Editorial

Hui Chen

Department of Mathematics and Computer Science,
Virginia State University,
1 Hayden Dr., P.O. Box 9068,
Petersburg, Virginia 23806, USA
E-mail: huichen@ieee.org

Bo Sun

Department of Computer Science,
Lamar University,
211 Red Bird Lane, P.O. Box 10056,
Beaumont, TX 77710, USA
E-mail: bo.sun@lamar.edu

Biographical notes: H. Chen is with the Department of Mathematics and Computer Science, Virginia State University. Before he worked as a software developer in industry, he spent a few years in geophysical research. His primary research interest is in computer systems and networking. He served as journal guest editors and various IEEE conference program committees. He is a member of the IEEE and the ACM. His research has been supported by the US National Science Foundation.

B. Sun is an Associate Professor with the Department of Computer Science, Lamar University, Beaumont, Texas. His research interests include security issues of wireless networks and other communications systems. His research has been supported by the US National Science Foundation and the 2006 Texas Advanced Research Program. He is a member of the IEEE.

As computers and computer networks are integrated into every aspect of human endeavour, security concerns have attracted increased public attention. Recent security and data breaches claimed many high- profile victims,[1] such as the RSA Security division of the EMC Corporation, Lockheed Martin, Sony's Playstation Networks, branches of US Governments, and Epsilon.[2] These security and data breaches demonstrate unprecedented challenges to individuals, academia, industry, and governments to make computers and computer networks *secure* and *usable*.

The IEEE International Workshop on Security in Computers, Networking and Communications (SCNC) is an international forum for researchers, developers, and practitioners to demonstrate new ideas, techniques, and tools on secure and usable computer and communications systems and user privacy, new threats to confidentiality, integrity, and usability of computer and communications systems and user privacy, for users to exchange their experience in new tools and techniques that lead to improvement of security, integrity, and usability of computer and communication systems.

The workshop (SCNC 2011) was held in conjunction with the 30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011) on April 15, 2011, in Shanghai, China. The workshop featured 26 paper presentations contributed from many renowned institutions world-wide. This special issue presents the extended work of 7 selected papers among the 26 papers.

Demand on improving the quality of health and medical care while making it affordable challenges even the richest countries in the world. eHealth has potential to improve the quality and lower the cost of the care. An important topic in eHealth is to protect sensitive data such as electronic medical records from unintended access. In the paper entitled 'ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing', Barua et al. propose an access control solution for eHealth systems that provide different access privileges to data requesters base on their roles and guarantee data integrity and confidentiality of patient's health information at an acceptable communication delay.

Anonymous network systems is a means to protect personal freedom and privacy. In the paper entitled 'A three dimensional sender anonymity metric', Jaggi et al. proposes an anonymity measure to quantify the overall anonymity level on the web after having examined inadequacies of the measures proposed in prior literature. They also provide the justification of their anonymity measure from distinct perspectives of three important aspects, a users, a system designer, and an attacker, leading to a three-dimensional sender anonymity measuring approach on the Web.

Two papers in this special issue study authentication mechanism. In the paper entitled ‘Improved IP multimedia subsystem authentication mechanism for 3G-WLAN networks’, Sharma and Leung proposes an authentication mechanism for heterogeneous networks consisting of 3G and WLAN networks (3G-WLAN networks). They demonstrate that 3G- WLAN networks require a multi-pass authentication procedure before availing access to IP Multimedia Subsystem (IMS), the multi-pass authentication procedure adds significant overhead and leads to possible service quality degradations. Aimed to mitigate the problem, the proposed IMS authentication procedure is a one-pass procedure and is verified using the Automated Validation of Internet Security Protocols and Applications (AVISPA) security analyser. The results establish that the proposed authentication procedure is lightweight and robust.

In the paper entitled ‘A source authentication scheme using network coding’, Fathy et al. propose a Source Authentication scheme using Network Coding. The proposed scheme is characterised with embedded authentication data within the network coding Global Encoding Vectors. They demonstrate the feasibility, provide a detailed security analysis, and estimate the throughput of the proposal via computer simulations.

Trust propagation has been a long-standing research concern in trustworthy computing. In the paper entitled ‘Rendezvous based trust propagation to enhance distributed network security’, Cheng et al. argue that most of existing trust propagation methods are not suitable for many wireless networks due to a heavy burden induced by flooding trust values in the networks. They propose a rendezvous-based trust propagation method where a rendezvous node is being used as a refer node and trust calculation and aggregation are considered along the recommendation path from the rendezvous to the requester. Performance evaluation shows 66% overhead reduction for trust propagation when compared to flood-based methods.

Liu et al. examine a piece of widely used productivity software, Microsoft Word, and reveals a telling story. Their paper entitled ‘Hidden Information in Microsoft Word’, demonstrates concealed information embedded in Microsoft Word documents sufficient to recover identities and behaviour of the users. It provides a set of suggestions on the best practices that users can take to share Microsoft Documents.

In the paper entitled ‘Exclusion-intersection encryption’, Chow and Yiu argue that Identity-Based Encryption (IBE) can enable secure and flexible role-based access control. They propose a variant of IBE, namely, *Exclusion-Intersection Encryption* to provide role-based access control on plaintext message encrypted in ciphertext. The paper indicates that the *Exclusion-Intersection Encryption* may be more suitable than traditional PKI-based schemes, hierarchical identity- based encryption schemes or attribute-based encryption schemes, for scenarios where ad-hoc collaborative group work are often and compact private keys are desirable.

The above papers demonstrate continued efforts to make the computers, computer communication and networks secure and usable. They touch many security related problems ranging from authentication, privacy, anonymity, access control to encryption, and ranging from theory to practice. We appreciate the authors who contributed extended work to this special issue. We thank all the authors who have submitted to the workshop. We owe a great deal to the reviewers and technical committee members who provided timely reviews on the submitted papers. We are grateful to the outstanding leadership of IEEE INFOCOM 2011 organising committee. Last, but not the least, we appreciate the efforts of the IJSN editorial staff which has made this special issue possible.

Notes

[1] Lulz Security, a group of hackers who have claimed responsibility of many victims listed in this paper. See Lulz Security’s press releases at http://lulzsecurity.com/releases/

[2] Epsilon is a marketing firm, whose customers include JPMorgan Chase, Citibank, Target, Walgreens, Barclays Bank, US Bancorp, Walt Disney, Marriott, Ritz-Carlton, Best Buy, L.L. Bean, Home Shopping Network, TiVo, and the College Board. For more information, see the story at http://www.nytimes.com/2011/04/05/business/05hack.html