Table of Contents

Session 1: Cloud and Virtualization

Verifying Trustworthiness of Virtual Appliances in Collaborative Environments 1
Cornelius Namiluko, Jun Ho Huh, and Andrew Martin

Towards a Trustworthy, Lightweight Cloud Computing Framework for Embedded Systems 16
Kurt Dietrich and Johannes Winter

Session 2: Physically Unclonable Functions

Side-Channel Analysis of PUFs and Fuzzy Extractors 33
Dominik Merli, Dieter Schuster, Frederic Stumpf, and Georg Sigl

Coalition Resistant Anonymous Broadcast Encryption Scheme Based on PUF 48
Łukasz Krzywiecki and Mirosław Kutyłowski

A Practical Device Authentication Scheme Using SRAM PUFs 63
Patrick Koeberl, Jiangtao Li, Anand Rajan, Claire Vishik, and Wei Wu

Session 3: Mobile Device Security

Practical Property-Based Attestation on Mobile Devices 78
Kari Kostiainen, N. Asokan, and Jan-Erik Ekberg

Taming Information-Stealing Smartphone Applications (on Android) ... 93
Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W. Freeh

Towards Permission-Based Attestation for the Android Platform (Short Paper) 108
Ingo Bente, Gabi Dreo, Bastian Hellmann, Stephan Heuser, Joerg Vieweg, Josef von Helden, and Johannes Westhuis

Session 4: Socio-Economic Aspects of Trust

Trusting to Learn: Trust and Privacy Issues in Serious Games 116
Miguel Malheiros, Charlene Jennett, Will Seager, and M. Angela Sasse

Bibliografische Informationen
http://d-nb.info/1011530503

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Modifying Trust Dynamics through Cooperation and Defection in Evolving Social Networks 131
Luca Allodi, Luca Chiodi, and Marco Cremonini

Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites (Short Paper) 146
Yang Wang, Gregory Norcie, and Lorrie Faith Cranor

Session 5: Hardware Trust

Systematic Security Assessment at an Early Processor Design Stage 154
Ruirui Huang, David Grawrock, David C. Doughty, and G. Edward Suh

CPU Support for Secure Executables 172
Peter Williams and Rick Boivie

Extracting Device Fingerprints from Flash Memory by Exploiting Physical Variations 188
Pravin Prabhu, Ameen Akel, Laura M. Grupp, Wing-Kei S. Yu, G. Edward Suh, Edwin Kan, and Steven Swanson

Enforcing Executing-Implies-Verified with the Integrity-Aware Processor 202
Michael LeMay and Carl A. Gunter

Session 6: Access Control

Home-Network Threats and Access Controls 217
Mark Baugher and Victor Lortz

Contego: Capability-Based Access Control for Web Browsers (Short Paper) 231
Tongbo Luo and Wenliang Du

Session 7: Privacy

Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information 239
Emiliano De Cristofaro, Yanbin Lu, and Gene Tsudik

CertainLogic: A Logic for Modeling Trust and Uncertainty (Short Paper) 254
Sebastian Ries, Sheikh Mahbub Habib, Max Mühlhäuser, and Vijay Varadharajan

Session 8: Trust Issues in Routing

AS-TRUST: A Trust Quantification Scheme for Autonomous Systems in BGP 262
Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West, Sampath Kannan, Boon Thau Loo, Oleg Sokolsky, and Insup Lee

Incentivizing Responsible Networking via Introduction-Based Routing 277
Gregory Frazier, Quang Duong, Michael P. Wellman, and Edward Petersen

Session 9: Crypto-Physical Protocols

Catching the Cuckoo: Verifying TPM Proximity Using a Quote Timing Side-Channel (Short Paper) 294
Russell A. Fink, Alan T. Sherman, Alexander O. Mitchell, and David C. Challener

Group Distance Bounding Protocols (Short Paper) 302
Srdjan Capkun, Karim El Defrawy, and Gene Tsudik

Author Index 313