Information Security Practice and Experience

First International Conference, ISPEC 2005
Singapore, April 11-14, 2005
Proceedings
Table of Contents

Network Security

Risk Assessment of Production Networks Using Honeynets – Some Practical Experience
   Stephan Riebach, Erwin P. Rathgeb, Birger Toedtmann .......................... 1

POSSET – Policy-Driven Secure Session Transfer
   Philip Robinson, Christian Schaefer, Thomas Walter ......................... 13

Modeling and Evaluation of Security Architecture for Wireless Local Area Networks by Indexing Method: A Novel Approach
   Debabrata Nayak, D.B. Phatak, V.P. Gulati ................................. 25

Robust Routing in Malicious Environment for Ad Hoc Networks
   Zhongchao Yu, Chuk-Yang Seng, Tao Jiang, Xue Wu, William A. Arbaugh .................. 36

Cryptographic Techniques I

Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation
   Patrick P. Tsang, Victor K. Wei ........................................ 48

Tracing Traitors by Guessing Secrets. The q-Ary Case
   Marcel Fernandez, Miguel Soriano, Josep Cotrina .......................... 61

Probabilistic Analyses on Finding Optimal Combinations of Primality Tests in Real Applications
   Heejin Park, Sang Kil Park, Ki-Ryong Kwon,
   Dong Kyue Kim ...................................................... 74

Countermeasures for Preventing Comb Method Against SCA Attacks
   Mustapha Hedabou, Pierre Pinel, Lucien Bénéteau .......................... 85
## Secure Architecture I

### An Email Worm Vaccine Architecture

*Stelios Sidiroglou, John Ioannidis, Angelos D. Keromytis, Salvatore J. Stolfo*

97

### Enforcing the Principle of Least Privilege with a State-Based Privilege Control Model

*Bin Lian, Heng Liu, Wenchang Shi, Yanjun Wu*

109

### Security On-demand Architecture with Multiple Modules Support

*Yanjun Wu, Wenchang Shi, Hongliang Liang, Qinghua Shang, Chongyang Yuan, Bin Lian*

121

### Measuring Resistance to Social Engineering

*Hågen Hasle, Yngve Kristiansen, Ketil Kintel, Einar Snekkenes*

132

## Access Control

### Conformance Checking of RBAC Policy and Its Implementation

*Frode Hansen, Vladimir Oleshchuk*

144

### A Practical Aspect Framework for Enforcing Fine-Grained Access Control in Web Applications

*Kung Chen, Chih-Mao Huang*

156

### A Task-Oriented Access Control Model for WfMS

*Xu Liao, Li Zhang, Stephen C.F. Chan*

168

## Intrusion Detection

### A Brief Observation-Centric Analysis on Anomaly-Based Intrusion Detection

*Zonghua Zhang, Hong Shen*

178
Detection of Distributed Denial of Service Attacks Using Statistical Pre-processor and Unsupervised Neural Networks

*Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari* ........................................ 192

Visual Spoofmg of SSL Protected Web Sites and Effective Countermeasures

*Andre Adelsbach, Sebastian Gajek, Jörg Schwenk* .................. 204

Model Redundancy vs. Intrusion Detection

*Zhuowei Li, Amitabha Das, Sabu Emmanuel* .................. 217

**Applications and Case Studies**

An Open Approach for Designing Secure Electronic Immobilizers

*Kerstin Lemke, Ahmad-Reza Sadeghi, Christian Stüble* .............. 230

An Empirical Study on the Usability of Logout in a Single Sign-On System

*Mikael Linden, Inka Vilpola* ........................................ 243

Secure Software Delivery and Installation in Embedded Systems

*André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi* .............. 255

A Restricted Multi-show Credential System and Its Application on E-Voting

*Joseph K. Liu, Duncan S. Wong* ........................................ 268

**Secure Architecture II**

Recard: Using Recommendation Cards Approach for Building Trust in Peer-to-Peer Networks

*Hany A. Samuel, Yasser H. Dakrouy, Hussein I. Shahein* ............. 280

Using Trust for Restricted Delegation in Grid Environments

*Wenbao Jiang, Chen Li, Shuang Hao, Yiqi Dai* ..................... 293

Computer Vulnerability Evaluation Using Fault Tree Analysis

*Tao Zhang, Mingzeng Hu, Xiaochun Yun, Yongzheng Zhang* ............. 302
An Identity-Based Grid Security Infrastructure Model

Xiaoqin Huang, Lin Chen, Linpeng Huang, Minglu Li .................. 314

Data Security

Towards Multilateral-Secure DRM Platforms

Ahmad-Reza Sadeghi, Christian Stüle ................................. 326

Hiding Data in Binary Images

Chin-Chen Chang, Chun-Sen Tseng, Chia-Chen Lin .................. 338

Performance Analysis of CDMA-Based Watermarking with Quantization Scheme

Yanmei Fang, Limin Gu, Jiwu Huang ................................. 350

Protecting Mass Data Basing on Small Trusted Agent

Fangyong Hou, Zhiying Wang, Kui Dai, Yun Liu .................. 362

Cryptographic Techniques II

On the Security of Some Nonrepudiable Threshold Proxy Signature Schemes

Zuowen Tan, Zhuojun Liu, Mingsheng Wang ......................... 374

Token-Controlled Public Key Encryption

Joonsang Baek, Reihaneh Safavi-Naini, Willy Susilo ................ 386

A New Class of Codes for Fingerprinting Schemes

Marcel Fernandez, Miguel Soriano, Josep Cotrina .................. 398

t-Out-of-n String/Bit Oblivious Transfers Revisited

Qianhong Wu, Bo Qin, Changjie Wang, Xiaofeng Chen, Yuming Wang ......................... 410

Author Index .............................................................. 423