

Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering

304

Editorial Board Members

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong, China

Geoffrey Coulson

Lancaster University, Lancaster, UK

Falko Dressler

University of Erlangen, Erlangen, Germany

Domenico Ferrari

Università Cattolica Piacenza, Piacenza, Italy

Mario Gerla

UCLA, Los Angeles, USA

Hisashi Kobayashi

Princeton University, Princeton, USA

Sergio Palazzo

University of Catania, Catania, Italy

Sartaj Sahni

University of Florida, Gainesville, USA

Xuemin (Sherman) Shen

University of Waterloo, Waterloo, Canada

Mircea Stan

University of Virginia, Charlottesville, USA

Xiaohua Jia

City University of Hong Kong, Kowloon, Hong Kong

Albert Y. Zomaya

University of Sydney, Sydney, Australia


More information about this series at <http://www.springer.com/series/8197>


Songqing Chen · Kim-Kwang Raymond Choo ·
Xinwen Fu · Wenjing Lou ·
Aziz Mohaisen (Eds.)

Security and Privacy in Communication Networks


15th EAI International Conference, SecureComm 2019
Orlando, FL, USA, October 23–25, 2019
Proceedings, Part I

Editors

Songqing Chen 
George Mason University
Fairfax, VA, USA

Xinwen Fu 
Boston University
Lowell, MA, USA

Aziz Mohaisen 
University of Central Florida
Orlando, FL, USA

Kim-Kwang Raymond Choo 
The University of Texas at San Antonio
San Antonio, TX, USA

Wenjing Lou
Virginia Tech
Blacksburg, VA, USA

ISSN 1867-8211 ISSN 1867-822X (electronic)
Lecture Notes of the Institute for Computer Sciences, Social Informatics
and Telecommunications Engineering
ISBN 978-3-030-37227-9 ISBN 978-3-030-37228-6 (eBook)
<https://doi.org/10.1007/978-3-030-37228-6>

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The importance of ensuring security and privacy in communications networks is recognized by both the research and practitioner community. This is, for example, evidenced by the establishment of the U.S. Cyber Command as a unified combatant command in May 2018. This is also the focus of the 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2019).

This proceedings contains 56 papers, which were selected from 149 submissions (i.e. acceptance rate of 37.6%) from universities, national laboratories, and the private sector from across the USA as well as other countries in Europe and Asia. All the submissions went through an extensive review process by internationally-recognized experts in cybersecurity.

Any successful conference requires the contributions of different stakeholder groups and individuals, who have selfishly volunteered their time and energy in disseminating the call for papers, submitting their research findings, participating in the peer reviews and discussions, etc. First and foremost, we would like to offer our gratitude to the entire Organizing Committee for guiding the entire process of the conference. We are also deeply grateful to all the Technical Program Committee members for their time and efforts in reading, commenting, debating, and finally selecting the papers. We also thank all the external reviewers for assisting the Technical Program Committee in their particular areas of expertise as well as all the authors, participants, and session chairs for their valuable contributions. Support from the Steering Committee and EAI staff members was also crucial in ensuring the success of the conference. It has been a great privilege to be working with such a large group of dedicated and talented individuals.

We hope that you found the discussions and interactions at SecureComm 2019 intellectually stimulating, as well as enjoyed what Orlando, FL, had to offer. Enjoy the proceedings!

September 2019

Xinwen Fu
Kim-Kwang Raymond Choo
Aziz Mohaisen
Wenjing Lou

Organization

Steering Committee

Imrich Chlamtac	University of Trento, Italy
Guofei Gu	Texas A&M University, USA
Peng Liu	Pennsylvania State University, USA
Sencun Zhu	Pennsylvania State University, USA

Organizing Committee

General Chairs

Xinwen Fu	University of Central Florida, USA
Kim-Kwang Raymond Choo	The University of Texas at San Antonio, USA

TPC Chair and Co-chairs

Aziz Mohaisen	University of Central Florida, USA
Wenjing Lou	Virginia Tech, USA

Sponsorship and Exhibit Chair

Qing Yang	University of North Texas, USA
-----------	--------------------------------

Local Chairs

Clay Posey	University of Central Florida, USA
Cliff C. Zou	University of Central Florida, USA

Workshops Chairs

Kaiqi Xiong	University of South Florida, USA
Liang Xiao	Xiamen University, China

Publicity and Social Media Chairs

Yao Liu	University of South Florida, USA
Zhen Ling	Southeast University, China

Publications Chairs

Songqing Chen	George Mason University, USA
Houbing Song	Embry-Riddle Aeronautical University, USA

Web Chairs

Bryan Pearson	University of Central Florida, USA
Yue Zhang	University of Central Florida, USA

Panels Chairs

Simon (Xinming) Ou	University of South Florida, USA
Craig A. Shue	Worcester Polytechnic Institute, USA

Demos Chair

Song Han	University of Connecticut, USA
----------	--------------------------------

Tutorials Chair

Yong Guan	Iowa State University, USA
-----------	----------------------------

Technical Program Committee

Amro Awad	University of Central Florida, USA
Kai Bu	Zhejiang University, China
Yinzhi Cao	Johns Hopkins University, USA
Eric Chan-Tin	Loyola University Chicago, USA
Kai Chen	Chinese Academy of Sciences, China
Yu Chen	Binghamton University - SUNY, USA
Sherman S. M. Chow	The Chinese University of Hong Kong, Hong Kong, China
Jun Dai	California State University, Sacramento, USA
Karim Elish	Florida Polytechnic University, USA
Birhanu Eshete	University of Michigan, USA
Debin Gao	Singapore Management University, Singapore
Le Guan	University of Georgia, USA
Yong Guan	Iowa State University, USA
Yongzhong He	Beijing Jiaotong University, China
Murtuza Jadliwala	The University of Texas at San Antonio, USA
George Kesidis	Pennsylvania State University, USA
Joongheon Kim	Chung-Ang University, South Korea
Hyoungshick Kim	Sungkyunkwan University, South Korea
Gokhan Kul	Delaware State University, USA
Laurent L. Njilla	Air Force Research Laboratory, USA
Yingjiu Li	Singapore Management University, Singapore
Jingqiang Lin	Chinese Academy of Sciences, China
Zhiqiang Lin	The Ohio State University, USA
Yao Liu	University of South Florida, USA
Javier Lopez	UMA, Spain
Wenjing Lou	Virginia Tech, USA
Rongxing Lu	University of New Brunswick, Canada

Ashraf Matrawy	Carleton University, Canada
Aziz Mohaisen	University of Central Florida, USA
Vaibhav Rastogi	Northwestern University, USA
Sankardas Roy	Bowling Green State University, USA
Pierangela Samarati	University of Milan, Italy
Mohamed Shehab	UNC Charlotte, USA
Seungwon Shin	KAIST, South Korea
Houbing Song	Embry-Riddle Aeronautical University, USA
Jeffrey Spaulding	Niagara University, USA
Martin Strohmeier	University of Oxford, UK
Wenhai Sun	Purdue University, USA
Qiang Tang	New Jersey Institute of Technology, USA
A. Selcuk Uluagac	Florida International University, USA
Eugene Vasserman	Kansas State University, USA
Cong Wang	City University of Hong Kong Shenzhen Research Institute, Hong Kong, China
Huihui Wang	Jacksonville University, USA
Qian Wang	Wuhan University, China
An Wang	Case Western Reserve University, USA
Edgar Weippl	SBA Research, Austria
Susanne Wetzl	Stevens Institute of Technology, USA
Dinghao Wu	Pennsylvania State University, USA
Mengjun Xie	The University of Tennessee at Chattanooga, USA
Fengyuan Xu	Nanjing University, China
Shouhuai Xu	The University of Texas at San Antonio, USA
Shucheng Yu	Stevens Institute of Technology, USA
Jiawei Yuan	Embry-Riddle Aeronautical University, USA
Xingliang Yuan	Monash University, Australia
Fareed Zaffar	LUMS University, Pakistan
Xiao Zhang	Palo Alto Networks, USA
Junjie Zhang	Wright State University, USA
Kuan Zhang	University of Nebraska-Lincoln, USA
Wensheng Zhang	Iowa State University, USA
Yuan Zhang	Nanjing University, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Cliff Zou	University of Central Florida, USA

Contents – Part I

Blockchains

Trustless Framework for Iterative Double Auction Based on Blockchain	3
<i>Truc D. T. Nguyen and My T. Thai</i>	
Towards a Multi-chain Future of Proof-of-Space	23
<i>Shuyang Tang, Jilai Zheng, Yao Deng, Ziyu Wang, Zhiqiang Liu, Dawu Gu, Zhen Liu, and Yu Long</i>	
Secure Consistency Verification for Untrusted Cloud Storage by Public Blockchains	39
<i>Kai Li, Yuzhe Tang, Beom Heyn (Ben) Kim, and Jianliang Xu</i>	
An Enhanced Verifiable Inter-domain Routing Protocol Based on Blockchain	63
<i>Yaping Liu, Shuo Zhang, Haojin Zhu, Peng-Jun Wan, Lixin Gao, and Yaoxue Zhang</i>	

Internet of Things

Edge-Assisted CNN Inference over Encrypted Data for Internet of Things . . .	85
<i>Yifan Tian, Jiawei Yuan, Shucheng Yu, Yantian Hou, and Houbing Song</i>	
POKs Based Secure and Energy-Efficient Access Control for Implantable Medical Devices	105
<i>Chenglong Fu, Xiaojiang Du, Longfei Wu, Qiang Zeng, Amr Mohamed, and Mohsen Guizani</i>	
USB-Watch: A Dynamic Hardware-Assisted USB Threat Detection Framework.	126
<i>Kyle Denney, Enes Erdin, Leonardo Babun, Michael Vai, and Selcuk Uluagac</i>	
Automated IoT Device Fingerprinting Through Encrypted Stream Classification	147
<i>Jianhua Sun, Kun Sun, and Chris Shenefiel</i>	

Catching Malware

DeepCG: Classifying Metamorphic Malware Through Deep Learning of Call Graphs	171
<i>Shuang Zhao, Xiaobo Ma, Wei Zou, and Bo Bai</i>	
ChaffyScript: Vulnerability-Agnostic Defense of JavaScript Exploits via Memory Perturbation	191
<i>Xunchao Hu, Brian Testa, and Heng Yin</i>	
Obfuscifier: Obfuscation-Resistant Android Malware Detection System	214
<i>Zhiqiang Li, Jun Sun, Qiben Yan, Witawas Srisa-an, and Yutaka Tsutano</i>	
Closing the Gap with APTs Through Semantic Clusters and Automated Cybergames	235
<i>Steven Gianvecchio, Christopher Burkhalter, Hongying Lan, Andrew Sillers, and Ken Smith</i>	

Machine Learning

Stochastic ADMM Based Distributed Machine Learning with Differential Privacy	257
<i>Jiahao Ding, Sai Mounika Errapotu, Haijun Zhang, Yanmin Gong, Miao Pan, and Zhu Han</i>	
Topology-Aware Hashing for Effective Control Flow Graph Similarity Analysis	278
<i>Yuping Li, Jiyong Jang, and Xinming Ou</i>	
Trojan Attack on Deep Generative Models in Autonomous Driving.	299
<i>Shaohua Ding, Yulong Tian, Fengyuan Xu, Qun Li, and Sheng Zhong</i>	
FuncNet: A Euclidean Embedding Approach for Lightweight Cross-platform Binary Recognition	319
<i>Mengxia Luo, Can Yang, Xiaorui Gong, and Lei Yu</i>	

Everything Traffic Security

Towards Forward Secure Internet Traffic	341
<i>Eman Salem Alashwali, Pawel Szalachowski, and Andrew Martin</i>	
Traffic-Based Automatic Detection of Browser Fingerprinting.	365
<i>Rui Zhao, Edward Chow, and Chunchun Li</i>	
Measuring Tor Relay Popularity	386
<i>Tao Chen, Weiqi Cui, and Eric Chan-Tin</i>	

SoK: ATT&CK Techniques and Trends in Windows Malware	406
<i>Kris Oosthoek and Christian Doerr</i>	

Communicating Covertly

Covert Channels in SDN: Leaking Out Information from Controllers to End Hosts	429
<i>Jiahao Cao, Kun Sun, Qi Li, Mingwei Xu, Zijie Yang, Kyung Joon Kwak, and Jason Li</i>	

Victim-Aware Adaptive Covert Channels	450
<i>Riccardo Bortolameotti, Thijs van Ede, Andrea Continella, Maarten Everts, Willem Jonker, Pieter Hartel, and Andreas Peter</i>	

Random Allocation Seed-DSSS Broadcast Communication Against Jamming Attacks.	472
<i>Ahmad Alagil and Yao Liu</i>	

A Loss-Tolerant Mechanism of Message Segmentation and Reconstruction in Multi-path Communication of Anti-tracking Network.	490
<i>Changbo Tian, YongZheng Zhang, Tao Yin, Yupeng Tuo, and Ruihai Ge</i>	

Let's Talk Privacy

Ticket Transparency: Accountable Single Sign-On with Privacy-Preserving Public Logs	511
<i>Dawei Chu, Jingqiang Lin, Fengjun Li, Xiaokun Zhang, Qiong Xiao Wang, and Guangqi Liu</i>	

Decentralized Privacy-Preserving Reputation Management for Mobile Crowdsensing.	532
<i>Lichuan Ma, Qingqi Pei, Youyang Qu, Kefeng Fan, and Xin Lai</i>	

Location Privacy Issues in the OpenSky Network Crowdsourcing Platform	549
<i>Savio Sciancalepore, Saeif Alhazbi, and Roberto Di Pietro</i>	

Privacy-Preserving Genomic Data Publishing via Differentially-Private Suffix Tree.	569
<i>Tanya Khatri, Gaby G. Dagher, and Yantian Hou</i>	

Author Index	585
------------------------	-----

Contents – Part II

Deep Analytics

TL;DR Hazard: A Comprehensive Study of Levelsquatting Scams	3
<i>Kun Du, Hao Yang, Zhou Li, Haixin Duan, Shuang Hao, Baojun Liu, Yuxiao Ye, Mingxuan Liu, Xiaodong Su, Guang Liu, Zhifeng Geng, Zaifeng Zhang, and Jinjin Liang</i>	
Account Lockouts: Characterizing and Preventing Account Denial-of-Service Attacks.	26
<i>Yu Liu, Matthew R. Squires, Curtis R. Taylor, Robert J. Walls, and Craig A. Shue</i>	
Application Transiency: Towards a Fair Trade of Personal Information for Application Services.	47
<i>Raquel Alvarez, Jake Levenson, Ryan Sheatsley, and Patrick McDaniel</i>	
CustomPro: Network Protocol Customization Through Cross-Host Feature Analysis	67
<i>Yurong Chen, Tian Lan, and Guru Venkataramani</i>	

Systematic Theory

On the Security of TRNGs Based on Multiple Ring Oscillators	89
<i>Xinying Wu, Yuan Ma, Jing Yang, Tianyu Chen, and Jingqiang Lin</i>	
Secrecy on a Gaussian Relay-Eavesdropper Channel with a Trusted Relay . . .	108
<i>Keke Hu, Xiaohui Zhang, and Yongming Wang</i>	
Target Information Trading - An Economic Perspective of Security.	126
<i>Jing Hou, Li Sun, Tao Shu, and Husheng Li</i>	
Cyber Threat Analysis Based on Characterizing Adversarial Behavior for Energy Delivery System	146
<i>Sharif Ullah, Sachin Shetty, Anup Nayak, Amin Hassanzadeh, and Kamrul Hasan</i>	

Bulletproof Defenses

The Disbanding Attack: Exploiting Human-in-the-Loop Control in Vehicular Platooning	163
<i>Ali Al-Hashimi, Pratham Oza, Ryan Gerdes, and Thidapat Chantem</i>	

Generic Construction of ElGamal-Type Attribute-Based Encryption Schemes with Revocability and Dual-Policy	184
<i>Shengmin Xu, Yinghui Zhang, Yingjiu Li, Ximeng Liu, and Guomin Yang</i>	
Online Cyber Deception System Using Partially Observable Monte-Carlo Planning Framework	205
<i>Md Ali Reza Al Amin, Sachin Shetty, Laurent Njilla, Deepak K. Tosh, and Charles Kamhoua</i>	
SEVGuard: Protecting User Mode Applications Using Secure Encrypted Virtualization.	224
<i>Ralph Palutke, Andreas Neubaum, and Johannes Götzfried</i>	
Blockchains and IoT	
A Behavior-Aware Profiling of Smart Contracts	245
<i>Xuetao Wei, Can Lu, Fatma Rana Ozcan, Ting Chen, Boyang Wang, Di Wu, and Qiang Tang</i>	
A Performance-Optimization Method for Reusable Fuzzy Extractor Based on Block Error Distribution of Iris Trait.	259
<i>Feng Zhu, Peisong Shen, and Chi Chen</i>	
Detecting Root-Level Endpoint Sensor Compromises with Correlated Activity.	273
<i>Yunsen Lei and Craig A. Shue</i>	
Footprints: Ensuring Trusted Service Function Chaining in the World of SDN and NFV	287
<i>Montida Pattaranantakul, Qipeng Song, Yanmei Tian, Licheng Wang, Zonghua Zhang, and Ahmed Meddahi</i>	
Security and Analytics	
Hecate: Automated Customization of Program and Communication Features to Reduce Attack Surfaces.	305
<i>Hongfa Xue, Yurong Chen, Guru Venkataramani, and Tian Lan</i>	
Phish-Hook: Detecting Phishing Certificates Using Certificate Transparency Logs	320
<i>Edona Faslilja, Hasan Ferit Enişer, and Bernd Prünster</i>	
IIFA: Modular Inter-app Intent Information Flow Analysis of Android Applications.	335
<i>Abhishek Tiwari, Sascha Groß, and Christian Hammer</i>	

Power Analysis and Protection on SPECK and Its Application in IoT	350
<i>Jing Ge, An Wang, Liehuang Zhu, Xin Liu, Ning Shang, and Guoshuang Zhang</i>	
 Machine Learning, Privately	
Adversarial False Data Injection Attack Against Nonlinear AC State Estimation with ANN in Smart Grid	365
<i>Tian Liu and Tao Shu</i>	
On Effectiveness of Adversarial Examples and Defenses for Malware Classification	380
<i>Robert Podschwadt and Hassan Takabi</i>	
PrivC—A Framework for Efficient Secure Two-Party Computation.	394
<i>Kai He, Liu Yang, Jue Hong, Jinghua Jiang, Jieming Wu, Xu Dong, and Zhuxun Liang</i>	
CoRide: A Privacy-Preserving Collaborative-Ride Hailing Service Using Blockchain-Assisted Vehicular Fog Computing.	408
<i>Meng Li, Liehuang Zhu, and Xiaodong Lin</i>	
 Better Clouds	
Non-Interactive MPC with Trusted Hardware Secure Against Residual Function Attacks.	425
<i>Ryan Karl, Timothy Burchfield, Jonathan Takeshita, and Taeho Jung</i>	
A Study of the Multiple Sign-in Feature in Web Applications	440
<i>Marwan Albahar, Xing Gao, Gaby Dagher, Daiping Liu, Fengwei Zhang, and Jidong Xiao</i>	
Authenticated LSM Trees with Minimal Trust	454
<i>Yuzhe Tang, Kai Li, and Ju Chen</i>	
Modern Family: A Revocable Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX	472
<i>Alexandros Bakas and Antonis Michalas</i>	
 ATCS Workshop	
A Nature-Inspired Framework for Optimal Mining of Attribute-Based Access Control Policies	489
<i>Masoud Narouei and Hassan Takabi</i>	
Author Index	507