Lecture Notes in Computer Science 8267

For further volumes:
http://www.springer.com/series/7410

Yongdae Kim · Heejo Lee
Adrian Perrig (Eds.)

Information Security Applications

14th International Workshop, WISA 2013
Jeju Island, Korea, August 19–21, 2013
Revised Selected Papers

Springer

Editors
Yongdae Kim
KAIST
Daejeon
Republic of South Korea

Adrian Perrig
ETH
Zurich
Switzerland

Heejo Lee
Korea University
Seoul
Republic of South Korea

ISSN 0302-9743
ISSN 1611-3349 (electronic)
ISBN 978-3-319-05148-2
ISBN 978-3-319-05149-9 (eBook)
DOI 10.1007/978-3-319-05149-9
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014933576

LNCS Sublibrary: SL 4 – Security and Cryptology

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

WISA 2013, the 14th International Workshop on Information Security Applications, was held during August 19–21 in the Ocean Suites Jeju Hotel, Jeju Island, Republic of Korea. The conference 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 National Security Research Institute (NSRI), the Korea Internet Security Agency (KISA), and the Security Global Alliance (SGA).

We received 39 valid submissions from 16 countries, of which 15 were accepted for the full-paper track and two for the short abstract track. These proceedings contain the revised versions of the 15 full papers and two short papers. Every paper received at least three independent reviews. For the Best Paper Award, the Program Committee (PC) selected "Dynamic Surveillance: A Case Study with Enron Email Data Set" by Heesung Do, Byung Choi, and Heejo Lee. Moreover, "Bifocals: Analyzing WebView Vulnerabilities in Android Applications" by Erika Chin, and David Wagner received the Best White Hat Award. The Best SoK Paper Award was given to "SoK: Lessons Learned From SSL/TLS Attack" by Christopher Meyer, and Jorg Schwenk.

There were five invited talks, Kyoungsoo Park delivered "Building High-Performance Networked Security Systems on Low-Cost Commodity Hardware," and Wenyuan Xu spoke on "Tire Pressure Sensor vs. Utility Meters: From Good Intention to Vulnerabilities" on August 19. In addition, Seungwon Shin presented "Redesigning Network Security Applications with Software Defined Networking," and Jeonghyun Yi delivered "Deobfuscating Dexguard-Bytecode Obfuscator on Android" on August 20. Moreover, on August 21, Brent Kang spoke on "HW-Assisted Kernel Security Monitoring." We also had one keynote speech: Adrian Perrig delivered "Accountable Key Infrastructure (AKI): A Proposal for a Public-Key Validation Infrastructure." Excellent invited speeches along with a keynote speech as well as 17 regular and short paper presentations made a lof of participants stay until the last minute of the workshop. We thank all for their participation.

We would like to thank the authors of all submissions, regardless of whether their papers were accepted or not. Their work made this conference possible. We are extremely grateful to the PC members for their enormous investment of time and effort in the difficult and delicate process of review and selection. We would like to thank Jin Kwak, who was the organizing chair in charge of the local organization and finances. Special thanks go to Sungjae Hwang for providing and setting up the review software. We are most grateful to Donghoon Lee and Moti Yung, the WISA 2012 program chairs, for their timely information and replies to the host of questions we posed during the process.

August 2013

Yongdae Kim
Heejo Lee
Adrian Perrig

Organization

General Chair

Seokwoo Kim	Hansei University, Korea

Steering Committee

Bart Preneel	Katholieke University, Leuven, Belgium
Changseop Park	Dankook University, Korea
Daeho Kim	JoongBu University, Korea
Dongho Won	Sungkyunkwan University, Korea
Heungyoul Youm	Soonchunhyang University, Korea
Hideki Imai	Chuo University, Japan
Hongsub Lee	Konkuk University, Korea
Jooseok Song	Yonsei University, Korea
Kilhyun Nam	Korea National Defense University, Korea
Kwangjo Kim	KAIST, Korea
Minsub Rhee	Dankook University, Korea
Piljoong Lee	POSTECH, Korea
Sangjae Moon	Kyungpook National University, Korea
Sehun Kim	KAIST, Korea

Program Committee

Co-chairs

Yongdae Kim	KAIST, Korea
Heejo Lee	Korea University, Korea
Adrian Perrig	ETH, Switzerland

Committee Members

Bo-Yin Yang	Academia Sinica, Taiwan
Brent Kang	George Mason University, USA
Byung-Gon Chun	Microsoft Research, USA
Collin Mulliner	Northeastern University, USA
Eugene Vasserman	Kansas State University, USA

Guofei Gu	Texas A&M, USA
Haibo Chen	Shanghai Jiao Tong University, China
Hiroaki Kikuchi	Meiji University, Japan
Jong Kim	Postech, Korea
Jon Oberheide	Duo security, USA
Julianor Rizzo	Independent Researcher, Argentina
Jeonghyun Yi	Soongsil University, Korea
Jung-Chan Na	ETRI, Korea
Junghwan Rhee	NEC Lab, USA
Kazuhiro Minami	Institute of Statistical Mathematics, Japan
Kiwook Sohn	NSRI, Korea
Kyoungsoo Park	KAIST, Korea
Man Ho Au	University of Wollongong, Australia
Nicholas j. Hopper	University of Minnesota -Twin Cities, USA
Nico Golde	Technical University of Berlin, Germany
Ralf-Philipp Weinmann	University of Luxembourg, Germany
Sangjin Lee	Korea University, Korea
Sang Kil Cha	CMU, USA
Seungjin Lee	Grayhash Inc., Korea
Seungjoo Kim	Korea University, Korea
Srdjan Capkun	ETH, Switzerland
Stuart Schechter	MSR, USA
Syed Ali Khayam	NUST, Pakistan
Taekyoung Kwon	Yonsei University, Korea
Taesoo Kim	MIT, USA
Tarjei Mandt	Azimuth, Norway
Thorsten Holz	Ruhr-University Bochum, Germany
Tielei Wang	Georgia Tech, USA
Wenyuan Xu	University of South Carolina, USA
Xiaobo Chen	McAfee, USA
Xiaofeng Wang	Indiana University, USA
Xuhua Ding	SMU, Singapore
Yingjiu Li	SMU, Singapore
Yoojae Won	KISA, Korea
Yuji Ukai	Fourteenforty Research Institute, Japan
Zhenkai Liang	NUS, Singapore
Zhen Ling	Southeast University, China

Organization Committee

Chair

Jin Kwak	Soonchunhyang University, Korea

Committe Members

Changhoon Lee	Seoul National University of Science & Technology
Donghoon Lee	Korea University, Korea
Hyobeom Ahn	Kongju National University, Korea
Imyoung Lee	Soonchunhyang University, Korea
Jongsung Kim	Kookmin University, Korea
Jungtaek Seo	National Security Research Institute, Korea
Kijung Ahn	Jeju National University, Korea
Kungho Lee	Korea University, Korea
Kyungho Son	KISA, Korea
Namje Park	Jeju National University, Korea
Sangsoo Yeo	Mokwon University, Kore

Contents

Cryptography

LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors . . . 3
Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee

Some New Weaknesses in the RC4 Stream Cipher 28
Jing Lv, Bin Zhang, and Dongdai Lin

Improvements on Reductions among Different Variants of SVP and CVP . . . 39
Gengran Hu and Yanbin Pan

A General Method to Evaluate the Correlation of Randomness Tests 52
Limin Fan, Hua Chen, and Si Gao

Social Network Security

Improving Social Network-Based Sybil Defenses by Rewiring and Augmenting Social Graphs 65
Aziz Mohaisen and Scott Hollenbeck

Dynamic Surveillance: A Case Study with Enron Email Data Set. 81
Heesung Do, Peter Choi, and Heejo Lee

Mobile Security

Towards Elimination of Cross-Site Scripting on Mobile Versions of Web Applications 103
Ashar Javed and Jörg Schwenk

Punobot: Mobile Botnet Using Push Notification Service in Android 124
Hayoung Lee, Taeho Kang, Sangho Lee, Jong Kim, and Yoonho Kim

Bifocals: Analyzing WebView Vulnerabilities in Android Applications. 138
Erika Chin and David Wagner

Network Security

We Are Still Vulnerable to Clickjacking Attacks: About 99 % of Korean Websites Are Dangerous 163
Daehyun Kim and Hyoungshick Kim

Resistance Is Not Futile: Detecting DDoS Attacks without Packet Inspection . . . 174
Arjun P. Athreya, Xiao Wang, Yu Seung Kim, Yuan Tian, and Patrick Tague

SoK: Lessons Learned from SSL/TLS Attacks 189
Christopher Meyer and Jörg Schwenk

Looking Future

Foundational Security Principles for Medical Application Platforms 213
Eugene Y. Vasserman and John Hatcliff

Network Iron Curtain: Hide Enterprise Networks with OpenFlow. 218
YongJoo Song, Seungwon Shin, and Yongjin Choi

Towards a Methodical Evaluation of Antivirus Scans and Labels 231
Aziz Mohaisen, Omar Alrawi, Matt Larson, and Danny McPherson

Privacy

Assured Supraliminal Steganography in Computer Games 245
Anton Mosunov, Vineet Sinha, Heather Crawford, John Aycock,
Daniel Medeiros Nunes de Castro, and Rashmi Kumari

A Cloud and In-Memory Based Two-Tier Architecture
of a Database Protection System from Insider Attacks 260
Cheolmin Sky Moon, Sam Chung, and Barbara Endicott-Popovsky

Author Index 273