INSTITUT DES HAUTES ETUDES

POUR LE DEVELOPPEMENT DE LA CULTURE, DE LA

SCIENCE ET DE LA TECHNOLOGIE EN BULGARIE

International Symposium

Recent Developments in Cryptography and Information Security

September 11-13, 2008
National Institute of Education, Oriahovitza, Bulgaria

Organized by

Minu Balkanski Foundation

General Information and Application form

SYMPOSIUM PROFILE

This second year edition of the International Symposium on Recent Developments in Cryptography and Information Security will follow the established model to "meet" Theory with Application. The program for 2008 is focussed on some theoretical foundations and their practical implementations in sensitive information protection and security areas. Special focus will be given to payments and finances.

MAIN SUBJECTS AND TOPICS

- **Cryptography for Personal Secure Devices**
- **E-signature and Secure Encryption – Modern Trends**
- **Finances, Banking and Payments – Trust & Security**
- **Cryptography - Bridging Theory with Practice**

Personal secure devices are tamper-resistant hardware tokens with cryptographically-enabled CPUs that are designed to withstand attacks on the information contained within. Smart cards, RFIDs and SIM cards for GSM mobile phones are examples of such devices. Other types of such secure devices take different form-factors and use different technologies for ensuring tamper-resistance and security of information. However, the storage and CPU limitations as well as the possible hardware attacks (e.g., side-channel attacks) give rise to a particularly challenging set of cryptography problems, where classical cryptographic algorithms turn out to be insufficient. The symposium will focus on both theoretical problems and applications: hardware limitations and how they make the classical cryptographic methods insufficient; known software and hardware attacks with an emphasis on side-channel attacks; practical applications in digital transactions, mobile phone security, etc.

New trends in secure and trusted information exchange, based on encryption and e-signatures models and algorithms will be covered. This will include also organizational aspects of trust and security, as well as specific regulations and implementation in complex domains like financial and bourse transactions, secure payments, various aspects of challenges in micro-payments, mobile payments. General and specific international security standards will be critically reviewed.

Finally, an in depth discussion on how to bridge theory with practical needs and technology developments, will open new areas for research and development activities. to meet the increasing demand for trusted and consistent information.

INVITED SPEAKERS (Preliminary list)

- Prof. Adi Shamir – Weizmann Institute, Israel
- Prof. David Jao, University of Waterloo, Canada
- Emmnuel Thomé - INRIA, France
- Dr. Pierre Girard – Gemalto, La Ciotat, France
- Dr. Francois Koeune – UC Louvain, Belgium
- Prof. Jean-Jacques Quisquater – UC Louvain, Belgium
- Dr. Ramarathnam Venkatesan – Microsoft Research
- Dr. Apostol Vassilev – NetIDSys, Austin, TX, USA
- Dr. Mladen Dimitrov- Université Paris Diderot, France
- Dimitar Jetchev - University of California at Berkeley, US

ORGANIZING COMMITTEE

Organizing Committee Chair:
Prof. Minko Balkanski, IHE, France

Organizing Committee Members:
Dr. Simeon Anguelov, Bulgarian Academy of Sciences, Bulgaria
Prof. Sava Grozdev, Bulgarian Academy of Sciences, Bulgaria
Prof. Antonii Slavinski, New Bulgarian University, Bulgaria
Peter Statev, ICT Cluster, Bulgaria
Petar Nedjalkov, AIS, Bulgaria

General Secretary
Mariana Assenova

PROGRAM COMMITTEE

Program Committee Chair:
Dr.George Sharkov, ESI Center Eastern Europe, Bulgaria

Program Committee Members:
Prof. Stefan Dodunekov, Institute of Mathematics and Informatics at BAS, Bulgaria
Dr. Mladen Dimitrov, Université Paris Diderot, France
Dimitar Jetchev, University of California at Berkeley, USA
Raffi Aslanian, IT expert, Versailles, France
Prof. David Jao, University of Waterloo, Canada
Dr. Ramarathnam Venkatesan, Microsoft Research, USA
Prof. Jaime Perez, City University of Seattle, USA

LOCATION

The Symposium will take place in the conference center of the National Institute of Education in Oriahovitza, a small village near Stara Zagora. The center is equipped with conference rooms, lecture rooms and computer facilities. Located at the foot of the beautiful Sredna Gora mountain and famous for its wineries, the village is nowadays hosting various international cultural and scientific events organized by Minu Balkanski Foundation.

IMPORTANT DATES

- June 1, 2008 – registration deadline
- July 1, 2008 – deadline for abstracts
- July 15, 2008 – acceptance
- September 11, 2008 - arrival and registration

SPONSORS

Minu Balkanski Foundation

WHO SHOULD ATTEND

The symposium is tailored for researchers, students and professionals involved and interested in these special theoretical and practical areas. Both users and developers of applications will benefit from the program. Industry representatives will discover new opportunities for development and bridging with theory. Authorities using or supporting secure communications and information exchange are welcomed.

The participants will be awarded a certificate of completion of theoretical and practical workshop on Cryptography and Information Security.

APPLICATIONS MUST BE SENT ELECTRONICALLY TO:
Minko Balkanski: minko.balkanski@gmail.com

Please, include the following information:

LAST NAME: ……...……
FIRST NAME:…….....
TITLE: ……...
DATE OF BIRTH: ……
SEX:……
ORGANIZATION:……...…….
ADDRESS:…….
……..……
CITY:……POSTAL CODE:……
COUNTRY:……
PHONE:……FAX:……
E-MAIL:…….

I intend to present a paper **YES** **NO**
If yes, please, specify the topic:

Registration fee including accommodation and meals: **600 BGN (300 EUR).**
Payment at registration or by bank transfer to:
Minu Balkanski Fondation, Oriahovitza
Bulbank, Stara Zagora
Bulbank UniCredit Group BIC, SWIFT code : BFTBBGSF
IBAN for transfers in BGN: **BG58BFTB76301074862454**
IBAN for transfers in USD: **BG52BFTB76301175730728**

Limited funding will be available for *graduate students*. To apply, please, send a curriculum vitae and a motivation letter to:

Prof. Minko Balkanski
2, Avenue de Camoëns
75116 Paris, France
e-mail: minko.balkanski@gmail.com

Recommendation letters are not required but strongly encouraged.