matthew Roughan, *Privacy-preserving fraud detection across multiple phone record databases*, IEEE Transactions on Dependable and Secure Computing (2015). 32, 46

[HRP+17] Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, Negar Negar, William Enck, Ahmad Sadeghi, and Patrick Traynor, *Phonion: Practical protection of metadata in telephony networks*, PoPETs, July 2017. 37

[HS05a] Constantinos S. Hilas and John N. Sahalos, *User profiling for fraud detection in telecommunication networks*, 5th Int. Conf. technology and automation, 2005, pp. 382–387. 32

[HS05b] Constantinos S Hilas and John N Sahalos, *User profiling for fraud detection in telecommunication networks*, 5th International conference on technology and automation, 2005, pp. 382–387. 44

[HSS10] William S. Horton, Daniel H. Spieler, and Elizabeth Shriberg, *A corpus analysis of patterns of age-related change in conversational speech*, Psychology and Aging, 2010, pp. 708–713. 124

[i3 12] i3 Forum, *Fraud classification and recommendations on dispute handling within the wholesale telecom industry*, April 2012. 26, 28

[Inf14] Infinit Contact, *Why is India losing 70% of call center business to the Philippines*, available at: http://www.infinitcontact.com/blog/india-losing-70-call-center-business-philippines/, May 2014. 109

[Int07] International Telecommunication Union, *Supplement 1: Best practice guide on countering misuse of e.164 number resources*, 2007. 17, 83, 89

[Int17] ———, *Uiprn*, https://www.itu.int/en/ITU-T/inr/unum/Pages/uiprn.aspx, 2017. 89, 143

[ITC+13] Jelena Isacenkova, Olivier Thonnard, Andrei Costin, Davide Balzarotti, and Aurelien Francillon, *Inside the scam jungle: A closer look at 419 scam email operations*, IWCC (co-located with S&P), IEEE, May 2013. 38

[ITU96] *Network grade of service parameters and target values for circuit switched public land mobile services, ITU, rec-e.771*, 1996. 72

[ITU98] ITU, *Itu-t recommendation e.155: International premium rate service*, ITU Recommendataion, March 1998. 28

[ITU99] *Network grade of service parameters and target values for circuit-switched services in the evolving ISDN, ITU, rec-e.721*, 1999. 72

[ITU16] ITU Study Group 3, Question 9/3, *Ott bypass*, International Telecommunication Union: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=10892#TOP, march 2016, Editors: Rim Belhassine-Cherif and Chafik Jallouli. 61

[Jef84] G. Jefferson, *Transcription notation*, Structures of Social Interaction (1984), A light version that we use is available at: pages.ucsd.edu/~johnson/COGS102B/JeffersonianNotation.doc. 115, 123, 166

[JJS+12] Nan Jiang, Yu Jin, Ann Skudlark, Wen-Ling Hsu, Guy Jacobson, Siva Prakasam, and Zhi-Li Zhang, *Isolating and analyzing fraud activities in a large cellular network via voice call graph analysis*, Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services, MobiSys '12, ACM, 2012, pp. 253–266. 46

[Joh12] Mark Johnson, *Demystifying communications risk: A guide to income risk management in the communications sector*, Ashgate Publishing Limited, 2012. 16, 17, 22, 25, 26, 32

[Jol17] *Jolly Roger Telephone Company*, http://www.jollyrogertelco.com/, 2017. 112

[Jon06] Stephen Jones, *Interconnect billing and reconciliation*, January 2006, Available at: http://www.purebill.com/column/pb060123.html. 9

[Jos11] Jeffrey L. Josephson, *The Economics of Business-to-Business (B2B) Telemarketing*, document by JV/M Inc, available at: http://www.jvminc.com/Clients/JVP/Economics.pdf, 2011. 110

[JR00] F. Joachim and B. Rainer, *Method for identifying a mobile phone user or for eavesdropping on outgoing calls*, Patent, Rohde & Schwarz, 2000, EP1051053. 24, 29

[KD12] M. Korczynski and A. Duda, *Classifying service flows in the encrypted skype traffic*, 2012 IEEE ICC, June 2012, pp. 1064–1068. 65, 80

[Ker12] A. D. Keromytis, *A comprehensive survey of voice over ip security research*, IEEE Communications Surveys Tutorials **14** (2012), no. 2. 29

[KKK+15] Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim, *Breaking and fixing volte: Exploiting hidden data channels and mis-implementations*, CCS, ACM, 2015. 24

[KLJ00] Hakan Kvarnstrom, Emilie Lundin, and Erland Jonsson, *Combining fraud and intrusion detection-meeting new requirements*, In Proceedings of the fifth Nordic Workshop on Secure IT systems (NordSec2000), 2000, pp. 12–13. 44

[KLSH04] Yufeng Kou, Chang-Tien Lu, S. Sirwongwattana, and Yo-Ping Huang, *Survey of fraud detection techniques*, IEEE International Conference on Networking, Sensing and Control, 2004, vol. 2, 2004, pp. 749–754 Vol.2. 45

[Kok17] KIM FAI Kok, *Truecaller insights special report*, available at: https://blog.truecaller.com/2017/04/19/truecaller-us-spam-report-2017/, April 2017. 131

[LaC14] John LaCour, *Vishing campaign steals card data from customers of dozens of banks*, https://info.phishlabs.com, April 2014. 38

[Lan12] Philippe Langlois, *SCCP hacking, attacking the SS7 & SIGTRAN applications*, 26th Chaos Communication Congress, 2012. 23

[Lap13] Phil Lapsley, *Exploding the phone: The untold story of the teenagers and outlaws who hacked ma bell*, Grove Press, 2013. 31

[LB10] Jean-Yves Le Boudec, *Performance evaluation of computer and communication systems*, Computer and communication sciences, EPFL Press London, Lausanne, 2010. 67

[len17] *Lenny!*, available at: https://www.youtube.com/watch?v=Gj7AgYt4C6c&list=PLduL71_GKzHHk4hLga0n0GWrXlhl-i_3g, 2017. 110

[Lev16] NAT Levy, *Amazon's $2.5M Alexa Prize seeks chatbot that can converse intelligently for 20 minutes*, available at: http://www.geekwire.com, September 2016. 112

[LF12] A. Lahmadi and O. Festor, *A framework for automated exploit prevention from known vulnerabilities in voice over ip services*, IEEE Transactions on Network and Service Management **9** (2012), no. 2, 114–127. 44

[LFS88] Stephen J. Lupker, Gregory J. Fleet, and Brian R. Shelton, *Callers' perceptions of post-dialling delays: the effects of a new signalling technology*, Behaviour & Information Technology **7** (1988), no. 3, 263–274. 72

[LH06] Yee-Lin Lai and Kai-Lung Hui, *Internet opt-in and opt-out: Investigating the roles of frames, defaults and privacy concerns*, ACM SIGMIS CPR, 2006. 79

[Lik32] Rensis Likert, *A technique for the measurement of attitudes*, Archives of Psychology **142** (1932), 1–55. 76

[LNW+14] Martina Lindorfer, Matthias Neugschwandtner, Lukas Weichselbaum, Yanick Fratantonio, Victor van der Veen, and Christian Platzer, *ANDRUBIS-1,000,000 Apps Later: A View on Current Android Malware Behaviors*, Proceedings of the International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2014. 135

[Luc13] Vincent A. Lucas, *Authenticated caller ID plus regulatory changes*, Document Presented to the FTC Robocall Challenge, May 2013. 40

[LWW+17] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu, *Fbs-radar: Uncovering fake base stations at scale in the wild*, NDSS, 2017. 29

[Mak] *PBX security*, http://www.makeitsecure.org/en/pbx-security.html. 30

[Mar16] Aude Marzuoli, *Call me: Gathering threat intelligence on telephony scams to detect fraud*, Talk by Pindrop, available at: www.blackhat.com, August 2016. 103

[MASX] Hossen Mustafa, AhmadSadeghi, Steffen Schulz, and Wenyuan Xu, *You can call but you can't hide: Detecting caller ID spoofing attacks*, DSN'14, June. 29

[Mat05] R. Mattison, *The telco revenue assurance handbook*, 2005. 17, 25

[Maz04] Harrie Mazeland, *Responding to the double implication of telemarketers' opinion queries*, Discourse Studies **6** (2004), no. 1, 95–115. 130

[Maz06] ______, *Conversation analysis*, Encyclopedia of language and linguistics **3** (2006), 153–162. 112

[MBSS13] Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert, *SMS-based one-time passwords: Attacks and defense*, DIMVA, 2013. 30

[McA13] Neil McAllister, *Call centers under attack in targeted cyber-blackmail scheme*, April 2013. 37

[McC11] Dan McCue, *AT&T says data miners defrauded it*, August 2011, http://www.courthousenews.com/2011/08/16/39024.htm complaint: http://www.courthousenews.com/2011/08/16/Spoof.pdf. 37

[McD16] Cathal McDaid, *SS7 Security : Putting the pieces together*, www.adaptivemobile.com, April 2016. 28

[Mel00] W.H Melody, *Telecom myths: the international revenue settlements subsidy*, Telecommunications Policy **24** (2000), no. 1. 33

[Meu14] Meucci Solutions, *False answer supervision*, 2014. 27

[Mic] *Avoid tech support phone scams*, https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx. 2, 38, 138

[MKDP16] A. Marzuoli, H. A. Kingravi, D. Dewey, and R. Pienta, *Uncovering the landscape of fraud and spam in the telephony channel*, 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), December 2016, pp. 853–858. 103, 115, 116

[MLMD12] V. Matić, A. Lebl, D. Mitić, and M. Dukić, *Estimation of post dialling delay in telephone networks*, Przeglad Elektrotechniczny **R. 88, nr 5b** (2012), 154–156. 72

[Mna15] Moktar Mnakri, *Regulating "over-the-top" services-need and efficicency*, Arab Regional Forum on Future Networks: Regulatory and Policy Aspects in Converged Networks, May 2015. 58

[MR07] Deepankar Medhi and Karthikeyan Ramasamy, *Network routing - algorithms, protocols, and architectures.*, Morgan Kaufmann, 2007. 60

[MSN17] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis, *Dial one for scam: A large-scale analysis of technical support scams*, NDSS, 2017. 38, 111, 122

[MZJP] Ilona Murynets, Michael Zabarankin, Roger Jover, and Adam Panagia, *Analysis and detection of SIMbox fraud in mobility networks*, INFOCOM'14. 31, 35, 46, 80

[New13] Daniel Newman, *Toll fraud: A network and security threat*, Digitalist Mag, May 2013. 38

[Nex] *Details about FAS (False Answer Supervision)*, Nexmo, Dec'16. 35, 72

[NF12] Elin Nolsoe Nielsen and France Telecom-Orange, *Draft report on the article 28(2) universal service directive: A harmonised berec cooperation process*, BEREC, November 2012. 84

[NGT11] Yacin Nadji, Jonathon Giffin, and Patrick Traynor, *Automated remote repair for mobile malware*, ACSAC, ACM, 2011. 36

[NNSE07] Mohamed Nassar, Saverio Niccolini, Radu State, and Thilo Ewald, *Holistic voip intrusion detection and prevention system*, Proceedings of the 1st International Conference on Principles, Systems and Applications of IP Telecommunications (New York, NY, USA), IPTComm '07, ACM, 2007, pp. 1–9. 48

[no_a] *How do I waste a telemarketers time?*, available at: http://no-more-calls.com/how-to-waste-a-telemarketers-time-2/. 110

[no_b] *How does wasting a telemarketers time cost them money?*, available at: http://no-more-calls.com/how-to-waste-a-telemarketers-time/.

[Noh14] Karsten Nohl, *Mobile self-defense*, Talk at 31st Chaos Communication Congress, December 2014. 28

[nom17] *Stop robocalls and telemarketers with Nomorobo*, available at: https://www.nomorobo.com/, 2017. 102

[Nor09] Neal R. Norrick, *Interjections as pragmatic markers*, Journal of Pragmatics **41** (2009), no. 5, 866 – 891. 123

[NPA15] *How lnp works*, https://www.npac.com/number-portability/how-lnp-works, 2015. 34

[NSF06] Mohamed Nassar, Radu State, and Olivier Festor, *Intrusion detection mechanisms for voip applications*, 3rd Annual VoIP Security Workshop, Berlin, Germany **179** (2006). 29

[NSF07] M. Nassar, R. State, and O. Festor, *Voip honeypot architecture*, Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on, May 2007, pp. 109–118. 48

[Ofc05] *The scope of the mobile operators' 2G cellular licences issued under section 1(1) of the Wireless Telegraphy Act 1949 and the legal status of the use of GSM gateways*, Ofcom, March 2005. 31

[one16] *Ray, Anna, Maya, and Tracy from Verde Energy spend an entire hour with Lenny*, available at: https://www.youtube.com/watch?v=D-RAlSGWQlI&t=2s, September 2016. 110

[OTT15] *Smart regulation for OTT growth*, Asia Internet Coalition, whitepaper, October 2015. 24, 58

[OTT16] *New threat to mobile network operator revenues*, Revector Company Blog, February 2016, http://www.revector.com/index.php/new-threat-ott/. 55

[Pag16] Pierluigi Paganini, *Researchers hack WhatsApp accounts through SS7 protocol*, arstechnica.com, May 2016. 29

[Pet15] J. Peterson, *Authenticated identity management in the Session Initiation Protocol*, IETF Internet-Draft, 2015. 29, 134

[pin17] *Phone fraud stops here*, available at: https://www.pindrop.com/, 2017. 102

[PLCY13] Jon Peterson, Hong Liu, Ben Campbell, and James Yu, *Using E.164 numbers with the Session Initiation Protocol (SIP)*, RFC 3824, 2013. 24

[PLSMG10] Clifton Phua, Vincent Cheng-Siong Lee, Kate Smith-Miles, and Ross W. Gayler, *A comprehensive survey of data mining-based fraud detection research*, CoRR **abs/1009.6119** (2010). 45

[Pra] *Phone scam callers get owned!*, https://www.youtube.com/channel/UCxRY9vRnEfnijWJjfUE9xzQ. 110

[pre16] *Top predictive dialers, cloud call centers, power dialers, auto dialers - Terminology*, available at: https://www.telephonelists.biz, 2016. 101

[PRI17] ERIC PRIEZKALNS, *Araxxe Warns That EU Rules Encourage CLI Fraud*, Commsrisk Article, February 2017. 33

[Pro04] Niels Provos, *A virtual honeypot framework*, Proceedings of the 13th Conference on USENIX Security Symposium, SSYM'04, USENIX Association, 2004. 47

[PS07] VASSILIS PREVELAKIS and DIOMIDIS SPINELLIS, *The athens affair*, IEEE Spectrum, June 2007, https://spectrum.ieee.org/telecom/security/the-athens-affair. 37

[PST14] Jon Peterson, Henning Schulzrinne, and Hannes Tschofenig, *Secure telephone identity problem statement and requirements*, IETF Request for Comments 7340. 24, 29

[PT16] J. Peterson and S. Turner, *Secure telephone identity credentials*, IETF Internet-Draft, 2016. 29

[PTL15] Javier Pastor, Michael Tuexen, and John Loughney, *Security Considerations for Signaling Transport (SIGTRAN) Protocols*, RFC 3788, 2015. 23

[RBA+17] Bradley Reaves, Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton, *Authenticall: Efficient identity and content authentication for phone calls*, 26th USENIX Security Symposium (USENIX Security 17) (Vancouver, BC), USENIX Association, 2017, pp. 575–592. 30

[RBT16] Bradley Reaves, Logan Blue, and Patrick Traynor, *Authloop: End-to-end cryptographic authentication for telephony over voice channels*, 25th USENIX Security Symposium (USENIX Security 16) (Austin, TX), 2016, pp. 963–978. 30, 47, 134

[RD88] J. S. Richters and C. A. Dvorak, *A framework for defining the quality of communications services*, Comm. Mag. **26** (1988), no. 10, 17–23. 72

[Red16] *Lenny's history & why he isn't creative commons*, 2016, https://www.reddit.com/r/itslenny/comments/5lcfwq/. 110

[Ret95] G. Retske, *The international callback book: An insider's view*, SOLVOX, Incorporated, 1995. 33, 34

[RMN+99a] Saharon Rosset, Uzi Murad, Einat Neumann, Yizhak Idan, and Gadi Pinkas, *Discovery of fraud rules for telecommunications - challenges and solutions*, ACM KDD, 1999. 32

[RMN+99b] ———, *Discovery of fraud rules for telecommunications- challenges and solutions*, Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (New York, NY, USA), KDD '99, ACM, 1999, pp. 409–413. 44

[Ros71] Ron Rosenbaum, *Secrets of the little blue box*, Esquire MAG, 1971. 31

[Ros15] Ian Ross, *Exposing fraud: Skills, process and practicalities*, Wiley Corporate F&A, November 2015. 17

[RSB+15] Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor, *Boxed out: Blocking cellular interconnect bypass fraud at the network edge*, USENIX Security, 2015. 31, 35, 44, 47, 59, 61, 65, 80

[Sac72] Harvey Sacks, *An initial investigation of the usability of conversational data for doing sociology*, Studies in social interaction (David Sudnow, ed.), Free Press, New York, 1972, pp. 31–74. 113

[Sac92] ______, *Lectures on conversation*, vol. 1-2, Basil Blackwell, Oxford, 1992. 113

[SAE12] Jose Sobreira, Raul Azevedo, and Tal Eisner, *TM Forum Fraud Management Group Activities*, May 2012. 17

[San] Maui Sanford, *A coordinated approach on the international telecommunications scene between governments from the pacific and a non-governmental organisation*, The Pacific Islands Telecommunications Association (PITA), Available at: http://www.upf.pf/IMG/pdf/07-TIC-Sanford-PITA.pdf. 86

[SBA+15] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert, *Practical attacks against privacy and availability in 4G/LTE mobile communication systems*, CoRR (2015). 29

[SCCB05] Micah Sherr, Eric Cronin, Sandy Clark, and Matt Blaze, *Signaling vulnerabilities in wiretapping systems.*, IEEE Security & Privacy (2005). 23

[Sch68] Emanuel A. Schegloff, *Sequencing in conversational openings*, American Anthropologist **70** (1968), no. 6, 1075–1095. 112

[Sch86] ______, *The routine as achievement*, Human Studies **9** (1986), no. 2, 111–151. 119

[Sec14] *The surging threat of telephony denial of service attacks*, Securelogix Whitepaper, October 2014. 31

[SF16] Merve Sahin and Aurélien Francillon, *Over-The-Top bypass: Study of a recent telephony fraud*, CCS, ACM, 2016. 3, 143

[SFGA17] Merve Sahin, Aurélien Francillon, Payas Gupta, and Mustaque Ahamad, *Sok: Fraud in telephony networks*, Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17), EuroS&P'17, IEEE, April 2017. 2, 141

[SFK$^+$12] Sebastian Schrittwieser, Peter Fruhwirt, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Markus Huber, and Edgar R. Weippl, *Guess who's texting you? evaluating the security of smartphone messaging applications.*, NDSS, 2012. 62

[Shi16] Laura Shin, *Hackers Have Stolen Millions Of Dollars In Bitcoin – Using Only Phone Numbers*, www.forbes.com, December 2016. 2, 139

[SIM16] *How SIM swap fraud happens and what to do*, https://toughnickel.com/scams-fraud/sim-swap-fraud, April 2016. 30

[SJS77] Emanuel A Schegloff, Gail Jefferson, and Harvey Sacks, *The preference for self-correction in the organization of repair in conversation*, Language **53** (1977), no. 2, 361–382. 112

[sno] *Snoopsnitch project*, opensource.srlabs.de/projects/snoopsnitch. 29

[Sob15] Art Sobczak, *42 telesales, telemarketing, inside sales, and cold calling tips you can use right now to get more business and avoid rejection*, available at: http://businessbyphone.com/telemarketing-tips/, 2015. 119

[SRF17] Merve Sahin, Marc Relieu, and Aurélien Francillon, *Using chatbots against voice spam: Analyzing lenny's effectiveness*, Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), SOUPS'17, USENIX, July 2017. 3, 123, 145

[SS73] Harvey Sacks and Emanuel A. Schegloff, *Opening up closings*, Semiotica **8** (1973), no. 4, 289–327. 112, 113

[SS14] Maliheh Shirvanian and Nitesh Saxena, *Wiretapping via mimicry: Short voice imitation man-in-the-middle attacks on crypto phones*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA), CCS '14, ACM, 2014, pp. 868–879. 37

[SSJ74] H. Sacks, E.A. Schegloff, and G. Jefferson, *A simplest systematics for the organization of turn-taking for conversation*, Language **50** (1974), no. 4, Part 1, 696–735. 112

[STI] *Secure Telephone Identity Revisited (STIR)*, https://datatracker.ietf.org/wg/stir/charter/. 29

[Suba] Subex, *Bypass Fraud- Are you getting it right?*, Whitepaper. 16, 34, 35, 140

[Subb] Subex Limited, *Concept note on PBX hacking*, http://www.subex.com/pdf/PBXHacking.pdf. 30

[Sub13] ______, *Subex wholesale fraud management survey*, 2013. 19, 25, 33, 34, 35, 84

[sui07] *Suing a telemarketer: How I spent my summer vacation*, available at: https://www.privacyrights.org, October 2007. 102

[Tab16] Judith L. Tabron, *Linguistic features of phone scams: A qualitative survey*, 11th Annual Symposium on Information Assurance (ASIA'16) (2016). 111

[Tal15] Talks To Telemarketers , *Predictive Dialers and Robocalls are poor Marketing*, document by JV/M Inc, available at: http://www.tormentingtelemarketers.com/2015/09/predictive-dialers-and-robocalls-are-poor-marketing/, September 2015. 131

[Tao] *Taoa.net* , *Lenny!*, https://www.youtube.com/playlist?list=PLduL71_GKzHHk4hLga0n0GWrX1hl-i_3g. 114

[Tao15] *Lenny, the bot that tricks telemarketers*, 2015, http://toao.net/595-lenny. 113

[TDO13] *TDoS attacks on public safety communications*, http://krebsonsecurity.com/wp-content/uploads/2013/04/DHSEM-16-SAU-01-LEO.pdf, March 2013. 37

[TDZA16a] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn, *SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May 2016. 17, 37, 38, 45, 109, 111, 131, 133, 145

[TDZA16b] ______, *Toward Authenticated Caller ID Transmission: The Need for a Standardized Authentication Scheme in Q.731.3 Calling Line Identification Presentation*, ITU Kaleidoscope - ICTs for a Sustainable World, Nov 2016. 30, 134

[The13] The Telecom Compliance News Press, *How CallerId4U, Inc. Profits Directly from Illegal Robocalls*, https://telemarketerspam.wordpress.com/, February 2013. 40

[the14] theguardian.com, *Londoners give up eldest children in public Wi-Fi security horror show*, Sept. 2014. 80

[thr16] *[NSFW] Telemarketer tells Lenny not to play with someone whose job it is to mess with him*, available at: https://www.youtube.com/watch?v=GBSok8sPEM0, June 2016. 120

[TIB+14] Kurt Thomas, Dmytro Iatskiv, Elie Bursztein, Tadek Pietraszek, Chris Grier, and Damon McCoy, *Dialing back abuse on phone verified accounts*, CCS, ACM, 2014. 2, 138

[Tim15] Anna Tims, *SIM swap gives fraudsters access-all-areas via your mobile phone*, September 2015. 30

[Tol15] *5 tips for businesses to prevent telecom toll fraud*, Transnexus Whitepaper, April 2015. 38

[Traa] *Hacking premium rate number schemes*, Newsletter. 83

[Trab] TransNexus, *Telecom fraud guide*, http://transnexus.com/resources/telecom-fraud-guide. 16, 27, 33, 36, 140

[Trac] ———, *Toll free fraud*, available at http://transnexus.com/resources/telecom-fraud-guide/toll-free-fraud/. 28

[Tra09] Dustin Trammell, *Metasploit telephony*, Blackhat, July 2009, http://www.blackhat.com/presentations/bh-usa-09/TRAMMELL/BHUSA09-TrammellDruid-MetasploitTele-PAPER.pdf. 37

[Tra13] TransNexus, *The face of traffic pumping*, available at http://transnexus.com/the-face-of-traffic-pumping/, February 2013. 27

[Tra15a] *International premium rate number market*, TransNexus Whitepaper, 2015. 28, 83, 87, 89

[Tra15b] *Location routing number fraud*, http://transnexus.com/resources/telecom-fraud-guide/location-routing-number-fraud/, 2015. 34

[Tra15c] TransNexus, *Phone app traffic pumping fraud*, http://transnexus.com/phone-app-traffic-pumping-fraud/, October 2015. 27

[Twi] Twilio, http://www.twilio.com. 7

[Val12] Jeff Valentine, *3 reasons the call center is far from dead*, available at: http://mashable.com/2012/04/24/call-center-death-exaggerated/#5o3Fc5GKiZqF, April 2012. 109

[Voi] *Reasons to Become a VoIP Reseller*, http://www.voiproutes.com/reseller/. 7

[Voi12] *Fake false answer supervision (fas) service*, http://www.voip-info.org/wiki/view/Fake+False+Answer+Supervision+(FAS)+service, 2012. 35

[Voi16] *CNAM Lookup Services List*, http://www.voip-info.org/wiki/view/CNAM, 2016. 28

[VTD15] Pierre-Antoine Vervier, Olivier Thonnard, and Marc Dacier, *Mind your blocks: On the stealthiness of malicious bgp hijacks*, NDSS, 2015. 26

[Wan16] YONGDONG Wang, *Your next new best friend might be a robot*, available at: http://nautil.us/issue/33/attraction/your-next-new-best-friend-might-be-a-robot, February 2016. 112

[Was14] Naser Al Wasmi, *Telecoms regulator says viber is 'unlicensed' in the UAE*, September 2014, The National UAE. 24, 57, 58

[Wei66] Joseph Weizenbaum, *Eliza;a computer program for the study of natural language communication between man and machine*, Commun. ACM **9** (1966), no. 1, 36–45. 112

[Wei05] Gary M. Weiss, *Data mining in telecommunications*, pp. 1189–1201, Springer US, Boston, MA, 2005. 44, 45

[WFS+08] H Welte, H Freyther, D Spaar, S Schmidt, D Willmann, J Luebbe, T Seiler, and A Eversberg, *OpenBSC*, 2008, http://openbsc.osmocom.org/trac/wiki/OpenBSC. 29

[Wik] *Phone fraud*, https://en.wikipedia.org/wiki/Phone_fraud. 16

[Wil] Tom Wilson, *Network fraud - bypass/premium rate number - IRS*. 95

[Yat13] Colin Yates, *International revenue share fraud webinar*, Dec 2013. 83

[ZDYZ14] Mu Zhang, Yue Duan, Heng Yin, and Zhiruo Zhao, *Semantics-aware android malware classification using weighted contextual api dependency graphs*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, ACM, 2014. 135

[ZWYJ07] Ruishan Zhang, Xinyuan Wang, Xiaohui Yang, and Xuxian Jiang, *Billing attacks on sip-based voip systems*, WOOT, 2007. 29