ISC 2014

The 17th Information Security Conference

12-14 October 2014

CPD-3.28, 3/F, Central Podium Level
The Jockey Club Tower, Centennial Campus, HKU

DAY 1 12 October 2014, Sun

09:00 - 09:10 Opening Remark

09:10 - 10:50 Session 1: Web Security (Chair: Jakub Szefer)

09:10 - 09:40 Nick Nikiforakis (Stony Brook University), Marco Balduzzi (TrendMicro), Lieven Desmet, Frank Piessens, Wouter Joosen (iMinds-DistriNet)
- Soundsquatting: Uncovering the use of homophones in domain squatting

09:40 - 10:10 Martin Stopczynski, Michael Zugelder (Technische Universität Darmstadt)
- Reducing User Tracking through Automatic Web Site State Isolations

10:10 - 10:30 Ashar Javed (Horst Görtz Institute for IT-Security, Ruhr-University Bochum), Jens Riemer (TÜViT Informationstechnik GmbH), Joerg Schwenk (Horst Görtz Institute for IT-Security, Ruhr-University Bochum)
- SIACHEN: A Fine-grained Policy Language for the Mitigation of Cross-Site Scripting Attacks

10:30 - 10:50 Wanpeng Li, Chris Mitchell (Royal Holloway, University of London)
- Security Issues in OAuth 2.0 SSO Implementations

10:50 - 11:10 Tea Break

11:10 - 11:40 Session 2: Implementation (Chair: Lucas C.K. Hui)

Fangyu Zheng[1, 2, 3], Wuqiong Pan[1, 2], Jingqiang Lin[1, 2], Jiwu Jing[1, 2], Yuan Zhao[1, 2, 3] ([1]State Key Laboratory of Information Security, Institute of Information Engineering, [2]Data Assurance and Communication Security Research Center, [3]University of Chinese Academy of Sciences)
- Exploiting the Floating-Point Computing Power of GPUs for RSA

11:40 - 12:40 Session 3: Invited Talk (I) (Chair: Sherman S.M. Chow)

Ahmad-Reza Sadeghi (Technische Universität Darmstadt)
- Gone with the Gadgets: The Continuing Arms Race of Return-oriented Programming Attacks and Defenses

12:40 - 14:00 Lunch
Maxim's, 4/F, Chong Yuet Ming Amenities Centre, HKU

14:00 - 15:00 **Session 4: Public-Key Encryption I**
(Chair: Shoichi Hirose)

14:00 - 14:30 Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay
(Indian Institute of Technology Kharagpur)
- Fully Secure Self-Updatable Encryption in Prime Order Bilinear Groups

14:30 - 15:00 Xianhui Lu, Bao Li, Dingding Jia (State Key Laboratory of Information Security, Institute of Information Engineering; and Data Assurance and Communication Security Research Center, Chinese Academy of Sciences)
- Related-Key Security for Hybrid Encryption

15:00 - 15:30 **Session 5: Information Leakage**
(Chair: Shoichi Hirose)

Michele Boreale (Università di Firenze),
Michela Paolini (IMT Lucca Institute for Advanced Studies)
- On Formally Bounding Information Leakage by Statistical Estimation

15:30 - 15:50 **Tea Break**

15:50 - 17:20 **Session 6: Symmetric Key Cryptography**
(Chair: Shengli Liu)

15:50 – 16:20 Alex Biryukov, Dmitry Khovratovich (University of Luxembourg)
- PAEQ: Parallelizable Permutation-based Authenticated Encryption

16:20 - 16:50 Gaoli Wang (Donghua University, and State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences), Yanzhao Shen (Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, and School of Mathematics, Shandong University)
- (Pseudo-)Preimage Attacks on Step-Reduced HAS-160 and RIPEMD-160

16:50 - 17:20 Lin Jiao (TCA, Institute of Software, and Graduate University, Chinese Academy of Sciences), Bin Zhang (TCA, and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences), Mingsheng Wang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences)
- Revised Algorithms for Computing Algebraic Immunity against Algebraic and Fast Algebraic Attacks

DAY 2 13 October 2014, Mon

09:10 - 10:30 Session 7: Firewall and Forensics
(Chair: Lucas C.K. Hui)

09:10 - 09:40 Yingxin Cheng, Fu Xiao, Bin Luo, Rui Yang, Hao Ruan
(Software Institute, Nanjing University, China)
- Investigating the Hooking Behavior: A page-level memory monitoring method for Live Forensics

09:40 - 10:10 Sebastian Biedermann (Technische Universität Darmstadt),
Jakub Szefer (Yale University)
- SystemWall:
An Isolated Firewall using Hardware-based Memory Introspection

10:10 - 10:30 Yichen Wei, Fei Xu, Xiaojun Chen, Yiguo Pu, Jinqiao Shi, Sihan Qing
(Institute of Information Engineering, Chinese Academy of Sciences)
- Winnowing Double Structure for Wildcard Query in Payload Attribution

10:30 - 11:00 Tea Break

11:00 - 12:40 Session 8: Mobile Security
(Chair: Xiapu Luo)

11:00 - 11:30 Britton Wolfe (Indiana University - Purdue University Fort Wayne),
Karim Elish, Danfeng Yao (Virginia Tech)
- Comprehensive Behavior Profiling for Proactive Android Malware Detection

11:30 - 12:00 Daoyuan Wu, Rocky K-C Chang (The Hong Kong Polytechnic University)
- Analyzing Android Browser Apps for file:// Vulnerabilities

12:00 - 12:20 Javier Gonzalez[1], Michael Hölzl[2], Peter Riedl[2], Philippe Bonnet[1],
Rene Mayrhofer[2] ([1]IT University of Copenhagen, Denmark,
[2]University of Applied Sciences Upper Austria, Campus Hagenberg)
- A Practical Hardware-Assisted Approach to Customize Trusted Boot for Mobile Devices

12:20 - 12:40 Xingjie Yu[1, 2, 3], Bo Chen[4], Zhan Wang[1, 2], Bing Chang[1, 2, 3], WenTao Zhu[1, 2],
Jiwu Jing[1, 2] ([1]State Key Laboratory of Information Security, Institute of Information Engineering, [2]Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, [3]University of Chinese Academy of Sciences, [4]Stony Brook University)
- MobiHydra: Pragmatic and Multi-Level Plausibly Deniable Encryption Storage for Mobile Devices

12:40 - 14:00 Lunch
Senior Common Room, 14/F, KK Leung Building, HKU

14:00 - 15:00 **Session 9: Invited Talk (II)**
(Chair: Sherman S.M. Chow)

Shengli Liu (Shanghai Jiao Tong University)
Public-Key Encryption with Provable Security:
Challenges and Approaches

15:00 - 16:00 **Session 10: Zero-Knowledge Proofs and Arguments**
(Chair: Tanaka Keisuke)

15:00 - 15:30 Ning Ding (NTT Secure Platform Laboratories, Japan;
and Shanghai Jiao Tong University, China)
- Obfuscation-Based Non-Black-Box Extraction and Constant-Round Zero-Knowledge Arguments of Knowledge

15:30 - 16:00 Sven Laur (University of Tartu, Estonia), Bingsheng Zhang (National and Kapodestrian University of Athens, Greece)
- Lightweight Zero-Knowledge Proofs for Crypto-Computing Protocols

16:00 - 16:20 **Tea Break**

16:20 - 17: 40 **Session 11: Outsourcing and Multi-party Computations**
(Chair: Ahmad-Reza Sadeghi)

16:20 - 16: 50 Yihua Zhang, Marina Blanton (University of Notre Dame)
- Efficient Secure and Verifiable Outsourcing of Matrix Multiplications

16:50 - 17: 20 Toomas Krips (University of Tartu, and STACC, Estonia),
Jan Willemson (Cybernetica, and STACC, Estonia)
- Hybrid Model of Fixed and Floating Point Numbers in Secure Multiparty Computations

17:20 - 17: 40 Duane Wilson, Giuseppe Ateniese (Johns Hopkins University)
- "To Share or Not to Share" in Client-Side Encrypted Clouds

18:00 **Meeting up at Conference Venue for Reception Banquet**

Dragon King Restaurant (Chinese Cuisine)
12/F World Trade Centre, 280 Gloucester Road, Causeway Bay, Hong Kong
Tel: +852 2895 2288
http://www.dragonkinggroup.com/en/causewaybay.php

- Coach Pick-up 18:15 tentatively
Meeting point: Conference Venue at 18:00

- or, By yourself
Please arrive the restaurant at 19:30

DAY 3 14 October 2014, Tue

09:00 - 10:20 Session 12: Intrusion and Malware Detection
(Chair: Michele Boreale)

09:00 - 09:20 Weizhi Meng (City University of HongKong; Institute for Infocom Research, Singapore), Wenjuan Li, Lam For Kwok (City University of Hong Kong)
- An Evaluation of Single Character Frequency-Based Exclusive Signature Matching in Distinct IDS Environments

09:20 - 09:40 Sharath Hiremagalore, Daniel Barbara, Dan Fleck, Walter Powell, Angelos Stavrou (George Mason University)
- transAD: An Anomaly Detection Network Intrusion Sensor for the Web

09:40 - 10:00 Pinghai Yuan, Qingkai Zeng
(State Key Laboratory for Novel Software Technology, Nanjing University)
- Using Machine Language Model for Mimimorphic Malware Detection

10:00 - 10:20 Ryan Farley, Xinyuan Wang (George Mason University)
- CodeXt:
Automatic Extraction of Obfuscated Attack Code from Memory Dump

10:20 - 11:00 Session 13: Public-Key Encryption II
(Chair: Siu Ming Yiu)

10:20 - 10:40 Zhiquan Lv[1, 3], Cheng Hong[1], Min Zhang[1, 2], Dengguo Feng[1]
([1]Trusted Computing and Information Assurance Laboratory,
Institute of Software, Chinese Academy of Sciences,
[2]State Key Laboratory of Computer Science, Institute of Software,
Chinese Academy of Sciences
[3]University of Chinese Academy of Sciences)
- Expressive and Secure Searchable Encryption in the Public Key Setting

10:40 - 11:00 Murat Osmanoglu, Qiang Tang, Aggelos Kiayias
(University of Connecticut; and National and Kapodistrian U. of Athens)
- Graded Encryption, or how to play "Who wants to be a millionaire?" distributively

11:00 - 11:20 Tea Break

11:20 - 12:40 Session 14: Authentication (Chair: Masahiro Mambo)

11:20 - 11:50 Li Xi, Jianxiong Shao, Dengguo Feng
(Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences)
- ARBRA:
Anonymous Reputation-Based Revocation with Efficient Authentication

11:50 - 12:20 Fei Tang[1, 2, 3], Hongda Li[1, 2], Bei Liang[1, 2, 3] ([1]SKLOIS, Institute of Information Engineering Chinese Academy of Sciences, [2]Data Assurance and Communication Security Research Center Chinese Academy of Sciences, [3]University of Chinese Academy Science)
- Attribute-Based Signatures for Circuits from Multilinear Maps

12:20 - 12:40 Daniel Slamanig, Raphael Spreitzer, Thomas Unterluggauer
(Graz University of Technology, IAIK)
- Adding Controllable Linkability to Pairing-Based Group Signatures For Free

12:40 - 14:00 Lunch
Senior Common Room, 14/F, KK Leung Building, HKU

14:00 - 15:30 Session 15: Attacks (Chair: Kehuan Zhang)

14:00 - 14:30 Shouling Ji, Weiqing Li (Georgia Institute of Technology),
Mudhakar Srivatsa (IBM T. J. Watson Research Center),
Jing Selena He (KSU), Raheem Beyah (Georgia Institute of Technology)
- Structure based Data De-anonymization of Social Networks and Mobility Traces

14:30 - 14:50 Christopher Jämthagen, Linus Karlsson, Paul Stankovski, Martin Hell
(Lund University)
- eavesROP: Listening for ROP payloads in data streams

14:50 - 15:10 Donald Ray, Jay Ligatti (University of South Florida)
- Defining Injection Attacks

15:10 - 15:30 Martin Salfer, Hendrik Schweppe (BMW Forschung und Technik GmbH),
Claudia Eckert (Technische Universität München)
- Efficient Attack Forest Construction for Automotive On-board Networks

15:30 - 15:40 Closing Remarks

16:00 Meeting up at Conference Venue for Reception Gathering

Mijas Spanish Restaurant-Stanley
1 Shop 102, Murray House, Stanley Plaza, Stanley, Hong Kong
Tel: +852 2899 0858
http://www.kingparrot.com/restaurants.php?id=18

- Coach Pick-up 16:15 tentatively
Meeting point: Conference Venue at 16:00

- or, By yourself
Please arrive the restaurant at 18:00 pm