ENISA Quarterly Review

Vol. 5, No. 3, September 2009

IN THIS EDITION

A Letter from the Executive Director	**2**
A Word from the Editor	**3**
Resilience and Information Sharing	**4**
A Resilient and Secure Internet Infrastructure	4
Occasional Curiosity or Regular Routine? Evaluating the reliability of the Internet infrastructure	6
Three European 'Trusted Information Sharing' Projects	7
Critical Information Infrastructure Protection	**9**
Public-Private Partnership for CIIP – Case Finland	9
Interdependency between Energy and Telecommunications	11
Emerging and Future Risks	**13**
Identification of Emerging and Future Risks in a 2011 eHealth Scenario	13
Drivers of Emerging and Future Threats in ICT Infrastructures	15
Skills and Certifications	**16**
Cyber-Security Skills – The Cost of Ignorance	16
Penetration Testing – What's That?	16
A New Qualification to Guarantee Secure Software Engineering Skills	18
Awareness and End-User Issues	**19**
End-user Security: Misused and Misunderstood?	19
Human Factors in the Dependability of IP Networks	20
Technologies	**22**
A Secure Approach for Embedded Systems in Japan	22
tNAC: trusted Network Access Control	23

enisa 5th ANNIVERSARY
European Network and Information Security Agency

ISSN1830-3609

EMERGING AND FUTURE RISKS

Drivers of Emerging and Future Threats in ICT Infrastructures

Sotiris Ioannidis, Evangelos Markatos, Engin Kirda and Christopher Kruegel




Computer systems, networks and Internet users are under constant threat from cyber-attacks. A threat is any indication, circumstance or event with the potential to cause harm to an Information and Communications Technologies (ICT) infrastructure and the assets that depend on this infrastructure. Identifying and evaluating threats early enough is critical for protecting both infrastructures and citizens. Of course this is an extremely challenging endeavour. The past has witnessed many stunning scientific and technical advances, and these advances have transformed society and the way people use and rely on information technology. But attackers are also very creative and constantly invent new ways of abusing technologies and applications either for financial gain or simply because they enjoy virtual vandalism. Trying to accurately predict possible new threats is therefore no easy task, but it is important to think about the potential risks and threats of emerging technologies and their applications. Otherwise, one would surrender to the enemy and, at best, simply react to his new attacks.

Operating along those lines, the scientific community involved in the FORWARD project has been systematically working to identify emerging and future threats in ICT infrastructures. The FORWARD project is a co-ordination action, supported by the European Commission, whose purpose is to facilitate an agenda of research problems by mobilising the critical mass of European researchers in network and systems security. FORWARD has brought together more than 100 experts from academia, industry and government, creating the critical mass needed to identify the emerging and future security threats in network and systems security. Having completed two public workshops and hundreds of multi-party communications, the FORWARD community has identified the dimensions that drive the security threats of the future. These dimensions serve as the main drivers of development in general, and allow us to set a framework in which each working group can systematically explore threats.

The four main dimensions identified are the following:

New technologies: By new technologies, we mean technical advances that provide functionality that simply was not there before. Clearly, this is very difficult to predict, but there are certain drivers, such as Moore's law, that have been valid for a long time. Extrapolating these steady trends, we foresee *much faster networks* (both wired and wireless), a substantial increase in parallelism (*multi-core* machines) and better energy and battery technology, which will catalyse the prevalence of mobile computing. Computing devices will also become smaller and cheaper. As a result, they will become more widespread, and they will be able to support more and richer applications.

New applications: New applications means completely new uses of technology, uses that typically did not exist before or do not have a counterpart in the real world. One important set of emerging applications is *social networks*: tools that have rapidly reached a significant proportion of the population and that support social interactions among large user groups. Another interesting class of new applications revolves around the idea of *software as a service* – a model in which applications are hosted by providers on a large-scale computing infrastructure, such as a cloud. This deployment and computing model is profoundly different from the traditional client-server model, presenting new challenges in security and privacy.

New business models: With new business models, we refer to the fact that certain services or applications that might already exist in some form start increasingly to rely on a working ICT infrastructure. For example, online shopping, online banking, and even eGovernment would be considered new business models in our taxonomy. That is, these services did exist before (as retail stores, banks and offices), but they are now increasingly carried out via ICT. In addition, these services do not represent a fundamentally different application, since they are typically instances of well known models of computing that are simply adapted to suit the business case.

New social dynamics and the human factor: This category takes into account possible changes in the way that people approach and use technology and certain applications. For example, young people are becoming increasingly sophisticated in their use of ICT, and at the same time ICT users in general are increasingly willing to entrust devices and applications with a significant amount of private information. This opens up the possibility for a wide variety of new threats.

The results of FORWARD are expected to be used not only by researchers, but also by policy-makers who want to facilitate a road towards a more secure cyber-space. Thus, researchers, policy-makers, decision-makers and practitioners are encouraged to follow the activities of FORWARD and provide their feedback at www.ict-forward.eu/.

Sotiris Ioannidis (sotiris@ics.forth.gr) is an Associate Researcher at the Distributed Computing Systems Laboratory of FORTH-ICS and an Adjunct Professor at the Computer Science Department of the University of Crete.

Evangelos Markatos (markatos@ics.forth.gr) is the Director of the Distributed Computing Systems Laboratory at FORTH-ICS, a Professor of Computer Science at the University of Crete and a member of ENISA's Permanent Stakeholders' Group.

Engin Kirda (ek@iseclab.org) is Associate Professor at Eurecom and an Adjunct Professor at the Technical University of Vienna.

Christopher Kruegel (chris@cs.ucsb.edu) is an Assistant Professor and the holder of the Eugene Aas Chair in Computer Science in the Computer Science Department of the University of California, Santa Barbara.