Kefei Chen Robert Deng Xuejia Lai
Jianying Zhou (Eds.)

Information Security Practice and Experience

Second International Conference, ISPEC 2006
Hangzhou, China, April 11-14, 2006
Proceedings

Springer

Table of Contents

Cryptoanalysis

DPA-Resistant Finite Field Multipliers and Secure AES Design
Yoo-Jin Baek, Mi-Jung Noh 1

Signed MSB-Set Comb Method for Elliptic Curve Point Multiplication
Min Feng, Bin B. Zhu, Cunlai Zhao, Shipeng Li 13

Diophantine Approximation Attack on a Fast Public Key Cryptosystem
Baocang Wang, Yupu Hu 25

Further Security Analysis of XTR
Dong-Guk Han, Tsuyoshi Takagi, Jongin Lim 33

Network Security I

A Counting-Based Method for Massive Spam Mail Classification
Hao Luo, Binxing Fang, Xiaochun Yun 45

Model and Estimation of Worm Propagation Under Network Partition
Ping Wang, Binxing Fang, Xiaochun Yun 57

Tackling Worm Detection Speed and False Alarm in Virus Throttling
Jangbok Kim, Jaehong Shim, Gihyun Jung, Kyunghee Choi 67

Network Security II

Using Data Field to Analyze Network Intrusions
Feng Xie, Shuo Bai 78

Adversarial Organization Modeling for Network Attack/Defense
Ji Wu, Chaoqun Ye, Shiyao Jin 90

A Novel Dynamic Immunization Strategy for Computer Network Epidemics
Zhifei Tao, Hai Jin, Zongfen Han, En Cheng 100

Preventing Web-Spoofing with Automatic Detecting Security Indicator
Fang Qi, Feng Bao, Tieyan Li, Weijia Jia, Yongdong Wu 112

Security Protocol

Security Protocol Analysis with Improved Authentication Tests
Xiehua Li, Shutang Yang, Jianhua Li, Hongwen Zhu 123

A Protocol of Member-Join in a Secret Sharing Scheme
Xiao Li, Mingxing He 134

More on Shared-Scalar-Product Protocols
Huafei Zhu, Feng Bao, Tieyan Li, Ying Qiu 142

Communication Security

Efficient Public Key Broadcast Encryption Using Identifier of Receivers
Jung Wook Lee, Yong Ho Hwang, Pil Joong Lee 153

A Practical Clumped-Tree Multicast Encryption Scheme
Ling Dong, Kefei Chen 165

Trojan Horse Attack Strategy on Quantum Private Communication
Jinye Peng, Guangqiang He, Jin Xiong, Guihua Zeng 177

Signature and Key Agreement

Linkable Democratic Group Signatures
Mark Manulis, Ahmad-Reza Sadeghi, Jörg Schwenk 187

Identity-Based Key Agreement with Unilateral Identity Privacy Using Pairings
Zhaohui Cheng, Liqun Chen, Richard Comley, Qiang Tang 202

Short (Identity-Based) Strong Designated Verifier Signature Schemes
Xinyi Huang, Willy Susilo, Yi Mu, Futai Zhang 214

Identity Based Key Insulated Signature
Yuan Zhou, Zhenfu Cao, Zhenchuan Chai 226

Application I

Design and Implementation of an Extended Reference Monitor for Trusted Operating Systems
Hyung Chan Kim, Wook Shin, R.S. Ramakrishna, Kouichi Sakurai 235

A Design and Implementation of Profile Based Web Application Securing Proxy
Youngtae Yun, Sangseo Park, Yosik Kim, Jaecheol Ryou 248

An Efficient and Practical Fingerprint-Based Remote User Authentication Scheme with Smart Cards
Muhammad Khurram Khan, Jiashu Zhang 260

Application II

Domain-Based Mobile Agent Fault-Tolerance Scheme for Home Network Environments
Gu Su Kim, Young Ik Eom 269

Using π-Calculus to Formalize Domain Administration of RBAC
Yahui Lu, Li Zhang, Yinbo Liu, Jiaguang Sun 278

An Efficient Way to Build Secure Disk
Fangyong Hou, Hongjun He, Zhiying Wang, Kui Dai 290

Practical Forensic Analysis in Advanced Access Content System
Hongxia Jin, Jeffery Lotspiech 302

Cryptographic Techniques

Security Analysis of a Server-Aided RSA Key Generation Protocol
Tianjie Cao, Xianping Mao, Dongdai Lin 314

Integrating Grid with Cryptographic Computing
Zhonghua Jiang, Dongdai Lin, Lin Xu, Lei Lin 321

Three-Round Secret Handshakes Based on ElGamal and DSA
Lan Zhou, Willy Susilo, Yi Mu 332

System Security

Securing C Programs by Dynamic Type Checking
Haibin Shen, Jimin Wang, Lingdi Ping, Kang Sun 343

A Chaos-Based Robust Software Watermarking
Fenlin Liu, Bin Lu, Xiangyang Luo 355

Privately Retrieve Data from Large Databases
Qianhong Wu, Yi Mu, Willy Susilo, Fangguo Zhang 367

An Empirical Study of Quality and Cost Based Security Engineering
Seok Yun Lee, Tai-Myung Chung, Myeonggil Choi 379

Author Index 391