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
Wei Ming Khoo and Pietro Liò

Detecting Insufficient Access Control in Web Applications .............................................................................11
George Nosevich and Andrew Petukhov

I/O Attacks in Intel PC-based Architectures and Countermeasures ..................................................................19
Fernand Lone Sang, Vincent Nicomette, and Yves Deswarte

CAPTCHuring Automated (Smart) Phone Attacks .............................................................................................27
Iasonas Polakis, Georgios Kontaxis, and Sotiris Ioannidis

Outsourcing Malicious Infrastructure to the Cloud ............................................................................................35
Georgios Kontaxis, Iasonas Polakis, and Sotiris Ioannidis

Demarcation of Security in Authentication Protocols .......................................................................................43
Naveed Ahmed and Christian Damsgaard Jensen

Part II: Research Roadmap Papers

The MINESTRONE Architecture Combining Static and Dynamic Analysis
Techniques for Software Security ..........................................................................................................................53
Angelos D. Keromytis, Salvatore J. Stolfo, Junfeng Yang, Angelos Stavrou, Anup Ghosh, Dawson Engler, Marc Dacier, Matthew Elder, and Darrell Kienzle

The Free Secure Network Systems Group: Secure Peer-to-Peer Networking and Beyond ................................57
Christian Grotboff

Adapting Econometric Models, Technical Analysis and Correlation Data to Computer Security Data ................59
Spyros K. Kollias, Vasileios Vlachos, Alexandros Papanikolaou, and Vassilis Assimakopoulos
A Trustworthy Architecture for Wireless Industrial Sensor Networks: Research Roadmap of EU TWISNet Trust and Security Project

Markus Wehner, Sven Zeisberg, Alexis Olivier, Nouba Oulba, Laura Gheorghe, Emil Slusanschi, Basil Hess, Felix von Reischach, Mike Ludwig, and David Bateman

Mapping Systems Security Research at Chalmers

M. Almgren, Z. Fu, E. Jonsson, P. Kleberger, A. Larsson, F. Moradi, T. Olorsson, M. Papatriantafilou, L. Pirzadeh, and P. Tsigas

Exploring the Landscape of Cybercrime

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

CLEARER: CrySyS Laboratory Security and Privacy Research Roadmap

Levente Buttyán, Márk Félegyházi, and Boldizsár Bencsáth

Towards Malware-Resistant Networking Environment

Dennis Gamayunov

Research Roadmap on Security Measurements

Xenofontas Dimitropoulos

From SSIR to CIDre: A New Security Research Group in Rennes, France

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


James Clarke, Neeraj Suri, Michel Riguidel, and Aljosa Pasic

System Security Research at Newcastle

Jeff Yan

Security Research at NASK: Supporting the Operational Needs of a CERT Team and More

Piotr Kijewski and Adam Kozakiewicz

The Security Aspects of the Research Activities in IICT-BAS

Kiril Boyanov

Less is More—A Secure Microkernel-Based Operating System

Adam Lackorzynski and Alexander Warg

Computer Security and Machine Learning: Worst Enemies or Best Friends?

Konrad Rieck

Systems Security at VU University Amsterdam

Herbert Bos, Lorenzo Cavallaro, and Andrew S. Tanenbaum

System Security Research at Birmingham: Current Status and Some Future Work

Marco Cova
The SPARCHS Project: Hardware Support for Software Security ..........................................................119
   Simha Sethumadhavan, Salvatore J. Stolfo, Angelos Keromytis, Junfeng Yang, and David August
Malicious Website Detection: Effectiveness and Efficiency Issues .......................................................123
   Birhanu Eshete, Adolfo Villafiorita, and Komminist Weldemariam
Systems Security Research at Politecnico di Milano ........................................................................127
   Federico Maggi and Stefano Zanero
Systems Security Research at Ruhr-University Bochum ....................................................................131
   Thorsten Holz

Author Index ............................................................................................................................................135