

Preface

With the rapid development of Internet-based technologies and the increasing reliance of society on these technologies, providing security and assurance to information systems has become a critical endeavor for practitioners and the various stakeholders impacted by information and system insecurities.

In fact, the omnipresence of threats of malicious attacks has raised the importance of devising new paradigms and solutions in addition to professional skills, knowledge, and human resources in the area of information assurance. This book is a compilation of peer-reviewed papers from the first International Workshop on Information Security, Assurance, and Trust (I-SAT 2016), which introduce novel research targeting technical aspects of protecting information security and establishing trust in the digital space.

The book consists of eight chapters outlined as follows.

Chapter 1 is a brief introduction on the context of emerging security threats and a discussion of the need for new security paradigms in tackling these threats.

Chapter 2 presents contemporary and emerging botnet architectures and discusses best practices in protecting against such threats and how these protection schemes could possibly be evaded.

Chapter 3 introduces a new approach for leveraging behavioral biometrics for online fraud detection.

Chapter 4 introduces a suite of online tools to automate the complex computations involved in analyzing hardware Trojan viruses. This represents an important step in mastering the complexity involved in locating malicious modifications in integrated circuit design and implementation.

Chapter 5 presents a multimodal biometric system that combines at the feature level mouse and eye movement biometrics for user authentication. In this system, mouse movement and eye movement data are collected simultaneously and aligned based on timestamps.

Chapter 6 takes on the pressing challenge of protecting online exam integrity by introducing a multimodal biometric framework involving three modalities, namely, mouse dynamics, keystroke dynamics, and face biometrics.

Chapter 7 tackles lingering limitations in anomaly detection in computing systems (e.g., false alerts, low detection accuracy) by presenting an enhanced CUSUM algorithm for network anomaly detection. The new algorithm enables modeling various features from different sources and reporting alerts according to some decision strategies.

Chapter 8 provides a final summary of the research presented in previous chapters and discusses future trends and challenges in tackling emerging cybersecurity threats.

Victoria, BC, Canada
Vancouver, BC, Canada
Toronto, ON, Canada

Issa Traoré
Ahmed Awad
Isaac Woungang

Information Security Practices

Emerging Threats and Perspectives

Traore, I.; Awad, A.; Woungang, I. (Eds.)

2017, VII, 104 p. 51 illus., 31 illus. in color., Hardcover

ISBN: 978-3-319-48946-9