ISC 2013

The 16th Information Security Conference

Dallas, Texas, USA, November 13-15, 2013

Wednesday November 13, 2013

8:45am Opening remarks

Security of Operating Systems 9:00am – 10:00am

9:00am Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection
Irfan Ahmed, Golden G. Richard Iii, Aleksandar Zoranic and Vassil Roussev (**Best Paper Award**)

9:30am Lightweight Attestation and Secure Code Update for Multiple Separated Microkernel Tasks
Steffen Wagner, Christoph Krauß and Claudia Eckert

10:00am Coffee break

Invited Speaker 10:30am – 11:30am

How to Misuse, Use, and Mitigate Side Channels in Virtualized Environments
Michael Reiter (University of North Carolina at Chapel Hill)

Formal Methods

11:30am Formal analysis of ECC-based Direct Anonymous Attestation schemes in Applied Pi Calculus
Li Xi, Yu Qin and Dengguo Feng

12:00pm Lunch

Secret Sharing 1:40pm – 2:40pm

1:40pm The Security Defect of a Multi-pixel Encoding Method
Teng Guo, Feng Liu, Chuankun Wu, Young-Chang Hou, Yawei Ren and Weng Wang

2:10pm Encrypted Secret Sharing and Analysis by Plaintext Randomization
Stephen Tate, Roopa Vishwanathan and Scott Weeks

Wednesday November 13, 2013

Encryption 2:40pm – 3:50pm

2:40pm Round-Efficient Private Stable Matching from Additive Homomorphic Encryption
Tadanori Teruya and Jun Sakuma

3:10pm Efficient and Fully Secure Forward Secure Ciphertext-Policy Attribute-Based Encryption
Takashi Kitagawa, Hiroki Kojima, Nuttapong Attrapadung and Hideki Imai

3:30pm Reducing Public Key Sizes in Bounded CCA-Secure KEMs with Optimal Ciphertext Length
Takashi Yamakawa, Shota Yamada, Takahiro Matsuda, Goichiro Hanaoka and Noboru Kunihiro

3:50pm Coffee break

Malware & Critical Infrastructures 4:20pm – 5:30pm

4:20pm 4GMOP: Mopping the Malware Initiated Traffic in Mobile Networks
Marian Kühnel and Ulrike Meyer

4:50pm Design and Analysis of a Sophisticated Malware Attack against Smart Grid
Byungho Min and Vijay Varadharajan

5:10pm Multi-Round Attacks on Structural Controllability Properties for Non-Complete Random Graphs
Cristina Alcaraz, Estefania Etchevés Miciolino and Stephen Wolthusen

Thursday November 14, 2013

Cryptanalysis 8:45am – 10:05am

8:45am Improved Meet-in-the-Middle Attacks on Round-Reduced ARIA
Dongxia Bai and Hongbo Yu

9:15am Establishing Equations: the Complexity of Algebraic and Fast Algebraic Attacks Revisited
Lin Jiao, Bin Zhang and Mingsheng Wang

9:45am Factoring a multi-prime modulus N with random bits
Routo Terada and Reynaldo C. Villena

10:05am Coffee break

Invited Speaker 10:35am – 11:35am

How to Draw Graphs: Seeing and Redrafting Large Networks in Security and Biology
G. R. Blakley, IACR Fellow
(Joint work with Bob Blakley and Sean Blakley)

Block Ciphers & Stream Ciphers 11:35am – 12:15pm

11:35am Faster 128-EEA3 and 128-EIA3 Software
Billy Brumley and Roberto Avanzi

11:55am Merging the Camellia, SMS4 and AES S-boxes in a single S-box with composite bases
Alberto Martínez-Herrera, Carlos Mex-Perera and Juan Nolazco-Flores

12:15pm Lunch

Entity Authentication 2:00pm – 3:10pm

2:00pm Offline Dictionary Attack on Two Password Authentication Schemes using Smart Cards
Ding Wang and Ping Wang

2:30pm Self-blindable Credential: Towards Anonymous Entity Authentication Upon Resource-constrained Devices
Yanjiang Yang, Xuhua Ding, Haibing Lu, Jian Weng and Jianying Zhou

2:50pm Practical & Provably Secure Distance-Bounding
Ioana Boureanu, Aikaterini Mitrokotsa and Serge Vaudenay

Usability & Risk Perception 3:10pm – 4:00pm

3:10pm On the Viability of CAPTCHAs for Use in Telephony Systems: A Usability Field Study
Niharika Sachdeva, Nitesh Saxena and Ponnurangam Kumaraguru

3:40pm Cars, Condoms, and Facebook
Vaibhav Garg and Jean Camp

4:00pm Coffee break

Access Control 4:30pm – 5:20pm

4:30am Achieving Revocable Fine-Grained Cryptographic Access Control over Cloud Data
Yanjiang Yang, Xuhua Ding, Haibing Lu, Zhiguo Wan and Jianying Zhou

5:00pm Fine-Grained Access Control for HTML5-Based Mobile Applications in Android
Lusha Wang, Xing Jin, Tongbo Luo and Wenliang Du

7:00pm Gala Dinner

Friday November 15, 2013

Computer Security 9:00am – 9:30am

9:00am CrowdFlow: Efficient Information Flow Security
Christoph Kerschbaumer, Eric Hennigan, Stefan Brunthaler, Per Larsen and Michael Franz

Privacy Attacks 9:30am – 10:20am

9:30am DroidTest: Testing Android Applications for Leakage of Private Information
Sarker Tanveer Ahmed Rumee and Donggang Liu

10:00am A Dangerous Mix: Large-scale analysis of mixed-content websites
Ping Chen, Nick Nikiforakis, Lieven Desmet and Christophe Huygens

10:20am Coffee break

Cryptography 10:50am – 12:30pm

10:50am Ordered Multisignature Schemes under the CDH Assumption without Random Oracles
Naoto Yanai, Masahiro Mambo and Eiji Okamoto

11:10am Human Assisted Randomness Generation Using Computer Games
Mohsen Alimomeni and Reihaneh Safavi-Naini

11:40am Security ranking among assumptions within the Uber assumption framework
Antoine Rojat and Antoine Joux

12:10pm A Secure and Efficient Method for Scalar Multiplication on Supersingular Elliptic Curve over Binary Fields
Matheus Fernandes de Oliveira and Marco Aurélio Amaral Henriques

12:30pm End of the scientific program.

3:00pm-5:30pm Optional Walking Tour to the JFK Memorial, including the The Sixth Floor Museum