Preface

COLLABORATIVE SECURITY AND TRUST MANAGEMENT

Security is usually centrally managed, for example in the 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 the 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 papers, 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