

Embedded Systems and Communications Security (ESCS) 2009 Advance Program

(In conjunction with IEEE SRDS 2009, Niagara Falls, NY, USA)

Sunday September 27, 2009

8:00 am - 9:00 am Breakfast/Registration

9:00 am - 9:05 am Opening Remarks - Vinodh Gopal, Intel Corporation

9:05 am -10:25 am Session 1 – Chair: Miroslav Velez, Aries Design Automation
Hardware Mechanism and Performance Evaluation of Hierarchical Page-Based Memory Bus Protection

Lifeng Su (STMicroelectronics), Albert Martinez (STMicroelectronics), Pierre Guillemi (STMicroelectronics), Sébastien Cerdany (Télécom ParisTech), Renaud Pacalety (Télécom ParisTech)

On the Complexity of Probabilistic Key Pre-distribution Schemes

Mahalingam Ramkumar (Mississippi State University)

Hierarchical Concealed Data Aggregation for Wireless Sensor Networks

Suat Ozdemir (Gazi University, Turkey), Yang Xiao (The University of Alabama Tuscaloosa)

Highly-Resilient Services for Critical Infrastructures

Giuliana Santos Veronese (Universidade de Lisboa, Portugal), Miguel Correia (Universidade de Lisboa, Portugal), Alysson Neves Bessani (Universidade de Lisboa, Portugal), Lau Cheuk Lung (Universidade Federal de Santa Catarina – Brazil)

10:25 am -10:45 am Coffee Break

10:45 am -11:45 am Keynote Address - “Message Digests for the Twenty-First Century: An Overview of the NIST SHA-3 Cryptographic Hash Algorithm Competition”, Alan Kaminsky (Rochester Institute of Technology)

11:45 am -1:00 pm Lunch

1:00 pm - 2:00 pm Session 2 – Chair: Berk Sunar (Worcester Polytechnic Institute)
Fast and Constant-Time Implementation of Modular Exponentiation

Vinodh Gopal, James Guilford, Erdinc Ozturk, Wajdi Feghali, Gil Wolrich, Martin Dixon (Intel Corporation)

SensorEar: A Sensor Network Based Eavesdropping System

Ge Ruan, Soumya Jain and Sencun Zhu (The Pennsylvania State University)

Accelerating Techniques for Rapid Mitigation of Phishing and Spam Emails
Pranil Gupta, Ajay Nagrale and Shambhu Upadhyaya (University at Buffalo)

2:00 pm - 2:45 pm **Invited Talk - “Embedded Security and Survivability”, Phil Koopman, Carnegie Mellon University**

2:45 pm – 3:15 pm **Coffee Break**

3:15 pm - 4:00 pm **Invited Talk - “Challenges and Opportunities in Embedded System Security: A View from the Trenches” Nachiketh Potlapally, Intel Corporation**

4:00 pm - 4:45 pm **Panel Discussion**
Panelists: Mike Kurdziel, Harris Corporation, Berk Sunar, Worcester Polytechnic Institute and Miroslav Velez, Aries Design Automation

4:45 pm **Wrap-Up and Closing Remarks**