CARDIS'04

Sixth Smart Card Research and Advanced Application IFIP Conference

WG 8.8 — Smart Cards
WG 11.2 — Small System Security

Since 1994, CARDIS has been the premier international research conference dedicated to smart cards and their applications. Every two years the scientific community meets together for the conference.
Ten years after, like its predecessors and back to Europe and France, CARDIS'04 will bring together researchers and practitioners in the development and deployment of smart card technologies and applications.
The smart card, or, by extension, smart device with its processing power and link to its owner, is the good candidate for the person representation in the Information Society. Smart card or smart device will be the potential human representation or delegate in Ambient Intelligence (Pervasive Computing), where every appliances and computers will be connected, and where control and trust of your environment will be the next decade challenge.
Smart card research is of increasing importance as the need for information security increases rapidly, especially in response to new and urgent demands. Smart card with its security features is a seed of secure system and will play a huge role in ID management.
In many computer science areas, smart cards introduce new dimensions and disciplines. Disciplines like hardware design, operating system, modelling system, cryptography or distributed systems find new areas of applications or issues but also smart cards create new challenge for these domains.
Unlike events devoted to commercial and application aspects of smart cards, CARDIS conferences gather researchers and technologists who are focused in all aspects of the design, development, deployment, validation and application of smart cards or smart personal devices.

PROGRAMME

Tuesday 24 August 2004
10h30-12h

Opening session: Yves Deswarte, Pierre Paradinas & Jean-Jacques Quisquater

Invited talk

Belgian Electronic Identity Card: Security, Interoperability and Integration Aspects - Olivier Libon (Federal Public Service on Information and Communication Technology, Belgium)

13h30-15h
Java Cards

Session chair: Joachim Posegga (University of Hamburg, Germany)

Invited presentation: *Smart Cards in Love* – Bertrand du Castel (Axalto, USA)

Enforcing High-Level Security Properties For Smart Card Applets - Mariela Pavlova, Gilles Barthe, Lilian Burdy, Marieke Huisman, Jean-Louis Lanet (INRIA, France)

On-the-Fly Metadata Stripping for Embedded Java Operating Systems - Christophe Rippert, Damien Deville (INRIA Futurs, IRCICA/LIFL, France)

15h30-17h30
Privacy

Session chair: Jean-Jacques Quisquater (UCL, Belgium)

Privacy Issues in RFID Banknotes Protection Schemes - Gildas Avoine (EPFL-LASEC, Switzerland),

Smartcard-Based Anonymization - Anas Abou El Kalam, Yves Deswarte (LAAS-CNRS, France), Gilles Trouessin (Ernst & Young, France), Emmanuel Cordonnier (ETIAM, France)

Privacy Protecting Protocols for Revocable Digital Signatures - István Zsolt Berta, Levente Buttyán, István Vajda (Budapest U. Technology and Economics, Hungary)

Anonymous Services Using Smart Cards and Cryptography - Sébastien Canard, Jacques Traoré (France Telecom R&D, France)

Wednesday 25 August 2004
10h30-12h
Side-Channel Attacks

Session chair: Jan Verschuren (TNO, The Netherlands)

Efficient Countermeasures against Power Analysis - Tetsuya Izu, Kouichi Itoh, Masahiko Takenaka (Fujitsu Laboratories Ltd., Japan)

Smart-Card Implementation of Elliptic Curve Cryptography and DPA-type Attacks - Marc Joye (Gemplus, France)

Differential Power Analysis Model and Some Results - Sylvain Guilley, Philippe Hoogvorst, Renaud Pacalet (GET / Télécom Paris, France)

13h30-15h
Fault Injection Attacks

Session chair: Peter Honeymann (University of Michigan, USA)

Place and Route for Secure Standard Cell Design - Kris Tiri, Ingrid Verbauwhede (UCLA, USA)

A Survey on Fault Attacks - Christophe Giraud, Hugues Thiebeauld (Oberthur Card Systems, France)

A Differential Fault Analysis Attack Resistant Architecture of the Advanced Encryption Standard - Mark Karpovsky, Konrad J. Kulikowski, Alexander Taubin (Boston U., USA)

15h30-17h
Middleware 1

Session chair: Peter Hartel (U. of Twente, Netherlands)

Secure Network Card Implementation of a Standard Network Stack in a Smart Card - Michael Montgomery, Asad Ali, Karen Lu, (Axalto, USA)

A Pattern Oriented Lightweight Middleware for Smartcards - Jean-Michel Douin (CEDRIC-CNAM, France), Jean-Marie Gilliot (ENST Bretagne, France)

Card-Centric Framework - Providing I/O Resources for Smart Cards - Pak-Kee Chan, Chiu-Sing Choy, Cheong-Fat Chan, Kong-Pang Pun (Chinese U. Hong-Kong, Hong-Kong)

Thursday 26 August 2004
10h30-12h
Cryptographic Protocols

Session chair: Jean-Bernard Fischer (OCS, France)

On the Security of DeKaRT - Gilles Piret, François-Xavier Standaert, Gaël Rouvroy, Jean-Jacques Quisquater (UCL Crypto Group, Belgium)

An Optimistic Fair Exchange Protocol for Trading Electronic Rights - Masayuki Terada (NTT DoCoMo, Japan), Makoto Iguchi, Masayuki Hanadate, Ko Fujimura (NTT, Japan)

Accountable Ring Signatures: A Smart Card Approach - Shouhuai Xu (U. Texas at San Antonio, USA), Moti Yung (Columbia U., USA)

13h30-15h
Middleware 2

Session chair: Pierre Paradinas (CNAM/CEDRIC)

Invited presentation: *Smart Cards, Framework and Application Models* – Jean-Jacques Vandewalle (Gemplus, France)

Checking and Signing XML Using Java Smart Cards - Nils Gruschka, Florian Reuter, Norbert Luttenberger (Christian-Albrechts-U. Kiel, Germany)

XML Agent on Smart Cards - Sunil Sayyaparaju, Deepak B. Phatak (IIT Bombay, India)

15h-15h30
Closing Session with Best Student Paper Award.