Program

Monday 10/25/2010 Registration and Reception

Registration 3:00-7:00 PM

Steering Committee Meeting
Board suite Room 5:00-6:00 PM

Reception 7:30-9:30 PM
Poolside & Hillsboro Room

Program

Tuesday 10/26/2010

8:00 - 8:30 AM Coffee, danish etc

8:30 - 8:50 AM Conference opening - Welcoming comments by Assoc. Dean for Research Dr. Ram Narayanan

Session 1, 9:00-11:00 AM* *Attacks and analysis*

1. (41) Kota Ideguchi, Elmar Tischhauser and Bart Preneel. Improved Collision Attacks on the Reduced-Round Groestl Hash Function
2. (9) Yi Lu and Yvo Desmedt. Improved Distinguishing Attack on Rabbit
3. (45) Hassan Jameel Asghar, Shujun Li, Josef Pieprzyk and Huaxiong Wang. Cryptanalysis of the Convex Hull Click Human Identification Protocol
4. (5) Nadhem AlFardan and Kenny Paterson. An analysis of DepenDNS

Coffee etc

Session 2, 11:30 - 1:00 PM *Analysis*

1. (124) Elena Andreeva, Bart Mennink and Bart Preneel. Security Reductions of the Second Round SHA-3 Candidates
2. (59) Özgür Dagdelen and Marc Fischlin. Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents
3. (1) Marcos Simplicio, Paulo Barreto and Tereza Carvalho. Revisiting the Security of the Alred Design

Lunch

Session 3, 2:00-4:00 PM *Authentication, PIR and Content Identification*

1. (127) Christian Wachsmann, Ahmad-Reza Sadeghi, Liqun Chen, Kurt Dietrich, Hans Löhr and Johannes Winter. Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices
2. (63) Elaine Shi, Yuan Niu, Markus Jakobsson and Richard Chow. Implicit Authentication through Learning User Behavior
3. (130) Jonathan Trostle and Andy Parrish. Efficient Computationally Private Information Retrieval from Anonimity or Trapdoor Groups
4. (104) Yali Liu, Dipak Ghosal, Biswanath Mukherjee and Ahmad-Reza Sadeghi. Video Streaming Forensic - Content Identification with Traffic Snooping

Coffee etc

Session 4, 4:30-6:00 PM *Privacy*

1. (80) Georg Neugebauer, Ulrike Meyer and Susanne Wetzel. Fair and Privacy-Preserving Multi-Party Protocols for Reconciling Ordered Input Sets
2. (58) Arne Tauber and Thomas Rössler. Enhancing Security and Privacy in Certified Mail Systems using Trust Domain Separation
3. (100) Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelee and Ingrid Verbauwhede. Privacy-preserving ECC-based grouping proofs for RFID.

NB. *Presentations are for 25 minutes at most, with an additional 5 minutes for questions

Wednesday 10/27/2010

8:00 - 8:30 AM Coffee, danish etc

Session 5, 8:30-10:30 AM *Malware, Crimeware and Code Injection*

1. (101) Xinyuan Wang and Xuxian Jiang. Artificial Malware Immunization based on Dynamically Assigned Sense of Self
2. (96) Zhi Xin, Huiyu Chen, Hao Han, Bing Mao and Li Xie. Misleading Malware Similarities Analysis by Automatic Data Structure Obfuscation
3. (113) Vasilis Pappas, Brian Bowen and Angelos Keromytis. Architectures for Scalable Crimeware Swindling
4. (93) Elias Athanasopoulos. RaJa: Cross-Site Scripting Detection and Prevention using JavaScript Randomization

Coffee etc

Session 6, 11:00-12:30 PM *Intrusion Detection*

1. (67) Lei Wei, Michael Reiter and Katen Mayer-Patel. Summary-Invisible Networking: Techniques and Defenses
2. (99) Natalia Stakhanova, Hanli Ren and Ali Ghorbani. Selective Regular Expression Matching
3. (102) Davidson Boccardo, Tiago Nascimento, Raphael Machado, Charles Prado and Luiz Carmo. Traceability of Excutable Codes using Neural Networks

Lunch

Session 7, 2:00-3:30 PM *Side Channels*

1. (120) Jorge Guajardo and Bart Mennink. On Side-Channel Resistant Block Cipher Usage
2. (103) Geir Olav Dyrkolbotn, Knut Wold and Einar Snekkenes. Security Implications of Crosstalk in Switching CMOS Gates
3. (118) Ye Zhu. On Privacy Leakage through Silence Suppression

7:30 – 10:00 PM Gala Dinner

Thursday 10/28/2010

8:00 - 8:30 AM Coffee, danish etc

Session 8, 8:30-10:30 AM *Cryptography*

1. (13) Julien Cathalo and Christophe Petit. One-Time Trapdoor One-Way Functions
2. (106) Anderson Nascimento, Mayana Pereira, Raphael Dowsley and Goichiro Hanaoka. Public Key Encryption Schemes with Bounded CCA Security and Optimal Ciphertext Length based on the CDH and HDH Assumptions
3. (76) Ping Yu and Rui Xue. A Short Signature Scheme from the RSA Family
4. (75) Masayuki Abe, Kristiyan Haralambiev and Miyako Ohkubo. Efficient Message Space Extension for Automorphic Signatures

Coffee etc

Session 9, 11:00-12:00 PM *Smartphones*

1. (64) Mauro Conti, Vu Thien Nga Nguyen and Bruno Crispo. CRePe: Context-Related Policy Enforcement for Android
2. (129) Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi and Marcel Winandy. Privilege Escalation Attacks on Android

Session 10, 12:00-12:30 PM *Biometrics*

1. (57) Bendik Mjaaland, Patrik Bours and Danilo Gligoroski. Walk the Walk: Attacking Gait Biometrics by Imitation

Lunch

Session 11, 2:00-3:00 PM *Cryptography, Application*

1. (6) Kun Peng and Feng Bao. Efficient Multiplicative Homomorphic E-Voting
2. (15) Patricia Everaere, Isabelle Simplot-Ryl and Issa Traoré. Double Spending Protection for E-Cash based on Risk Management

Session 12, 3:00-3:30 PM *Buffer Overflow*

1. (117) Donghai Tian, Xi Xiong, Changzhen Hu and Peng Liu. Integrating Offline Analysis and Online Protection to Defeat Buffer Overflow Attacks

Coffee etc

Session 13, 4:00-5:00 PM *Cryptography, Theory*

1. (121) Zhiwei Li and Weichao Wang. Deciding Recognizability under Dolev-Yao Intruder Model
2. (36) Kazuki Yoneyama. Indifferentiable Security Reconsidered: Role of Scheduling

End of Conference