Collaborative Financial Infrastructure Protection

Roberto Baldoni • Gregory Chockler
Editors

Collaborative Financial Infrastructure Protection

Tools, Abstractions, and Middleware

Springer

Editors
Roberto Baldoni
Dipartimento di Ingegneria Informatica,
Automatica e Gestionale Antonio Ruberti
Università degali Studi di Roma
"La Sapienza"
Roma
Italy

Gregory Chockler
IBM Research – Haifa
Haifa University Campus, Mount Carmel
Haifa
Israel

ISBN 978-3-642-20419-7 e-ISBN 978-3-642-20420-3
DOI 10.1007/978-3-642-20420-3
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011946180

ACM Computing Classification (1998): C.2, J.1, K.6, H.4, D.4

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Security is, I would say, our top priority, because for all the exciting things you will be able to do with computers—organizing your lives, staying in touch with people, being creative—if we don't solve these security problems, then people will hold back.

Bill Gates

To Dora, Edoardo, Camilla, and Luca

To Hana, Naomi, Michael, and Daniel.

Foreword

Societies have grown such a dependence on informatics, that a large part of their assets relies on the availability and correct operation of interconnected computer services. Of the several critical information infrastructures (CIIs) supporting the above-mentioned societal services, the financial infrastructure is an extremely important example. At the date of publishing of this book, the world is experiencing intense turmoil caused by instability in the financial sectors. Furthermore, their interdependence is such that countries' crises contaminate each other, and local problems quickly become global.

Two things become obvious: (i) the financial infrastructure (FI) is a crucial asset whose balance is easily disturbed by "natural" causes; (ii) this organisational vulnerability is amplified by FI stakeholders traditionally operating in isolation, as well as by technical vulnerabilities in the supporting computer systems and networks. Given this scenario, the FI is a natural target for cyber attack, with ample margin for damage. This is confirmed by recent public statistics of actual intrusions and, still, given the traditionally discreet posture of the sector, we may be just looking at the tip of the iceberg.

The ComMiFin EU project had the great merit of tackling this problem with the adequate valences, through a balanced mix of state and financial sector stakeholders on one side, and technology suppliers and researchers on the other.

Based on the argument that FI components are more vulnerable if they operate alone, the project took what seems to be the right approach, and, following the motto *unity makes strength*, it studies the problem of Collaborative Financial Infrastructure Protection, from its roots to concrete solutions, and presents it in two parts. Groups of authors from the project deal with several relevant subjects, in a flow made easy by the contribution of editors Roberto Baldoni and Gregory Chockler.

In the first part, the several groups of authors from the project start by characterising the sector and the risks and vulnerabilities it is subject to, and then detailing a selection of real attack scenarios and common protection strategies. One of the pillars of the proposed solution is *collaboration*, a sensitive issue for financial sector operators. In consequence, the book introduces a model of interacting banks and guides the reader through the risks and benefits of an information sharing process,

motivating potential followers for the approach. The second part deals with a concrete proposal to implement such a collaborative information sharing and protection infrastructure, in the form of middleware components guaranteeing trust and enforcing privacy. In a set of very practical chapters, the several components and their merits are presented.

The result is a very interesting and timely work which, by its completeness and coverage of the problems of the information infrastructures of the financial sector, should be a must read for any stakeholder of the sector.

Lisbon, Portugal Paulo Esteves Verssimo

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

Contents

Contributors

Enrico Angori Elsag Datamat, Rome, Italy; SelexElsag, Roma, Italy

Leonardo Aniello Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Roma, Italy

Roberto Baldoni Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Roma, Italy

Walter Beyeler Sandia National Laboratories, New Mexico, Albuquerque, NM, USA

Vita Bortnikov IBM, Research Division, Haifa, Israel

Dmitri Botvich Waterford Institute of Technology, Waterford, Ireland

Gregory Chockler IBM, Research Division, Haifa, Israel

Michele Colajanni University of Modena and Reggio Emilia, Modena, Italy

György Csertán OptXware Research and Development Ltd., Budapest, Hungary

Eliezer Dekel IBM, Research Division, Haifa, Israel

Giuseppe Antonio Di Luna Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Roma, Italy

Atle Dingsor Kredit Tilsynet, Oslo, Norway

Hisain Elshaafi Waterford Institute of Technology, Waterford, Ireland

László Gönczy OptXware Research and Development Ltd., Budapest, Hungary

Hamza Ghani Technical University of Darmstadt, Darmstadt, Germany

Robert Glass Sandia National Laboratories, New Mexico, Albuquerque, NM, USA

Abdelmajid Khelil Technical University of Darmstadt, Darmstadt, Germany

Davide Lamanna Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Roma, Italy

Gennady Laventman IBM, Research Division, Haifa, Israel

Giorgia Lodi Consorzio Interuniversitario Nazionale Informatica (CINI), Roma, Italy

Matteo Lucchetti Poste Italiane, Roma, Italy

Mirco Marchetti University of Modena and Reggio Emilia, Modena, Italy

Jimmy McGibney Waterford Institute of Technology, Waterford, Ireland

Michele Messori University of Modena and Reggio Emilia, Modena, Italy

Luca Montanari Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Roma, Italy

Barry P. Mulcahy Waterford Institute of Technology, Waterford, Ireland

Hani Qusa Dipartimento di Ingegneria Informatica, Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza", Roma, Italy

Neeraj Suri Technical University of Darmstadt, Darmstadt, Germany

Gábor Urbanics OptXware Research and Development Ltd., Budapest, Hungary

Ymir Vigfusson School of Computer Science, Reykjavík University, Reykjavík, Iceland

Acronyms

ABI	Italian Banking Association
ADSL	Asymmetric digital subscriber line
AN	Agilis node
AS	Agilis site
ATM	Automated teller machine
CA	Central Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CASoS	Complex Adaptive System of Systems
CEP	Complex event processing
CERT	Computer Emergency Response Team
CI	Critical infrastructure
CII	Critical information infrastructure
CINS	Critical Infrastructure Notification System
CIP	Critical infrastructure protection
COBIT	Control Objectives for Information and related Technology
CP	Closed port
CPS	Collaborative processing system
CPU	Central processing unit
CSS	Cascading Style Sheets
CVE	Common Vulnerabilities and Exposures
C&C	Command and control
CoMiFin	Communication Middleware for Monitoring Financial Critical Infrastructure
DDoS	Distributed denial of service
DHT	Distributed hash table
DMZ	Demilitarized zone
DNS	Domain Name System
DPI	Deep packet inspection
DR	Detection rate
DoS	Denial of service

EDP	Electronic data processing
EECTF	European Electronic Crime Task Force
ENISA	European Network and Information Security Agency
EPC	European Payments Council
EPL	Event Processing Language
FC	Failed connection
FI	Financial infrastructure
FI-ISAC	Financial Institutions Information Sharing and Analysis Center
FN	False negative
FP	False positive
FPR	False positive rate
FS/ISAC	Financial Services Information Sharing and Analysis Center
FSM	Finite state machine
FTP	File Transfer Protocol
GB	Gigabyte
GHz	Gigahertz
GQM	Goal question metric
GSM	Global System for Mobile communications
Gbit	Gigabit
HDFS	Hadoop Distributed File System
HIDS	Host-based intrusion detection system
HOC	Half-open connection
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
ICT	Information and communication technologies
IDS	Intrusion detection system
IP	Internet Protocol
IPS	Intrusion prevention system
IPSec	IP Security
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center
ISM	Information security management
ISP	Internet service provider
ISSG/CISEG	Information Security Support Group/Cybercrime Information Sharing Expert Group
ITSG	IT Security Group
JMS	Java Message Service
JT	Job Tracker
KPI	Key performance indicator
LAN	Local area network
LCG	Linear congruential generator
LEA	Law enforcement agency
LSE	London Stock Exchange
MAC	Media Access Control

MB	Megabyte
MDA	Model-driven architecture
MEP	Mediated event processing
MOM	Message-oriented middleware
Mbit	Megabit
MitB	Man in the Browser
MitM	Man in the Middle
NCB	National Central Bank
NIDS	Network-based intrusion detection system
NIPS	Network-based intrusion prevention system
NIST	National Institute of Standards and Technology
NRPE	Nagios Remote Plugin Executor
NSCA	Nagios Service Check Acceptor
NSM	National Security Authority
OS	Operating system
OTP	One-time password
PC	Personal computer
PCI DSS	Payment Card Industry Data Security Standard
PDD	Presidential Decision Directive
PGP	Pretty Good Privacy
PIN	Personal identification number
POJO	Plain Old Java Object
POS	Point of sale
PRNG	Pseudo-random number generator
QoS	Quality of service
RAM	Random access memory
RDBMS	Relational database management system
RFC	Request for Comments
RMI	Remote Method Invocation
ROI	Return on investment
RSA	Rivest, Shamir, and Adleman
SDT	Security, dependability, and trust
SEP	Simple event processing
SEPA	Single Euro Payments Area
SIEM	Security information and event management
SLA	Service level agreement
SLS	Service level specification
SME	Small or medium enterprise
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SOC	Secure Operations Center
SP	Stream processing
SQL	Simple query language
SR	Semantic Room
SSL	Secure Sockets Layer

SWIFT	Society for Worldwide Interbank Financial Telecommunication
SoD	Segregation of duties
TCO	Total cost of ownership
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TM	Trust management
TN	True negative
TP	True positive
TT	Task tracker
UDP	User Datagram Protocol
UML	Unified Modeling Language
URL	Uniform Resource Locator
VM	Virtual machine
VPN	Virtual private network
WAN	Wide area network
WSLA	Web service level agreement
WXS	IBM WebSphere eXtreme Scale
XML	Extensible Markup Language
XOR	Exclusive OR