

2018 IEEE Conference on Dependable and Secure Computing (DSC 2018)

**Kaohsiung, Taiwan
10 – 13 December 2018**



**IEEE Catalog Number: CFP18J65-POD
ISBN: 978-1-5386-5791-1**

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18J65-POD
ISBN (Print-On-Demand):	978-1-5386-5791-1
ISBN (Online):	978-1-5386-5790-4

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Table of Contents

Sponsors	03
Organization	04
Overview	08
Regular Track: Computer Systems, Networks and Software/Hardware	09
Experience and Practice	10
Manuscript Format	11
Tentative Conference Program	12
Keynote Talk #1	13
Keynote Talk #2	14
Full Program	
12/10 Mon IoT DSC#1 [top]	21
Session Chair : Prof. Morris Chang (University of South Florida)	
(34) An Over-the-Blockchain Firmware Update Framework for IoT Devices	22
Alexander Yohan and Nai-Wei Lo	
(42) A Lightweight Compound Defense Framework Against Injection Attacks in IIoT	30
Po-Wen Chi and Ming-Hung Wang	
(61) slimIoT: Scalable Lightweight Attestation Protocol For the Internet of Things	38
Mahmoud Ammar, Mahdi Washha, Gowri Sankar Ramachandran and Bruno Crispo	
(73) PAST: Protocol-Adaptable Security Tool for Heterogeneous IoT Ecosystems	46
Antonino Rullo, Elisa Bertino and Domenico Sacc`a	
12/10 Mon Data Security DSC #2 [top]	54
Session Chair : Prof. Hiroaki Kikuchi (Meiji University)	
(26) Secret Sharing Schemes Using Modulo-2 ^m Arithmetic Operations	55
Hidenori Kuwakado	
(36) A Bandwidth-Efficient Middleware for Encrypted Deduplication	62
Helei Cui, Cong Wang, Yu Hua, Yuefeng Du and Xingliang Yuan	
(37) Efficient Key-Aggregate Proxy Re-Encryption for Secure Data Sharing in Clouds	70
Wei-Hao Chen, Chun-I Fan and Yi-Fan Tseng	
(56) Efficient Key Agreement Protocol for Smart Sensors	74
Albert Guan and Chin-Laung Lei	



12/10 Mon Authentication and Privacy DSC #3 [top]	81
Session Chair : Prof. Nai-Wei Lo (National Taiwan University of Science and Technology)	
(23) PriBioAuth: Privacy-Preserving Biometric-Based Remote User Authentication	82
Yangguang Tian, Yingjiu Li, Ximeng Liu, Robert Huijie Deng and Binanda Sengupta	
(54) Impact Assessment of Password Reset PRMitM attack with Two-factor Authentication	90
Kota Sasa and Hiroaki Kikuchi	
(46) A Homomorphic LWE-Based Verifiable Electronic Voting System	98
Chen Wu, Shaohua Tang and Xingfu Yan	
(43) CORE: Cooperative Encryption with Its Applications to Controllable Security Services	106
Ruei-Hau Hsu, Jemin Lee, Tony Q.S. Quek and Chun-I Fan	
(20) Differentially Private Principal Component Analysis Over Horizontally Partitioned Data	114
Sen Wang and J. Morris Chang	
12/11 Tue Software Security DSC #4 [top]	122
Session Chair : Prof. Toshihiro Yamauchi (Okayama University)	
(12) Dynamic Path Pruning in Symbolic Execution	123
Ying-Shen Chen, Wei-Ning Chen, Che-Yu Wu, Hsu-Chun Hsiao and Shih-Kun Huang	
(15) Use-After-Free Mitigation via Protected Heap Allocation	131
Mingbo Zhang and Saman Zonouz	
(18) Finder: Automatic ICC Data Reconstruction for Long-Term Runtime Semantics	139
Chia-Wei Hsu, Sheng-Ru Wei and Shihpyng Shieh	
(24) Mitigating Over-Permissible Transfer for Control Flow Integrity	148
Chung-Kuan Chen, Shang-Kuei Chen and Shihpyng Shieh	
12/11 Tue EP (DSC #5) [top]	156
Session Chair : Prof. George Kesidis (Pennsylvania State University)	
(25) DeepMemIntrospect: Recognizing Data Structures in Memory with Neural Networks	157
Chung-Kuan Chen, E-Lin Ho and Shihpyng Shieh	
(32) Network Security for IOT using SDN: TImely DDoS Detection	159
Narmadha Sambandam, Mourad Hussein and Noor Siddiqi	
(75) Design and Implement Binary Fuzzing based on libFuzzer	161
Wei-Chieh Chao, Si-Chen Lin, Yi-Hsien Chen, Chin-Wei Tien and Chun-Ying Huang	



12/11 Tue Attack and Defenses DSC #6 [top]	163
Session Chair : Prof. Po-Wen Chi (National Taiwan Normal University)	
(11) Skipping Sleeps in Dynamic Analysis of Multithreaded Malware	164
Yoshihiro Oyama	
(35) Additional Kernel Observer to Prevent Privilege Escalation Attacks by Focusing on	172
System Call Privilege Changes	
Toshihiro Yamauchi, Yohei Akao, Ryota Yoshitani, Yuichi Nakamura and Masaki Hashimoto	
(38) Resilient and Scalable Cloned App Detection using Forced Execution and Compression	180
Trees	
Mohamed Elsabagh, Ryan Johnson and Angelos Stavrou	
(47) MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using	188
Speaker-to-Speaker Communication	
Mordechai Guri, Yosef Solewicz and Yuval Elovici	
(74) Moving-target Defense against Botnet Reconnaissance and an Adversarial Coupon-Collec	196
tion Model	
George Kesidis, Yuquan Shan, Neda Nasiriani, Takis Konstantopoulos, Daniel Fleck and Angelos Stavrou	
12/12 Wed Networking DSC #7 [top]	204
Session Chair : Dr. Koichiro Amemiya (Fujitsu Laboratories Ltd.)	
(29) Setting Malicious Flow Entries Against SDN Operations: Attacks and Countermeasures	205
Cheng-Hsu Lin, Chi-Yu Li and Kuochen Wang	
(33) Segment Routing Green Spine Switch Management Systems for Data Center Networks	213
Ose Osamudiamen and Chung-Horng Lung	
(21) Differentiating and Predicting Cyberattack Behaviors using LSTM	221
Ian Perry, Lutz Li, Christopher Sweet, Shao-Hsuan Su, Fu-Yuan Cheng, Shanchieh Jay Yang and Ahmet Okutan	
(81) Vague Set based FMEA Method for Risk Evaluation of Safety Related Systems	229
Kuo-Sui Lin and Chih-Chung Chiu	

12/12 Wed IoT Workshop #1 [top]	237
Session Chair : Prof. Chia-Mei Chen (National Sun Yat-sen University)	
(65) Enforcing Policy-Based Security Models for Embedded SoCs within the Internet of Things	238
Matthew Hagan, Fahad Manzoor Siddiqui, Sakir Sezer, Kieran McLaughlin and Boojoong Kang	
(87) Blockchain-based Authentication in IoT Networks	246
Chi Ho Lau, Alan K H Yeung and Fan Yan	
(90) AnchorCAN: Anchor-based Secure CAN Communications System	254
Hsiao-Ying Lin, Zhuo Wei, Yanjiang Yang, Yadong Wei, Kang Tang and Qingdi Sha	
(67) Stochastic Bitstream Processors on FPGAs to Compute Data From Sensors for Fault-Tolerant IoT	261
Rui Policarpo Duarte	
(59) The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual?	269
Tien-Ho Chang, Chia-Mei Chen, Gu-Hsin Lai and Jiunn-Wu Lin	
12/13 Thu Networking Workshop #2 [top]	273
Session Chair : Prof. Ruei-Hau Hsu (National Sun Yat-sen University)	
(13) OTMEN: Offloading Traffic Monitoring to Edge Nodes in Software-Defined Datacenter Networks	274
Amer Aljaedi, C. Edward Chow, Ehab Ashary and Francisco Torres-Reyes	
(16) ANN Mechanism for Network Traffic Anomaly Detection in the Concept Drifting Environment	282
Rua-Huan Tsaih, Shin-Ying Huang, Mao-Ci Lian and Yennun Huang	
(45) Closed-Loop DDoS Mitigation System in Software Defined Networks	288
Henan Kottayil Hyder and Chung-Horng Lung	
(64) Load Balancing using ECMP in Multi-Stage Clos Topology in a Datacenter	294
Harpreet Kaur Dhaliwal and Chung-Horng Lung	

12/13 Thu Cryptography and Applications Workshop #3 [top]	301
Session Chair : Dr. Arijit Karati (National Sun Yat-sen University)	
(76) An Identity-based Fair Contract Signing Protocol Constructed by the Confirmation Signature ..	302
Chih Hung Wang	
(84) Secure Hierarchical Bitcoin Wallet Scheme Against Privilege Escalation Attacks	308
Chun-I Fan, Yi-Fan Tseng, Hui-Po Su, Ruei-Hau Hsu and Hiroaki Kikuchi	
(9) Bipolar Dual-LFSR Reseeding for Low-Power Testing	316
Jen Cheng Ying, Wang Dauh Tseng and Wen Jiin Tsai	
(71) CC-Tracker: Interaction Profiling Bipartite Graph Mining for Malicious Network Activity	323
Detection	
Tzung-Han Jeng, Yi-Ming Chen, Chien-Chih Chen, Chuan-Chiang Huang and Kuo-Sen Chou	
(93) Empirical Analysis of Japanese Passwords	N/A
Nonoko Ai and Akira Kanaoka	
12/13 Thu Privacy Workshop #4 [top]	335
Session Chair : Prof. Jia-Ning Luo (Ming Chuan University)	
(27) Forged seal imprint identification based on regression analysis on imprint borders and	336
metrics comparisons	
Wei-Ho Chung, Mu-En Wu, Yeong-Luh Ueng and Yu-Hsuan Su	
(48) A Privacy-Preserving Metro Passenger Flow Acquisition and Query System based on	341
Crowd-Sensing	
Caiqin Nong, Shaohua Tang and Yuanyuan Zhang	
(53) Risk of Bitcoin Addresses to be Identified from Features of Output Addresses	349
Kodai Nagata, Hiroaki Kikuchi and Fan Chun-I	
(30) A Thin Client Model to Querying Encrypted Databases in Cloud	N/A
Brajendra Panda and Victor Fuentes Tello	
(63) Improving Tor Hidden Service Crawler Performance	362
Jonghyeon Park, Hyunsu Mun and Youngseok Lee	

Poster [top]	371
(41) Offline Transferable E-Cash mechanism	372
Jia-Ning Luo and Ming Hour Yang	
(44) Counterfeit Fingerprint Detection of Outbound HTTP Traffic with Graph Edit Distance	374
Chi-Kuan Chiu, Te-En Wei, Hsiao-Hsien Chang and Ching-Hao Mao	
(58) Detection of DNS Tunneling by Feature-free Mechanism	376
Chia-Min Lai, Bo-Ching Huang, Shin-Ying Huang, Ching-Hao Mao and Hahn-Ming Lee	
(60) On the Authentication of Certificateless RSA Public Key	378
Wu-Chuan Yang, Lien-Yuan Ting and Tzu-Chun Kuo	
(85) Low-Power Command Protection using SHA-CRC Inversion-based Scrambling Technique	380
for CAN-Integrated Automotive Controllers	
Daejin Park and Jihun Kim	
(86) OWASP Risk Analysis Driven Security Requirements Specification for Secure Android	382
Mobile Software Development	
Kai Qian, Reza Parizi and Dan Lo	
(88) Optimizing the Sequence of Vulnerability Scanning Injections	384
Koichi Funaya, Samir Bajaj, Kumar Sharad and Alok Srivastava	
(91) Proactive Approach to Secure Android Mobile Applications	N/A
Quyen Nguyen and Arun Sood	