Book Title: Intrusion Detection and Prevention for Mobile Ecosystems
To be published by CRC Series in Security, Privacy and Trust - Taylor & Francis

Introduction:

During the last few years mobile devices such as smartphones and tablets have penetrated the market at a very high pace. From an end-user perspective, the unprecedented advantages these devices offer, revolve not only around their high mobility, but also extend to their ease of use and the pluralism of their applications. As the penetration of mobile devices increases, the development of mobile apps follow this frantic rate, by being built in great numbers on a daily basis. On the downside, this mushrooming of mobile networks and portable devices has attracted the interest of several kinds of aggressors who possess a plethora of invasion techniques in their artillery. Such ill-motivated entities systematically aim to steal or manipulate users' or network data, and even disrupt their operation to their legitimate users.

Their goal is assisted by the fact that while a continuously increasing number of users has embraced mobile platforms and associated services, most of them are not security-savvy and usually follow naive privacy preservation practices on their routinely interaction with their devices. Until now, a great mass of research work and practical experiences have alerted the community about the nature and severity of these threats that equally affect end-users, providers and even organizations.

One can identify several reasons behind this new wave of malware and invasion tactics: First, mobile devices are used extensively for sensitive tasks, including bank transactions, e-payments, etc., private interaction such as engagement in social media applications, or even mission critical processes in healthcare. Second, smart, ultraportable, and even wearable devices such as smartwatches and smartglasses are highly personal, thus can be correlated with a single user; they embed several sensors and functionalities capable of collecting many details about the context of users, while they are constantly connected to the Internet. Third, numerous researches and case studies have shown that despite the ongoing progress, native security mechanisms of modern mobile operating systems can be outflanked. Even worse, most of the applied wireless communication technologies are eventually proven to be prone to numerous attacks. Admittedly, under this mindset, the attack surface for evildoers grows, leading as well to the augmentation of the volume and sophistication of malware apps designed to act against mobile devices of any kind. To cope with this situation, defenders need to deploy smarter and more advanced security measures along with legacy ones.

Objective of the book:

The aim of this book is to solicit state-of-the-art contributions from both scientists and practitioners working in intrusion detection and prevention for mobile networks, services, and devices. Both chapters dealing with fundamental theory, techniques, applications, as well as practical experiences concerning intrusion detection and prevention for the mobile ecosystem will be considered. Surveys, simulations, practical results and case studies are also welcomed.

Recommended Topics:

This book welcomes chapters on a wide range of issues related to its theme. Indicative topics of interest include, but are not limited to, the following:

- Methods and practices for locating the source of attacks.
- Cross-layer based intrusion and prevention detection.
- Lightweight cryptography for dealing with intrusions and attacks in the mobile ecosystem.
- Intelligent detection of wireless or mobile attacks (misuse detection, anomaly detection).
- Soft computing, machine learning, and artificial intelligence for intrusion detection in mobile ecosystems.
- Agent-based intrusion surveillance, detection and prevention.
- Novel attacks on wireless networks, mobile operating systems and services.
- Standardization efforts related to intrusion detection and prevention for the mobile ecosystem.
- Penetration testing tools and metrics of network assurance.
- Security and privacy considerations for the emerging field of Internet of Things.
- Malware detection, analysis and removal in mobile realms.

- Datasets and frameworks for the study of malware/intrusive mobile behavior.
- Trusted monitoring and data collection for malware/intrusion detection.
- Efficient identification of malicious behavior prior and after installation.
- Mobile botnets (C&C architectures, covert channels, etc.).
- Mobile operating systems security and privacy (Android, iOS, Windows Phone, etc.).
- Identification of attacks against the wireless interfaces of devices (NFC, Bluetooth, WiFi, LTE, LTE-Advanced, etc.).
- Biometric user authentication and continuous authentication for Smartphones (hand-waving, keystroke dynamics, interaction with touchscreen, gait, signature, voice and behavioral profiling for authenticating the end-user)
- Rooting and Jailbreaking of mobile platforms.
- Privacy and security issues for wearable devices.
- Users' awareness to security solutions for mobile devices.

Chapter Proposals/Full Chapters submission:
Chapter proposals and full chapters can be submitted using email attachments to editors via email (gkamb@aegean.gr) with the email subject of "Chapters for Intrusion Detection and Prevention for Mobile Ecosystems". Authors of accepted proposals will be notified by around March 15, 2016, but final acceptance will still depend upon a review of the resulting chapter.

Authors should send the chapters in single column format (single spaced, 10 point Times Roman font, 8.5 x 11-inch page size).
-The maximum number of pages for the proposal is 2.
-The full chapter submission can have about 16 to 25 pages, but more are allowed.

Important dates:
Full Chapter Submission: July 15, 2016
Notification: August 31, 2016
Final Chapter Submission: September 20, 2016

Editor Information:
Dr. Georgios Kambourakis
Dept. of Information and Communication Systems Engineering
University of the Aegean, Samos, Greece
gkamb@aegean.gr

Dr. Asaf Shabtai
Dept. of Information Systems Engineering
Ben-Gurion University of the Negev, Israel
shabtaia@bgu.ac.il

Dr. Constantinos Kolias
Computer Science Dept.
George Mason University, Fairfax, VA, USA
kkolias@gmu.edu

Dr. Dimitrios Damopoulos
Computer Science Dept.
Stevens Institute of Technology, Hoboken NJ, USA
ddamopou@stevens.edu