SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2012; **5**:831–833
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.598

GUEST EDITORIAL

Defending against insider threats and internal data leakage

By Ilsun You, Gabriele Lenzini, Marek R. Ogiela and Elisa Bertino, Guest Editors

In the last decade, computer science researchers have been working hard to prevent attacks against the security of information systems. Different adversary models have incarnated the malicious entities against which researchers have defined security properties, identified security vulnerabilities, and engineered security defenses. These adversaries were usually intruders, that is, outsiders trying to break into a system's defenses.

However, security reports clearly reveal that an increasing number of threats come presently from insiders. Insiders are legally authorized individuals who have, or used to have, access to corporate resources. Their illegal activities are not easily distinguishable from the uncommon but legal activities executed by honest corporate users.

To detect insiders' illegal activities is therefore hard, to recover after a security breach by an insider is expensive, and even though insider attacks occur less frequently than outsider, their consequences are far more severe. Insiders can cause significant damages to enterprises, companies, and countries. They can threaten an enterprise's reputation, weaken national and international competitiveness, and compromise a country's overall business.

Therefore, it is necessary to develop countermeasures that are able to evaluate and to contain the risks of unauthorized accesses coming from insiders. Those countermeasures—physical, managerial, and technical—should construct an integral security management system that is able to protect, internally as well as externally, a company's major information assets.

This special issue collects scientific studies and works on security technologies and management systems designed to protect an organization's information systems from corporate *intrusions*. It aims to be the showcase for researchers who look at state-of-the-art solutions about preventing leakage of organizations' information caused by insiders or by insiders' actions. This special issue consists of one invited contribution and seven carefully selected scientific papers.

The invited paper, *Reverse-safe Authentication Protocol for Secure USB Memories*, by K. Lee, K. Yim, and E. Spafford, opens the special issue. This paper studies the *security of USB memories*. These small but capacious storage devices are extremely handy. People use them to carry personal and professional information, including pieces of very sensitive and valuable data. Unfortunately, USB memory devices are easy to steal, and once they are lost or stolen, their valuable content can be hacked.

Although USB data can be encrypted and USB access can require authentication, hackers are able to break into a USB device's protections by reverse-engineering. This invited paper analyzes a large set of attacks against the three most used families of USB authentication protocols: plaintext ID and password, hashed ID and password, and challenge response. It also proposes and comments an innovative authentication protocol whose security overtakes that of existing products.

The first paper, *Minimizing Insider Misuse Through Secure Identity Management*, by L. Fuchs and G. Pernul, addresses a serious problem in companies' security management: *identity chaos*. This problem arises when identities and authorization policies are badly managed. In a situation of identity chaos, users have multiple roles and identities, different privileges, obligations, and responsibilities; likewise, user access rights are spread across a variety of security domains. Such a chaotic situation is a fertile humus for insiders who take advantage of mistakenly assigned rights and gain unauthorized access to pieces of information that should be usually off their control. This paper describes a methodology, called *Structured and Security Identity Management*, that helps gather across-domain identity information, remove orphan accounts, cleanse account data, group access rights on the basis of job functions and organizational structure, and suggest user roles that may serve in role-based access controls. This paper's innovative management reduces, or it avoids in the first place, identity chaos, the authors prove.

The next paper, *A Comparison of One-class Bag-of-words User Behavior Modeling Techniques for Masquerade Detection*, by M. B. Salem and S. J. Solfo, studies *masquerade attacks*. Masquerade attacks consist of actions apparently coming from a legitimate user, but instead performed by someone impersonating the honest insider. This usually happens after that the insider's digital identity has been stolen. Uncovering a masquerade attack is difficult. It requires to profile user behavior and to detect abnormal patterns indicative of an impersonation. The paper compares the accuracy and the performances of two strategies for profiling user behavior: one-class support vector machines and Hellinger distance-based technique. The experimental evaluation shown in this paper proves that one-class support vector machines suit better operational masquerade detection monitoring systems.

Detecting insider activities, precisely malicious actions by insiders who have gained administrative privileges, is the main topic of *Enhancing Directory Virtualization to Detect Insider Activity*, by W. Claycomb, D. Shin, and A. Gail-Joon. This work proposes an architecture that, by building a policy-

based detection and an analysis framework on top of directory virtualization, helps unveil insider attacks directed against *directory services*. Directory services are used within an organization to share information about users and computers, as well as to authenticate identities and to provide credential for access control. They are usually targeted by insiders who want to steal sensitive company's data resource. Typical malicious actions upon directory services are the following: creating new users, changing some group's membership, and resetting user passwords. Directory virtualization allows a system-wide overview of multiple data sources. Upon this global view, this paper proposes to build role-based access control policies that describe healthy user accounts in terms of interdependences and relationships with other data sources. Virtualization is also what enables the architecture to seek for unauthorized changes in multi-disparate date sources and for violations of system-wide access control policies. This paper intensively evaluates the proposed architecture and discusses related experimental results.

The work *Identity Management-based Social Trust Model for Mediating an Information Sharing and a Privacy Enhancement*, by K. Mucheol, S. Jiwanand, N. Sanghyun and H. Sangyong, is about a framework for *identity management in social networks*. More easily than in other digital systems, in online social spaces, people's sharing of information leads to leakage of sensitive data and to violation of privacy. Ideally, the access to resources should be restricted and ruled by policies bound to identities and roles. In social networks, however, individuals have several different identities and roles that change frequently as people join or leave social groups. Thus, the concept of *identity* needs to be redefined. The framework that this paper proposes is a group-aware identity management that combines relationship-based identity and role-based identity. The relationship-based identity derives from the direct and indirect trust relationships between friends. The role-based identity depends on users' roles in various social interactions. This paper's solution works well even in social networks that suffer of the sparsity problem, that is, in digital communities with little information for one individual to estimate the trustworthiness in the others.

Sometimes, insiders gain access by installing malwares on machines they want to control. A post-mortem analysis, after a malware's strike, can help retrieve information useful to contain the spread of insider intrusions. This is the topic of the paper *MalPEFinder: Fast and Retrospective Assessment of Data Breaches in Malware Attacks*, by L. Shun-Te and C. Yi-Ming. This paper's work describes MalPEFinder, a tool that retrospectively detects files that have fallen victims of a malware's attack and that assesses the extension of the consequent data breach. The authors have tested it against 52 common malwares, and they prove it to have better performances (i.e., detection and false positive rates) than Splunk, a common malware detection software.

Acting on a wider scale than that of malware's, *botnet attacks* have wreaked greater havoc worldwide. Botmasters endeavor to subjugate as many PCs as possible to have a fleet of platforms from where to initiate malign actions, such as egg downloading, launching denial-of-service attacks, spamming, spying, and spreading more botnets. The paper *Adaptive Learning and Mining Model for Botnet Propagation Early Detection and Size Estimation*, by K. Do Hoon, uses multivariate stream data classification with *simple text classifiers* to monitor port-scanning traffics due to botnets: from that, it generates diverse botnet propagation patterns. String patterns are trained through the hidden Markov model, and botnet's actual activities can be detected by pattern matching, or by analysis of similarities, with the trained scanning patterns. The authors prove that this paper's technique raises early detection rates by more than 30.6% on the total average, with the false positive hovering below 6% and the F-measure over 90%.

The last work, *ACT: Towards Unifying the Constructs of Attack and Defense Trees*, by R. Arpan, K. Dong Seong, and T. Krisor, focuses on attack/defense models. Those models help quantify security in terms of losses caused by attacks and of gains obtained from enforcing security defenses. The paper describes an innovative model of this kind, called *attack countermeasure tree* (ACT). It allows to model attacks as well as detection and mitigation mechanisms and to generate attack/defense scenarios. It is also possible to perform qualitative and probabilistic analysis in terms of costs, importance, risks, impacts, and return-on-attack and return-on-investment indicators. ACT is a non-state–space model: as such, it avoids the state–space explosion problem, which afflicts similar models such as the attack/response trees.

In conclusion, this special issue offers a groundbreaking view of recent advances in ideas and strategies for defending digital systems from insider threats and for reducing the consequent internal data leakage. This special issue offers to its readers both future research directions and viable commercial inspiration for innovative applications.

We would like to thank Wiley, the publisher of this collection. Special thanks to the editor-in-chief, Prof. Hsiao-Hwa Chen, for his effort, advices, and constant and patient guidance, which have accompanied us all along the time required to bring this special issue to its final version. We thank all the anonymous reviewers for their precious time and their contribution in reviewing all the papers. Their effort helped us select the excellent papers that compose this monograph. Finally, we thank the authors of this special issue's papers. Without their contributions, this volume would not have been possible. We wish you all an enjoyable reading.

Guest Editors

Ilsun You
Korean Bible University, South Korea
E-mail: ilsunu@gmail.com

Gabriele Lenzini
SnT/University of Luxembourg, Luxembourg

Marek R. Ogiela
AGH University of Science and Technology, Poland

Elisa Bertino
Purdue University, U.S.A.

Security Comm. Networks 2012; **5**:831–833 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

AUTHORS' BIOGRAPHIES

Prof. Ilsun, You - Ilsun You received his M.S. and Ph.D. degrees in Computer Science from Dankook University, Seoul, Korea in 1997 and 2002, respectively. From 1997 to 2004, he worked for the THIN multimedia Inc., Internet Security Co., Ltd., and Hanjo Engineering Co., Ltd. as a research engineer. Since 2005, he has been a professor in the School of Information Science at the Korean Bible University. His research interests include internet security, authentication, access control, MIPv6, and ubiquitous computing. He has served or is currently serving on the program committees of international conferences and workshops such as MobiWorld, IMIS, MIST, CISIS, BWCCA, and so forth. Also, he serves as an editor or on the editorial board for International Journal of Space-based and Situated Computing (IJSSC), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Computing and Informatics (CAI), Journal of Computer Systems, Networks, and Communications, International Journal of Smart Home (IJSH), and Journal of Korean Society for Internet Information (KSII). In addition, he has served as a guest editor of several journals such as Wireless Communications and Mobile Computing (WCMC), Mobile Information Systems (MIS), Wireless Personal Communications (WPC), Information Sciences, Journal of Intelligent Manufacturing (JIM), Ad Hoc and Sensor Wireless Networks (AHSWN), Intelligent Automation and Soft Computing (AutoSoft), Computing and Informatics (CAI), and Information Systems Frontiers (ISF). He is a member of the IEICE, KSII, KIISC, IEEK, and KIPS.

Dr. Gabriele, Lenzini - G. Lenzini, Ph.D., studied Information Science and Computer Science at the University of Pisa and obtained his Ph.D. in Computer Science at the Twente Universiteit. He conducted his research at the University of Pisa and CNR (Italian Council of Research) in Italy, and University of Twente and Telematica Instituut for ICT research in The Netherlands. From February 2010, he is an associate researcher at the Interdisciplinary Centre of Reliability, Security and Trust of the University of Luxembourg. Lenzini′s expertise includes formal models for security, privacy and trust, design of secure systems, and analysis and validation of system security (web services, authentication protocols, context-aware architectures, and location-based services). He is an author of about 30 scientific publications. He has been a PC in a large number of conferences and workshops in the area of security, privacy, and trust. He has been chair of the Context Awareness and Trust workshops (CAT07, CAT08, CAT09, and CAT10), Location-based Services Location Assurance and Privacy workshop (LASP), and recently Socio-technical Aspects in Security and Trust workshops (STAST 2011 and STAST 2012).

Prof. Marek, R Ogiela - Marek R. Ogiela D., SC, Ph.D., works at the AGH University of Science and Technology in Krakow. In 1992, he graduated from the Mathematics and Physics Department at the Jagiellonian University. In 1996, for his honors in doctoral thesis on syntactic methods of analysis and image recognition, he was awarded the title of Doctor of Control Engineering and Robotics at the Faculty of Electrical, Automatic Control, Computer Science, and Electronic Engineering of the AGH University of Science and Technology. In 2001, he was awarded the title of Doctor Habilitated in Computer Science for his research on medical image automatic analysis and understanding. In 2005, he received a professor title in technical sciences. He is a member of numerous world scientific associations (IEEE–senior member, SPIE–senior member, SIIM, etc.) as well as of the Forecast Committee "Poland 2000 Plus" of the Polish Academy of Science and a member of Interdisciplinary Scientific Committee of the Polish Academy of Arts and Sciences (Biocybernetics and Biomedical Engineering Section in the years 2003–2011). He is an author of more than 220 scientific international publications on pattern recognition and image understanding, artificial intelligence, IT systems, and biocybernetics; of recognized monographs in the field of cryptography and IT techniques; and of an innovative approach to cognitive medical image analysis. For his achievements in these fields, he was awarded many prestigious scientific honors, including Prof. Takliński's award (twice) and the first winner of Prof. Engel's award.

Prof. Elisa, Bertino - Elisa Bertino is a professor of Computer Science at Purdue University and serves as a research director of the Center for Education and Research in Information Assurance and Security (CERIAS) and an interim director of Cyber Center (Discovery Park). Previously, she was a faculty member and department head at the Department of Computer Science and Communication of the University of Milan. She is a fellow of the IEEE and the ACM. She received the IEEE Computer Society Technical Achievement Award for outstanding contributions to database systems and database security and advanced data management systems and the IEEE Computer Society Tsutomu Kanai Award for pioneering and innovative research contributions to secure distributed systems in 2002 and 2005, respectively.