[Call for Participation]

Title: **From Theory to WhiteHat: Cryptology and Cyber Resilience**

Dates: 10-17 July 2016

Format: Summer school - One intensive week of theory, practice, discussions and cultural exchange: 4-hour lectures and tutorials by international experts extended with practical workshops, labs and seminars, simulations, round-table discussions and working groups on hot topics

Place: "National Institute of Education", Oriahovitza, Bulgaria

Organizers: Balkanski-Panitza Institute for Advanced Studies (BPIAS): www.bpias.org
European Software Institute Center Eastern Europe (ESI CEE): www.esicenter.bg
Minu Balkanski Foundation: www.balkanski-foundation.org
[and IT industry, academic partners, law-enforcement and defense authorities]

SUMMER SCHOOL PROFILE

To prepare the researchers and IT practitioners for the digital security and resilience of our e-business and e-life TOMORROW, we must foresee and develop on what will be AFTER TOMORROW.

The focus of this year's summer school is once again to ***Bridge Theory to Practice*** by gathering world class leaders in the field with young researchers, IT security practitioners, e-business innovators, business resilience managers and cyber-defense professionals. The School will build on the CryptoBG*2012 – CryptoBG*2015 and the earlier International Symposiums on Recent Developments in Cryptography and Information Security. The topics answer the e-competences demand for modern industry and society, aligned with the Europe 2020 Digital Agenda, the NATO Smart Defense initiative and Multi National capacity development (addressing 2035+).

The Summer School is a milestone of a longer-term joint program of the organizers (BPIAS, ESI CEE, Minu Balkanski Foundation, and international partners), last year for the first time in cooperation with IACR. The program is composed by trainings on IT and information security (form schools to universities), series of lectures and visiting speakers at, awareness campaign for the civil digital society, and forming an operational Cyber-Defense cluster.

The latest trends and state-of-the-art open problems are linked to practical aspects and case studies on use or miss-use of the information, our digital identity and trust. We want to foster forming the Bulgarian research and scientific community, serving the IT industry, all IT-enabled services (like banking, e-Health, e-Administration, industries), and the Knowledge Society in Bulgaria and the entire region.

It all starts with Alice and Bob, a secret and a need for a confidential sender-receiver channel, the A and B of ***Cryptography***. Numerous mathematical methods, such as number theory, combinatorics, coding theory, complexity theory and algorithms, are applied for secure transmission of messages. Fast-growing technologies serve both the healthy and the dark side. The challenge is to construct high-complexity encodings that would still take millions of years for decoding with the most powerful supercomputer and the most efficient known attacks. ***Cryptography*** is practically everywhere, in all software or hardware system – internet, emailing, mobile devices, access control and password authentication, digital signatures, network and systems security.

Cryptography is the basis, but still not a guarantee for the Cyber Security and ***Cyber Defense*** – the complex area which controls the risks related to the use of various computer systems and creates computer platforms, languages and applications according to established security rules and compliances. Here we combine technologies with methodologies, organization and awareness for higher internet security, systems and mobile security, content protection, digital rights management, and more general – resilient and sustainable operations at all levels and areas.

MAIN TOPICS AND PROGRAM

Topics of the year – the specific focus areas for 2016 edition will be:

- **e-ID and e-voting**
- **IoT** – crypto and security for smart devices – Internet of Things, Industrial Internet standardization, smart robots, homes, clothes and gadgets
- **Security for Industrial Systems** – **ICS/SCADA** systems and **Cyber Defense**

Theory

- curve-based and pairing-based cryptography
- elliptic curve cryptography (ECC), symmetric key
- lattice-based cryptography
- efficient arithmetic and integer factorization
- functional encryption – identity-based encryption (IBE) and attribute-based encryption (ABE)
- blind signatures and e-voting schemes
- secure communications, secure computation

Practice

- personal secure devices, mobile security
- security in the cloud – searchable encryption lab
- side-channel resistance – practical labs and simulation
- secure architectures, "security by design" aspects, secure coding
- enhancing the capabilities of symmetric and asymmetric encryption algorithms
- biometrics for security, multi-factor security (incl. "intuitive" methods)
- e-Voting – practical realization

And your favorite *CTF*BG round (Capture The Flag)* by CyResLab (of ESI CEE) RED <>BLUE teams in 3 sessions:

- CTF "warm up" & challenges explained
- active security – MITM demos, PKI & SSL, Secure Coding digest
- CTF*BG Ultimate

The program will also include several ***discussions*** on hot topics identified by leading companies and partners supporting CryptoBG*2016, organizers and participants themselves. The participants are welcome to communicate their research topics and results.

LIST OF LECTURERS

Dr. Nadia El Mrabet (Associate professor at École des Mines de Saint-Étienne, France) – *Intro to cryptography for IoT; Introduction to ECC (Elliptic Curves) and pairing; Practical labs in C/C++/Java or Sage*
Dr. Laurent Poinsot (Associate professor at University of Paris 13, currently in École de l'air, France) –*Quantum Cryptography*
Dr. Claude Barral (CEO Bactech, France) – *All you ever wanted to know about fingerprint recognition… and its bypassing!*
Dr. Nicolas Gama (Université de Versailles, France) – *Crypto fundamentals, Practical labs, and challenges for CTF (TBC)*
Dr. Mariya Georgieva (Gemalto, France) – *A homomorphic LWE based e-voting scheme;*

Introduction to E-voting; eID
Dr. Elena Andreeva (KU Leuven, Belgium) – *Authenticated encryption (TBC)*
Dr. Dimitar Jetchev (EPFL, Switzerland) – *Cryptology in the cloud: Searchable encryption (TBC)*
Dr. George Sharkov (ESI CEE, MoD, Bulgaria) – *Architecture and design for a National Cyber Security and Resilience system*
Yavor Papazov (ESI CEE, Bulgaria) – *Active Security*

Workshop with simulations prepared by the CyResLab of ESI Center.

Materials: The *CryptoBG*Summer School - Lecture Notes* will be available for participants to download during and after the summer school (special publication series is under consideration).

WHO SHOULD ATTEND

The Summer School 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 as well as potential partnerships. Authorities using or supporting secure communications and information exchange are welcomed. Cyber-defense professionals and officers will gain both know-how and foresight to meet the "unknown".

LOCATION

The Summer School traditionally takes 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.
Map: http://goo.gl/maps/kBc40

ORGANIZING COMMITTEE

Prof. Minko Balkanski, IHE, France	minko.balkanski@balkanski-foundation.org
Dr. George Sharkov, ESI CEE, Bulgaria	gesha@esicenter.bg
Prof. Dimitar Jetchev, EPFL, Switzerland	dimitar.jetchev@epfl.ch
Mariya Georgieva, Université de Caen, France	maria.georgievabs@gmail.com

INVITATION TO PARTICIPATE

You are kindly invited to **participate** or delegate a person from your organization.

Participation fee: *900 BGN/450 EUR/500 USD* (*incl. accommodation, meals, logistics; no transport)*
Please express your interest before ***1 June 2016*** *and return the* ***Registration form before 15 June 2016****!* ***The Registration Form could also be found on the website of the Summer School at: www.cryptobg.org.***

For Bulgarian students: As usual a limited number of scholarships will be available, so please apply with motivational letter (free text), in addition to the Registration form and a short CV.

For Sponsors: Your support is highly appreciated – as co-funding, student scholarships, or in-kind ***- please contact us for your sponsor package!***

Please address questions and confirm your interest to:

Dr. George Sharkov: gesha@esicenter.bg
Prof. Dimitar Jetchev: dimitar.jetchev@epfl.ch
Prof. Minko Balkanski minko.balkanski@balkanski-foundation.org
Dr. Mariya Georgieva mariya.georgieva@gemalto.com
Organizing Committee info@cryptoBG.org (phone: +359 2 489 9740)

Latest information, as well as materials from previous editions of the Summer School and other extras could be found at: www.cryptobg.org