Preface

The recent virus attacks on the control center of the Iranian nuclear plants[1] as well as those targeting the telecommunication and power grid infrastructures of Estonia[2] and Georgia[3] show how cyber attacks against the critical infrastructure (CI) are becoming increasingly prevalent and disruptive. In many respects, this results from growing exposure of the CI IT to the Internet, which is in turn motivated by the desire to cut operational costs by switching to open networking technologies and off-the-shelf computing equipment.

The Critical Infrastructure Protection (CIP) Survey, recently released by McAfee,[4] found that 53% of the interviewed CI IT security experts have experienced at least ten cyber attacks in the last five years, and 90% expect that the number of cyber attacks will grow in the short to medium term. In addition, the survey indicated that today, one out of five attacks is accompanied by an extortion, and financial institutions are often subject to some of the most sophisticated and large-scale cyber attacks and frauds. For example, an extensive financial fraud that hit the world-wide credit card system in 2008 involved clones of hundreds of credit cards, which were created in 49 countries, and subsequently used at ATMs to withdraw a total of 9 million US dollars. This fraud was carried out within a few minutes and was only discovered at a later stage by analyzing and correlating all the information of the transactions involved. By far, the most prevalent cyber attack against financial institutions is the distributed denial of service against their web-based services, which render them unavailable for legitimate users for prolonged periods of time. Such attacks have been shown to incur serious tangible costs, which, according to some estimates, could exceed 6 million US dollars per day. This is in addition to numerous intangible costs associated among others with damage to reputation and degraded user experience.

[1] IW32.Stuxnet Dossier, Symantec Security Response, 2011.

[2] 2007 Cyberattacks on Estonia, wikipedia.org.

[3] Cyberattacks during the 2008 South Ossetia war, wikipedia.org.

[4] In the Crossfire—Critical Infrastructure in the Age of Cyber War, McAfee, 2010.

The global scope and massive scales of today's attacks necessitate global situational awareness, which cannot be achieved by the isolated local protection systems residing within the IT boundaries of individual financial institutions. There is a growing realization in the financial community of the necessity of information sharing, which however, at this point, is mostly done through rudimentary means (such as daily phone consultations among the security experts). The obstacles hampering adoption of more advanced communication means range from cultural to governance ones, such as incompatible privacy protection legislations.

The goal of this book is to study autonomous computing platforms as the means to enable cross-organizational information and resource sharing within the financial sector without compromising the individual institutions' security, privacy, and other constraints. We analyze the structure of a financial infrastructure, its vulnerabilities to cyber attacks, and the current countermeasures, and then we show the advantages of sharing information among financial players to detect and react more quickly to cyber attacks. We also investigate obstacles from organizational, cultural, and legislative viewpoints. We demonstrate the viability of an information sharing approach from an ITC perspective by exploring how massive amounts of information being made available through a sharing mechanism can be leveraged to create defense systems capable of protecting against globally scoped cyber attacks and frauds in a timely fashion.

In particular, the book introduces the Semantic Room (SR) abstraction, through which interested parties can form trusted contractually regulated federations for the sake of secure information sharing and processing. SRs are capable of supporting diverse types of input data, ranging from security events detected in real time to historical information about past attacks. They can be deployed on top of an IP network and (depending on the needs of the individual participants) can be configured to operate in either peer-to-peer or cloud-centric fashion. Each SR has a specific strategic objective to meet (e.g., detection of botnets, stealthy scan, and man-in-the-middle attacks) and has an associated contract specifying the set of rights and obligations for governing the SR membership and the software infrastructure for data sharing and processing. Individual SRs can communicate with each other in a producer-consumer fashion resulting in a modular service-oriented architecture.

The material is organized into the following two parts.

- Part I explores general issues associated with information sharing in the financial sector. Chapter 1 provides background information on the financial sector, with the focus on its IT organization, vulnerabilities to cyber attacks, and state-of-the-art protection strategies. Additionally, it explores the value of information sharing for facilitating global cooperation and protection. Chapter 2 proposes a model of interacting banks, and explores risks, costs, and benefits associated with participation in the information sharing process. Finally, Chap. 3 presents an overview of possible attack scenarios. It provides detailed descriptions of some cyber attacks as well as IT protection systems employed by financial institutions to guard themselves against those threats.
- Part II presents the CoMiFin middleware for collaborative protection of the financial infrastructure developed as a part of the EU project by the same name

(www.comifin.edu) funded by the Seventh Framework Programme (FP7). Chapter 4 describes the CoMiFin architecture and introduces the Semantic Room abstraction. We discuss various aspects of enforcing trust and privacy within each SR (Chap. 6) and compliance monitoring (Chap. 5). Finally, Chaps. 7, 8, and 9 present concrete implementations of the SR based on three different event processing technologies.

Part I presents a survey of various types of CIs along with their vulnerability analysis, which, to the best of our knowledge, has not yet appeared in textbookstyle publications. It is self-contained and might be of independent interest. The design, implementation, and case studies of the collaborative protection middleware, whose functionality is motivated by the analysis presented in Part I, appears in Part II.

The content of the book does not require specific prerequisites. Holding an undergraduate or a graduate degree in computer science (with some familiarity with cyber security) is sufficient to follow the material. The content of the book is particularly well suited to CI protection practitioners, people working at national and European Working Groups establishing information sharing processes among independent organizations (not necessarily restricted to protection from cyber attacks or to the financial setting) at both the military and civil levels, professionals of event processing and security, and the academic audience.

The editors want to thank primarily all the authors who have contributed to this book. A special thank goes to Giorgia Lodi, who helped us in fixing many details of the book and who is also one of the main pillars of CoMiFin. The editors are also indebted to all the persons who have been involved in the CoMiFin project during its lifetime, including Luca Nicoletti and Andrea Baghini (Italian Ministry of Economics and Finance), András Pataricza (Budapest University of Technology and Economics), Massimo Santelli (SelexElsag), and Jim Clarke (Waterford Institute of Technology). Special thanks go to Angelo Marino and Mario Scillia from the European Commission for having closely followed CoMiFin activities, providing appropriate suggestions for the technical and project management side. Members of the CoMiFin Financial Advisory Board were also instrumental in focusing on issues relevant for the financial players. The following have served as Board members: Thomas Kolher (Chair—Group Information Security at UBS), Finn Otto Hansen (SWIFT Board), Henning H. Arendt (@bc), Guido Pagani (Bank of Italy), Ferenc Alfldi (Capital Budapest Bank), Bernhard M. Hammerli (University of Lucerne), Matteo Lucchetti (ABI, currently Poste Italiane), and Ferenc Fazekas (Groupama). The editors also want to acknowledge Wikipedia, from which the definitions of many of the glossary terms have been taken.

Rome, Italy — Roberto Baldoni
Haifa, Israel — Gregory Chockler

http://www.springer.com/978-3-642-20419-7

Collaborative Financial Infrastructure Protection
Tools, Abstractions, and Middleware
Baldoni, R.; Chockler, G. (Eds.)
2012, XXII, 226 p., Hardcover
ISBN: 978-3-642-20419-7