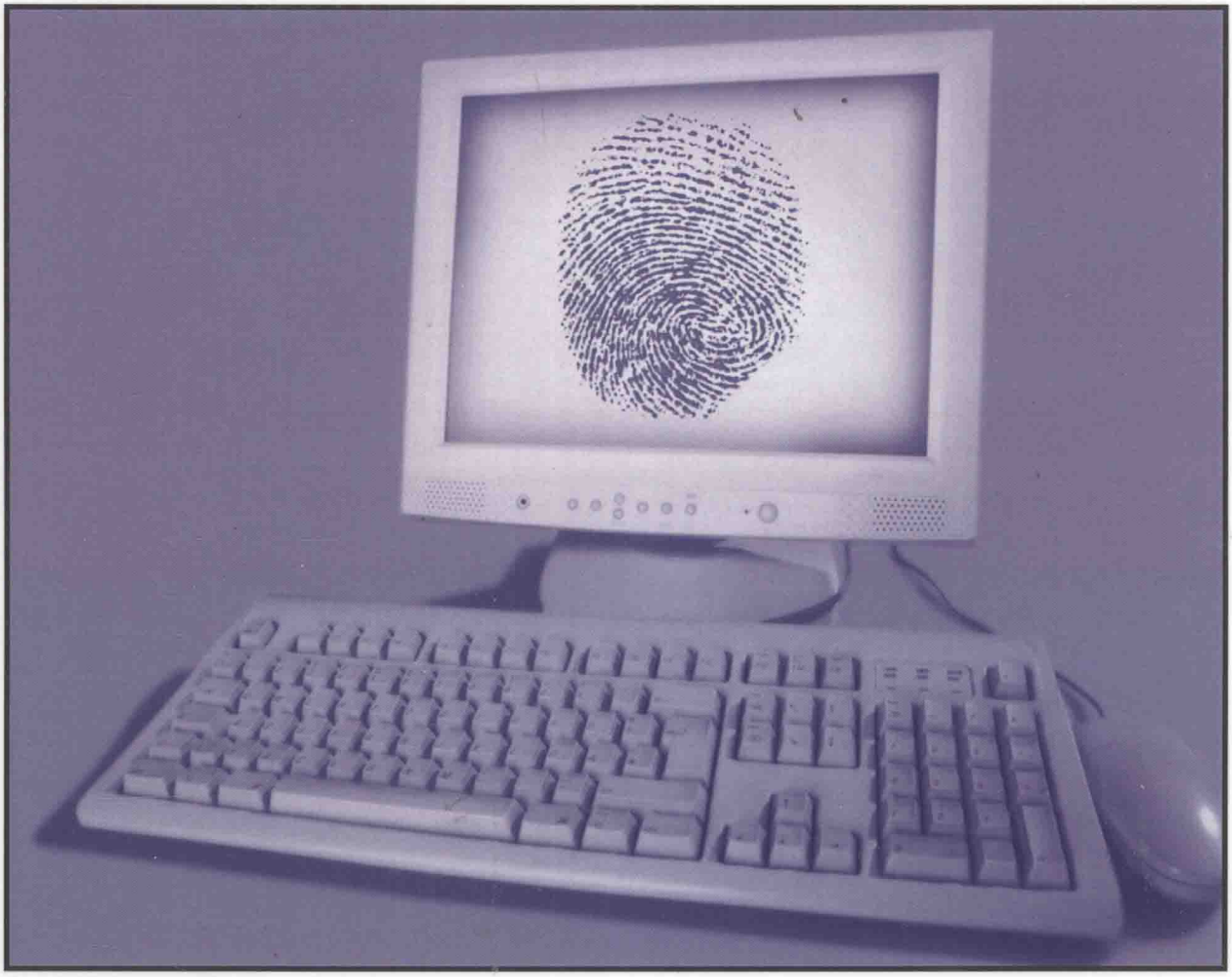
PREMIER REFERENCE SOURCE

Collaborative Computer Security and Trust Management



JEAN-MARC SEIGNEUR & ADAM SLAGELL

Collaborative Computer Security and Trust Management

Jean-Marc Seigneur
Université de Genève, Switzerland

Adam Slagell
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign, USA

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Senior Managing Editor: Jamie Snavely
Assistant Managing Editor: Michael Brehm
Publishing Assistant: Sean Woznicki
Typesetter: Michael Brehm, Jamie Snavely
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

Library of Congress Cataloging-in-Publication Data

Collaborative computer security and trust management / Jean-Marc Seigneur and Adam Slagell, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book combines perspectives of leading researchers in collaborative security to discuss recent advances in this burgeoning new field"--Provided by publisher.
ISBN 978-1-60566-414-9 (hbk.) -- ISBN 978-1-60566-415-6 (ebook) 1. Computer security. 2. Public key infrastructure (Computer security) 3. Data protection. 4. Computer networks--Security measures. 5. Computer crimes--Prevention. I. Seigneur, Jean-Marc. II. Slagell, Adam, 1977-
QA76.9.A25C6145 2010
005.8--dc22
2009019505

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

cal sphere. For this, no apologies, because it is only with better instruments, those which already exist and also those we need to invent, that we can advance the trusted agenda of the e-governed. The Internet has created wealth, mobilities, and opportunities for work, leisure and learning at an unparalleled scale. It has also spawned a rash of global threats and intrusions into our everyday lives, creating apprehension and insecurity. Research which can help decision-makers and governments to learn, constanty, how best to built collaborative trust between themselves and their citizens or clients is one important pillar in rebuilding trust in the Internet age. And it is not just trust in the process of data management which is at stake, but trust in the clear and stated ability and resolve of democracies to master for its peoples their entitlement to the widened, secure, and better life offered by the Information Age.

Andrew Robinson
European Consular and Commercial Office, UK
Member of the EC Integrated Project R4eGov (2006-9)
into eGovernment secure interoperability systems

Andrew Robinson *is Hon Consul for France in the UK, and adviser on European and international strategic opportunities to both private and public sectors. His wide experience with EC programmes extends over 20 years experience, including most recently major EC research projects such as eJustice and R4eGov, both of which inform his Preface to this book. He is Chairman of the European Consular and Commercial Office, and joint creator of the first Franco-German Consulate in the EU in 2004. He is also a Member of the Fraud Forum in NE England, introducing the importance of cross-border interoperability, trust and security, which informs much of his current professional work. He is a Chevalier (Knight) of the Order of Merit, and the Chevalier of the Academic Palms by the French Government for his services to Franco-British and European collaboration. His career spans senior posts in universities, government service, and the private sector.*

Preface

COLLABORATIVE SECURITY AND TRUST MANAGEMENT

Security is usually centrally managed, for example in a form of policies duly executed by individual nodes. An alternative trend of using collaboration and trust to provide security has gained momentum over the past few years. Instead of centrally managed security policies, nodes may use specific knowledge (both local and acquired from other nodes) to make security-related decisions. For example, in reputation-based schemes, the reputation of a given node (and hence its security access rights) can be determined based on the recommendations of peer nodes. As systems are being deployed on ever-greater scale without direct connection to their distant home base, the need for self management is rapidly increasing. Interaction after interaction, as the nodes collaborate, there is the emergence of a digital ecosystem that can be driven by trust. By guiding the local decisions of the nodes, for example, with whom the nodes collaborate, global properties of the ecosystem where the nodes operate may be guaranteed. Thus, the security property of the ecosystem may be driven by self-organizing mechanisms based on trust. Depending on which local collaboration is preferred, a more trustworthy ecosystem may emerge.

In more traditional computer environments, there is the need of increased sharing of security evidence, for example, concerning network logs that have to encompass several network domains in order to detect more quickly new types of network attacks. However, network administrators are still reluctant to share their network logs with external parties due to the risk of exposing their remaining network security holes through these network logs.

This book is a collection of recent scientific contributions to this emerging field of security through collaboration. The foreword by Dr. Andrew Robinson underlines the ethical challenges for security through collaboration in the information society. Then, the first chapter delves into the issues of sharing electronic assets within this knowledge economy. The second chapter focuses on another application domain, namely, collaborative intrusion detection. The third chapter underlines the tensions that may arise when sharing security evidence between different organisations and suggests potential solutions to mitigate these tensions. Chapter 4 presents how anonymisation techniques have been developed to help reduce risk and manage the trade-offs between privacy, security and the need to openly share network information. Chapter 5 introduces three applications in another application domain, namely, the collaborative business-to-business application domain: collaborative benchmarking, fraud detection and supply chain management. Many of these applications could not be realised if no appropriate measures for protecting the collaborating parties' data are taken. The protecting measure based on trust management is explained in the sixth chapter. In Chapter 7, trust management is applied to the specific application domain of recommender systems. The eighth chapter shows the importance of collaboration in enhancing security of mobile agents that migrate among computing devices to achieve tasks on behalf of users. Another particular application domain where trust-based collaboration is used for increased security,

namely wireless sensors network security, is surveyed in chapter 9. Chapter 10 investigates how new hardware technologies such as trust computing can help regarding increased collaborative security given that trusted computing helps to establish trust into business partners' computing machineries. Chapter 11 discusses how to achieve the right trade-off between loss of privacy and increased security in distributed computing environments using credentials. We also suggest reading the two following paperschapters, included in the selected readings section, to get an overview of trust management for fostering collaborative environments: "A Proposition for Developing Trust and Relational Synergy in International e-Collaborative Groups" and "Trust-Based usage Control in Collaborative environment."

After reading the chapters, the readers will have a clear overview of security through collaboration and that it can be applied to many different application domains. We hope that it will foster further use of security through collaboration in other application domains.

Jean-Marc Seigneur
Université de Genève, Switzerland

Adam Slagell
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign, USA

Acknowledgment

This material is in part based upon work supported by the European Commission under its Framework Programs. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the European Commission.

This material is also in part based upon work supported by the National Science Foundation under Award No. CNS 0524643. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Table of Contents

Selected Readings

Detailed Table of Contents

for the representation of nodes within the collaboration model. Second, they introduce and evaluate an algorithm for the formation of detection groups. After conducting a vulnerability analysis of the system, the authors demonstrate the validity of CIMD by examining two different scenarios inspired sociology where the collaboration is advantageous compared to the non-collaborative approach. They evaluate the benefit of CIMD by simulation in a novel packet-level simulation environment called NeSSi (Network Security Simulator) and give a probabilistic analysis for the scenarios.

Chapter 3

Security often requires collaboration, but when multiple stakeholders are involved, it is typical for their priorities to differ or even conflict with one another. In today's increasingly networked world, cyber security collaborations may span organizations and countries. In this chapter, the authors address collaboration tensions, their effects on incident detection and response, and how these tensions may potentially be resolved. The authors present three case studies of collaborative cyber security within the U.S. government and discuss technical, social, and regulatory challenges to collaborative cyber security.They suggest possible solutions and present lessons learned from conflicts. Finally, tje authors compare collaborative solutions from other domains and apply them to cyber security collaboration. Although they concentrate their analysis on collaborations whose purpose is to achieve cyber security, the authors believe this work applies readily to security tensions found in collaborations of a general nature as well.

Chapter 4

It is desirable for many reasons to share information, particularly computer and network logs. Researchers need it for experiments, incident responders need it for collaborative security, and educators need this data for real world examples. However, the sensitive nature of this information often prevents its sharing. Anonymization techniques have been developed in recent years that help reduce risk and navigate the trade-offs between privacy, security and the need to openly share information. This chapter looks at the progress made in this area of research over the past several years, identifies the major problems left to solve and sets a roadmap for future research.

Chapter 5

Collaborative business applications are an active field of research and an emerging practice in industry. This chapter will focus on data protection in B2B applications which offer a wide range of business models and architecture, since often equal partners are involved in the transactions. It will present three distinct applications, their business models, security requirements and the newest solutions for solving these problems. The three applications are collaborative benchmarking, fraud detection and supply chain management. Many of these applications will not be realized if no appropriate measure for protecting the collaborating parties' data are taken. This chapter focuses on the strongest form of data protection. The business secrets are kept entirely secret from other parties (or at least to the degree possible). This also corresponds to the strongest form of privacy protection in many instances. The private information does not leave the producing system, (i.e., data protection), such that the information producer remains its sole owner. In case of B2B application, the sensitive data are usually business secrets, and not personally identifiable data as in privacy protection.

Chapter 6

There have been many trust management systems which are exclusively based on credentials. In this chapter, the authors propose an approach with a unified framework for trust management that can address the above mentioned limitations of current trust management systems. The unified framework uses a consistent way to cover a broad variety of trust mechanisms including credentials, reputation, local data storage, and environment parameters.

Chapter 7

This chapter surveys and discusses relevant works in the intersection among trust, recommendations systems, virtual communities, and agent-based systems. The target of the chapter is showing how, thanks to the use of trust-based solutions and artificial intelligent solutions like that understanding agents-based systems, the traditional recommender systems can improve the quality of their predictions. Moreover, when implemented as open multi-agent systems, trust-based recommender systems can efficiently support users of mobile virtual communities in searching for places, information, and items of interest.

Chapter 8

Mobile agents are self-contained programs that migrate among computing devices to achieve tasks on behalf of users. Autonomous and mobile agents make it easier to develop complex distributed sys-

tems. Many applications can benefit greatly from employing mobile agents, especially e-commerce. For instance, mobile agents can travel from one e-shop to another, collecting offers based on customers' preferences. Mobile agents have been used to develop systems for telecommunication networks, monitoring, information retrieval, and parallel computing. Characteristics of mobile agents, however, introduce new security issues which require carefully designed solutions. On the one hand, malicious agents may violate privacy, attack integrity, and monopolize hosts' resources. On the other hand, malicious hosts may manipulate agents' memory, return wrong results from system calls, and deny access to necessary resources. This has motivated research focused on devising techniques to address the security of mobile-agent systems. This chapter surveys the techniques securing mobile-agent systems. The survey categorizes the techniques based on the degree of collaboration used to achieve security. This categorization resembles the difference between this chapter and other surveys in the literature where categorization is on the basis of entities/parts protected and underlying methodologies used for protection. This survey shows the importance of collaboration in enhancing security and discusses its implications and challenges.

Chapter 9

Like wired network security, wireless sensor network (WSN) security encompasses the typical network security requirements which are: confidentiality, integrity, authentication, non-repudiation and availability. At the same time, security for WSNs differs from traditional security designed for classical wired networks in many points because of the new constraints imposed by WSN technology. Many aspects are due to the limited resources (memory space, CPU ...) and infrastructure-less property of WSNs. Therefore traditional security mechanisms cannot be applied directly and WSNs are more prone to existing and new threats than traditional networks. Typical threats are the physical capture of sensor nodes, the service disruption due to the unreliable wireless communication. Parameters specific to WSN characteristics may help to reduce the effect of threats. Examples of existing measures are efficient WSN power management strategies that can dynamically adjust the node cycles (sleeping or awake mode) based on the current network workload or the use of redundant information to locally detect lying nodes. In addition to adjusting existing WSN characteristics that impact security, establishing trust and collaboration is essential in WSNs for many reasons such as the high distribution of sensor nodes or the goal-oriented nature of many sensing applications. This chapter emphasizes the need of collaboration between sensor nodes and shows that establishing trust between nodes and using reputation reported by collaborating nodes can help mitigate security issues.

Chapter 10

The term "trusted computing" refers to a technology developed by the Trusted Computing Group. It mainly addresses two questions: "Which software is executed on a remote computer?" and "How can secret keys and other security sensitive data be stored and used safely on a computer?". In this chapter the authors introduce the ideas of the trusted computing technology first and later explain how it can help us with establishing "trust" into a business partner (e.g., for B2B or B2C interactions). More precisely: the authors explain how to establish trust into the business partner's computing machinery. So in their chapter "trust" means, that one business partner can be sure, that the other business partner's computing system behaves in an expected and non malicious manner. The authors define "trust" as something that can be measured by cryptographic functions on one computer and be reported towards and evaluated by the business partner's computer, not as something that is derived from observations or built upon legal contracts.

Chapter 11

In distributed computing environments, it is often needed to establish trust before entities interact together. This trust establishment process involves making each entity ask for some credentials from the other entity, which implies some privacy loss for both parties. The authors present a system for achieving the right privacy-trust tradeoff in distributed environments. Each entity aims to join a group in order to protect its privacy. Interaction between entities is then replaced by interaction between groups on behalf of their members. Data sent between groups is saved from dissemination by a self-destruction process. Simulations performed on the system implemented using the Aglets platform show that entities requesting a service need to give up more private information when their past experiences are not good, or when the requesting entity is of a paranoid nature. The privacy loss in all cases is quantified and controlled.

Selected Readings

Chapter 12

Trust and relational development represents a critical challenge in online collaboration groups. Often the problem is attributed to several factors including physical distances, time differences, cultures, and other contributing factors. The challenge in virtual teams centers on creating a successful cohort that functions as a team and develops a sense of trust and cohesion in the process of accomplishing respective group goals. However, the lack of trust in online groups hinders relational development. The author contends that while online collaboration can be clouded by problems with trust and relational synergy as a whole,

the problem is exacerbated in international online or e-Collaborative groups. The development of trust is essential to relational synergy and warmth that fosters successful task and social goal accomplishment. After reviewing related and extant research in online communication, the author offers some practical suggestions for facilitating and sustaining trust and relational synergy in international online collaboration with information communication technologies (ICTs).

Chapter 13

Most access control models have formal access control rules to govern the authorization of a request from a principal. In pervasive and collaborative environments, the behaviors of a principal are uncertain due to partial information. Moreover, the attributes of a principal, requested objects, and contexts of a request are mutable during the collaboration. A variety of such uncertainty and mutability pose challenges when resources sharing must happen in the collaborative environment. In order to address the above challenges, the authors propose a framework to integrate trust management into a usage control model in order to support decision making in an ever-changing collaborative environment. First, a trust value of a principal is evaluated based on both observed behaviors and peer recommendations. Second, the usage-based access control rules are checked to make decisions on resource exchanges. The authors' framework handles uncertainty and mutability by dynamically disenrolling untrusted principals and revoking granted on-going access if access control rules are no longer met. They have applied our trust-based usage control framework to an application of file sharing.

Foreword

TRUST, TRANSPARENCY AND COLLABORATION: THE ETHICAL CHALLENGE TO THE INFORMATION SOCIETY

E-Government and the E-Governed: The Challenge Ahead

2007 may come to be seen as a pivotal year for e-government. The pivot was that curse of politicians- unexpected and destabilizing events – anticipated by some experts, but unheeded in many ICT programme developments. It was the year that the drive for e-government services suffered a series of highly media-sensitive setbacks, despite the surge in people using the Internet for both public and private purposes, especially retail uses. In the public domain there is the UK Government, for example, scoring well in international benchmarking, and moving to consolidate its own dispersed websites into two, one for citizen services, the other for business services. But despite such advances, a series of data losses on a large scale, with some data turning up in the USA, raises questions about how citizens and their children can be fully protected in what has been an open, often outsourced data management culture. These problems are having a political effect also, with large-scale IT schemes, such as the national identity card project, and the on-going IT for Health project in the NHS, coming under closer scrutiny from all sides. Even in the private sector, the problems of on-line fraud, e-banking security concerns as exemplified by the Societe Generale affair, and identity theft risk denting the wider need for trust among customers. A realisation is emerging that citizens' needs and customers' demands are not quite the same thing. Questions are being asked about control, accountability, trust and security, not just at national and international level but within regions as well. These will assume an even greater urgency and political potency when the sharing of data across borders by public administrations is accelerated in the years ahead. People will demand even greater control over cross-border data management systems where their personal data is concerned. This has profound implications for political cultures within countries and within collaborative inter-state constructs such as the EU, demanding a new culture based on citizen-centric expectations understood, acted upon and protected by their e-government guardians.

REBUILDING THE BRIDGE OF TRUST

If 2007 was a pivotal year for data assurance management, 2008 and beyond will be years when a range of questions will be raised entwining technology and politics as never before, and with civic concepts such as trust, security, fairness and transparency bridging both technology and politics.

The following list of questions will inform the debate: