

Session III.4 Session on Security and Usability

[18th May – 16:30-18:30]

Organisers:

- Dr Nick Papanikolaou, Cloud and Security Lab, HP Labs, Bristol, UK (np1@hp.com)
- Prof Fabio Massacci, Dipartimento di Ingegneria e Scienza dell'Informazione, Universita di Trento, Trento, Italy (Fabio.Massacci@unitn.it)

Speakers and Panellists:

- Dr Corrado Leita, Symantec Research Labs Europe
- Dr Florian Mansmann, Department of Informatics, Universität Konstanz
- Dr Ronald Marx, Fraunhofer SIT, Darmstadt
- Prof Kai Rannenberg, T-Mobile Chair of Mobile Business & Multilateral Security, Goethe University, Frankfurt
- Prof Angela Sasse, Information Security Group, Department of Computer Science, University College London
- Prof Frank Stajano, Computer Laboratory, University of Cambridge

Agenda

Time	Speaker	Title/Topic
16:30 – 16:50	Corrado Leita	Security And Usability: Challenges And Consequences
16:50 – 17:10	Angela Sasse	Designing Productive Security Systems
17:10 – 17:30	Kai Rannenberg	Security, Privacy, Identity Management and Usability - an application-driven approach
17:30 – 17:45	Frank Stajano	Understanding scam victims: seven principles for systems security
17:45 – 18:00	Florian Mansmann	Fighting Cybercrime with Visual Analytics
18:00 – 18:30	PANEL	Discussion with questions from the audience

Abstracts

Speaker: **Dr Corrado Leita, Symantec Research Labs Europe**

Title: **Security And Usability: Challenges And Consequences**

Abstract:

Usability and security are often perceived as contrasting concepts: the need to achieve strong security is often in contrast to the need of making the software easy to use. The failure to correctly address this trade-off is at the center of many bad practices and security incidents that have reached the press headlines in the last years,

such as the Stuxnet incident and the outbreak of rogue security software. During this talk I will build upon the analysis of some recent security incidents, and show through these real-world examples the challenges associated to effectively combining the need for strong security with that of correctly interfacing the security primitives with the end users.

**Speaker: Prof Angela Sasse, Information Security Group,
Department of Computer Science, University College London**

Title: Designing Productive Security Systems

Abstract:

The number of systems and services that people interact with has increased rapidly over the past 20 years. Most of those systems and services require security controls. In practice, most current security controls are not effective because those who have to interact with them can't - or won't - operate them as intended by security designers. Leading security researchers and practitioners have framed the problem as "humans being the weakest link in the security chain".

Over the past decade, research on "usable security" has focussed on developing "better user interfaces" for security controls. In this talk, I will explain why this approach cannot succeed - it is based on a shallow understanding of "usability", which assumes that - if only people could understand how to operate security controls properly - they would. The problem, however, is that most security controls provide a poor fit into individual tasks and business processes, and consume far too much effort for too little return. I will outline a new approach to integrating security controls into individual tasks and business processes.

**Speaker: Prof Kai Rannenberg, T-Mobile Chair of Mobile Business & Multilateral Security,
Goethe University, Frankfurt**

Title: Security, Privacy, Identity Management and Usability - an application-driven approach

Abstract:

Both Security and Privacy are often considered to be at odds with the usability of ICT systems and applications. The main reason for this is that users usually don't use ICT systems or applications to protect their security or privacy, but to achieve application oriented goals, e.g. to stay in contact with one's peers in a social network. Therefore security and privacy are considered "secondary" functions and any effort to deal with them is considered an inconvenience, as it does not contribute to achieve the "primary" goals of the respective ICT use. This puts an additional challenge to any try to raise the usability of security or privacy functionality, as any try is stuck in a trade-off between the extra effort the security or privacy functionality requires and the benefit, that the user can see from the functionality, while (s)he has to deal with the effort. Moreover in most situations the effort is required immediately, while the benefit can only be seen in the long run (e.g. when users are bothered with controlling the flow of information out of their personal domain).

An approach to handle this situation is to design and develop security and privacy functionality from the point of view of the respective application, as it was done in the project PICOS (Privacy and Identity Management for Community Services, www.picos-project.eu). This presentation will report on this approach and how security and privacy functionality can become more application and user oriented, when users derive it from what they consider "their" application. The respective structuring of the functionality may be at odds with any "classic" structuring of functionality, but it helps users to better relate to the functionality, as they better understand what it is good for. A special role is played by Identity Management, as it relates directly to the way how users present themselves in social networks. The application oriented approach may also help

towards a more general usability-oriented structuring of security and privacy functionality, when the approaches from different applications are put in relation to each other and generalized.

Speaker: Prof Frank Stajano, Computer Laboratory, University of Cambridge

Title: Understanding scam victims: seven principles for systems security

Abstract:

The success of many attacks on computer systems can be traced back to the security engineers not understanding the psychology of the system users they meant to protect. We examine a variety of scams and short cons that were investigated, documented and recreated for the BBC TV programme The Real Hustle and we extract from them some general principles about the recurring behavioural patterns of victims that hustlers have learnt to exploit. We argue that an understanding of these inherent human factors vulnerabilities, and the necessity to take them into account during design rather than naïvely shifting the blame onto the gullible users, is a fundamental paradigm shift for the security engineer which, if adopted, will lead to stronger and more resilient systems security.

Speaker: Dr Florian Mansmann, Department of Informatics, Universität Konstanz

Title: Fighting Cybercrime with Visual Analytics

Abstract:

Cybercrime has become a major issue in the Internet and many automated approaches have been invented to protect valuable assets of the network infrastructure. Despite the fact that network administrators have learned how to block the vast majority of attacks, their intelligent opponents keep finding novel ways of breaking security mechanisms. A direct consequence of the growing complexity of security systems is an enormous amount of security alerts not only in large but also in medium-sized networks. As a result manual inspection of each such alert has become infeasible in many cases. The core topic of this talk will be to point out how visual analytics can be used to fight cybercrime. In particular, it will be shown that the combination of automated and visual analysis techniques can empower administrators to derive valuable information from large amount of network traffic and security alerts and to make informed decisions in time-critical situations. The insight gained in this process can then result in a refinement of existing security mechanisms and ultimately lead to the critical competitive advantage in the tight arms race against the attackers.