Journal of Computer Security 16 (2008) 261–264
IOS Press

Guest Editors' Introduction

George O.M. Yee [a], Chunming Rong [b] and Laurence T. Yang [c]
[a] *Institute for Information Technology, National Research Council Canada, Ottawa, Ontario, Canada*
E-mail: george.yee@nrc.ca
[b] *Department of Electronics and Computer Technology, University of Stavanger, Stavanger, Norway*
E-mail: chunming.rong@uis.no
[c] *Department of Computer Science, St. Francis Xavier University, Antigonish, Nova Scotia, Canada*
E-mail: lyang@stfx.ca

The modern world runs on information. As a result, the word "security" is probably the most often mentioned word today in connection with information. Indeed, the world has found that security threats know no boundaries as they endanger networks and distributed systems wherever such systems are found. The importance of security lies in the fact that all systems are vulnerable to attack, whether they are traditional computer networks, or recent advances such as sensor networks, P2P computing, or ubiquitous computing. Security protects systems from an ever growing number of malicious threats such as virus and man-in-the-middle attacks. With the growing impact of the electronic society, security and its related areas privacy and trust, are now fundamentally important to the conduct of business via the Internet, involving the real-time, distributed, electronic exchange of information across different applications, across different platforms, and across enterprise borders.

The Third IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS-07) provided a meeting place for researchers from universities, government, and industry to get together and discuss recent progress in the areas of network and distributed systems security. This special issue of the *Journal of Computer Security* aims to address research into security solutions that demonstrate the challenges of security at fundamental levels of application for all areas of information technology. It contains extended versions of four of the best papers from SSNDS-07. We are pleased to serve as guest editors for this special issue. We summarize each paper as follows.

In the first paper, "Accelerated AES implementations via generalized instruction set extensions", Elbirt presents a general purpose instruction set extension for a 32-bit SPARC V8 compatible processor core that improves the performance of Galois Field fixed field constant multiplication, a core element of the AES. He shows that the extension speeds up AES encryption when compared to pure software implementations at a justifiable small hardware cost. Elbirt claims that the speed improvement matches that of previously proposed AES-specific instruction set extensions while providing a generalized implementation format suitable for other algorithms that employ Galois Field fixed field constant multiplication.

The second paper, "On replacing cryptographic keys in hierarchical key management systems", by Kayem, Akl and Martin, proposes an algorithm that minimizes the cost of key replacement when group membership changes for a group whose members have access to protected data that is governed by a hierarchical key management system. The algorithm associates a timestamp with each key. When group membership changes, instead of re-keying and re-encrypting the affected data, only the timestamps are updated and new verification credentials computed.

In the third paper, "Coprocessor-based hierarchical trust management for software integrity and digital identity protection", Wang and Dasgupta present an approach to defend against malware and rootkits that may be unaffected by normal security measures. They describe a hierarchical trust management scheme in which the root of trust is in a tamper-proof hardware co-processor on a PCI bus. The co-processor checks the OS kernel for integrity, which in turn checks other components until it is established that the entire system is free of rootkits. Wang and Dasgupta claim that their checker can be extended to encompass all applications and anti-virus software.

In the fourth and final paper, "Protection against unauthorized access and computer crime in Norwegian enterprises", Hagen, Sivertsen and Rong present a selection of findings from the Norwegian Computer Crime and Security Survey 2006 and evaluate the strengths and weaknesses of the survey. One surprising result is that there are large differences in security practices between small and large enterprises, even for security measures that should have been implemented by all enterprises, independent of size. Consistent with previous surveys, the 2006 survey shows that the number of reported cyber crime incidents is low due to weak detection mechanisms.

The papers in this special issue illustrate some of the current challenges and research areas pertinent to security technologies for networks and distributed systems. At the same time, they also amplify the many issues that remain to be addressed. New topics will emerge, and shifts to allow focus on personal needs, as well as enterprise requirements will no doubt occur. As this happens, it becomes increasingly important to understand the issues associated with the inter-play between security technologies and computing systems, resulting in trusted systems that are sound, adaptable and evolvable.

We thank the authors for their excellent contributions and patience. We also gratefully acknowledge the thorough work of all the reviewers for this special issue.

Short bio

George O.M. Yee is a Senior Research Scientist in the Information Security Group, Institute for Information Technology, National Research Council Canada (NRC). Prior to joining the NRC in late 2001, he spent over 20 years at Bell-Northern Research and Nortel Networks. George received his PhD (Electrical Engineering), MSc (Systems and Information Science), and BSc (Mathematics) from Carleton

University, Ottawa, Canada, where he contributes as an Adjunct Research Professor. George is on the Editorial Review Board of several international journals and is a Senior Member of IEEE, and member of ACM and Professional Engineers Ontario. He was a General Co-Chair of the 2007 IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS-07), and was a member of the organizing committees of the 2006 International Conference on Privacy, Security and Trust (PST 2006) and the 2006 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2006). Dr. Yee's research interests include security and privacy for e-services and e-business, as well as engineering software for security, reliability, and performance. He has published over sixty papers within the last six years. His personal web site is at http://georgeyee.ca.

Chunming Rong received his PhD degrees in Computer Science from the University of Bergen in Norway in 1998. In 1995–1998, he was a research fellow at the University of Bergen. In 2001–2003, he was a post-doc researcher funded by Simula Research Laboratory. Currently, he is a professor and chair of the computer science section at the University of Stavanger. Chunming serves also as an adjunct professor at the University Graduate Centre, University of Oslo, since 2005. He was presented with the ConocoPhilips Communication Award (Norway) in 2007. His paper "*New infinite families of 3-designs from preparata codes over* Z_4" was awarded as Editor's Choice in *Discrete Mathematics* in 1999. Prof. Rong is an associate editor for the *International Journal of Computer Science & Applications (IJCSA)* – ISSN 0972-9038, and served in the editorial board for the *International Journal of Mobile Communications (IJMC)* – ISSN 1470-949X for 2003–2006. He was chairman of the board for the Foundation of the Norwegian Computer Science Conference (NIK) in 2005–2007. Currently, he serves as board member of the Norwegian Information Security Network (NISNet) for 2007–2011, as member of the Norwegian Informatics Council, and member of the workgroup for Information Security in Integrated Operation at the Norwegian Oil Industry Association (OLF). As project manager, Prof. Rong has received grants from the Research Council of Norway for three large projects in recent years. His research interests include computer and network security, wireless communications, cryptography, identity management, electronic payment, coding theory and semantic information integration.

Laurence Tianruo Yang is a professor at St. Francis Xavier University, Canada. His research includes high performance computing and networking, embedded systems, ubiquitous/pervasive computing and intelligence. He has published around 280 papers in refereed journals, conference proceedings and book chapters in these areas. He has been involved in more than 100 conferences and workshops as a program/general conference chair and more than 200 conferences and workshops as a program committee member. Laurence served as the vice-chair of IEEE Technical Committee of Supercomputing Applications (TCSA) until 2004, currently is the chair of IEEE Technical Committee of Scalable Computing (TCSC), the chair of IEEE Task force on Intelligent Ubiquitous Computing and the co-chair of IEEE

Task force on Autonomic and Trusted Computing. He is also in the executive committee of the IEEE Technical Committee of Self-Organization and Cybernetics for Informatics, the executive committee of IFIP Working Group 10.2 on Embedded Systems, and the executive committee of IEEE Technical Committee of Granular Computing. In addition, he is the editor-in-chief of 9 international journals and some book series. He is serving as an editor for around 20 international journals. He has been acting as an author/co-author or an editor/co-editor of 30 books from Kluwer, Springer, Nova Science, American Scientific Publishers, and John Wiley & Sons. Dr. Yang has won five Best Paper Awards (including from the IEEE 20th International Conference on Advanced Information Networking and Applications (AINA-06)), one IEEE Best Paper Award in 2007, one IEEE Outstanding Paper Award in 2007, one Best Paper Nomination, a Distinguished Achievement Award in 2005, a Distinguished Contribution Award in 2004, an Outstanding Achievement Award in 2002, the Canada Foundation for Innovation Award in 2003, and the University Research/Publication/Teaching Award 99-02/02-05/05-07.