

Table of Contents

Network Security I

Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones	1
<i>Thorsten Holz, Markus Engelberth, and Felix Freiling</i>	
User-Centric Handling of Identity Agent Compromise.....	19
<i>Daisuke Mashima, Mustaque Ahamad, and Swagath Kannan</i>	
The Coremelt Attack	37
<i>Ahren Studer and Adrian Perrig</i>	

Information Flow

Type-Based Analysis of PIN Processing APIs.....	53
<i>Matteo Centenaro, Riccardo Focardi, Flaminia L. Luccio, and Graham Steel</i>	
Declassification with Explicit Reference Points	69
<i>Alexander Lux and Heiko Mantel</i>	
Tracking Information Flow in Dynamic Tree Structures	86
<i>Alejandro Russo, Andrei Sabelfeld, and Andrey Chudnov</i>	

Network Security II

Lightweight Opportunistic Tunneling (LOT).....	104
<i>Yossi Gilad and Amir Herzberg</i>	
Hide and Seek in Time — Robust Covert Timing Channels.....	120
<i>Yali Liu, Dipak Ghosal, Frederik Armknecht, Ahmad-Reza Sadeghi, Steffen Schulz, and Stefan Katzenbeisser</i>	
Authentic Time-Stamps for Archival Storage	136
<i>Alina Oprea and Kevin D. Bowers</i>	

Language Based Security

Towards a Theory of Accountability and Audit	152
<i>Radha Jagadeesan, Alan Jeffrey, Corin Pitcher, and James Riely</i>	
Reliable Evidence: Auditability by Typing	168
<i>Nataliya Guts, Cédric Fournet, and Francesco Zappa Nardelli</i>	

PCAL: Language Support for Proof-Carrying Authorization Systems ...	184
<i>Avik Chaudhuri and Deepak Garg</i>	

Network Security III

ReFormat: Automatic Reverse Engineering of Encrypted Messages	200
<i>Zhi Wang, Xuxian Jiang, Weidong Cui, Xinyuan Wang, and Mike Grace</i>	
Protocol Normalization Using Attribute Grammars	216
<i>Drew Davidson, Randy Smith, Nic Doyle, and Somesh Jha</i>	
Automatically Generating Models for Botnet Detection	232
<i>Peter Wurzinger, Leyla Bilge, Thorsten Holz, Jan Goebel, Christopher Kruegel, and Engin Kirda</i>	

Access Control

Dynamic Enforcement of Abstract Separation of Duty Constraints	250
<i>David Basin, Samuel J. Burri, and Günter Karjoth</i>	
Usable Access Control in Collaborative Environments: Authorization Based on People-Tagging	268
<i>Qihua Wang, Hongxia Jin, and Ninghui Li</i>	
Requirements and Protocols for Inference-Proof Interactions in Information Systems	285
<i>Joachim Biskup, Christian Gogolin, Jens Seiler, and Torben Weibert</i>	

Privacy - I

A Privacy Preservation Model for Facebook-Style Social Network Systems	303
<i>Philip W.L. Fong, Mohd Anwar, and Zhen Zhao</i>	
New Privacy Results on Synchronized RFID Authentication Protocols against Tag Tracing	321
<i>Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini</i>	
Secure Pseudonymous Channels	337
<i>Sebastian Mödersheim and Luca Viganò</i>	

Distributed Systems Security

Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing	355
<i>Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou</i>	

Content Delivery Networks: Protection or Threat?	371
<i>Sipat Triukose, Zakaria Al-Qudah, and Michael Rabinovich</i>	
Model-Checking DoS Amplification for VoIP Session Initiation	390
<i>Ravinder Shankesi, Musab AlTurki, Ralf Sasse, Carl A. Gunter, and José Meseguer</i>	

Privacy - II

The Wisdom of Crowds: Attacks and Optimal Constructions	406
<i>George Danezis, Claudia Diaz, Emilia Käsper, and Carmela Troncoso</i>	
Secure Evaluation of Private Linear Branching Programs with Medical Applications	424
<i>Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	
Keep a Few: Outsourcing Data While Maintaining Confidentiality	440
<i>Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati</i>	

Security Primitives

Data Structures with Unpredictable Timing	456
<i>Darrell Bethea and Michael K. Reiter</i>	
WORM-SEAL: Trustworthy Data Retention and Verification for Regulatory Compliance	472
<i>Tiancheng Li, Xiaonan Ma, and Ninghui Li</i>	
Corruption-Localizing Hashing	489
<i>Giovanni Di Crescenzo, Shaoquan Jiang, and Reihaneh Safavi-Naini</i>	

Web Security

Isolating JavaScript with Filters, Rewriting, and Wrappers	505
<i>Sergio Maffeis, John C. Mitchell, and Ankur Taly</i>	
An Effective Method for Combating Malicious Scripts Clickbots	523
<i>Yanlin Peng, Linfeng Zhang, J. Morris Chang, and Yong Guan</i>	
Client-Side Detection of XSS Worms by Monitoring Payload Propagation	539
<i>Fangqi Sun, Liang Xu, and Zhendong Su</i>	

Cryptography

Formal Indistinguishability Extended to the Random Oracle Model	555
<i>Cristian Ene, Yassine Lakhnech, and Van Chan Ngo</i>	
Computationally Sound Analysis of a Probabilistic Contract Signing Protocol	571
<i>Mihhail Aizatulin, Henning Schnoor, and Thomas Wilke</i>	
Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption	587
<i>Rakesh Bobba, Himanshu Khurana, and Manoj Prabhakaran</i>	

Protocols

A Generic Security API for Symmetric Key Management on Cryptographic Devices	605
<i>Véronique Cortier and Graham Steel</i>	
ID-Based Secure Distance Bounding and Localization	621
<i>Nils Ole Tippenhauer and Srdjan Čapkun</i>	
Secure Ownership and Ownership Transfer in RFID Systems	637
<i>Ton van Deursen, Sjouke Mauw, Saša Radomirović, and Pim Vullers</i>	

Systems Security and Forensics

Cumulative Attestation Kernels for Embedded Systems	655
<i>Michael LeMay and Carl A. Gunter</i>	
Super-Efficient Aggregating History-Independent Persistent Authenticated Dictionaries	671
<i>Scott A. Crosby and Dan S. Wallach</i>	
Set Covering Problems in Role-Based Access Control	689
<i>Liang Chen and Jason Crampton</i>	

Author Index	705
-------------------------------	-----