2003

Proceedings of the

10th ACM Conference on Computer and Communications Security

Washington, DC, USA • October 27-31, 2003

Edited by: Vijay Atluri & Peng Liu

Sponsored by: ACM SIGSAC

with contributions from

Center for Secure Information Systems, George Mason University,
Defense Advanced Research Projects Agency,
IBM Research, and Microsoft Research

acm
PRESS

Table of Contents

CCS'03 Conference Organization viii

External Reviewers x

Session 1: Keynote

Chair: S. Jajodia

- **Privacy Cognizant Information Systems** 1
  R. Agrawal (*IBM Almaden Research Center)*

Session 2: DOS Protection

Chair: R. Thomas

- **DoS Protection for UDP-Based Protocols** 2
  C. Kaufman (*IBM*), R. Perlman (*Sun Microsystems Laboratories*), B. Sommerfeld (*Sun Microsystems*)
- **Using Graphic Turing Tests to Counter Automated DDoS Attacks Against Web Servers** 8
  W. G. Morein, A. Stavrou, D. L. Cook, A. D. Keromytis, V. Misra, D. Rubenstein (*Columbia University*)
- **Robust Correlation of Encrypted Attack Traffic Through Stepping Stones by Manipulation of Interpacket Delays** 20
  X. Wang, D. S. Reeves (*North Carolina State University*)
- **Hop-Count Filtering: An Effective Defense Against Spoofed DDoS Traffic** 30
  C. Jin (*California Institute of Technology*), H. Wang (*College of William and Mary*), K. G. Shin (*University of Michigan*)

Session 3: Sensor Networks

Chair: V. Gligor

- **A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks** 42
  W. Du, J. Deng (*Syracuse University*), Y. S. Han (*National Chi Nan University*), P. K. Varshney (*Syracuse University*)
- **Establishing Pairwise Keys in Distributed Sensor Networks** 52
  D. Liu, P. Ning (*North Carolina State University*)
- **LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks** 62
  S. Zhu, S. Setia, S. Jajodia (*George Mason University*)

Session 4: Access Control

Chair: G.-J. Ahn

- **XML Access Control Using Static Analysis** 73
  M. Murata, A. Tozawa, M. Kudo, S. Hada (*IBM Tokyo Research Laboratory*)
- **On Permissions, Inheritance and Role Hierarchies** 85
  J. Crampton (*University of London*)
- **Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs** 93
  E. Damiani, S. De Capitani di Vimercati (*Università di Milano*), S. Jajodia (*George Mason University*), S. Paraboschi (*Università di Bergamo*), P. Samarati (*Università di Milano*)

Session 5: Privacy/Anonymity

Chair: S. Stubblebine

- **The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy** 103
  A. Juels (*RSA Laboratories*), R. L. Rivest (*Massachusetts Institute of Technology*), M. Szydlo (*RSA Laboratories*)
- **Receiver Anonymity via Incomparable Public Keys** 112
  B. R. Waters, E. W. Felten, A. Sahai (*Princeton University*)
- **k-Anonymous Message Transmission** 122
  L. von Ahn, A. Bortz, N. J. Hopper (*Carnegie Mellon University*)

Session 6: Authentication and Signature Schemes

Chair: P. Syverson

- **On the Performance, Feasibility, and Use of Forward-Secure Signatures** 131
  E. Cronin, S. Jamin (*University of Michigan*), T. Malkin (*Columbia University*),
  P. McDaniel (*AT&T Labs—Research*)
- **Print Signatures for Document Authentication** 145
  B. Zhu, J. Wu (*Institute for Infocomm Research*), M. S. Kankanhalli (*National University of Singapore*)
- **Efficiency Improvements for Signature Schemes with Tight Security Reductions** 155
  J. Katz, N. Wang (*University of Maryland*)
- **Origin Authentication in Interdomain Routing** 165
  W. Aiello, J. Ioannidis, P. McDaniel (*AT&T Labs—Research*)

Session 7: Information Warfare

Chair: J. Park

- **Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies** 179
  P. Liu, W. Zang (*Pennsylvania State University*)
- **Monitoring and Early Warning for Internet Worms** 190
  C. C. Zou, L. Gao, W. Gong, D. Towsley (*University of Massachusetts at Amherst*)
- **Learning Attack Strategies from Intrusion Alerts** 200
  P. Ning, D. Xu (*North Carolina State University*)

Session 8: Cryptographic Protocols/Network Security

Chair: A. Rubin

- **Automatic Generation of Two-Party Computations** 210
  P. MacKenzie (*Bell Laboratories, Lucent Technologies*), A. Oprea, M. K. Reiter (*Carnegie Mellon University*)
- **A Composable Cryptographic Library with Nested Operations** 220
  M. Backes, B. Pfitzmann, M. Waidner (*IBM Research Division*)
- **Efficient Self-Healing Group Key Distribution with Revocation Capability** 231
  D. Liu, P. Ning, K. Sun (*North Carolina State University*)
- **Security Proofs for an Efficient Password-Based Key Exchange** 241
  E. Bresson (*CELAR*), O. Chevassut (*Berkeley National Laboratory*),
  D. Pointcheval (*CNRS-École normale superieure*)

Session 9: Intrusion Detection

Chair: P. Liu

- **Anomaly Detection of Web-based Attacks** ... 251
  C. Kruegel, G. Vigna (*University of California at Santa Barbara)*
- **Enhancing Byte-Level Network Intrusion Detection Signatures with Context** ... 262
  R. Sommer (*TU München)*, V. Paxson (*Lawrence Berkeley National Laboratory)*
- **Countering Code-Injection Attacks with Instruction-Set Randomization** ... 272
  G. S. Kc, A. D. Keromytis (*Columbia University)*, V. Prevelakis (*Drexel University)*
- **Randomized Instruction Set Emulation to Disrupt Binary Code Injection Attacks** ... 281
  E. G. Barrantes, D. H. Ackley, S. Forrest, T. S. Palmer, D. Stefanović, D. D. Zovi (*University of New Mexico)*

Session 10: Emerging Applications

Chair: P. Ning

- **Obfuscation of Executable Code to Improve Resistance to Static Disassembly** ... 290
  C. Linn, S. Debray (*University of Arizona)*
- **PPay: Micropayments for Peer-to-Peer Systems** ... 300
  B. Yang, H. Garcia-Molina (*Stanford University)*
- **A New CRT-RSA Algorithm Secure Against Bellcore Attacks** ... 311
  J. Blömer, M. Otto (*Paderborn University)*, J.-P. Seifert (*Secure Mobile Solutions)*

Session 11: Analysis and Verification

Chair: S. Shieh

- **MECA: an Extensible, Expressive System and Language for Statically Checking Security Properties** ... 321
  J. Yang, T. Kremenek, Y. Xie, D. Engler (*Stanford University)*
- **Constraint Differentiation: A New Reduction Technique for Constraint-Based Analysis of Security Protocols** ... 335
  D. Basin, S. Mödersheim, L. Viganò (*ETH Zurich)*
- **Buffer Overrun Detection using Linear Programming and Static Analysis** ... 345
  V. Ganapathy, S. Jha (*University of Wisconsin at Madison)*, D. Chandler, D. Melski, D. Vitek (*Grammatech Inc.)*
- **Cryptographic Tamper Evidence** ... 355
  G. Itkis (*Boston University)*

Author Index ... 365