Guest Editorial: Special issue on Next Generation Networks and Systems Security

Carol Fung[1] and Weverton Cordeiro[2]
[1]Virginia Commonwealth University, USA
cfung@vcu.edu
[2]Federal Institute of Pará @ Itaituba, Brazil (IFPA)
weverton.cordeiro@ifpa.edu.br

With the emergence of the next generation networking and system technologies such as cloud computing, software defined networking, and the Internet of things, significant changes have been brought to how networks are designed, deployed, and managed. The research work of in these areas has been important and highly active in the past few years. In this context, security has been one of the major concerns and there is a prominent trend in the growing demand on the security research in such fields. The raising question is: how to design a secure next generation network? We are searching for answers from many different aspects, such as the architecture design of a secure system, privacy-preserving communication, secure data management, trustworthy evaluation for agents in a secure system, and the management of a secure system. In this special issue, we aims to bring together the state-of-the-art research on the various security aspects of next-generation networking technologies and service management frameworks.

This special issue on "Next Generation Networks and Systems Security" attempts to highlight some of the latest research addressing those challenges. It collects a series of papers on the important topics, More specifically:

- The first paper, entitled "Robust Detection of Rogue Signals in Cooperative Spectrum Sensing" is brought by Jackson et al. [1] and deals with security in the context of Cognitive Radio Networks (CNRs), a paradigm that has attacted significant attention from industry and academia, specially for its promising potential of bringing affordable Internet access to rural areas and developing regions. Cognitive Radio Networks takes advantage of cooperative radio frequency sensing to detect which channels are available for data transmission (white spaces) within a given area. An attacker however may disguise itself as a legitimate participant of the network, and falsely report an unused channel as active (in use). Cognitive Radio Networks use reputation systems to ban those nodes, and an attacker may use this protection against the network itself, by misleading legitimate users into making false reports about spectrum occupation. Jackson et al. addresses this problem by proposing a community-detection clustering algorithm to distinguish between malicious/malfunctioning sensors from well-behaved sensors that are misguided by rogue signals.

- The paper of Mehrdad Nojoumian and Douglas R. Stinson [3], entitled "Sequential Secret Sharing as a New Hierarchical Access Structure", proposes sequential secrete sharing (SQS), a new hierarchical secret sharing protocol as a new application of dynamic threshold schemes. In this cryptographic primitive, players with various levels of authority progressively construct a sequence of secret sharing schemes with different (but related) secrets and thresholds in the absence of the dealer. Although there are existing hierarchical secret sharing schemes, only a single secret is shared among the players who are in different authority levels. The proposed SQS extended overcomes this limitation and enabled the sharing of a sequence of secretes among players with various levels of authorities.

Journal of Internet Services and Information Security (JISIS), volume: 5, number: 2 (May), pp. 1-3

- The third paper, entitled "Disincentivizing Malicious Users in RecDroid Using Bayesian Game Model", approaches the problem of attackers trying to tamper with RecDroid (a crowd-sourcing recommendation system) in order to misguide users into granting access permissions to malicious apps newly installed on their Smartphone. Rashidi and Fung [4] solve this problem by proposing a game theoretic model, in which RecDroid and attacker become players, each with a well-defined objective: while the attacker seeks to maximize the dissemination of faulty recommendations that reach legitimate users, RecDroid seeks to minimize the proportion of those recommendations that actually go through. RecDroid uses a costly, trusted expert verification whenever stakes become too high that some recommendation is potentially faulty. In this game, the attacker is disincentivized to perform a faulty move whenever the chances of him being caught become too high.

- Finally our fourth paper, entitled "Securing Implantable Cardioverter Defibrillators Using Smartphones" and written by Jiwan Ninglekhu et al. [2], proposes a novel security framework to protect Implantable Cardioverter Defibrillators (ICDs) using Smartphones. ICDs are small battery powered Implantable Medical Devices that are introduced in the patient's body to treat irregular heartbeats known as arrhythmias. The compromise of this type of device can be life threatening. This paper enforces the authenticated and authorized communication between the patient's ICD and EP controlled by an authorized physician through mediates secure communication and providing an audio/visual interface to keep the patient in-the-loop to monitor the communication occurring between the ICD and EP.

We are confident that the papers included in this special issue illustrate some of the most relevant issues investigated in the field of networking security, and might provide some interesting insights and research directions to the audience.

The Guest Editors would like to thank the Editor-in Chief (Dr. Ilsun You) for the guidance, feedback, and encouragement in the process of coming up with this special issue. More importantly, we would like to thank all authors and reviewers for their valuable input to this process, which was undoubtedly essential for making this special issue a reality. We hope you enjoy it!

References

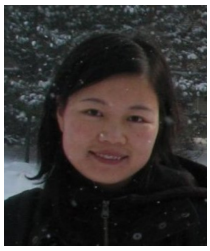
[1] D. Jackson, W. Zang, Q. Gu, and M. Yu. Robust detection of rogue signals in cooperative spectrum sensing. *Journal of Internet Services and Information Security (JISIS)*, 5(2):4–22, May 2015.

[2] J. Ninglekhu, R. Krishnan, E. John, and M. Panday. Securing implantable cardioverter defibrillators using smartphones. *Journal of Internet Services and Information Security (JISIS)*, 5(2):46–63, May 2015.

[3] M. Nojoumian and D. R. Stinson. Sequential secret sharing as a new hierarchical access structure. *Journal of Internet Services and Information Security (JISIS)*, 5(2):23–31, May 2015.

[4] B. Rashidi and C. Fung. Disincentivizing malicious users in recdroid using bayesian game model. *Journal of Internet Services and Information Security (JISIS)*, 5(2):32–45, May 2015.

Author Biography



Carol Fung received her Bachelor degree and Master degree in computer science from the university of Manitoba (Canada), and her PhD degree in computer science from the university of Waterloo (Canada). Her research interests include collaborative intrusion detection networks, social networks, security issues in mobile networks and medical systems, location-based services for mobile phones, and machine learning in intrusion detection. She is the recipient of the young professional award in IEEE/IFIP IM 2015, Alumni Gold Medal of university of Waterloo in 2013, best dissertation awards in IM2013, the best student paper award in CNSM2011 and the best paper award in IM2009. She received numerous prestige awards and scholarships including Google Anita Borg scholarship, NSERC Postdoc fellowship, David Cheriton Scholarship, NSERC Postgraduate Scholarship, and President's graduate scholarship. She has been a visiting scholar at POSTECH (South Korea), a software engineer intern at Google, and a research intern at BlackBerry.

Weverton Cordeiro received his Bachelor (2007) degree in Computer Science from the Federal University of Pará, Brazil, and M.Sc. (2009) and Ph.D. (2014) degrees also in Computer Science from the Federal University of Rio Grande do Sul, Brazil. His research interests include identity management in large scale distributed systems, network function virtualization and software defined networking, information technology service management, networking measurement and security, and wireless ad hoc networks. He was a recipient of a Microsoft Research Latin American Ph.D. Fellowship (2011), and held internship positions at Hewlett Packard and Microsoft Research. He is an Associate Professor position at the Federal Institute of Pará @ Itaituba, and a Post-doctoral Fellow at the Federal University of Rio Grande do Sul.