ICICS 2008 :: Programme

Information on the **pre-conference social event** and the **conference banquet** is available at the end of this document.

A PDF version of the conference programme is available for download.

Programme

20 October, 2008 (Monday)	21 October, 2008 (Tuesday)	22 October, 2008 (Wednesday)
09:00-09:20: Coffee break 09:20-09:30: Opening remarks (Mark Ryan) 09:30-10:30: Invited talk I (Chair: Liqun Chen) 10:30-11:00: Coffee break 11:00-13:00: Paper session I :: Authentication (Chair: Peng Ning)	09:00-09:30: Coffee break 09:30-10:30: Invited talk II (Chair: Guilin Wang) 10:30-11:00: Coffee break 11:00-13:00: Paper session IV :: Access control (Chair: Joshua Guttman)	09:00-09:30: Coffee break 09:30-10:30: Invited talk III (Chair: Mark Ryan) 10:30-11:00: Coffee break 11:00-13:00: Paper session VII :: Applied cryptography (Chair: Khoongming Khoo)
13:00-14:30: Lunch served in Bar Pravda, Hyatt Hotel	13:00-14:30: Lunch served in Bar Pravda, Hyatt Hotel	13:00-14:30: Lunch served in Bar Pravda, Hyatt Hotel
14:30-16:00: Paper session II :: Side-channel analysis (Chair: Nicolas Courtois) 16:00-16:30: Coffee break 16:30-18:00: Paper session III :: Cryptanalysis (Chair: Raphael C.-W. Phan)	14:30-16:00: Paper session V :: Software security (Chair: Peter Ryan) 16:00-16:30: Coffee break 16:30-18:00: Paper session VI :: System security (Chair: John Clarke)	14:30-16:00: Paper session VIII :: Security protocols (Chair: Liqun Chen) 16:00-16:10: Farewell (Mark Ryan) 16:10-16:40: Coffee break
19:30-22:00: Conference banquet at La Bastille (Enquiries: Andy Brown)	Delegates to make own dinner arrangements	END

All conference talks take place in the **Sonata Room**, located on the ground floor of the Hyatt hotel. The ICICS registration desk is situated just inside this room and is open from 08:30 to 12:00 on Monday 20th October and Tuesday 21st October.

All delegates are provided with an Internet access card, which entitles them to 24 hours of wireless Internet access within the conference venue. Further access cards can be purchased from the Hyatt hotel's reception desk.

The ICICS Organising Committee would like to wish all delegates a productive and cheerful time at our conference. If you have any enquiries, we have a sticker on our badge which you can use to identify us.

Invited talks

Beyond the 80-bit Barrier *Invited talk I*
Nigel Smart

Abstract: I will discuss the issue raised by moving cryptographic systems from the 80-bit security level to the 128-bit security level and beyond. Despite AES being around for around eight years the asymmetric algorithm key sizes have not yet caught up. I will explain why RSA is no longer viable at these security levels, and will explain some recent deployments of elliptic curve cryptography.

DoS-Resistant Broadcast Authentication in Wireless Sensor Networks *Invited talk II*
Peng Ning

Abstract: Recent technological advances have made it possible to develop distributed sensor networks consisting of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate in short distances through wireless links. Such sensor networks are ideal candidates for a wide range of applications such as monitoring of critical infrastructures and military operations. In hostile environments, the security and resiliency of such sensor networks becomes a critical issue. However, it is very challenging to build secure and resilient sensor networks due to several unique features of sensor networks, such as the resource constraints on sensor nodes and exposure to node captures and physical attacks. In this talk, I will present some recent results on mitigating Denial of Service (DoS) attacks against broadcast authentication in wireless sensor networks, as well as secure and DoS-resistant code dissemination, an application that requires broadcast authentication.

Attestation: Evidence and Trust *Invited talk III*
Joshua D. Guttman

Abstract: Attestation is the activity of making a claim about properties of a target by supplying evidence to an appraiser. An open-ended framework for attestation is desirable for safe support to sensitive or high-value activities on heterogeneous networks. We identify five central principles to guide development of attestation systems. We argue that (i) attestation must be able to deliver temporally fresh evidence; (ii) comprehensive information about the target should be accessible; (iii) the target, or its owner, should be able to constrain disclosure of in- formation about the target; (iv) attestation claims should have explicit semantics to allow decisions to depend on several claims; and (v) the underlying attestation mechanism must be trustworthy. We propose an architecture for attestation that is guided by these principles, as well as an implementation that adheres to this architecture. Virtualized platforms, which are increasingly well supported on stock hardware, provide a natural basis for our attestation architecture.

Paper session I :: Authentication

- *A novel solution for end-to-end integrity protection in signed PGP mail*
  Lijun Liao and Joerg Schwenk
  Ruhr-University Bochum, Germany
  Abstract [+/-]
- *Unclonable Lightweight Authentication Scheme*

Ghaith Hammouri, Erdinc Ozturk, Berk Birand and Berk Sunar
WPI, USA
Abstract [+/-]

- *Threat Modelling in User Performed Authentication*
  Xun Dong, John Clark and Jeremy Jacob
  University of York, UK
  Abstract [+/-]
- *Access with Fast Batch Verifiable Anonymous Credentials*
  Ke Zeng
  NEC Labs, China
  Abstract [+/-]

Paper session II :: Side-channel analysis

- *Quantifying Timing Leaks and Cost Optimisation*
  Alessandra Di Pierro (a), Chris Hankin (b) and Herbert Wiklicky (b)
  a) University of Verona, Italy
  b) Imperial College London, UK
  Abstract [+/-]
- *Method for Detecting Vulnerability to Doubling Attacks*
  Chong Hee Kim and Jean-Jacques Quisquater
  UCL, Belgium
  Abstract [+/-]
- *Side channel analysis of some hash based MACs: A response to SHA-3 requirements*
  Praveen Gauravaram and Katsuyuki Okeya
  a) Technical University of Denmark, Denmark
  b) Hitachi, Japan
  Abstract [+/-]

Paper session III :: Cryptanalysis

- *Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0*
  Nicolas Courtois and Blandine Debraize
  University College London, UK
  Abstract [+/-]
- *Analysis of the Attacking Reduced-Round Versions of the SMS4*
  Deniz Toz and Orr Dunkelman
  Middle East Technical University, Turkey
  Katholieke Universiteit Leuven, Belgium
  Abstract [+/-]
- *Applying Time-Memory-Data Trade-Off to Meet-in-the-Middle Attack*
  Choy Valerie, Khoong Ming Khoo and Chuan Wen Loe
  DSO National Laboratories, Singapore
  Abstract [+/-]

Paper session IV :: Access control

- *Beyond User-to-User Access Control for Online Social Networks*
  Mohamed Shehab (a), Anna Squicciarini (b) and Gail-Joon Ahn (a)
  University of North Carolina at Charlotte, USA
  Penn State University, USA

Abstract [+/-]

- *Revocation Schemes for Delegation Licences*
  Meriam Ben Ghorbel Talbi (a,b), Frédéric Cuppens (a), Nora Cuppens (a), and Adel bouhoula (b)
  a) Département RSM Telecom Bretagne, France
  b) Ecole superieure des communications de Tunis, Tunisia
  Abstract [+/-]
- *Reusability of Functionality-Based Application Confinement Policy Abstractions*
  Z. Cliffe Schreuders and Christian Payne
  Murdoch University, Australia
  Abstract [+/-]
- *Towards Role based Trust Management without Distributed Searching of Credentials*
  Gang Yin, Huaimin Wang, JianQuan Ouyang, Ning Zhou, Dianxi Shi
  National University of Defense Technology, China
  Abstract [+/-]

Paper session V :: Software security

- *BinHunt: Automatically Finding Semantic Differences in Binary Programs*
  Debin Gao (a), Mike Reiter (b) and Dawn Song (c)
  a) Singapore Management University, Singapore
  b) University of North Carolina at Chapel Hill, USA
  c) University of California, Berkeley, USA
  Abstract [+/-]
- *Enhancing Java ME Security Support with Resource Usage Monitoring*
  Paolo Mori, Fabio Martinelli, Alessandro Castrucci and Francesco Roperti
  IIT-CNR, Italy
  Abstract [+/-]
- *Pseudo-randomness Inside Web Browsers*
  Guan Zhi, Zhang Long, Zhong Chen and Nan Xianghao
  Peking University, China
  Abstract [+/-]

Paper session VI :: System security

- *Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data*
  Henrich Christopher Poehls
  University of Passau, Germany
  Abstract [+/-]
- *Embedding Renewable Cryptographic Keys into Continuous Noisy Data*
  Ileana Buhan, Jeroen Doumen, Pieter Hartel, Qiang Tang, and Raymond Veldhuis
  University of Twente, Netherlands
  Abstract [+/-]
- *Automated Device Pairing for Asymmetric Pairing Scenarios*
  Nitesh Saxena and Md. Borhan Uddin
  Polytechnic University, New York, USA
  Abstract [+/-]

Paper session VII :: Applied cryptography

- *Key Recovery Attack on Stream Cipher Mir-1 Using a Key-dependent S-box*
  Yukiyasu Tsunoo (a), Teruo Saito (b), Hiroyasu Kubo (b) and Tomoyasu Suzaki (a)

a) NEC Corporation, Japan
b) NEC Software Hokuriku, Ltd, Japan
Abstract [+/-]

- *Towards an Information Theoretic Analysis of Searchable Encryption*
  Saeed Sedghi, Jeroen Doumen, Pieter Hartel and Willem Jonker
  University of Twente, Netherlands
  Abstract [+/-]
- *A Bootstrap Attack on Digital Watermarks in the Frequency Domain*
  Sam Behseta (a), Charles Lam (b), and Robert L. Webb (c)
  a) California State University, Fullerton, USA
  b) California State University, Bakersfield, USA
  c) California Polytechnic State University, USA
  Abstract [+/-]
- *Improved Data Hiding Technique for Shares in Extended Visual Secret Sharing Schemes*
  Rabia Sirhindi, Saeed Murtaza, and Mehreen Afzal
  National University of Sciences and Technology, Pakistan
  Abstract [+/-]

Paper session VIII :: Security protocols

- *Efficient Multi-Authorizer Accredited Symmetrically Private Information Retrieval*
  Mohamed Layouni (a), Maki Yoshida (b), and Shingo Okamura (b)
  a) McGill University, Montreal, Quebec, Canada
  b) Osaka University, Japan
  Abstract [+/-]
- *Specification of Electronic Voting Protocols Properties using ADM Logic : FOO Case Study*
  Mehdi Talbi (a), Benjamin Morin (a), Valérie Viet Triem Tong (a), Adel bouhoula (b), and Mohamed Mejri (c)
  a) Ecole Superieure d'Electricite de Rennes, France
  b) Ecole Superieure des Communications de Tunis, Tunisia
  c) Université Laval, Canada
  Abstract [+/-]
- *Publicly Verifiable Remote Data Integrity*
  Ke Zeng
  NEC Labs, China
  Abstract [+/-]

Pre-conference social event

The Organising Committee will be hosting an informal event for delegates arriving in Birmingham before 20 October. We will meet at James Brindley Pub (on the same street as Hyatt Regency) at **19:00** (BST) on **19 October**. After meeting and having a drink, we'll have dinner a restaurant close by, such as Blue Mango. This event is not included in the registration fee and delegates are expected to pay for their food and drink.

- How to find Hyatt Regency :: 2 Bridge Street, Birmingham, UK. B1 2JZ.
- How to find James Brindley Pub :: 12 Bridge Street, Birmingham, UK. B1 2JR.
- How to recognise members of the Organising Committee :: Liqun Chen, Mark Ryan, Guilin Wang, Andrew Brown, Ben Smyth, Hasan Qunoo.

Conference banquet

The ICICS banquet will take place on the evening of Monday 20th October, at La Bastille, starting at **19:30** (BST). *La Bastille* is Birmingham's premier French restaurant and has created a special menu for the ICICS banquet which

consists of a wide range of starters, main courses and desserts. A glass of wine and coffee are included.

- La Bastille :: 220 Corporation Street, Birmingham, UK. B4 6QB.
- A map of the route from Hyatt Regency to La Bastille
- A menu for the banquet

Page maintained by: ICICS Organising Committee
Content last updated: October 16 2008