

# Preface

Enterprise security is an important area since all types of organizations require secure and robust environments, platforms, and services to work with people, data, and computing applications. There are instances where security breaches and privacy concerns have been the main factors preventing organizations from putting their resources in public and community domains. Even in private domains, there is no escape from the threats to cyber security, privacy, trust, and risk. We live in an information age whereby there is a massive and rapid dissemination of information. Protecting our data, privacy, and rights has become increasingly important regardless of where we are based and in which organization we work. Challenges such as data ownership, trust, unauthorized access, and big data management should be resolved by using innovative methods, models, frameworks, case studies, and analysis to reduce risks imposed by data leakage, hacking, breach of privacy, and abuse of data. To adopt the best practices, papers that can fully address security, privacy, and risk concerns are welcome. We seek papers from both technical security (theory, prototype, experiments, simulations, proofs-of-concept, and product development) and information system security (review, frameworks, best practices, statistical analysis based on surveys and recommendations) that provide good recommendations and research contributions to enterprise security. The best papers from the ES 2015 workshop were selected for this book. This book presents comprehensive and intensive research into various areas of enterprise security including a chapter on “Challenges of Cloud Forensics” by Hamid Jahankhani and Amin Hosseini-Far, who discuss how cloud computing has generated significant interest in both academia and industry, but it is still an evolving paradigm. Cloud computing services are also a popular target for malicious activities, resulting in the exponential increase of cyber attacks. Digital evidence is the evidence that is collected from the suspect’s workstations or electronic media that could be used to assist computer forensics investigations. Cloud forensics involves digital evidence collection in the cloud environment. The current established forensic procedures and process models require major changes in order to be acceptable in a cloud environment. This chapter aims to assess the challenges that forensic examiners face in tracking down and using digital information stored in the cloud and discusses the importance of education and training for handling, managing, and investigating computer evidence.

Similarly, a chapter on the relationship between public budgeting and risk management – competition or driving? – by Yaotai Lu discusses how the world is rife with uncertainties. Risk management plays an increasingly important role in both the public sector and the private sector. Considering that government is the risk manager of last resort, government faces a vast variety of risks and disasters, either natural or man-made. Owing to scarce public resources and increasing public needs, government is not capable of financing all risk management programs. However, once a catastrophic event occurs, government must take immediate actions to control the event. Another interesting chapter on “Iris Biometrics Recognition in Security Management” by

Ahmad Ghaffari, Amin Hosseinian-Far, and Akbar Sheikh-Akbari discusses an application of iris recognition for human identification, which has significant potential for developing a robust identification system. This is due to the fact that the iris patterns of individuals are unique, differentiable from left to right eye, and are almost stable over the time. However, the performance of existing iris recognition systems depends on the signal processing algorithms they use for iris segmentation, feature extraction, and template matching. Like any other signal processing system, the performance of the iris recognition system depends on the existing level of noise in the image and can deteriorate as the level of noise increases.

The chapter on “Robust Enterprise Application Security with eTRON Architecture” by M. Fahim Ferdous Khan, Ken Sakamura, and Noboru Koshizuka presents the eTRON architecture, which aims at delineating a generic framework for developing secure e-services. At the core of the eTRON architecture lies the tamper-resistant eTRON chip that is equipped with functions for mutual authentication, encrypted communication, and strong access control. Besides the security features, the eTRON architecture also offers a wide range of functionalities through a coherent set of API commands so that programmers can develop value-added services in a transparent manner. This chapter discusses various features of the eTRON architecture, and presents three representative eTRON-based e-services in order to evaluate its effectiveness by comparison with other existing e-services.

We believe the approaches discussed in this chapter will significantly impact on industrial practice as well as research in the area of enterprise security. Enterprise security also includes new models of cloud-based enterprises. We hope you enjoy reading this book.

February 2017

Victor Chang  
Muthu Ramachandran  
Gary Wills  
Robert J. Walters

Enterprise Security

Second International Workshop, ES 2015, Vancouver,  
BC, Canada, November 30 – December 3, 2015, Revised  
Selected Papers

Chang, V.; Ramachandran, M.; Walters, R.J.; Wills, G.  
(Eds.)

2017, X, 277 p. 64 illus., Softcover

ISBN: 978-3-319-54379-6