3rd International Conference on Research in Security Standardisation

December 5-6, 2016

National Institute of Standards and Technology

Gaithersburg, Maryland

Administration Building/Green Auditorium

December 5, 2016 (Monday)

8:30 Badge Pick Up & Continental Breakfast

(if you registered "without catering" please purchase refreshments from the cafeteria)

9:30 – 9:40 Welcome and Opening Remarks – Lily Chen

9:40 – 11:10 Secure protocol standards *(Session Chair: David McGrew)*

1. **Analyzing and Fixing the QACCE security of QUIC**
   Hideki Sakurada, Kazuki Yoneyama, Yoshikazu Hanatani and Maki Yoshida
2. **Cross-Tool Semantics for Protocol Security Goals**
   Joshua Guttman, John Ramsdell and Paul Rowe
3. **Cryptanalysis of GlobalPlatform Secure Channel Protocols**
   Mohamed Sabt and Jacques Traore

11:10 – 11:40 Coffee Break

(if you registered "without catering" please purchase refreshments from the cafeteria)

11:40 – 12:40 Invited talk (I) *(Session Chair: Lily Chen)*

The Future of Security Standards

John Kelsey

12:40 – 2:10 Lunch *(NIST Cafeteria)*

If you registered "with catering", your lunch ticket is included in your badge holder.

2:10 – 3:10 Application Standards *(Session Chair: Debby Wallner)*

1. **NFC Payment Spy: A Privacy Attack on Contactless Payments**
   Maryam Mehrnezhad, Mohammed Aamir Ali, Feng Hao and Aad van Moorsel
2. **Security Analysis of the W3C Web Cryptography API**
   Kelsey Cairns, Harry Halpin and Graham Steel

3:10 -3:40 Coffee Break

(if you registered "without catering" please purchase refreshments from the cafeteria)

3:40 – 4:40 Strategies, Tradeoffs, and Decisions in Standardization (Session Chair: William Whyte)

1. **Algorithm Agility - Discussion on TPM 2.0 ECC Functionalities**
   Liqun Chen and Rainer Urian
2. **Reactive and Proactive Standardisation of TLS**
   Kenneth Paterson and Thyla van der Merwe

4:40 End of the first day of SSR

6:00 Conference Dinner (Copper Canyon Grill - adjacent to Courtyard Hotel)

Dinner is available to attendees that selected to register and pay with catering services.

Your ticket is included in your badge holder.

December 6, 2016 (Tuesday)

8:30 Badge Pick Up & Continental Breakfast

(if you registered "without catering" please purchase refreshments from the cafeteria)

9:30 – 11:00 Access Control and Group Key Management (Session Chair: Takeshi Chikazawa)

1. **Extending the UML Standards to Model Tree-Structured Data and their Access Control Requirements**
   Alberto De La Rosa Algarin and Steven Demurjian
2. **Attribute-based Access Control Architectures with the eIDAS Protocols**
   Frank Morgner, Paul Bastian and Marc Fischlin
3. **A Secure Multicast Group Management and Key Distribution in IEEE 802.21**
   Yoshikazu Hanatani, Naoki Ogura, Yoshihiro Ohba, Lily Chen and Subir Das

11:00 - 11:30 Coffee break

(if you registered "without catering" please purchase refreshments from the cafeteria)

11:30 – 12:30 Invited talk (II) ***(Session Chair: David McGrew)***

IEEE 1609.2 and Connected Vehicle Security: Standards Making in a Pocket Universe

William Whyte

12:30 – 2:00 Lunch *(NIST Cafeteria)*

If you registered "with catering", your lunch ticket is included in your badge holder.

2:00-3:00 Panel: Can security standards be ahead of the game?

Moderator: Salvatore Francomacaro, NIST

Panelists *Russ Housley*
David McGrew
Liqun Chen
Eric Hibbard

3:00 – 4:00 Hash-based Signature (Session Chair: Liqun Chen)

1. **State Management for Hash-Based Signatures**
   David McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin and Johannes Buchmann
2. **Analysis of a Proposed Hash-Based Signature Standard**
   Jonathan Katz

4:00 End of SSR 2016