

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Dooho Choi · Sylvain Guilley (Eds.)

Information Security Applications

17th International Workshop, WISA 2016
Jeju Island, Korea, August 25–27, 2016
Revised Selected Papers



Springer

Editors

Dooho Choi
ETRI
Daejeon
Korea (Republic of)

Sylvain Guilley
Secure-IC, S.A.S.
Paris
France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-56548-4

ISBN 978-3-319-56549-1 (eBook)

DOI 10.1007/978-3-319-56549-1

Library of Congress Control Number: 2017935962

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 17th International Workshop on Information Security Applications (WISA 2016) was held at Ramada Plaza Hotel, Jeju Island, Korea, during August 25–27, 2016. The workshop was hosted by the Korea Institute of Information Security and Cryptology (KIISC) and sponsored by the Ministry of Science, ICT and Future Planning (MSIP). It was also co-sponsored by the Korea Internet and Security Agency (KISA), the Electronics and Telecommunications Research Institute (ETRI), the National Security Research Institute (NSR), Jeju National University, and Kona.

The excellent arrangements were led by the WISA 2016 general chair, Prof. Im-Yeong Lee, and organizing chair, Prof. Ho-won Kim. This year WISA 2016 provided an open forum for exchanging and sharing of ongoing hot topics and results of research, development, and applications in information security areas.

The Program Committee prepared for an interesting program including four invited talks, from Dr. Ludovic Perret of Jussieu University (UPMC), Dr. Stjepan Picek of COSIC, KU Leuven, Prof. Beng Jin Teoh of Yonsei University, and Dr. Sangjoon Park of ETRI. The technical program also included an industrial session and a special event about technology exchange.

The workshop had seven tracks, namely, Cryptography (sessions 1 and 2-A), Authentication and ICT Convergent Security (session 2-B), Network Security (sessions 3-A and 4), Threats Analysis (sessions 3-B and 4), and Network and Application Security (session 5). We would like to thank all authors who submitted papers. Each paper was reviewed by at least three reviewers. External reviewers as well as Program Committee members contributed to the reviewing process from their particular areas of expertise. The reviewing and active discussions were hosted by a Web-based system, EDAS. Through this system, we could check the degree of similarity between the submitted papers and previously published papers to prevent plagiarism and self-plagiarism. Following the strict reviewing processes, 31 outstanding papers from nine countries were accepted for publication in this proceedings volume.

Many people contributed to the success of WISA 2016. We would like to express our deepest appreciation to each of the WISA Organizing and Program Committee members as well as the paper contributors. Without their endless support and sincere dedication and professionalism, WISA 2016 would have been impossible.

August 2016

Dooho Choi
Sylvain Guilley

Organization

General Chair

Im-Yeong Lee Soonchunhyang University, Korea

Organizing Committee Chair

Ho-won Kim Pusan National University, Korea

Organizing Committee

ByungHoon Kang	KAIST, Korea
Ikkyun Kim	ETRI, Korea
Sangchoon Kim	Kangwon National University, Korea
Yongdae Kim	KAIST, Korea
Changhoon Lee	Seoul National University of Science and Technology, Korea
Heejo Lee	Korea University, Korea
Ok yeon Lee	Kookmin University, Korea
HyungGeun Oh	NSR, Korea
NamJe Park	Jeju National University, Korea
Young-Ho Park	Sejong Cyber University, Korea
Jung-Taek Seo	Soonchunhyang University, Korea
Kyung-Hoo Son	KISA, Korea
YooJae Won	Chungnam National University, Korea

Program Co-chairs

Dooho Choi ETRI, Korea
Sylvain Guilley Telecom ParisTech and Secure-IC, France

Program Committee

Man Ho Au	Hong Kong Polytechnic University, SAR China
Selcuk Baktir	Bahcesehir University, Turkey
Sang Kil Cha	KAIST, Korea
Young-Tae Cha	KISA, Korea
Yue Chen	Florida State University, USA
Seong-je Cho	Dankook University, Korea
Hyoung-Kee Choi	Sungkyunkwan University, Korea
Yoon-Ho Choi	Pusan National University, Korea
Viktor Fischer	Laboratoire Hubert Curien, France

VIII Organization

Dong-Guk Han	Kookmin University, Korea
Jinguang Han	Nanjing University of Finance and Economics, China
Swee-Huay Heng	Multimedia University Malaysia
Yong-Sung Jeon	ETRI, Korea
Seung-Hun Jin	ETRI, Korea
Yousung Kang	ETRI, Korea
Geon Woo Kim	ETRI, Korea
Huy Kang Kim	Korea University, Korea
Ikkyun Kim	ETRI, Korea
Jong Kim	POSTECH, Korea
Soohyung Kim	ETRI, Korea
Daesung Kwon	NSR, Korea
Junho Kwon	Pusan National University, Korea
Taekyoung Kwon	Yonsei University, Korea
Donggeon Lee	Attached Institute of ETRI, Korea
Jong-Hyouk Lee	Sangmyung University, Korea
Mun-Kyu Lee	Inha University, Korea
Sung-Jae Lee	KISA, Korea
Zhen Ling	Southeast University, Bangladesh
Zhe Liu	University of Waterloo, Canada
Kirill Morozov	Kyushu University, Japan
Jung-Chan Na	ETRI, Korea
Kihyo Nam	Umlogics Inc., Korea
Elizabeth O'Sullivan	Queen's University Belfast, UK
Raphael Phan	Multimedia University, Malaysia
Stjepan Picek	KU Leuven, Belgium
Junghwan Rhee	NEC Laboratories America, USA
Kouichi Sakurai	Kyushu University, Japan
Seungwon Shin	KAIST, Korea
Tsuyoshi Takagi	Kyushu University, Japan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Jongwon Yoon	Hanyang University Korea
Dae Hyun Yum	Myongji University, Korea
Cong Zheng	Palo Alto Networks, USA

Contents

Does Query Blocking Improve DNS Privacy? Quantifying Privacy Under Partial Blocking Deployment	1
<i>Aziz Mohaisen, Ah Reum Kang, and Kui Ren</i>	
Measuring and Analyzing Trends in Recent Distributed Denial of Service Attacks	15
<i>An Wang, Aziz Mohaisen, Wentao Chang, and Songqing Chen</i>	
SD-OVS: SYN Flooding Attack Defending Open vSwitch for SDN	29
<i>Xinyu Liu, Beumjin Cho, and Jong Kim</i>	
Slowloris DoS Countermeasure over WebSocket	42
<i>Jongseok Choi, Jong-gyu Park, Shinwook Heo, Namje Park, and Howon Kim</i>	
Detecting Encrypted Traffic: A Machine Learning Approach	54
<i>Seunghun Cha and Hyoungshick Kim</i>	
Features for Behavioral Anomaly Detection of Connectionless Network Buffer Overflow Attacks	66
<i>Ivan Homoliak, Ladislav Sulak, and Petr Hanacek</i>	
A Behavior-Based Online Engine for Detecting Distributed Cyber-Attacks	79
<i>Yaokai Feng, Yoshiaki Hori, and Kouichi Sakurai</i>	
Influence Evaluation of Centrality-Based Random Scanning Strategy on Early Worm Propagation Rate	90
<i>Su-kyung Kwon, Bongsoo Jang, Byoung-Dai Lee, Younghae Do, Hunki Baek, and Yoon-Ho Choi</i>	
Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities	102
<i>Jeong Yoon Yang, So Jeong Kim, and Il Seok Oh(Luke)</i>	
A Practical Analysis of TLS Vulnerabilities in Korea Web Environment	112
<i>Jongmin Jeong, Hyunsoo Kwon, Hyungjune Shin, and Junbeom Hur</i>	
Doppelganger in Bitcoin Mining Pools: An Analysis of the Duplication Share Attack	124
<i>Yujin Kwon, Dohyun Kim, Yunmok Son, Jaeyeong Choi, and Yongdae Kim</i>	

Detecting Impersonation Attack in WiFi Networks Using Deep Learning Approach	136
<i>Muhamad Erza Aminanto and Kwangjo Kim</i>	
Pay as You Want: Bypassing Charging System in Operational Cellular Networks	148
<i>Hyunwook Hong, Hongil Kim, Byeongdo Hong, Dongkwan Kim, Hyunwoo Choi, Eunkyu Lee, and Yongdae Kim</i>	
Towards Automated Exploit Generation for Embedded Systems	161
<i>Matthew Ruffell, Jin B. Hong, Hyoungshick Kim, and Dong Seong Kim</i>	
Empirical Analysis of SSL/TLS Weaknesses in Real Websites: Who Cares?	174
<i>Sanghak Oh, Eunsoo Kim, and Hyoungshick Kim</i>	
Development of Information Security Management Assessment Model for the Financial Sector	186
<i>Eun Oh, Tae-Sung Kim, and Tae-Hee Cho</i>	
A Practical Approach to Constructing Triple-Blind Review Process with Maximal Anonymity and Fairness	198
<i>Jisoo Jung, Joo-Im Kim, and Ji Won Yoon</i>	
GIS Vector Map Perceptual Encryption Scheme Using Geometric Objects	210
<i>P.N. Giao, Suk-Hwan Lee, Kwang-Seok Moon, and Ki-Ryong Kwon</i>	
Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18	221
<i>Md. Al-Amin Khandaker, Yasuyuki Nogami, Hwajeong Seo, and Sylvain Duquesne</i>	
LRCRYPT: Leakage-Resilient Cryptographic System (Design and Implementation)	233
<i>Xiaoqi Yu, Nairen Cao, Gongxian Zeng, Ruojing Zhang, and Siu-Ming Yiu</i>	
Revocable Group Signatures with Compact Revocation List Using Vector Commitments	245
<i>Shahidatul Sadiah and Toru Nakanishi</i>	
The Quantum-Safe Revolution	258
<i>Jean-Charles Faugère and Ludovic Perret</i>	
New Integral Characteristics of KASUMI Derived by Division Property	267
<i>Nobuyuki Sugio, Yasutaka Igarashi, Toshinobu Kaneko, and Kenichi Higuchi</i>	

On Pseudorandomness in Stateless Sources	280
<i>Maciej Skorski</i>	
Algebraic Degree Estimation for Integral Attack by Randomized Algorithm	292
<i>Haruhisa Kosuge and Hidema Tanaka</i>	
Applications of Soft Computing in Cryptology	305
<i>Stjepan Picek</i>	
Parallel Implementations of LEA, Revisited	318
<i>Hwajeong Seo, Taehwan Park, Shinwook Heo, Gyuwon Seo, Bongjin Bae, Zhi Hu, Lu Zhou, Yasuyuki Nogami, Youwen Zhu, and Howon Kim</i>	
Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors, a Step Forward	331
<i>Hwajeong Seo, Taehwan Park, Shinwook Heo, Gyuwon Seo, Bongjin Bae, Lu Zhou, and Howon Kim</i>	
A Secure and Privacy Preserving Iris Biometric Authentication Scheme with Matrix Transformation	341
<i>Abayomi Jegede, Nur Izura Udzir, Azizol Abdullah, and Ramlan Mahmod</i>	
Exploration of 3D Texture and Projection for New CAPTCHA Design	353
<i>Simon S. Woo, Jingul Kim, Duoduo Yu, and Beomjun Kim</i>	
A Study on Feature of Keystroke Dynamics for Improving Accuracy in Mobile Environment	366
<i>Sung-Hoon Lee, Jong-Hyuk Roh, Soohyung Kim, and Seung-Hun Jin</i>	
Geocasting-Based Almanac Synchronization Method for Secure Maritime Cloud	376
<i>Donghyeok Lee and Namje Park</i>	
The Vessel Trajectory Mechanism for Marine Accidents Analysis	388
<i>Seung-hee Oh, Byung-gil Lee, and Byungho Chung</i>	
Author Index	397