Preface

This book is a collection of articles on security in large–scale open distributed systems and, in particular, issues pertaining to distributed and mobile object technologies. The role of open systems is to provide an infrastructure for assembling global applications out of software and hardware components coming from multiple sources. Open systems rely on publicly available standards to permit heterogeneous components to interact. The Internet is the archetype of an open distributed system. Standards such as HTTP, HTML, and XML together with the widespread adoption of the Java language are the cornerstones of many distributed systems. Distributed object technologies such as RMI, CORBA, and DCOM, as well as more ambitious mobile technologies (mobile agents, ambients, etc.) offer a large palette of approaches to building those systems.

While the benefits of these technological solutions are undeniable, they raise legitimate security questions. What kind of trust can we have in a system composed of components belonging to different organisations and used by users from all corners of the world? Open systems lack a common trusted computing base, and often have minimal authentication and authorisation frameworks. The possibility of moving code from site to site raises the stakes even higher. We must be able to establish trust among users and programs, and to specify policies that will regulate the use of resources and the spread of information. We must find ways to integrate untrusted downloaded programs with audited local code so that security remains meaningful. We must investigate means to systematically enforce security properties in programming languages for those systems. And, if everything else fails, we must be able to diagnose when policies have been breached and pinpoint the guilty party.

These are a few of the challenges facing us today. The papers in this collection are a snapshot of this very active research area.

The idea for this book arose from a number of discussions and presentations given at two workshops: the *ECOOP Workshop on Distributed Object Security* (EWDOS) and the *Mobile Object Systems: Secure Internet Mobile Computations* (MOS98) workshop held in June 1998 in conjunction with the European Conference on Object–Oriented Programming in Brussels. Both workshops were reviewed and the authors of the best papers of each invited to contribute to this volume. In addition to these core papers, a small number of classic papers in the field were reprinted. The outcome is a well balanced collection of papers that explore many of the essential questions outlined above.

Overview

The book is organised in three parts: (I) Foundations, (II) Concepts, and (III) Implementation, followed by an appendix.

Part I of the book contains chapters giving background and dealing with fundamental issues in trust, programming, and mobile computations in large scale open distributed systems. The paper by Swarup and Fábrega is a comprehensive study of trust in open distributed systems. The paper by Abadi discusses abstractions for protection and

the correctness of their implementation. The paper by Ancona et al. analyses the use of reflection to integrate authorisation mechanisms into an object–oriented system. The paper by Cardelli discusses the difficulties of computing with mobility and proposes a unified framework to overcome these difficulties based on mobile computational ambients. The paper by Hennesy and Riely studies the type safety properties of mobile code in an open distributed system. The paper by De Nicola et al. describes the security mechanisms of the programming language KLAIM, that is used to program mobile agents. The paper by Leroy and Rouaix formulates and proves security properties that well–typed applets possess and identifies sufficient conditions for the execution environment to be safe.

Part II contains descriptions of general concepts in security in open distributed systems. The paper by Blaze et al. describes the use of trust management engines to avoid the need to resolve "identities" in an authorisation decision. The paper by Aura discusses the advantages and limitations of delegation certificates in access control mechanisms. The paper by Brose proposes a new fine grained access control model for CORBA based on views. The paper by Tschudin introduces the concept of apoptosis (programmed death) in mobile code based services. The paper by Yee discusses the problem of ensuring confidentiality and integrity for mobile agents. The paper by Roth describes how two co–operating agents, executing on different machines, can be used to protect the confidentiality and integrity of the individual agent against tampering.

Part III contains papers detailing implementations of security concepts in open distributed systems. Most of the papers in this part also introduce new security concepts, but devote a large portion to a particular implementation of these concepts. The paper by Jaeger describes the use of role based access control policies in configurable systems and its implementation in the Lava Security Architecture. The paper by Grimm and Bershad discusses secure execution of possibly untrusted extensions in the SPIN extensible operating system. The paper by Jones describes a simple and efficient way of interposing code between user programs and the underlying system's interface. The paper by von Eicken et al. discusses the inadequacy of object references for access control and describes an implementation of capabilities in the J–Kernel. The paper by van Doorn et al. describes the implementation of secure network objects, which is an extension of Modula–3 network objects. The paper by Edjlali et al. describes an access control mechanism in which access is granted based on the history of interactions with the requesting principal. The paper by Alexander et al. discusses security issues in active networks, and the solutions that have been implemented in the Secure Active Network Environment. The paper by Hulaas et al. discusses the problem of mobile agent interactions in an open environment. The paper by Wilhelm et al. describes how trusted tamper resistant devices can be used to ensure the integrity of mobile agents.

Acknowledgements

We would like to thank the members of the programme committees of the two workshops. For EWDOS, they were: George Coulouris, Leendert van Doorn, Li Gong, Daniel Hagimont, Trent Jaeger. For MOS98, the committee included: Martín Abadi, Brian Bershad, Ciarán Bryce, Luca Cardelli, Giuseppe Castagna, Robert Gray, Leila

Ismail, Dag Johansen, Eric Jul, Doug Lea, Christian Tschudin, Dennis Volpano. Furthermore, we wish to thank: Vinny Cahill, Daniel LeMetayer, Tommy Thorn, Hitesh Tewari, and Mary Ellen Zurko for additional reviewing, and Alfred Hofmann from Springer–Verlag for his support in getting the volume published.

February 1999 J. Vitek and C. D. Jensen