Special Issue on Security and High Performance Computer Systems

Editorial

Malicious attacks on computer systems everyday propose many new challenges and, hence research on providing security in computing receives significant attention continuously. Some major challenges include unknown attack analysis, detection, and response. Another challenge is related to performances of such security tools. Indeed, new attacks require computationally complex analysis and thus require tools in high performance computer systems. We conducted a workshop in 2008 based on this theme.

This special issue of Journal of Computers contains expanded versions of eight selected papers from that Workshop on Security and High Performance Computing Systems (SHPCS 2008) as part of the 2008 International Conference High Performance Computing and Simulation (HPCS 2008), held in Nicosia, Cyprus 3 – 6 June 2008. SHPCS was held in Conjunction with the 22nd European Conference on Modeling and Simulation (ECMS 2008). SHPCS 2008, HPCS 2008 and ECMS 2008 were highly successful events whose joint programs provided the participants with high-quality papers in the area of security, simulation, modeling, performance evaluation and high performance computing systems. The technical program of SHPCS 2008 comprised 11 papers authored by researchers from 8 different countries. The eight papers selected deal with various aspects of security: attack, data collection, detection and prevention. Below, we briefly introduce the eight papers.

The paper by Bernaschi, Bisson, Gabrielli, and Tacconi proposes a dictionary based attack strategy against cryptosystems compliant to the OpenPGP standard. They developed a simplified mechanism to quickly test passphrases that might protect a specified private key ring. Only passphrases that pass this test complete the full validation procedure. The authors propose a distributed computing architecture to carry out large scale dictionary attacks using the proposed strategy. They experimented with their attack strategy in a test-bed consisting of 100baseT Ethernet LAN with 20 personal computers.

The paper by Briffaut, Lalande, and Toinard presents the design of a secured high-interaction honeypot that welcomes attackers, allows malicious activities but prevents system corruption. The clustered honeypot architecture consists of three types of hosts (1) mandatory access control, (2) Discretionary Access Conrol (DAC) and Microsoft Windows operating systems. Various off-the-shelf security tools are deployed to detect a corruption and to ease analysis. In addition, host and network information enabled them full analysis for complex scenario of attacks. In fact, in a second paper, Blanc, Clemente, Rouzaud-Cornbas, and Toinard classify the malicious distributed SELinux activities by using collected data from the honeypot.

Becker, Drozda, Schaust, Bohlmann, and Szczerbicka in their paper discuss and evaluate several learning algorithms according to their suitability for intrusion and attack detection. Learning algorithms subject to evaluation include bio-inspired approaches such as Artificial Immune Systems or Neural Networks, and classical such as Decision Trees, Bayes classifier, Support Vector Machines, k-Nearest Neighbors.

The paper by Dai, Guha, and Lee present an approach to detect unknown virus using dynamic instruction sequences from unknown executables. Following a data mining process, the authors perform feature extraction, feature selection and then build a classification model to learn instruction association patterns from both benign and malicious dataset automatically. Then by applying this classification model, the nature of an unknown program is predicted. Runtime instruction sequences are collected in a virtual program monitor designed by them.

Biscotti, Capuzzi, Cardinale, Pagliarecci, and Spalazzi present a hybrid approach to intrusion detection and prevention for web applications. This approach consists in combining anomaly detection, misuse detection, and a prevention module. The proposed system updates the misuse and anomaly model based on the feedback received by the security manager. From the results arises an improvement with respect to other state-of-the-art Web-IDSs.

Benerecetti, Cuomo, Peron consider the problem of verifying time–sensitive security protocols, where temporal aspects explicitly appear in the description. For that purpose, they present a model checking tool, TPMC, for the analysis of security protocols employing THLPSL (Timed High-Level Protocol Specification Language) as a specification language and UPPAAL as the model checking engine. They also report some experimental results on a number of timed and untimed security protocols.

The paper by Hahkala, Mikkonen, Silander, and White identifies the requirements, defines the architecture and the protocol for a pseudonymity system for grids. This pseudo-anonymous system will protect users from tracing them and their actions by others. The paper also discusses some appropriate applications of this architecture.

We would like to express our appreciation to the authors of the eight papers who made this special issue possible. Our sincere thanks also go to the referees who have provided their review reports in a timely manner and to the Editor-in-chief Prof. Dr. Prabhat Mahanti who have given us helpful instructions and guidance.

Guest Editors:

Luca Spalazzi
Dipartimento di Ingegneria Informatica, Gestionale e dell'Automazione
Università Politecnica delle Marche
I-60131 Ancona – Italy
Email address: spalazzi@diiga.univpm.it

Ratan Guha
University of Central Florida
School of Electrical Engineering and Computer Science
Orlando, FL 32816-2362
Email address: guha@cs.ucf.edu

Luca Spalazzi is associate professor at the Università Polietcnica delle Marche. He received the M.S. in Electronic Engineering and the Ph.D in Artificial Intelligent Systems from the University of Ancona, Italy in 1989 and 1994, respectively. He has worked as consultant at the Istituto di Ricerca Scientifica e Tecnologica (IRST), Trento, Italy. He was a visiting scholar at the Australian Artificial Intelligence Institute (AAII), Carlton, Vic., Australia and at the Computer Science Department, Stanford University, California. His research has been supported by grants from European Union and MURST (Italian Department of University and Scientific Research). His present research areas include Computer and Network Security (in cooperation with Italian State Police), Case-based Reasoning, Web Services, and Multi-agent Systems. He has served as a member of the program committee of several conferences, and as Chair of SHPCS since 2007.

Ratan Guha is a Professor of Computer Science at the University of Central Florida, Orlando. He received his B.Sc. degree with honors in Mathematics and M.Sc. degree in Applied Mathematics from University of Calcutta and received the Ph.D. degree in Computer Science from the University of Texas at Austin in 1970. He has authored over 125 papers published in various computer journals, book chapters and conference proceedings. His research interests include distributed systems, computer networks, security protocols, modeling and simulation, and computer graphics. His research has been supported by grants from the US Army Research Office, US National Science Foundation, STRICOM, PM-TRADE, NASA, and the State of Florida. He has served as a member of the program committee of several conferences, as the general chair of CSMA'98 and CSMA'2000 and as the guest co-editor of a special issue of the Journal of Simulation Practice and Theory. He is a member of ACM, IEEE, and SCS and served as a member of the Board of Directors of SCS from 2004 to 2006. He is currently serving in the editorial board of two journals: International Journal of Internet Technology and Secured Transactions (IJITST) published by Inderscience Enterprises, and Modelling and Simulation in Engineering published by Hindawi Publishing Corporation.