RFID and Privacy
A New Framework for RFID Privacy p. 1
Readers Behaving Badly: Reader Revocation in PKI-Based RFID Systems p. 19
Privacy-Preserving, Taxable Bank Accounts p. 37
Formal Analysis of Privacy for Vehicular Mix-Zones p. 55

Software Security
IntPatch: Automatically Fix Integer-Overflow-to-Buffer-Overflow Vulnerability at Compile-Time p. 71
A Theory of Runtime Enforcement, with Results p. 87
Enforcing Secure Object Initialization in Java p. 101
Flexible Scheduler-Independent Security p. 116

Cryptographic Protocols
Secure Multiparty Linear Programming Using Fixed-Point Arithmetic p. 168
A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on $\mathcal{Z}$-Protocols

Traffic Analysis
Website Fingerprinting and Identification Using Ordered Feature Sequences p. 199
Web Browser History Detection as a Real-World Privacy Threat p. 215
On the Secrecy of Spread-Spectrum Flow Watermarks p. 232
Traffic Analysis against Low-Latency Anonymity Networks Using Available Bandwidth Estimation p. 249

End-User Security
A Hierarchical Adaptive Probabilistic Approach for Zero Hour Phish Detection p. 268
Kamouflage: Loss-Resistant Password Management p. 286

Formal Analysis
Sequential Protocol Composition in Maude-NPA p. 303
Verifying Security Property of Peer-to-Peer Systems Using CSP p. 319
On Bounding Problems of Quantitative Information Flow p. 357

E-voting and Broadcast
On E-Vote Integrity in the Case of Malicious Voter Computers p. 373
Election Verifiability in Electronic Voting Protocols p. 389
Pretty Good Democracy for More Expressive Voting Schemes p. 405
Efficient Multi-dimensional Key Management in Broadcast Services p. 424

Authentication, Access Control, Authorization and Attestation
Caught in the Maze of Security Standards p. 441
User-Role Reachability Analysis of Evolving Administrative Role Based Access Control p. 455
An Authorization Framework Resilient to Policy Evaluation Failures p. 472
Optimistic Fair Exchange with Multiple Arbiters p. 488
Anonymity and Unlinkability
Speaker Recognition in Encrypted Voice Streams \hspace{1cm} p. 508
Evaluating Adversarial Partitions \hspace{1cm} p. 524
Providing Mobile Users’ Anonymity in Hybrid Networks \hspace{1cm} p. 540
Complexity of Anonymity for Security Protocols \hspace{1cm} p. 558
Network Security and Economics
k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks \hspace{1cm} p. 573

Are Security Experts Useful? Bayesian Nash Equilibria for Network Security Games with Limited Information \hspace{1cm} p. 588
RatFish: A File Sharing Protocol Provably Secure against Rational Users \hspace{1cm} p. 607
A Service Dependency Model for Cost-Sensitive Intrusion Response \hspace{1cm} p. 626
Secure Update, DOS and Intrusion Detection
Secure Code Update for Embedded Devices via Proofs of Secure Erasure \hspace{1cm} p. 643
Dial

Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.