Editors' Preface

Welcome to the first issue of the Journal of Computer Security. It is with great pleasure and anticipation that we affirm computer security as a research area, possessing its own distinct body of knowledge. For over ten years there has been an IEEE symposium featuring research in this area, and several other conferences and workshops have been created to absorb the expanding interest in evaluations, applications, and foundations. Papers on the most mature work have appeared irregularly in journals such as the IEEE Transactions on Software Engineering, the ACM Transactions on Computer Systems, and a few others. But many of us wished there were a journal that would always be there to serve a specialized readership of computer security researchers. We believe now that there is enough continuing research in computer security to sustain such a journal.

We have assembled a distinguished international editorial board. Besides supplying their expertise on various topics such as operating systems, network security, database security, modelling, and others, the editors act as points of contact and sources of information about the journal all over the world. Each submitted paper is assigned to a responsible editor, who will will obtain at least three detailed reviews for it, supplied by referees in the computer security community who are acknowledged experts in the topic of the paper.

The key to success of this journal, as any journal, is the contribution of publishable articles by you, the researchers. While this first issue will be followed by two special issues containing papers derived from presentations at the 1990 IEEE Symposium on Research in Security and Privacy, and the 1991 Computer Security Foundations Workshop, there will be an opportunity in later issues for prompt publication of submitted papers. This issue includes information for authors regarding the submission of manuscripts.

Scope

The Journal of Computer Security is an archival journal published quarterly. Its purpose is to present research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems. It will also provide a forum for ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. The Journal provides an opportunity to publish articles of greater depth and length than is possible in the proceedings of various existing conferences, as well as short papers. Like the symposia, it addresses an audience of researchers in computer security who can be assumed to have a more specialized background in this area than the readership of other archival publications.

The Journal welcomes contributions on all aspects of computer security: confidentiality, integrity, and assurance of service—that is, protection against unauthorized disclosure or modification of sensitive information, or denial of service. Of interest is a precise understanding of security policies through modelling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware systems implementing them.

A few of the topics of interest are: models of secure information flow, propagation of access rights, mechanisms for access control, covert channel detection and rate estimation, auditing and intrusion detection, operating system and processor architectures, tools and techniques for specification and verification of security properties, and design considerations applicable in the context of particular kinds of systems, such as databases, networks and distributed systems. The latter areas include such topics as inference control, authentication and key management protocols, and secure transaction processing. Papers on the role and application of cryptography in a secure system are appropriate. Issues of public policy may be appropriate if they have a clear impact on the research community. Software and hardware verification papers are appropriate in the context of a secure or safety-critical application.

About this issue

The first issue has papers on network security, access control, verification, and information flow. These papers have an abstract flavor, and employ a variety of models. A single issue will, of course, hardly scratch the surface of the diversity of computer security research. Future issues should include other areas, and cover implementation techniques as well as abstract models.

"Applying Formal Methods to the Analysis of a Key Management Protocol," by Catherine Meadows, documents the discovery of a security flaw in a protocol that was designed and believed to be correct by a recognized expert in the area of cryptography and authentication protocols. It is the first instance of such a discovery that was made using automated support. Perhaps as important is the fact that the paper gives a proof that a repaired version of the protocol is correct.

In "Proving Programs Secure and Correct Using Traces,"John McLean presents an argument for using trace specifications for developing correct, secure systems, and gives examples that show how programs can be specified using traces. The author also gives part of a trace semantics for a small procedural program language to illustrate how proofs of correctness for implementations can be formulated using the same trace formalism that is used in specification.

"Expressive Power of the Schematic Protection Model," by Ravi Sandhu, is one in a series of papers on the author's Schematic Protection Model (SPM). SPM is a capability-based model for which the safety question is efficiently decidable. In this paper, the author shows how some of the well-known protection models—Bell-LaPadula multilevel security model, take-grant models, and grammatical protection systems–can be modelled within his scheme.

"A Logical View of Secure Dependencies," by Pierre Bieber and Frederic Cuppens, proposes new semantics for a "permission" operator in modal logic. They give a definition of security which they compare with non-interference and other definitions of information-flow security. Their definition applies to systems that are not 'input-total.' This somewhat controversial notion says that a system may have input constraints that are not enforced by the system itself, but instead are assumed as a condition on the environment in which the system is installed.

This can lead to paradoxical examples in which a secure system copies high-sensitivity inputs to low-sensitivity outputs. The insecure information flow actually occurs externally in the environment, but the system requires that to happen by virtue of its input constraints. But the existence of counterintuitive examples does not necessarily preclude useful applications of the theory in other situations. The notion of input constraints makes sense when a system is intended to be used as a component, in the context of other components, to build larger systems which may turn out to be input-total.

We recommend this issue for your consideration.

Sushil Jajodia and Jonathan Millen