

# 2011 First SysSec Workshop

# SysSec 2011

## Table of Contents

Preface.....	viii
Committee Lists.....	ix
List of Reviewers.....	x

---

### Part I: Student Papers

Unity in Diversity: Phylogenetic-inspired Techniques for Reverse Engineering and Detection of Malware Families .....	3
<i>Wei Ming Khoo and Pietro Lió</i>	
Detecting Insufficient Access Control in Web Applications .....	11
<i>George Nosevich and Andrew Petukhov</i>	
I/O Attacks in Intel PC-based Architectures and Countermeasures .....	19
<i>Fernand Lone Sang, Vincent Nicomette, and Yves Deswarte</i>	
CAPTCHuring Automated (Smart) Phone Attacks .....	27
<i>Iasonas Polakis, Georgios Kontaxis, and Sotiris Ioannidis</i>	
Outsourcing Malicious Infrastructure to the Cloud .....	35
<i>Georgios Kontaxis, Iasonas Polakis, and Sotiris Ioannidis</i>	
Demarcation of Security in Authentication Protocols .....	43
<i>Naveed Ahmed and Christian Damsgaard Jensen</i>	

### Part II: Research Roadmap Papers

The MINESTRONE Architecture Combining Static and Dynamic Analysis Techniques for Software Security .....	53
<i>Angelos D. Keromytis, Salvatore J. Stolfo, Junfeng Yang, Angelos Stavrou, Anup Ghosh, Dawson Engler, Marc Dacier, Matthew Elder, and Darrell Kienzle</i>	
The Free Secure Network Systems Group: Secure Peer-to-Peer Networking and Beyond .....	57
<i>Christian Grothoff</i>	
Adapting Econometric Models, Technical Analysis and Correlation Data to Computer Security Data .....	59
<i>Spyros K. Kollias, Vasileios Vlachos, Alexandros Papanikolaou, and Vassilis Assimakopoulos</i>	

A Trustworthy Architecture for Wireless Industrial Sensor Networks: Research Roadmap of EU TWISNet Trust and Security Project .....	63
<i>Markus Webner, Sven Zeisberg, Alexis Olivereau, Nouba Oulba, Laura Gheorghe, Emil Slusanschi, Basil Hess, Felix von Reischach, Mike Ludwig, and David Bateman</i>	
Mapping Systems Security Research at Chalmers .....	67
<i>M. Almgren, Z. Fu, E. Jonsson, P. Kleberger, A. Larsson, F. Moradi, T. Olovsson, M. Papatriantafilou, L. Pirzadeh, and P. Tsigas</i>	
Exploring the Landscape of Cybercrime .....	71
<i>Zinaida Benenson, Andreas Dewald, Hans-Georg Eßer, Felix C. Freiling, Tilo Müller, Christian Moch, Stefan Vömel, Sebastian Schinzel, Michael Spreitzenbarth, Ben Stock, and Johannes Stüttgen</i>	
CLEARER: CrySyS Laboratory Security and Privacy Research Roadmap .....	75
<i>Levente Buttyán, Márk Félegyházi, and Boldizsár Bencsáth</i>	
Towards Malware-Resistant Networking Environment .....	79
<i>Dennis Gamayunov</i>	
Research Roadmap on Security Measurements .....	83
<i>Xenofontas Dimitropoulos</i>	
From SSIR to CIDre: A New Security Research Group in Rennes, France .....	86
<i>Emmanuelle Anceaume, Christophe Bidan, Sébastien Gambs, Guillaume Hiet, Michel Hurfin, Ludovic Mé, Guillaume Piolle, Nicolas Prigent, Eric Totel, Frédéric Tronel, and Valérie Viet Triem Tong</i>	
Building a Long Term Strategy for International Collaboration in Trustworthy ICT: Security, Privacy and Trust in Global Networks and Services .....	90
<i>James Clarke, Neeraj Suri, Michel Riguidel, and Aljosa Pasic</i>	
System Security Research at Newcastle .....	94
<i>Jeff Yan</i>	
Security Research at NASK: Supporting the Operational Needs of a CERT Team and More .....	96
<i>Piotr Kijewski and Adam Kozakiewicz</i>	
The Security Aspects of the Research Activities in IICT-BAS .....	100
<i>Kiril Boyanov</i>	
Less is More—A Secure Microkernel-Based Operating System .....	103
<i>Adam Lackorzynski and Alexander Warg</i>	
Computer Security and Machine Learning: Worst Enemies or Best Friends? .....	107
<i>Konrad Rieck</i>	
Systems Security at VU University Amsterdam .....	111
<i>Herbert Bos, Lorenzo Cavallaro, and Andrew S. Tanenbaum</i>	
System Security Research at Birmingham: Current Status and Some Future Work .....	115
<i>Marco Cova</i>	

The SPARCHS Project: Hardware Support for Software Security .....	119
<i>Simba Sethumadhavan, Salvatore J. Stolfo, Angelos Keromytis, Junfeng Yang, and David August</i>	
Malicious Website Detection: Effectiveness and Efficiency Issues .....	123
<i>Birbanu Esbete, Adolfo Villafiorita, and Komminist Weldemariam</i>	
Systems Security Research at Politecnico di Milano .....	127
<i>Federico Maggi and Stefano Zanero</i>	
Systems Security Research at Ruhr-University Bochum .....	131
<i>Thorsten Holz</i>	
<b>Author Index</b> .....	135