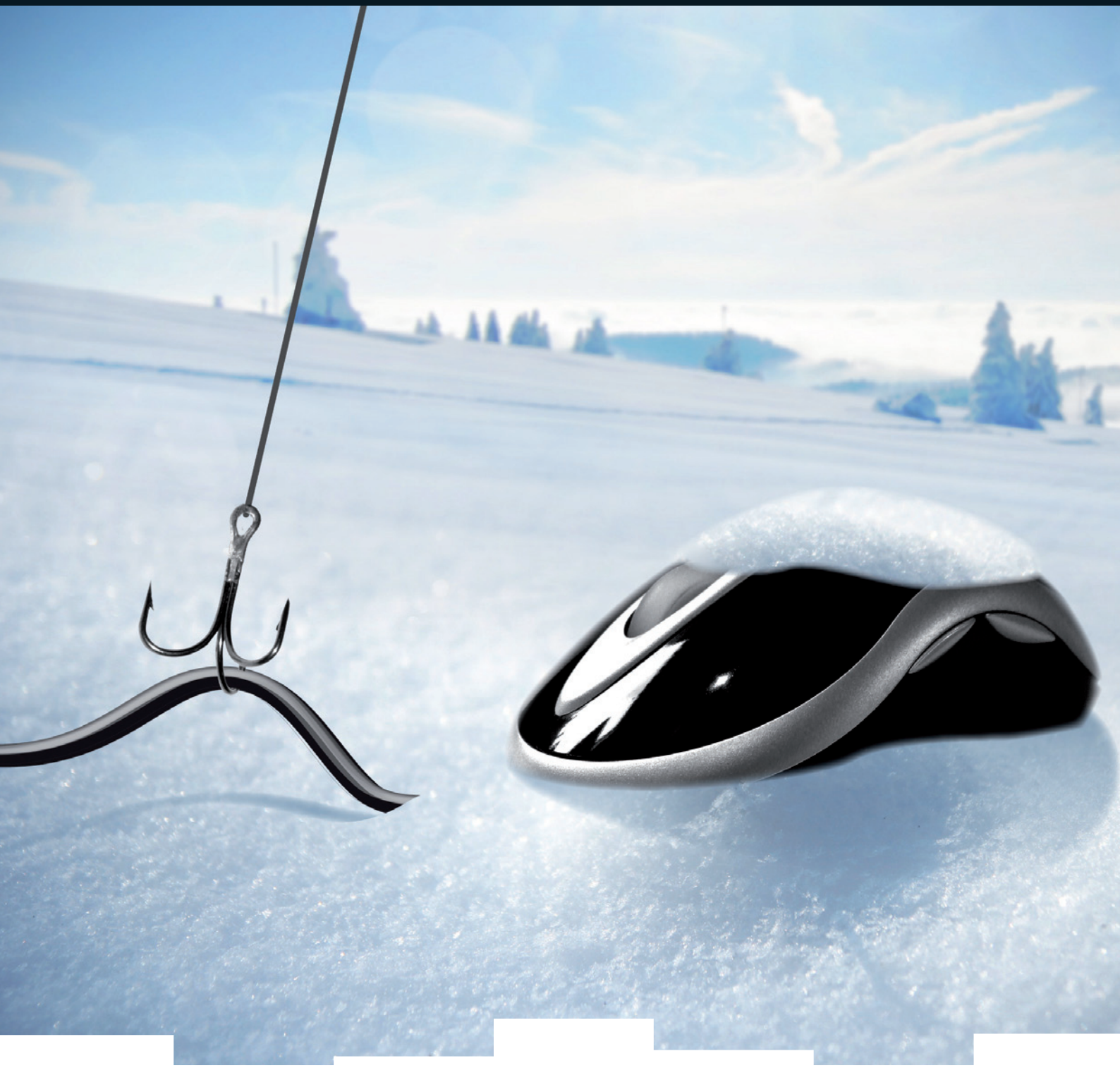
technicolor



THE SECURITY NEWSLETTER #21

WINTER 2012

THE SECURITY NEWSLETTER #21

In this Issue

Published Quarterly By
Technicolor Security & Content Protection Laboratories

Technical Editor: Eric Diehl

Editors: Sharon Ayalde

Contributors: Patrice Auffret
Gwenaël Doerr
Alain Durand
Marc Eluard
Raphael Gelloz
Olivier Heen
Stéphane Onno
Yves Maetz
Xavier Rolland-Nevière

EVP: Gary Donnan
CSO: Rachel Orand

Subscribe to the newsletter:
security.newsletter(at)technicolor.com

Report vulnerability:
security(at)technicolor.com

EDITORIAL

Anti-piracy is starting this new year with good omen. The first event is the shutdown of MegaUpload on January 19th. What a surprise! For many months, piracy due to illegal streaming has exceeded piracy due to Peer-To-Peer (P2P). MegaUpload became the flagship of cyber lockers, as "The Pirate Bay" is the flagship of P2P. With servers spread all over the world and operators also disseminated, their position seemed impregnable.

Nevertheless, a US grand jury indicted seven individuals and two societies of engaging in a racketeering conspiracy, conspiring to commit copyright infringement, conspiring to commit money laundering and two substantive counts of criminal copyright infringement. Following this decision, the FBI launched a vast operation ending up with the arrest of four individuals in New Zealand who should soon be transferred to the US, and the seizure of servers. Game over!

The second event is the voluntary shutdown of BTJunkie. Although not the largest torrent tracker site, BTJunkie was one important piece of the P2P landscape (5th position). Since the 14th of February, the site is closed. Are these two events related? To the best of our knowledge, BTJunkie was not under any legal suit.

Will that stop piracy? Of course, the answer is no. Obviously, we will see a serious slowdown of illegal download/streaming. As many people/promoting sites relied on MegaUpload, some time will be necessary to seed new cyber lockers with illegal content and to promote them. A successor to MegaUpload will most probably appear in the coming months. Then, was that operation useless? No. The content owners have demonstrated that there may be nothing such as an impregnable harbor for illegal content trading. In addition to the immediate temporary impact on piracy, it may send a strong, deterrent, pedagogical message to pirates (at least light-hearted ones).

A collateral effect may be that people will rethink the conditions to use free cloud storage. MegaUpload was also used for legitimate content storage. All this information is now lost as we may expect that their owner did not locally back it up. This is an interesting topic to explore.

2012 may be a very thrilling year in the security and content protection arena.

E. DIEHL
Technical Editor

THE SECURITY
NEWSLETTER
#21

BE OUR GUEST

Refik Molva

Hello Refik, may you introduce yourself?
I am a security researcher in computer and communication systems. I am a full professor at EURECOM and in addition, I am in charge of the Networking and Security Department at EURECOM.

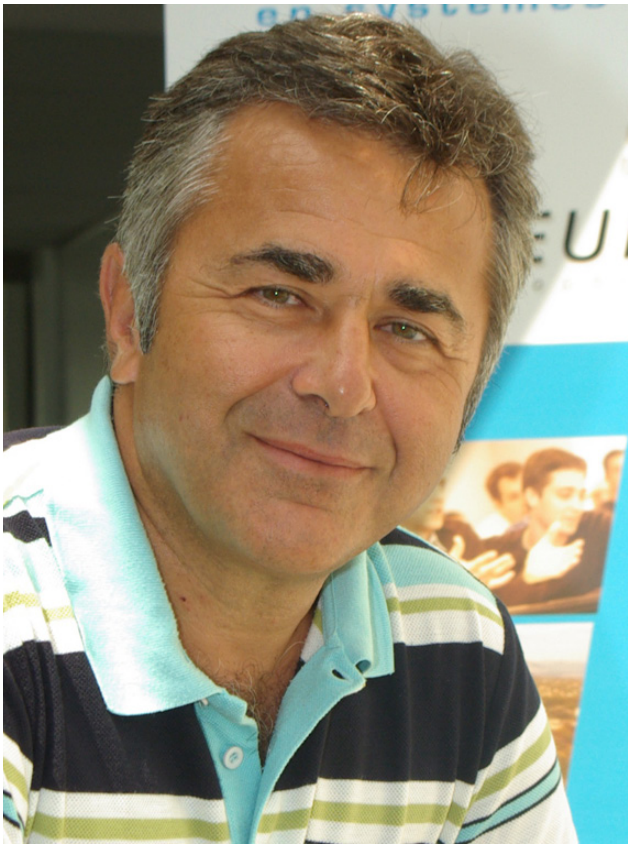
How did you get into security?
This comes back to the time when security was not seen as a full research topic. In 1989, I was a researcher at IBM Zurich and my main topic was networking. With my first line manager, Phil Janson, we wanted to explore a new domain so we visited other IBM labs in the US. Network security just came up as evidence. I started working with Moti Yung on the security of an authentication protocol and we discovered and fixed vulnerabilities. This was a seminal work under the codename KryptoKnight that paved the way for the outstanding security activity in IBM Zurich. That was my first contribution to network security, and I have never stopped since.

Three years later, I joined EURECOM as the only security researcher. Security kept being marginal, even deemed a bit suspicious, until the end of the nineties. With the advent of Internet, everything changed up to a point that now security is considered as an "easy" research topic since there is so much to do.

What are the main research domains that you have explored?
In the early days, my focus was very broad: applied cryptography, network security, protocols. But at that time, one could still afford to cover so many topics. From 2003, I focus on the design of security protocols using cryptographic techniques.

Whenever a new communication or computing paradigm arises, I try to spot original security problems raised by that paradigm. For instance, when multicast was a popular topic in networking, authentication of multicast flows was a brand new problem. Unlike unicast that can be addressed by symmetric message authentication techniques, multicast authentication inherently calls for asymmetric mechanisms. Asymmetric algorithms on the other hand are way too complex for real time traffic, so one had to come up with a new solution, that's what we did with Alain Pannetrat, my Ph.D. student by then.

Another example is with the advent of ad hoc networks that certainly raise several security requirements but only very few actually called for novel solutions. We were among the few research groups that identified selfishness as a new problem in ad-hoc networks and formalized it using game theory.



You did not mention privacy yet...
I was coming to this point. I currently investigate privacy problems in relation with cloud computing. Straightforward application of classical privacy mechanisms out of the crypto bag of tools is not sufficient: the additional difficulty comes from the very distributed nature of the cloud. Understanding this difficulty leads to new security protocol designs like, for instance, PRISM (Privacy-Preserving searches in Map-Reduce).

On that topic I want to stress that privacy does not only involve confidentiality. Unlinkability or even unobservability are equally important privacy requirements. Especially when applied to the cloud this might lead to exciting challenges. As an example, I can quote the apparent contradiction between cloud authentication and unlinkability.

THE SECURITY
NEWSLETTER
#21

Do you think there are unsolvable privacy issues?
No. At least not from a pure technology point of view. Problems arise from our capacity to state the real needs. For instance, there is an obvious contradiction between usages in social networks and the privacy of both personal data and Personally Identifiable Information.

A related difficulty is that many users do not spontaneously request privacy. This is counterbalanced by the recent European directive. This makes administrations aware of privacy issues and responsibilities, as well as organisms funding research, which I personally find a very good thing. Along the same lines, we recently were invited by public authorities to join a consortium in order to investigate privacy issues in a project involving RFID tags. This would have never happened without this directive.

Do you have any thought about research that you would like to share?
I am concerned about the overall trend with increasing constraints and short-term expectations from research. Research by definition can barely yield any useful outcome if constrained by concrete objectives. In the long run, betting on open-ended research will be much more profitable. A noteworthy counter-example is European R&D programs that claims to cover a broad range of goals from fundamental research through prototyping and standardization to business exploitation in projects within 2-3 year timeframe. Programs and funding for fundamental research should be separate from the ones for technology transfer and innovation, like NSF and DARPA are in the US.

Thank you!

R. MOLVA (EURECOM, Sophia Antipolis)
Interview by A. DURAND and O. HEEN

THE NEWS

Patriot Act vs. Cloud?

Signed by President Bush shortly after the attacks of 9/11, the Patriot Act aims at easing the gathering of data by American federal agencies in order to fight terrorism. Many people understand: "federal agencies may silently get data". Some US cloud providers view it as a competitive drawback as non-US customers may perceive it as a threat for their data. While this might make sense at a first glance, a deeper analysis shows this is not rational. Non-US, security aware customers would actually classify data regarding their sensitivity. Non-sensitive data may go in any cloud. Regional-sensitive data shall go in regional clouds (like EU data in EU provider OVH, OBS, etc.) and sensitive data out-of-the-cloud anyway. In this context, the Patriot Act[1] is not really a problem. Since most of the data is non-sensitive, the leading cloud provider will gather the largest market share regardless of regional laws and security context. This means the market is fairly competitive as long as the main amount of data in the cloud is non-sensitive, which seems to be currently the case.

O. HEEN

Ghost Click

First experiments on internet advertisement started in 1994.[2] Many monetizing strategies and tools are possible. Internet advertisement has become a multi-billion-dollar industry and therefore a new target of attacks.

Two years of collaboration between law enforcement and security researchers led to the arrest of six men who were operating a large fraud on internet advertisement: they are suspected to have made $14 million through click-jacking.[3]

The attack targeted the click referral principle where a host receives a small fee for redirecting a client to an advertised website. The attacker used a Domain Name System (DNS) changer malware. The malware redirected heavy traffic like iTunes or Netflix to other sites where they had advertisement agreements.

Four million computers are infected and their users may not be aware. The rogue DNS servers have been shutdown, and replaced by legitimate ones. Thus, the infected computers can still access the Internet. These servers will be operated until this spring, leaving some time for deceived users to detect the infection and correct their DNS settings.

1 'The USA PATRIOT Act: Preserving Life and Liberty', http://www.justice.gov/archive/ll/highlights.htm.
2 Rachel Arandilla, 'Rise and Fall of Online Advertising', 1st Web Designer, March 1, 2011, http://www.1stwebdesigner.com/design/online-advertising-history/.
3 'International Cyber Ring That Infected Millions of Computers Dismantled', FBI, http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911.