

# Contents

## Cryptography

LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors . . .	3
<i>Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee</i>	
Some New Weaknesses in the RC4 Stream Cipher . . . . .	28
<i>Jing Lv, Bin Zhang, and Dongdai Lin</i>	
Improvements on Reductions among Different Variants of SVP and CVP . . .	39
<i>Gengran Hu and Yanbin Pan</i>	
A General Method to Evaluate the Correlation of Randomness Tests . . . . .	52
<i>Limin Fan, Hua Chen, and Si Gao</i>	

## Social Network Security

Improving Social Network-Based Sybil Defenses by Rewiring and Augmenting Social Graphs . . . . .	65
<i>Aziz Mohaisen and Scott Hollenbeck</i>	
Dynamic Surveillance: A Case Study with Enron Email Data Set. . . . .	81
<i>Heesung Do, Peter Choi, and Heejo Lee</i>	

## Mobile Security

Towards Elimination of Cross-Site Scripting on Mobile Versions of Web Applications . . . . .	103
<i>Ashar Javed and Jörg Schwenk</i>	
Punobot: Mobile Botnet Using Push Notification Service in Android . . . . .	124
<i>Hayoung Lee, Taeho Kang, Sangho Lee, Jong Kim, and Yoonho Kim</i>	
Bifocals: Analyzing WebView Vulnerabilities in Android Applications. . . . .	138
<i>Erika Chin and David Wagner</i>	

## Network Security

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

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 Ayccock,  
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

Information Security Applications

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

Kim, Y.; Lee, H.; Perrig, A. (Eds.)

2014, XII, 273 p. 79 illus., Softcover

ISBN: 978-3-319-05148-2