As networked computer systems of all scales have come to constitute an integral and indispensable part of social infrastructures, the security and reliability of their software systems are now a major social concern. For more than the last three decades, the security of software systems has been an important area of computer science, yet it is a rather recent general recognition that technologies for software security are highly needed. This recognition was formed, of course, as a result of the social losses caused by recurring attacks against various server systems and the software failures of personal computers due to computer viruses. Many such attacks and failures could have been prevented with currently available techniques. Even in the immediate future, however, computers will be much more pervasive and will be operated by more complex software systems. The chances of creating security holes in their software construction will ever increase. Also, the attack methods and mechanisms will be much more sophisticated. Although we face such a grave reality, our technology for software security is still in its infancy. More intensive and wider ranging research is critical for making software social infrastructures secure and dependable.

The International Symposium on Software Security 2002, held in Keio University, Tokyo, November 8–10, 2002, aimed to provide a forum for research discussions and exchanges among world-leading scientists in the fields of both theoretical and system aspects of security in software construction. The program of the symposium was a combination of invited talks and selected presentations of research works. It included the most recent visions and research of the invited speakers, as well as 12 contributions of the research funded by a MEXT grant-in-aid for scientific research on the priority area “Implementation Scheme for Secure Computing.”

This volume is composed of revised versions of the papers read at the symposium. It covers recently developed topics such as the security of pervasive computing, P2P systems and autonomous distributed agents, secure software circulation, compilers for fail-safe C language, the construction of secure mail systems, type systems and multiset rewriting systems for security protocols, and privacy issues.

As the collected papers are strong, the editing process of this volume was smooth and enjoyable. But successfully holding the symposium itself required a lot of work, which was heavily dependent on staffs and graduate students of Keio University, the Tokyo University of Science, and the University of Tokyo. I would very much to thank them, especially for their enthusiasm. Finally, on behalf of the program committee, I would like to express our sincere thanks to the external reviewers whose names are listed on a separate page. Their comments significantly strengthened the papers.

December 2002

Akinori Yonezawa
**Organization**

**Program Committee**

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitsuhiro Okada</td>
<td>Keio University</td>
</tr>
<tr>
<td>Benjamin Pierce</td>
<td>University of Pennsylvania</td>
</tr>
<tr>
<td>Andre Seedrov (Co-chair)</td>
<td>University of Pennsylvania</td>
</tr>
<tr>
<td>Hideyuki Tokuda</td>
<td>Keio University</td>
</tr>
<tr>
<td>Akinori Yonezawa (Co-chair)</td>
<td>University of Tokyo</td>
</tr>
</tbody>
</table>

**Organizing Committee**

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kokichi Futatsugi</td>
<td>JAIST</td>
</tr>
<tr>
<td>Fumio Mizoguchi</td>
<td>Tokyo University of Science</td>
</tr>
<tr>
<td>Mitsuhiro Okada</td>
<td>Keio University</td>
</tr>
<tr>
<td>Benjamin Pierce</td>
<td>University of Pennsylvania</td>
</tr>
<tr>
<td>Andre Seedrov</td>
<td>University of Pennsylvania</td>
</tr>
<tr>
<td>Hideyuki Tokuda</td>
<td>Keio University</td>
</tr>
<tr>
<td>Akinori Yonezawa (Chair)</td>
<td>University of Tokyo</td>
</tr>
</tbody>
</table>

**Sponsors**

- Japanese Ministry of Education, Science and Culture (MEXT)
- National Science Foundation (NSF)
- Japanese Society for the Promotion of Science (JSPS)
- Keio University (G-Sec and Oogata Kenkyu Josei)
External Reviewers

Roy Campbell
Iliano Cervesato
Kokichi Futatsugi
Masami Hagiya
Kazuhiko Kato
Naoki Kobayashi
Catherine Meadows
Dale Miller
John Mitchell
George Necula
Kazuhiro Ogata
Robert Schneck
Tatsuro Sekiguchi
Etsuya Shibayama
Vitaly Shmatikov
Frank Stajano
Doug Tygar
Naoki Yonezaki
Dan Wallach
Table of Contents

Part 1: Security for Pervasive Computing
Towards Security and Privacy for Pervasive Computing ............... 1
Roy Campbell, Jalal Al-Muhtadi, Prasad Naldurg,
Geetanjali Sampemane, M. Dennis Mickunas

Security for Whom? (The Shifting Security Assumptions
of Pervasive Computing) ........................................... 16
Frank Stajano

Active Authentication for Pervasive Computing Environments ....... 28
Kenta Matsumiya, Soko Aoki, Masana Murase, Hideyuki Tokuda

Part 2: Security for P2P Systems and Autonomous
Distributed Agents
A Survey of Peer-to-Peer Security Issues .......................... 42
Dan S. Wallach

Autonomous Nodes and Distributed Mechanisms ..................... 58
John C. Mitchell, Vanessa Teague

Part 3: Privacy Issues
Privacy in Sensor Webs and Distributed Information Systems .......... 84
J.D. Tygar

Negotiated Privacy .................................................... 96
Stanislaw Jarecki, Patrick Lincoln, Vitaly Shmatikov

Part 4: Secure Software Circulation and Secure
C Language
SoftwarePot: An Encapsulated Transferable File System
for Secure Software Circulation .................................... 112
Kazuhiko Kato, Yoshihiro Oyama

Fail-Safe ANSI-C Compiler: An Approach to Making C Programs
Secure (Progress Report) ............................................. 133
Yutaka Oiwa, Tatsuro Sekiguchi, Eijiro Sumii, Akinori Yonezawa
Part 5: Securing Programs by Rewriting and Sandboxing

Types and Effects for Non-interfering Program Monitors .......................... 154
Lujo Bauer, Jarred Ligatti, David Walker

Flexible and Efficient Sandboxing Based on Fine-Grained Protection Domains .............................................. 172
Takahiro Shinagawa, Kenji Kono, Takashi Masuda

Enforcing Java Run-Time Properties Using Bytecode Rewriting ............. 185
Algis Rudys, Dan S. Wallach

Part 6: Secure Mail System Construction

AnZenMail: A Secure and Certified E-mail System ................................. 201
Etsuya Shibayama, Shigeki Hagihara, Naoki Kobayashi, Shin-ya Nishizaki, Kenjiro Taura, Takuo Watanabe

Formalization and Verification of a Mail Server in Coq ....................... 217
Reynald Affeldt, Naoki Kobayashi

Part 7: Some Security Systems

Design and Implementation of Security System Based on Immune System .................................................. 234
Hiroyuki Nishiyama, Fumio Mizoguchi

Design and Implementation of Access Control System for Smart Office Environment ........................................ 249
Wataru Yamazaki, Fumio Mizoguchi

Part 8: Proof-Carrying Code and Type Systems for Security Protocols

Typing One-to-One and One-to-Many Correspondences in Security Protocols .................................................. 263
Andrew D. Gordon, Alan Jeffrey

Proof-Carrying Code with Untrusted Proof Rules ............................... 283
George C. Necula, Robert R. Schneck

Part 9: Authentication Protocols

Verification of Authentication Protocols Based on the Binding Relation ....................................................... 299
Masami Hagiya, Ryo Takemura, Koichi Takahashi, Takamichi Saito

Hiding Names: Private Authentication in the Applied Pi Calculus ........... 317
Cédric Fournet, Martín Abadi
Environmental Requirements for Authentication Protocols ........... 339
   Ran Canetti, Catherine Meadows, Paul Syverson

Part 10: Multiset Rewriting for Protocol Analysis

A Comparison between Strand Spaces and Multiset Rewriting
for Security Protocol Analysis ................................................ 356
   I. Cervesato, N. Durgin, P. Lincoln, J. Mitchell, A. Scedrov

Data Access Specification and the Most Powerful Symbolic Attacker
in MSR ................................................................. 384
   Iliano Cervesato

Part 11: Verification Methods and Tools

A Logical Verification Method for Security Protocols Based
on Linear Logic and BAN Logic ............................................. 417
   Koji Hasebe, Mitsuhiro Okada

Formal Analysis of the iKP Electronic Payment
Protocols ................................................................. 441
   Kazuhiro Ogata, Kokichi Futatsugi

CafeOBJ as a Tool for Behavioral System Verification ............... 461
   Akira Mori, Kokichi Futatsugi

Author Index ............................................................. 471