A THIRD ERC GRANT
in 3 years at EURECOM

Davide Balzarotti

Professeur au Département
Systèmes de Communication

Getting a grant from the European Research Council is not an easy task but this is what Davide Balzarotti, Professor in the Security Department, has just accomplished. He is the third EURECOM professor to obtain an ERC grant in the past 3 years.

Davide, you just got an ERC Consolidator grant, one of the most prestigious research grants in Europe. What is your feeling today?

Everybody knows it is one of the most selective grants in Europe, so I'm obviously very proud of that. It is definitely a major step in my career. It is an important recognition for the efforts I have made to get this grant and for the relevance of the project I presented. Plus, I was told there are only 329 researchers across Europe - and 38 researchers in France - who got this grant this year, so I am particularly honoured to be one of them. I am also very happy for EURECOM since it has been awarded one ERC grant every year for the past 3 years… Considering there are only 23 professors, it is a real success!

Will this grant change your day-to-day life as a researcher at EURECOM?

I am sure it will! In different ways even. First, I won't have to worry about getting money for the next few years. The Consolidator grant is a five-year grant that represents €2 million. This grant is not only generous, it also offers recognition and visibility.

In fact, the two other ERC grantees at EURECOM - David Gesbert & Petros Elia - explained me that I will certainly be more solicited by the research community. It will also give me a lot of independence and creative freedom to conduct the project for which I got this grant: BITCRUMBS - Towards a Reliable and Automated Analysis of Compromised Systems. I will dedicate 70% of my time to the project but I can manage it the way I want depending on the people I will work with. I actually need to hire a team of seven researchers - five Ph.D. students and two post-docs - and one engineer.

On top of that, I will be involved in the EURECOM ERC committee that helps scientists benefit from the experience of the ones who already received such grants. This committee actually helped me a lot in writing my proposal, so I look forward to helping my colleagues in return.

BITCRUMBS seems to be a ground-breaking project in the computer security area. Could you explain its main objective?

BITCRUMBS is actually a brand new way of addressing computer security issues. And this ERC grant will help me pursue very ambitious research objectives with this project, which covers a wide range of digital security areas. I hope our results will change the way digital security will be managed in the future. The main objective of BITCRUMBS is to rethink what we call the "incident response" (IR). It is clear that research on prevention and detection helps make devices more secure, but since a 100% secure system does not exist, improving IR can be very useful too. Incident response addresses the aftermath of a digital security breach that, if not handled properly, can lead to data breach or a system collapse. We all know the risk of security breaches is now higher than ever. Attackers frequently break into corporate networks, government services and even critical infrastructures. Almost half of computers worldwide are infected by malware. A voting machine can be altered to rig the results of an election, a connected car can be hacked to drive down a cliff or a security camera can be controlled over the Internet to spy over our houses and our families. The problem is that we do not have the tools to analyze these attacks and understand their causes! This has to change.

With BITCRUMBS, I want to give investigators the possibility to quickly verify the state of compromised systems and help citizens trust the result of computer forensic investigations. In the future, I believe we should design digital systems the way we design airplanes - secure against crashes but also equipped with black boxes to collect all the data required to support an incident investigation.

What is your strategy to reach this objective?

I want to propose a more scientific and comprehensive methodology to analyse compromised systems. This should be done in three steps. The first part of the project will focus on measuring the effectiveness and accuracy of the techniques currently used to analyse compromised systems, and on assessing the reliability of their data sources. This will help increase the theoretical and scientific foundations of IR techniques. The second part of the project will focus on the design and implementation of new automated analysis techniques able to cope with advanced threats and the analysis of IoT devices. These techniques will have to be robust, scalable and generic – capable of working on different classes of devices. Of course, results given by these new techniques will need to be reliable and based on a solid theoretical foundation. The last step will introduce a new forensics analysis by design methodology. My goal is to provide a set of guidelines for the design of future systems and software - to help developers provide the required information to support the analysis of compromised systems.

What about the scientific and technological impacts?

I hope research conducted in BITCRUMBS will have a long-lasting impact - not only scientific - on the area of incident response and on the way we analyze compromised systems. First, BITCRUMBS will bring a scientific foundation to IR, based on repeatable experiments and precise measurements of the reliability of data and techniques used in current investigations. It will also have a practical impact since it will produce open source tools and improve existing software that are regularly used by companies and law enforcement to deal with computer attacks. Last but not least, BITCRUMBS will have an impact on our society. Improving the IR process will increase the trust that citizens have in the result of digital investigations. In order to clearly show the impact of BITCRUMBS in different fields and scenarios, we will address our objectives using real case studies borrowed from traditional computer software and embedded systems.

ERC grants: Facts & Figures

● The total budget allocated to the ERC for the period 2014-2020 is €13.1 billion

● This represent **17% of the overall Horizon 2020 budget** and give top researchers a chance to have far-reaching impact on science.

● ERC grantees have won prestigious prizes, including **6 Nobel Prizes, 4 Fields Medals and 5 Wolf Prize**

● There are **3 kinds of ERC** grants (depending on the experience of the applicant): Starting Grants – Consolidator Grants – Advanced Grants

● **ERC Consolidator grants** – the type OF ERC grant Davide got in 2017 – is worth in total **€630 million**

● ERC Consolidator Grants are awarded to researchers with **7-12 years of experience** since completion of PhD – and having a scientific track record showing great promise

● Only **38 scientists working in France** have been awarded this year - which makes France the 3rd country in terms of number of ERC grants, behind the United Kingdom and Germany

● The ERC has evaluated 2,538 research proposals this time, out of which **13% are funded**

● The funding (maximum of **€2 million per grant)**, is provided for up to **five years** and mostly covers the employment of researchers and other staff .