

Table of Contents

Message from Program Chairs	v
Conference Committee	vi
Distributed Systems	
<i>Session Chair: John Rushby</i>	
On Inter-Realm Authentication in Large Distributed Systems	2
<i>V.D. Gligor, S.-W. Luan, and J.N. Pato</i>	
Integrating Security in a Group Oriented Distributed System	18
<i>M. Reiter, K. Birman, and L. Gong</i>	
Authorization in Distributed Systems: A Formal Approach	33
<i>T.Y.C. Woo and S.S. Lam</i>	
Covert Channels	
<i>Session Chair: Tom Berson</i>	
Lattice Scheduling and Covert Channels	52
<i>W.-M. Hu</i>	
The Influence of Delay Upon an Idealized Channel's Bandwidth	62
<i>I.S. Moskowitz and A.R. Miller</i>	
Integrity Panel	
<i>Session Chair: Richard Kemmerer</i>	
Report of an Integrity Working Group (no paper)	
<i>M. Abrams, E. Amoroso, T. Lunt, and J. Williams</i>	
Cryptographic Protocols	
<i>Session Chair: Dan Nasset</i>	
Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks	72
<i>S.M. Bellovin and M. Merritt</i>	
On Message Integrity in Cryptographic Protocols	85
<i>S.G. Stubblebine and V.D. Gligor</i>	
Roles in Cryptographic Protocols	105
<i>E. Sneekenes</i>	
Security Models	
<i>Session Chair: George Dinolt</i>	
The Typed Access Matrix Model	122
<i>R.S. Sandhu</i>	
A Resource Allocation Model for Denial of Service	137
<i>J.K. Millen</i>	
Non-Monotonic Transformation of Access Rights	148
<i>R.S. Sandhu and G.S. Suri</i>	

Information Flow

Session Chair: Dale Johnson

A Logical Approach to Multilevel Security of Probabilistic Systems164
J.W. Gray III and P.F. Syverson

Using Traces of Procedure Calls to Reason About Composability 177
C. Meadows

Invited Speaker

Session Chair: John McLean

Security in Distributed Systems (no paper)
Butler Lampson

Concurrency Control

Session Chair: Tom Haigh

A Multilevel Transaction Problem for Multilevel Secure Database Systems and
Its Solution for the Replicated Architecture192
O. Costich and J. McDermott

A Two Snapshot Algorithm for Concurrency Control in Multi-Level Secure Databases . . . 204
P. Ammann, F. Jaeckle, and S. Jajodia

Alternative Correctness Criteria for Concurrent Execution of Transactions
in Multilevel Secure Databases 216
S. Jajodia and V. Atluri

Systems

Session Chair: Tanya Korelsky

Evolution of a Trusted B3 Window System Prototype 226
*J. Epstein, J. McHugh, R. Pascale, C. Martin, D. Rothnie, H. Orman,
A. Marmor-Squires, M. Branstad, and B. Danner*

A Neural Network Component for an Intrusion Detection System 240
H. Debar, M. Becker, and D. Siboni

An Optimal Solution to the Secure Reader-Writer Problem 251
G. Benson

Database Security

Session Chair: John Dobson

Security for Object-Oriented Database Systems260
J.K. Millen and T.F. Lunt

A "Natural" Decomposition of Multi-level Relations 273
F. Cuppens and K. Yazdanian

Appendix

BLACKER: Security for the DDN, Examples of A1 Security Engineering Trades286
C. Weissman

Author Index293