[Call for Participation]

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

Dates: 9-16 July 2017

Format: Summer school - One intensive week of practice, theory 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 (more information)

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.

This year's edition of the Summer School is like no other before. This year, we will focus on the most controversial aspect of cryptography and cyber-resilience – hacking. We believe that theory is better visualized through practice and this year's Summer School is all about practice. Apart from the traditional sessions Crypto fundamentals and Introductory topics, related to the core concepts of Cryptography, CryptoBG*2017 will offer to its participants advanced practical labs and workshops.

The School will build on the CryptoBG*2012 – CryptoBG*2016 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). The program is composed by trainings on IT and information security (from 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:

- **Cryptographic uses in commercial software**
- **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

- Elliptic Curve Cryptography (ECC), Symmetric Key, Lattice-Based Cryptography
- Homomorphic Encryption
- Personal Secure Devices, Mobile Security
- Functional Encryption – Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE)
- Curve-Based Cryptography and Pairing-Based Cryptography
- Secure Communications

Practice

- SDR-based GSM, Mobile Security
- Secure Architectures, "Security by Design" Aspects
- Biometrics for Security, Multi-Factor Security (including "intuitive" methods)
- Security in the Cloud
- Web Crypto – JWT, OAuth, OAuth Connect, TLS/SSL
- Client-Side Web Cryptography and SJCL
- Lower-level cryptographic software primitives – OpenSSL, Libsodium, etc.
- Side-Channel Resistance

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*2017, organizers and participants themselves. The participants are welcome to communicate their research topics and results.

Materials: The *CryptoBG*Summer School - Lecture Notes* will be available for participants to download during and after the summer school.

Workshop proceedings will be published in the Information and Security Journal

WHO SHOULD ATTEND

The Summer School is tailored for researchers, students and professionals involved and with strong in the area. 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
Dr. Mariya Georgieva, Gemalto, France	mariya.georgieva@gemalto.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 ***10 May 2017*** *and return the* ***Registration form before 15 May 2017****!* ***The Registration Form could 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 before May 1, 2017.

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: +359 883 421 983)

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