Editors' Preface

Computer security is a kind of game between two parties, the designer of a secure system, and a potential attacker. The designer is trying to maximize the attacker's effort, while minimizing the inconvenience to legitimate users. One way to maximize the attacker's effort is to make it infinite, by completely removing security vulnerabilities, or at least those in some category. Other vulnerabilities might be tolerated if the attacker's effort to exploit them is high enough, and if legitimate users would suffer from mechanisms strong enough to render the system invulnerable.

Another concern is the amount of time and effort that must be expended to implement and test a system, to ensure that it meets security specifications. That is really another game, in which the costs of development effort are traded against the risks taken by the users. At least, for now, in this forum, we place no limit on the effort researchers must spend to devise and weigh these options; our love of craft is such that no amount of study is too extreme.

The program chairs of the 1992 IEEE Symposium on Research in Security and Privacy have put together a special issue of papers from that symposium, Issue No. 2; their preface follows. Issues Nos. 2 and 3 of this volume have been combined under one cover. No. 3 has three papers introduced below.

Automated cryptographic key distribution in a network generally requires a protocol consisting of several steps, in order to protect against eavesdropping and message modification attacks. It is an inconvenience for a user to wait longer than necessary for these exchanges to take place, so it is of interest to minimize the number of messages in the key distribution protocol. "Optimality of Asynchronous 2-Party Security Data-Exchange Protocols", by Raphael Yahalom, shows that five messages are necessary and sufficient under certain conditions, using a symmetric, or single-key, encryption system.

The question of attacker effort is considered explicitly in "Towards Operational Measures of Computer Security". It asks whether the kind of quantitative approach taken in the field of software reliability can be carried over to security. Certain fundamental parameters would have to be different; in particular, the paper proposes that time-to-failure would be replaced by effort-to-breach. It calls attention to the assumptions underlying the use of probability distributions for relevant variables.

The object-oriented model for database management systems is attractive from a security point of view for a number of reasons. The authors of "A Kernelized Architecture for Multilevel Secure Object-Oriented Databases Supporting Write-Up", Roshan Thomas and Ravi Sandhu, feel that it offers a good match between real-world objects and their system counterparts, making labelling policies easier to understand and implement. Write-up operations are a challenge, however, in a distributed system where integrity must be supported without creating covert channels.

This double issue is remarkable for the variety of problems, types of systems, and approaches that it exhibits, all under the umbrella of computer security. We promise an even greater variety in upcoming issues.

Sushil Jajodia and Jonathan Millen