TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

SIX
research centre
sensor, information and communication systems

# Cyber Security
# and Today’s Communication Technologies

Thursday, the 30th of January, 2014
Brno University of Technology, Technická 12, Brno

| | |
|---|---|
| 09:00 to 09:40 | *Press conference*<br>Meeting room SF2.153<br>Individual visits of laboratories of the SIX Centre can be organized |
| 10:00 to 11:20 | *Cyber security and cryptography*<br>Seminar room SH2.173 |
| 10:00 to 10:20 | Richard Hlavatý, **Welcome**<br>Technology Platform of Energetic Security |
| 10:20 to 10:40 | Jonathan Rigelsford, **Cyber security and strategic alignment**<br>The University of Sheffield |
| 10:40 to 11:00 | Jan Hajný, **Advances in cryptography**<br>Brno University of Technology |
| 11:00 to 11:20 | Martin Drahanský, **Biometric security systems**<br>Brno University of Technology |
| 11:20 to 12:00 | *Coffee break* |
| 12:00 to 13:40 | *Cyber security: testing and monitoring*<br>Seminar room SH2.173 |
| 12:00 to 12:20 | JiříKalvoda, **Performance testing of networks: tool for minimizing security threats**, TR Instruments |
| 12:20 to 12:40 | Petr Kaštovský, **Monitoring applications for increasing security in 40G and 100G networks**, INVEA-TECH |
| 12:40 to 13:00 | Pavel Kosour, **Monitoring physical layer of optical fiber**<br>PROFiber Networking |
| 13:00 to 13:20 | LukášMalina, **Stress testing and distributed denial of service testing of network infrastructures**, Brno University of Technology |
| 13:20 to 15:15 | *Individual visits of laboratories of the SIX Centre can be organized* |

MINISTERSTVO PRŮMYSLU A OBCHODU
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
OPPI

# [10:00 to 11:20]
# Cyber Security and Cryptography

*Chair: Prof. Hans LudwigHartnagel, TechnischeUniversität Darmstadt, DE*

[10:00 to 10:20]

## Welcome

Richard Hlavatý

Technology Platform of Energetic Security

richard.hlavaty@tpeb.cz

[10:20 to 10:40]

## Cyber security and strategic alignment

Jonathan Rigelsford

Department of Electronic & Electrical Engineering
The University of Sheffield, Sheffield, UK

j.m.rigelsford@sheffield.ac.uk

This presentation highlights current issues being faced by Information Assurance and Cybersecurity professionals, in both the private and public sector. Security professionals have failed to inspire confidence throughout the enterprise because of poor communication skills and a failure to correctly identify their customer. More often than not, security professionals are reluctant to quantify the operational risk to their enterprise of a poor cyber security policy, even to their own board of directors or internal audit team. Only by effectively communicating the value of Information Assurance and Cybersecurity will security professionals be consulted to contribute to enterprise decisions. Questions to be considered include: what is the perceived threat to our organisation? What is the actual historical threat? and*What is the cost to our business if we do nothing?* With the pervasive expansion of integrated data and systems, the risks posed by failed cyber security policy can be catastrophic for both the enterprise and society as a whole. Cloud Computing, Smart Cities, and Smart Grids are introduced as case studies. Each scenario has its own risks and benefits, the importance is to understand and successfully communicate the balance of those risks.

Cloud computing offers easy access to large quantities of data and low cost computing power but it is important to understand the risks and international legal obligations associated with such systems. For example, with the adoption of cloud computing, an enterprise's customer database is unlikely to be electronically stored in one central location; so *Where is my data?* Data will be fragmented and distributed over many servers and many data centres. This poses both technical and commercial challenges – if you don't know where your data is stored then how can you protect it and how can you perform internal audit on your information assurance policy?

Highly integrated and interconnected Smart Cities offer a wide range of potential benefits to society as a whole, from telemedicine to improved transportation links. How can we best understand the threats to these systems and ensure that vendors and users of such technologies work safely?

Smart Grids provide the opportunity for more reliable transmission of energy and reduced operational energy overheads through intelligent load balancing, and internationally shared resources. Historically, spikes or surges in energy consumption were mitigated by having an auxiliary supply available, such as a coal fired power station, to provide surplus overhead energy to account for these events. Such a system is inefficient as the surplus energy is wasted. More recently fast response gas or hydro turbines have been used to compensate for predictable short duration high demand energy spikes. With increased use of renewable energy generation, supply is much harder to predict due to changes in the weather etc for solar and wind generation. Smart Grids therefore have a key role to play in our energy future. This poses several significant challenges to Cyber Security. How do we protect our domestic energy grids?, How do our decisions impact those of our neighbours?, and What is the risk of failure?. If a bank fails with the implementation of its Cyber Security policy it risks losing its customers and up to the value of the bank. If a national grid fails due to a cyber security attack then the entire gross domestic product (GDP) of the country and its neighbours are at risk.

Topics discussed in this presentation include:

*Strategic Alignment:* How Cyber Security and Information Assurance interface with other areas of the enterprise is critical to success.

*Communication:* The importance of effectively communicating the value of Cyber Security and advantages and disadvantages of Cloud Computing throughout the enterprise.

*Risk Management:* Specifically the lack of objective data and the difference in approach compared to other risk management organisations.

*Cloud Computing:* What is it and how does it impact Cyber Security and Information Assurance.

*Smart Cities:* The benefits and risks of an integrated society.

*Smart Grids:* Who controls the power and how we can ensure energy security.

[10:40 to 11:00]

## Advances in Cryptography

Jan Hajný

SIX, Department of Telecommunications
Brno University of Technology, Brno, CZ

hajny@feec.vutbr.cz

The variety of devices that are able to communicate over a network has increased significantly in recent years. Today, almost all mobile phones, audio devices, alarms, sensors or even smart home installations communicate over networks. With the expansion of these network-enabled devices, the demands on security increase significantly too. We must be able to implement highly secure ciphers on devices with extremely restricted resources. Both requirements, high security and operation with low resources, are met in so called lightweight ciphers.

In addition to traditional encryption, new challenges emerge in privacy protection. Ubiquitous electronic devices make tracing and profiling people easier. The topic of privacy protection and digital identity protection is addressed by Privacy-Enhancing Technologies (PETs).

The presentation will focus on recent advances in lightweight cryptography and privacy-enhancing cryptography. New methods and technologies, as well as the latest results of the SIX cryptology team, will be shown.

[11:00 to 11:20]

## Biometric security systems

Martin Drahanský

Faculty of Information Technology
Brno University of Technology, Brno, CZ

drahan@fit.vutbr.cz

In the talk, an overview of frequently used biometric security systems will be provided considering centralized and distributed solutions of an access to objects.

- - - - -

Přednáška bude zaměřena na přehled používaných biometrických bezpečnostních systémů s ohledem na centralizovaná a distribuovaná řešení přístupu k objektům.

# [12:00 to 13:20]
# Cyber Security: Testing and Monitoring

*Chair: Prof. Markus Rupp, Technische Universität Wien, AT*

[12:00 to 12:20]

## Performance testing of networks: tool for minimizing security threats

JiříKalvoda

TR Instruments, Brno, CZ

jkalvoda@trinstruments.cz

A performance testing of a network infrastructure at application layers L4 to L7 belongs to a reliable protection against cybernetic attacks and crimes. The testing is based on the emulation of a *real* operation which includes an application of various security threats.

We will present the latest testers which can enable us to simulate the behavior of up to a million of users and a large number of servers simultaneously. Using a single device, we can create a complex testing environment which covers all the aspects of a *real* operation, *real* network infrastructure, repeatability, potential error analysis and clear presentation of results.

The device provides tools for testing specific web systems which require specific forms of access and authentication (SSL, IPsec, …). Different types of *a harmful traffic* can be simulated (DoS, DDoS, worms, viruses). An extensive database of existing attacks and threats is available, and tolls for creating own attacks are provided. Using this platform, we can test applications from the viewpoint of errors and failures of servers, resistivity of load balancers, firewalls, switches, and we can verify their performance parameters. We can also verify the quality of the infrastructure and provided services both from the viewpoint of errors (packet loss, click away, etc.) and satisfaction of users (FPR, email, video, etc.).

- - - - -

Jednou ze základních metod prevence a vytvoření spolehlivé ochrany před kybernetickými útoky a kriminalitou je zátěžové testování síťové infrastruktury na aplikačních vrstvách L4 až L7, založené na vytváření *reálného* provozu  včetně aplikací různých bezpečnostních hrozeb.

Budou představeny špičkové testery, které umožňují simulovat chování až milionů uživatelů a současně i velkého množství aplikačních serverů, čímž lze za pomoci jednoho přístroje vytvořit kompletní testovací prostředí splňující všechny atributy reálného provozu, reálné sítové infrastruktury, opakovatelnosti, možnosti chybové analýzy a přehledné prezentace výsledků.

Jsou zde k dispozici nástroje pro testování specifických webových systémů vyžadujících speciální formy přístupu a autentifikace (SSL, IPsec, …). Je možno simulovat různé typy *škodlivého provozu* (DoS, DDoS, červi, viry). Dostupná je rozsáhlá databáze již existujících útoků a bezpečnostních hrozeb, ale lze také vytvářet a definovat útoky vlastní. S využitím této platformy lze testovat například aplikace z hlediska výskytu chyb a poruch serverů, odolnosti loadbalancerů, firewallů, switchů, včetně ověření jejich výkonnostních parametrů. Je možné také ověřit kvalitu infrastruktury a poskytovaných služeb, a to jak z hlediska vzniku chybových situací (packetloss, clickaway, atd.), tak i z pohledu uspokojení požadavků uživatelů (FTP, email, video, atd.).

[12:20 to 12:40]

### Monitoring applications for increasing security in 40G and 100G networks

Petr Kaštovský

INVEA-TECH, Brno, CZ

kastovsky@invea.com

The talk will be focused on problems of security in today's computer networks. We will explain the necessity of monitoring on the level of applications. Today's high-speed networks are challenging due to a huge amount of transferred data and a high number of provided applications. In the talk, we will introduce a concept of solving this challenging problem in high-speed spinal networks operating at 40 and 100 Gb/s.

- - - - -

V rámci přednášky bude krátce představena problematika bezpečnosti v moderních počítačových sítích a vysvětlena potřeba pro monitoring na úrovni aplikací. Současné vysokorychlostní sítě pak představují výzvu v podobě velkého objemu přenášených dat a také množství poskytovaných aplikací, a proto bude v další části přednášky představen koncept, jak takovou výzvu řešit ve vysokorychlostních páteřních sítích s rychlostmi 40 a 100 Gb/s.

[12:40 to 13:00]

### Monitoring physical layer of optical fiber

Pavel Kosour

PROFiberNetworking CZ s.r.o., Praha,CZ

pavel.kosour@profiber.cz

Principles and exploited technologies for the observation of physical parameters of optical fibers. Possibilities to detect tapping of optical fiber and basic mechanical detection by a passive switch. Monitoring optical fibers under operation to increase quality and security.

- - - - -

Principy a používané technologie pro sledování fyzikálních parametrů optických vláken. Možnosti detekce odposlechu optického vlákna a základní mechanická detekce pasivním spínačem. Monitorování provozovaných optických vláken pro zvýšení kvality a bezpečnosti.

[13:00 to 13:20]

## Stress testing and distributed denial of servicetesting of network infrastructures

Lukáš Malina

SIX, Department of Telecommunications
Brno University of Technology, Brno, CZ

malina@feec.vutbr.cz

Recently, Denial of Service (DoS) attacks were a significant threat to network infrastructures. At the beginning of the year 2013, the attackers were able to “shut down” major Czech corporations, including banks, telecommunication operators and news servers. The attacks were not focused on the Czech Republic only, the same type of attacks was deployed in many countries all over the world. A variant of the attack known as Distributed DoS (DDoS) was used. Currently, there is no effective countermeasure against these network attacks. The only defense is strong-enough infrastructure, adequate settings of network nodes and proper over-dimensioning of capacities. Testing against DDoS plays a crucial role in assuring security because it is the only way how to learn about the impact of the attack (e.g., stability of services, response time, recovery time, etc.).

The presentation will introduce the fundamentals of DDoS testing, show the professional equipment for DDoS testing and describe research directions in DDoS testing and propose countermeasures for the near future.