

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

254

Editorial Board

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong, Hong Kong

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, Florida, USA

Xuemin Sherman Shen

University of Waterloo, Waterloo, Canada

Mircea Stan

University of Virginia, Charlottesville, USA

Jia Xiaohua

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>

Raheem Beyah · Bing Chang
Yingjiu Li · Sencun Zhu (Eds.)

Security and Privacy in Communication Networks

14th International Conference, SecureComm 2018
Singapore, Singapore, August 8–10, 2018
Proceedings, Part I

Editors

Raheem Beyah
Klaus Advanced Computing Building
Georgia Institute of Technology
Atlanta, GA, USA

Bing Chang
Singapore Management University
Singapore, Singapore

Yingjiu Li
School of Information Systems
Singapore Management University
Singapore, Singapore

Sencun Zhu
Pennsylvania State University
University Park, PA, USA

ISSN 1867-8211 ISSN 1867-822X (electronic)
Lecture Notes of the Institute for Computer Sciences, Social Informatics
and Telecommunications Engineering
ISBN 978-3-030-01700-2 ISBN 978-3-030-01701-9 (eBook)
<https://doi.org/10.1007/978-3-030-01701-9>

Library of Congress Control Number: 2018940136

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018

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, express 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

We are delighted to introduce the proceedings of the 14th European Alliance for Innovation (EAI) International Conference on Security and Privacy in Communication Networks (SecureComm 2018), held in Singapore, in August 2018. SecureComm seeks high-quality research contributions in the form of well-developed papers. Topics of interest encompass research advances in all areas of secure communications and networking.

The technical program of SecureComm 2018 consisted of 33 full papers and 18 short papers in the main conference sessions. The conference sessions were: Session 1, IoT Security; Session 2, User and Data Privacy; Session 3, Mobile Security I; Session 4, Wireless Security; Session 5, Software Security; Session 6, Cloud Security I; Session 7, Mobile Security II; Session 8, Social Network and Enterprise Security; Session 9, Network Security I; Session 10, Applied Cryptography; Session 11, Network Security II; Session 12, Cloud Security II; and Session 13, Web Security.

Aside from the high-quality technical paper presentations, the technical program also featured two keynote speeches and one technical workshop. The two keynote speeches were given by Prof. Robert Deng from Singapore Management University, Singapore, and Prof. Zhiqiang Lin from Ohio State University, USA. The workshop organized was the 6th International Workshop on Applications and Techniques in Cyber Security (ATCS 2018). The ATCS workshop focused on all aspects of techniques and applications in cybersecurity research. The purpose of ATCS 2018 was to provide a forum for the presentation and discussion of innovative ideas, cutting-edge research results, and novel techniques, methods, and applications on all aspects of cyber security and machine learning.

Coordination with the Steering Committee co-chairs, Imrich Chlamtac and Guofei Gu, was essential for the success of the conference. We sincerely appreciate their constant support and guidance. It was also a great pleasure to work with such an excellent Organizing Committee team for their hard work in organizing and supporting the conference. In particular, we thank the Technical Program Committee, led by our co-chairs, Dr. Raheem Beyah and Dr. Sencun Zhu, who completed the peer-review process of technical papers and compiled a high-quality technical program. We are also grateful to the conference coordinator, Dominika Belisova, for her support and all the authors who submitted their papers to the SecureComm 2018 conference and workshops.

We strongly believe that the SecureComm conference provides a good forum for all researchers, developers, and practitioners to exchange ideas in all areas of secure communications and networking. We also expect that future SecureComm conferences will be successful and stimulating, as indicated by the contributions presented in this volume.

September 2018

Raheem Beyah
Bing Chang
Yingjiu Li
Sencun Zhu

Organization

Steering Committee Co-chairs

Imrich Chlamtac	University of Trento, Italy
Guofei Gu	Texas A&M University, USA

Steering Committee Members

Krishna Moorthy	IIT Madras, India
Sivalingam	
Peng Liu	Pennsylvania State University, USA

Organizing Committee

General Chair

Yingjiu Li	Singapore Management University, Singapore
------------	--

Technical Program Committee Co-chairs

Raheem Beyah	Georgia Tech, USA
Sencun Zhu	Pennsylvania State University, USA

Publications Chair

Bing Chang	Singapore Management University, Singapore
------------	--

Publicity and Social Media Co-chairs

Yangguang Tian	Singapore Management University, Singapore
Zhao Wang	Peking University, China
Sankardas Roy	Bowling Green State University, USA

Web Chair

Ximing Liu	Singapore Management University, Singapore
------------	--

Panels Chair

Min Suk Kang	National University of Singapore, Singapore
--------------	---

Local Chair

Li Tieyan	Shield Lab (Singapore), Huawei Technologies Co., Ltd., Singapore
-----------	--

Conference Manager

Dominika Belisova

EAI - European Alliance for Innovation

Technical Program Committee

Elisa Bertino	Purdue University, USA
Alvaro Cardenas	The University of Texas at Dallas, USA
Kai Chen	Institute of Information Engineering, Chinese Academy of Sciences, China
Yu Chen	State University of New York – Binghamton, USA
Sherman S. M. Chow	The Chinese University of Hong Kong, SAR China
Jun Dai	California State University, Sacramento, USA
Mohan Dhawan	IBM Research, India
Birhanu Eshete	University of Illinois at Chicago, USA
Debin Gao	Singapore Management University, Singapore
Le Guan	Pennsylvania State University, USA
Yong Guan	Iowa State University, USA
Yongzhong He	Beijing Jiaotong University, China
Lin Huang	Qihoo 360 Technology Co. Ltd., China
Heqing Huang	IBM Research, USA
Shouling Ji	Zhejiang University, China
Yier Jin	University of Florida, USA
Issa Khalil	Qatar Computing Research Institute (QCRI), Qatar
Lee Lerner	Georgia Institute of Technology, USA
Ming Li	University of Arizona, USA
Qinghua Li	University of Arkansas, USA
Qi Li	Tsinghua University, China
Xiaoqing Liao	College of William and Mary, USA
Yue-Hsun Lin	JD.com, USA
Zhiqiang Lin	The Ohio State University, USA
Yao Liu	University of South Florida, USA
Anyi Liu	Oakland University, USA
Giovanni Livraga	Università degli Studi di Milano, Italy
Javier Lopez	University of Malaga, Spain
Rongxing Lu	University of New Brunswick, Canada
Liran Ma	Texas Christian University, USA
Aziz Mohaisen	University of Central Florida, USA
Goutam Paul	Indian Statistical Institute, India
Rui Qiao	LinkedIn, USA
Sankardas Roy	Bowling Green State University, USA
Pierangela Samarati	Università degli Studi di Milano, Italy
Seungwon Shin	KAIST, South Korea
Kapil Singh	IBM Research, USA
Anna Squicciarini	Pennsylvania State University, USA
Martin Strohmeier	University of Oxford, UK

Kun Sun	George Mason University, USA
A. Selcuk Uluagac	Florida International University, USA
Zhiguo Wan	Shandong University, China
Cong Wang	City University of Hong Kong, SAR China
Wei Wang	Beijing Jiaotong University, China
Lanier Watkins	Johns Hopkins University, USA
Edgar Weippl	SBA Research, Austria
Dinghao Wu	Pennsylvania State University, USA
Jidong Xiao	Boise State University, USA
Kaiqi Xiong	University of South Florida, USA
Zhi Xu	Palo Alto Networks, USA
Shouhuai Xu	University of Texas at San Antonio, USA
Yi Yang	Fontbonne University, USA
Danfeng Yao	Virginia Tech, USA
Kai Zeng	George Mason University, USA
Chao Zhang	Tsinghua University, China
Fengwei Zhang	Wayne State University, USA
Yuqing Zhang	University of Chinese Academy of Sciences, China
Junjie Zhang	Wright State University, USA
Wensheng Zhang	Iowa State University, USA
Yongjun Zhao	The Chinese University of Hong Kong, SAR China
Yunlei Zhao	Fudan University, China
Cliff Zou	University of Central Florida, USA

Contents – Part I

IoT Security

A Secure Remote Monitoring Framework Supporting Efficient Fine-Grained Access Control and Data Processing in IoT.	3
<i>Yaxing Chen, Wenhai Sun, Ning Zhang, Qinghua Zheng, Wenjing Lou, and Y. Thomas Hou</i>	
Securing the Smart Home via a Two-Mode Security Framework.	22
<i>Devkishen Sisodia, Samuel Mergendahl, Jun Li, and Hasan Cam</i>	
Out of Kilter: Holistic Exploitation of Denial of Service in Internet of Things.	43
<i>Suhas Setikere, Vinay Sachidananda, and Yuval Elovici</i>	
Augmented Chain of Ownership: Configuring IoT Devices with the Help of the Blockchain	53
<i>Sophie Dramé-Maigné, Maryline Laurent, Laurent Castillo, and Hervé Ganem</i>	

User and Data Privacy

Secure and Efficient Multi-Party Directory Publication for Privacy-Preserving Data Sharing	71
<i>Katchaguy Areekijseeree, Yuzhe Tang, Ju Chen, Shuang Wang, Arun Iyengar, and Balaji Palanisamy</i>	
A Formal Logic Framework for the Automation of the Right to Be Forgotten.	95
<i>Abhishek Tiwari, Fabian Bendun, and Christian Hammer</i>	
Privacy-Preserving Biometric-Based Remote User Authentication with Leakage Resilience.	112
<i>Yangguang Tian, Yingjiu Li, Rongmao Chen, Nan Li, Ximeng Liu, Bing Chang, and Xingjie Yu</i>	
Differentially Private High-Dimensional Data Publication via Markov Network	133
<i>Fengqiong Wei, Wei Zhang, Yunfang Chen, and Jingwen Zhao</i>	

Mobile Security

Automated Identification of Sensitive Data via Flexible User Requirements . . .	151
<i>Ziqi Yang and Zhenkai Liang</i>	
Understanding Android Obfuscation Techniques: A Large-Scale Investigation in the Wild	172
<i>Shuaike Dong, Menghao Li, Wenrui Diao, Xiangyu Liu, Jian Liu, Zhou Li, Fenghao Xu, Kai Chen, XiaoFeng Wang, and Kehuan Zhang</i>	
Transparent Low-Latency Network Anonymisation for Mobile Devices	193
<i>Martin Byrenheid, Stefan Köpsell, Alexander Naumenko, and Thorsten Strufe</i>	
Inferring UI States of Mobile Applications Through Power Side Channel Exploitation	210
<i>Yao Guo, Junming Ma, Wenjun Wu, and Xiangqun Chen</i>	
PoliteCamera: Respecting Strangers' Privacy in Mobile Photographing	227
<i>Ang Li, Wei Du, and Qinghua Li</i>	
Lexical Mining of Malicious URLs for Classifying Android Malware	248
<i>Shanshan Wang, Qiben Yan, Zhenxiang Chen, Lin Wang, Riccardo Spolaor, Bo Yang, and Mauro Conti</i>	
Grandroid: Graph-Based Detection of Malicious Network Behaviors in Android Applications.	264
<i>Zhiqiang Li, Jun Sun, Qiben Yan, Witawas Srisa-an, and Shakthi Bachala</i>	
FGFDect: A Fine-Grained Features Classification Model for Android Malware Detection	281
<i>Chao Liu, Jianan Li, Min Yu, Bo Luo, Song Li, Kai Chen, Weiqing Huang, and Bin Lv</i>	

Wireless Security

An Adaptive Primary User Emulation Attack Detection Mechanism for Cognitive Radio Networks	297
<i>Qi Dong, Yu Chen, Xiaohua Li, Kai Zeng, and Roger Zimmermann</i>	
VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs	318
<i>Rens W. van der Heijden, Thomas Lukaseder, and Frank Kargl</i>	
Birds of a Feather Flock Together: Fuzzy Extractor and Gait-Based Robust Group Secret Key Generation for Smart Wearables	338
<i>Chitra Javali and Girish Revadigar</i>	

Unchained Identities: Putting a Price on Sybil Nodes in Mobile Ad Hoc Networks	358
<i>Arne Bochém, Benjamin Leiding, and Dieter Hogrefe</i>	

Software Security

Understanding the Hidden Cost of Software Vulnerabilities: Measurements and Predictions	377
<i>Afsah Anwar, Aminollah Khormali, DaeHun Nyang, and Aziz Mohaisen</i>	
Privacy-Enhanced Fraud Detection with Bloom Filters	396
<i>Daniel Arp, Erwin Quiring, Tammo Krueger, Stanimir Dragiev, and Konrad Rieck</i>	
FriSM: Malicious Exploit Kit Detection via Feature-Based String-Similarity Matching	416
<i>Sungjin Kim and Brent ByungHoon Kang</i>	
A Machine Learning Framework for Studying Domain Generation Algorithm (DGA)-Based Malware	433
<i>Tommy Chin, Kaiqi Xiong, Chengbin Hu, and Yi Li</i>	

Cloud Security

Se-Lambda: Securing Privacy-Sensitive Serverless Applications Using SGX Enclave	451
<i>Weizhong Qiang, Zezhao Dong, and Hai Jin</i>	
CAVAS: Neutralizing Application and Container Security Vulnerabilities in the Cloud Native Era	471
<i>Kennedy A. Torkura, Muhammad I. H. Sukmana, Feng Cheng, and Christoph Meinel</i>	
Shuffler: Mitigate Cross-VM Side-Channel Attacks via Hypervisor Scheduling	491
<i>Li Liu, An Wang, WanYu Zang, Meng Yu, Menbai Xiao, and Songqing Chen</i>	
Building Your Private Cloud Storage on Public Cloud Service Using Embedded GPUs	512
<i>Wangzhao Cheng, Fangyu Zheng, Wuqiong Pan, Jingqiang Lin, Huorong Li, and Bingyu Li</i>	
Secure and Efficient Outsourcing of Large-Scale Overdetermined Systems of Linear Equations	529
<i>Shiran Pan, Wen-Tao Zhu, Qiong Xiao Wang, and Bing Chang</i>	

Privacy-Preserving Multiparty Learning for Logistic Regression 549
 Wei Du, Ang Li, and Qinghua Li

Privacy-Preserving Outsourcing of Large-Scale Nonlinear Programming
to the Cloud. 569
 Ang Li, Wei Du, and Qinghua Li

A Verifiable and Dynamic Multi-keyword Ranked Search Scheme
over Encrypted Cloud Data with Accuracy Improvement 588
 Qi Zhang, Shaojing Fu, Nan Jia, and Ming Xu

Author Index 605

Contents – Part II

Social Network and Enterprise Security

A Mobile Botnet That Meets Up at Twitter	3
<i>Yulong Dong, Jun Dai, and Xiaoyan Sun</i>	
Detecting Suspicious Members in an Online Emotional Support Service	22
<i>Yu Li, Dae Wook Kim, Junjie Zhang, and Derek Doran</i>	
Towards a Reliable and Accountable Cyber Supply Chain in Energy Delivery System Using Blockchain	43
<i>Xueping Liang, Sachin Shetty, Deepak Tosh, Yafei Ji, and Danyi Li</i>	
Social Bot Detection Using Tweets Similarity	63
<i>Yahan Wang, Chunhua Wu, Kangfeng Zheng, and Xiujuan Wang</i>	

Network Security

A Multi-protocol Authentication Shibboleth Framework and Implementation for Identity Federation.	81
<i>Mengyi Li, Chi-Hung Chi, Chen Ding, Raymond Wong, and Zhong She</i>	
SDN-Assisted Network-Based Mitigation of Slow DDoS Attacks	102
<i>Thomas Lukaseder, Lisa Maile, Benjamin Erb, and Frank Kargl</i>	
A Holistic Approach Towards Peer-to-Peer Security and Why Proof of Work Won't Do	122
<i>Bernd Prüinster, Dominik Ziegler, Chrisitan Kollmann, and Bojan Suzic</i>	
A Robust Intrusion Detection Network Using Thresholdless Trust Management System with Incentive Design	139
<i>Amir Rezapour and Wen-Guey Tzeng</i>	
A Metapolicy Framework for Enhancing Domain Expressiveness on the Internet	155
<i>Gaurav Varshney and Pawel Szalachowski</i>	
Adaptive Deterrence of DNS Cache Poisoning	171
<i>Sze Yiu Chau, Omar Chowdhury, Victor Gonsalves, Huangyi Ge, Weining Yang, Sonia Fahmy, and Ninghui Li</i>	

Mission-Oriented Security Model, Incorporating Security Risk, Cost and Payout	192
<i>Sayed M. Saghaian N. E., Tom La Porta, Trent Jaeger, Z. Berkay Celik, and Patrick McDaniel</i>	

On the Feasibility of Fine-Grained TLS Security Configurations in Web Browsers Based on the Requested Domain Name	213
<i>Eman Salem Alashwali and Kasper Rasmussen</i>	

Applied Cryptography

Neural Network Based Min-entropy Estimation for Random Number Generators	231
<i>Jing Yang, Shuangyi Zhu, Tianyu Chen, Yuan Ma, Na Lv, and Jingqiang Lin</i>	

Improved Quantum Key Distribution Networks Based on Blom-Scheme	251
<i>Ya-Qi Song and Li Yang</i>	

Implementation of High Throughput XTS-SM4 Module for Data Storage Devices	271
<i>Liang Zheng, Changting Li, Zongbin Liu, Lingchen Zhang, and Cunqing Ma</i>	

Detecting and Defending Against Certificate Attacks with Origin-Bound CAPTCHAs	291
<i>Adil Ahmad, Faizan Ahmad, Lei Wei, Vinod Yegneswaran, and Fareed Zaffar</i>	

Web Security

FrameHanger: Evaluating and Classifying Iframe Injection at Large Scale.	311
<i>Ke Tian, Zhou Li, Kevin D. Bowers, and Danfeng (Daphne) Yao</i>	

Xilara: An XSS Filter Based on HTML Template Restoration	332
<i>Keitaro Yamazaki, Daisuke Kotani, and Yasuo Okabe</i>	

Local Storage on Steroids: Abusing Web Browsers for Hidden Content Storage and Distribution.	352
<i>Juan D. Parra Rodriguez and Joachim Posegga</i>	

ATCS Workshop

A Review and Costing of Lightweight Authentication Schemes for Internet of Things (IoT): <i>Towards Design of an Authentication Architecture for Smart Home Applications</i>	375
<i>Atlee M. Gamundani, Amelia Phillips, and Hippolyte N. Muyingi</i>	
A Survey of Big Data Security Solutions in Healthcare	391
<i>Musfira Siddique, Muhammad Ayzed Mirza, Mudassar Ahmad, Junaid Chaudhry, and Rafiqul Islam</i>	
Malware Detection for Healthcare Data Security	407
<i>Mozammel Chowdhury, Sharmin Jahan, Rafiqul Islam, and Junbin Gao</i>	
Secure Communication on NoC Based MPSoC.	417
<i>Gaurav Sharma, Soultana Ellinidou, Veronika Kuchta, Rajeev Anand Sahu, Olivier Markowitch, and Jean-Michel Dricot</i>	
Online Radicalisation Along a Continuum: From When Individuals Express Grievances to When They Transition into Extremism	429
<i>Yeslam Al-Saggaf</i>	
A Multiple Linear Regression Based High-Performance Error Prediction Method for Reversible Data Hiding	441
<i>Bin Ma, Xiaoyu Wang, Bing Li, and Yunqing Shi</i>	
A Secure AODV Protocol Improvement Scheme Based on Fuzzy Neural Network	453
<i>Tongyi Xie, Jiawei Mo, and Baohua Huang</i>	
What's in a Downgrade? A Taxonomy of Downgrade Attacks in the TLS Protocol and Application Protocols Using TLS	468
<i>Eman Salem Alashwali and Kasper Rasmussen</i>	
An Approach to Enhance Understanding of Digital Forensics Technical Terms in the Presentation Phase of a Digital Investigation Using Multimedia Presentations	488
<i>Niken Dwi Wahyu Cahyani, Ben Martini, Kim-Kwang Raymond Choo, and Helen Ashman</i>	
Event Reconstruction of Indonesian E-Banking Services on Windows Phone Devices	507
<i>Niken Dwi Wahyu Cahyani, Ben Martini, Kim-Kwang Raymond Choo, and Helen Ashman</i>	
Author Index	523