

# Contents

## Hardware-Enhanced Trusted Execution

PUF-Based Software Protection for Low-End Embedded Devices . . . . .	3
<i>Florian Kohnhäuser, André Schaller, and Stefan Katzenbeisser</i>	
Why Attackers Win: On the Learnability of XOR Arbiter PUFs . . . . .	22
<i>Fatemeh Ganji, Shahin Tajik, and Jean-Pierre Seifert</i>	
A Unified Security Analysis of Two-Phase Key Exchange Protocols in TPM 2.0 . . . . .	40
<i>Shijun Zhao and Qianying Zhang</i>	
On Making Emerging Trusted Execution Environments Accessible to Developers . . . . .	58
<i>Thomas Nyman, Brian McGillion, and N. Asokan</i>	

## Trust and Users

Computing Trust Levels Based on User's Personality and Observed System Trustworthiness. . . . .	71
<i>Michalis Kanakakis, Shenja van der Graaf, Costas Kalogiros, and Wim Vanobberghen</i>	
Enhancing the Trustworthiness of Service On-Demand Systems via Smart Vote Filtering . . . . .	88
<i>Christos V. Samaras, Ageliki Tsioliaridou, Christos Liaskos, Dimitris Spiliotopoulos, and Sotiris Ioannidis</i>	
Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness. . . . .	104
<i>Melanie Volkamer, Karen Renaud, Gamze Canova, Benjamin Reinheimer, and Kristoffer Braun</i>	

## Trusted Systems and Services

Trustworthy Memory Isolation of Linux on Embedded Devices . . . . .	125
<i>Hamed Nemati, Mads Dam, Roberto Guanciale, Viktor Do, and Arash Vahidi</i>	
LookAhead: Augmenting Crowdsourced Website Reputation Systems with Predictive Modeling . . . . .	143
<i>Sourav Bhattacharya, Otto Huhta, and N. Asokan</i>	

Ripple: Overview and Outlook . . . . .	163
<i>Frederik Armknecht, Ghassan O. Karame, Avikarsha Mandal, Franck Youssef, and Erik Zenner</i>	

Time to Rethink: Trust Brokerage Using Trusted Execution Environments . . .	181
<i>Patrick Koeberl, Vinay Phegade, Anand Rajan, Thomas Schneider, Steffen Schulz, and Maria Zhdanova</i>	

## Trust and Privacy

REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks . . . . .	193
<i>David Förster, Hans Löhr, Jan Zibuschka, and Frank Kargl</i>	

DAA-TZ: An Efficient DAA Scheme for Mobile Devices Using ARM TrustZone . . . . .	209
<i>Bo Yang, Kang Yang, Yu Qin, Zhenfeng Zhang, and Dengguo Feng</i>	

DAA-A: Direct Anonymous Attestation with Attributes . . . . .	228
<i>Liqun Chen and Rainer Urian</i>	

## Building Blocks for Trust

Proposed Processor Extensions for Significant Speedup of Hypervisor Memory Introspection . . . . .	249
<i>Andrei Luțăș, Sándor Lukács, Adrian Coleșa, and Dan Luțăș</i>	

MWA Skew SRAM Based SIMPL Systems for Public-Key Physical Cryptography . . . . .	268
<i>Qingqing Chen, Ulrich Rührmair, Spoorthy Narayana, Uzair Sharif, and Ulf Schlichtmann</i>	

Secure Erasure and Code Update in Legacy Sensors . . . . .	283
<i>Ghassan O. Karame and Wenting Li</i>	

Efficient Provisioning of a Trustworthy Environment for Security-Sensitive Applications . . . . .	300
<i>Adrian Coleșa, Sándor Lukács, Vlad Topan, Radu Ciocaș, and Adrian Pop</i>	

## Poster Session

Towards a Trust Model for Social Networks of Wireless Smart Objects: Work-in-Progress . . . . .	313
<i>Jonathan Ouoba, Cyril Cassagnes, and Tegawendé F. Bissyandé</i>	

BYOD for Android — Just add Java. . . . .	315
<i>Jessica Buttigieg, Mark Vella, and Christian Colombo</i>	
Script Fuzzing with an Attacker’s Mind-Set . . . . .	317
<i>John Galea and Mark Vella</i>	
Trust and Trustworthiness Maintenance: From Architecture to Evaluation . . .	319
<i>Mohamed Bishr, Christian Heinz, Torsten Bandyszak, Micha Moffie, Abigail Goldsteen, Willis Chen, Thorsten Weyer, Sotiris Ioannidis, and Costas Kalogiros</i>	
Increasing the Trustworthiness of Embedded Applications . . . . .	321
<i>Elias Athanasopoulos, Martin Boehner, Cristiano Giuffrida, Dmitry Pidan, Vassilis Prevelakis, Ioannis Sourdis, Christos Strydis, and John Thomson</i>	
Exploring Graph Centralities for Detecting Anomalous Behavior in Large Networks . . . . .	323
<i>Nidhi Rastogi and James Hendler</i>	
Extending the Operational Envelope of Applications . . . . .	325
<i>Vassilis Prevelakis and Mohammad Hamad</i>	
<b>Author Index</b> . . . . .	327

Trust and Trustworthy Computing

8th International Conference, TRUST 2015, Heraklion,

Greece, August 24-26, 2015, Proceedings

Conti, M.; Schunter, M.; Askoxylakis, I. (Eds.)

2015, XI, 328 p. 79 illus., Softcover

ISBN: 978-3-319-22845-7