EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

Projekt: energetická a kybernetická bezpečnost

III. etapa – aktualizace IAP

Praha 2014

Tento projekt je financován z ERDF prostřednictvím OPPI a ze státního rozpočtu ČR.

Obsah

Shrnutí III. etapy

V rámci třetí etapy projektu energetická a kybernetická bezpečnost TPEB naplnila cíle uvedené ve Strategické výzkumné agendě a zároveň dále upřesnila svůj Implementační akční plán. Klíčovou aktivitu spojenou se třetí etapou představovala příprava projektových žádostí pro národní i mezinárodní programy. Výsledkem této činnosti jsou především tři přijaté projektové žádosti podané v rámci programu EU Horizont 2020, ale také projekt soustředící se na stimulaci spolupráce v oblasti mezinárodního inovativního managementu a projekt zaměřující se na expertní vzdělávání v energetice.

Vstupem do projektových konsorcií v oblasti výzkumu, vývoje a inovací a jejich formováním TPEB naplňuje svůj nejvýznamnější dlouhodobý cíl, kterým je propojování výzkumné, vývojové a inovační základny s komerčním sektorem a koncovými uživateli, kteří většinou patří mezi státní instituce. V tomto smyslu se plně naplňují poslání a charakteristika TPEB jako public-private-partnership platformy.

Výše zmíněné projekty byly podány a přijaty k posouzení příslušnými institucemi. V rámci třetí etapy však vznikly také iniciální projektové žádosti, které jsou připraveny pro budoucí výzvy, které by měly vzejít z Technologické agentury ČR. Zároveň v průběhu etapy projektový tým nadále pracoval na formování dalších konsorcií, která budou v budoucnosti usilovat o projekty z programu H2020.

Významnou součástí třetí etapy, která genericky vyplynula z činnosti projektového, bylo rozšíření spolupráce TPEB s dalšími subjekty působícími v široce pojatém sektoru ochrany kritické infrastruktury. Kromě členských institucí a firem vstoupily do projektových konsorcií Fakulta vojenského zdravotnictví Univerzity obrany, Vojenský výzkumný ústav, Centrum biologické ochrany Těchonín či Státní úřad pro jadernou chemickou a biologickou ochranu. TPEB také navázala spolupráci s Národními kontaktními body pro program H2020 v oblasti bezpečnost (SECURITY) z ČR, Slovenska a Maďarska.

TPEB v neposlední řadě nadále naplňovala další ze svých cílů, jež je také ukotven ve Strategické a výzkumné agendě a Implementačním akčním plánu, který představuje aktivita ve vztahu k expertní i veřejné diskuzi prostřednictvím organizace vlastních workshopů a konferencí, zvané účasti na dalších konferencích a workshopech a publikováním článků upozorňujícím na relevanci dané agendy.

Stručný popis úspěšně podaných projektů

V souladu se svým dlouhodobým strategickým směřováním TPEB vstoupila do třech projektových konsorcií, která se ucházejí o podporu v programu Horizont 2020. První dvě projektové žádosti v rámci struktury H2020 směřují do oblasti výzkumu a inovací, kde se spojuje složka inovativního výzkumu s tržním uplatněním konkrétních technologií. Třetí pak

usiluje o podporu spolupráce mezi výzkumnými institucemi v oblasti aplikovaného výzkumu. Projektové žádosti tak počítají nejen s podporou výzkumu, ale také s vytvořením obchodní a marketingové strategie, která má vést ke konkrétnímu uplatnění dané technologie. V důrazu na praktické uplatnění inovací se H2020 liší od svých předchůdců – rámcových programů (FP – Framework program).

Prvním projekt, do kterého TPEB vstoupila jak partner, představuje **CySmart – Adaptive Cyber Security for Low Resource Wireless Communications Systems**. V čele projektového konsorcia stojí University of Sheffield a jeho součástí jsou výzkumné organizace a firmy ze Spojeného království, Německa, Rakouska, Francie a České Republiky. Z české strany na projektu kromě TPEB participují i VUT Brno a společnost Monet+. Cílem projektu je představit adaptivní řešení kybernetické bezpečnosti wireless ICT systémů kombinujících inovativní zabezpečení na úrovni kryptografické bezpečnosti i fyzické bezpečnosti. Součástí projektu je i ověření konceptu adaptivní bezpečnosti v reálném prostředí.

Druhý projekt, který vznikl za účasti TPEB – **OPTIMUS – Bringing Order to Chaos during MassiveVictim CBRN Incidents**, směřuje do oblasti ochrany v případě CBRN incident. V kontextu přípravy tohoto projektu TPEB navázala spolupráci s Fakultou vojenského zdravotnictví Univerzity obrany, Vojenským výzkumným ústavem, Centrem biologické ochrany Těchonín a Státním ústavem jaderné, chemické a biologické ochrany. Konsorcium vede řecká odnož britské společnosti EXUS, která má s evropskými projekty velmi bohaté zkušenosti. Cílem projektu je vytvořit UAV/UGV technologii, která by efektivně asistovala záchranným složkám v případech CBRN incidentů.

Projektové konsorcium má celkem 27 členů, kteří pocházejí z Řecka, Francie, Španělska, Norska. Itálie, Nizozemí, Kypru a České republiky. Početné konsorcium reflektuje skutečnost, že jeho součástí jsou vývojářské firmy, výzkumné instituce, ale i záchranářské struktury. Součástí projektu jsou i demonstrační piloty, v rámci kterých proběhne simulace C/B/R/N incidentu a následný zásah profesionálních záchranných složek, které budou využívat vyškoleny k využití technologie OPTIMUS. V ČR proběhne simulace biologického incidentu v Centru biologické ochrany v Těchoníně, které představuje v této oblasti špičkovou infrastrukturu. Podporu projektu z české strany vyjádřily i Generální ředitelství hasičského záchranného sboru, Fakultní nemocnice v Hradci Králové (spádová fakultní nemocnice pro Těchonín) či město Hradec Králové. Zájem o demonstrační workshop projevila také Evropská obranná agentura, mezi jejíž priority oblast CBRN dlouhodobě patří.

Pokud bude projekt podpořen, role TPEB bude opět spočívat v exploatační a diseminační roli spojené s iniciativami na úrovni koncových uživatelů, přičemž důraz bude kladen i na workshopy uspořádaní v institucích EU a NATO. Podobně jako v předchozím projektu bude využit expertní potenciál UNMZ v oblasti standardizace a certifikace, ke kterému bude tentokrát připojena expertíza v oblasti vojenských standardů, kterou dodají experti z Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti.

Kromě dvou výše uvedených projektů se TPEB významně angažovala v přípravě projektu výzkumné spolupráce mezi Centrem senzorických, informačních a komunikačních systémů

(SIX) a Technickou univerzitou ve Vídni (TUW), který byl podán do výzvy programu HORIZONT 2020, jenž nese označení WIDESPREAD-2014-1 *Teaming*.

Projekt výzkumné spolupráce mezi SIX a TUW s názvem **Advanced Wireless Technologies for Clever Engineering (ADWICE)** si klade za cíl vytvořit silné partnerství mezi SIX a TUW. Toto partnerství se stane základem konsorcia firem, veřejných institucí a univerzit, jejichž společným zájmem je výzkum v oblasti *chytré techniky*, využití výsledků tohoto výzkumu a případně jeho ekonomické zhodnocení. TPEB jako součást projektového konsorcia ADWICE přispěje svými zkušenostmi, vybudovanými vazbami a know-how k optimálnímu nastavení obchodního plánu a partnerských vazeb.

Projekt ADWICE pokrývá oblasti senzorických systémů, zpracování signálů, mobilních komunikací, radiofrekvenčních aplikací a kybernetické bezpečnosti. V širším smyslu se tak jedná o pro TPEB klíčové téma ochrany kritické infrastruktury. Kromě výše uvedené přímé participace TPEB na projektu budou ze spolupráce profitovat i členové TPEB, kteří mohou využívat výzkumných aktivit ADWICE a zároveň vstupovat do výzkumných projektů, které bude ADWICE řešit.

Projekt ADWICE svými dopisy zájmu podpořili i ministr školství Marcel Chládek, rektor Vysokého učení technického v Brně (pod nějž centrum SIX spadá), prorektoři TUW, Jihomoravské inovační centrum a více než dvacítka firem.

Kromě projektů podávaných v rámci programu H2020 převzala vůdčí roli v projektu **1st Workshop on Coordinating the EU R&D&I initiatives in the area of security in Visegrad**, který byl podán do projektové soutěže do Mezinárodního Višegrádského fondu. Cílem projektu je stimulovat spolupráci zemí V4 v oblasti mezinárodních výzkumných a inovačních projektů především pak v rámci H2020. Projekt vychází ze skutečnosti, že zatímco výzkumné instituce ze zemí V4 jsou relativně aktivní při pokusech získat podporu z Rámcových programů či nově H2020, aktivita firem v této oblasti je velmi nízká. TPEB by se tak ráda v čele mezinárodního středoevropského konsorcia pokusila zvýšit povědomí firem o možnosti tohoto financování výzkumu, vývoje a inovací, přičemž dlouhodobější cíl představuje snaha vytvořit funkční středoevropskou strukturu efektivního inovačního managementu, která podporovala tvorbu projektových žádostí ukotvených v regionu V4.

V rámci čistě tuzemských soutěží TPEB iniciovala projekt soutěžící o veřejnou zakázku v oblasti **Zajištění vzdělávacích a podpůrných služeb včetně e-learningu**, jejímž zadavatelem bylo Ministerstvo průmyslu a obchodu. TPEB v projektu naplňuje roli klíčového partnera, který by v případě úspěchu dané nabídky garantoval odborné školení v oblasti ochrany energetické kritické infrastruktury. V tomto ohledu by TPEB využila expertních kapacit svých členů (zejména Vysoké školy báňské a Vysokého učení technického v Brně). Vzhledem ke vzdělávacímu charakteru a soustředění se na expertní školení je projekt zcela v souladu s dlouhodobým zájmem a posláním TPEB.

Shrnutí výsledků III. etapy

Strategická výzkumná agenda a Implementační akční plán TPEB v kontextu projektu energetická a kybernetická bezpečnost počítají s aktivitami rozdělenými do 4 hlavních oblastí – komunikační technologie, kybernetická bezpečnost, technologie sledování prvků kritické infrastruktury a fyzická bezpečnost. Jakkoli je toto dělení analyticky vhodné, na úrovni konkrétních projektových žádostí se hranice mezi těmito jednotlivými oblastmi logicky stírají. Nejvýznamněji se to týká kybernetické bezpečnosti a komunikačních technologií, které jsou povětšinou v projektových výzvách vedeny pod společnou hlavičkou ICT.

V souladu s implementačním plánem a v rámci naplňování Strategické výzkumné agendy došlo v rámci první fáze projektu prostřednictvím analýz stávajícího stavu daných oblastí k identifikaci klíčových priorit, které by měly být nadále rozvíjeny. Ve druhé fázi pak byla v rámci studií rozvinuta problematika standardizace spojená s těmito prioritami. Tato expertní činnost umožnila přikročit ve třetí fázi k iniciaci projektových žádostí a k formování mezinárodních konsorcií.

Dosažené cíle:

- V rámci oblasti kybernetické bezpečnosti a komunikačních technologií byl úspěšně podán projekt **CySmart – Adaptive Cyber Security for Low Resource Wireless Communications Systems**, který byl přijat do výzvy H2020 ICT-32-2014: Cybersecurity, Trustworthy ICT

- V rámci oblasti kybernetické bezpečnosti a komunikačních technologií byl úspěšně podán projekt ADWICE- **Advanced Wireless Technologies for Clever Engineering**, který byl přijat do výzvy H2020 WIDESPREAD-2014-1 *Teaming*

- Jako předělový projekt mezi všemi čtyřmi oblastmi byl úspěšně podán projekt **OPTIMUS – Bringing Order to Chaos during Massive Victim CBRN Incidents**, který byl přijat do výzvy H 2020 DRS-2-2014 Crisis management topic 2: Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination and/or exposure

- Jako předělový projekt mezi všemi 4 oblastmi byl podán projekt **1st Workshop on Coordinating the EU R&D&I initiatives in the area of security in Visegrad**, který byl přijat do projektové soutěže v rámci Mezinárodního Višegrádského fondu.

- TPEB vstoupila jako partner do projektu **Zajištění vzdělávacích a podpůrných služeb včetně e-learningu** soutěžícího ve veřejné soutěži v rámci Operačního programu lidské zdroje a zaměstnanost, který byl vyhlášen Ministerstvem průmyslu a obchodu

- TPEB připravila několik dalších iniciálních verzí projektových žádostí, které budou v návaznosti na výzvy poslány do projektových soutěží Technologické agentury ČR a dalších programů.

- TPEB pracovala na vytváření dalších projektových žádostí a konsorcií, která budou usilovat o projekty v rámci výzev programu H2020

- TPEB přichystala výzkumně-vývojovou nabídku pro vznikající programy česko-čínské a česko-izraelské spolupráce.

- TPEB zorganizovala kulatý stůl, na které byly prezentovány aktivity TPEB v prvním pololetí roku 2014 a s členy i nečleny TPEB probírány možnosti další (nejen) projektové spolupráce.

- Zástupci TPEB se účastnili několika konferencí a workshopů, kde prezentovali schopnosti, aktivity a postoje TPEB k otázkám týkajícím se ochrany kritické infrastruktury.

Shrnutí aktivit v rámci jednotlivých kapitol

Jak už bylo zmíněno, reálné projektové žádosti logicky propojují jednotlivé oblasti. Pro snazší orientaci budou projekty představeny odděleně v kontextu jednotlivých kapitol, přičemž bude vždy zdůrazněna role TPEB na přípravě projektu a potenciálně také na řešení projektu.

Kybernetická bezpečnost, komunikační technologie a fyzická bezpečnost

CySmart – Adaptive Cyber Security for Low Resource Wireless Communications Systems

TPEB has cooperated on the preparation of the project proposal which was successfully submitted under the call ICT 32 2014 H2020. TPEB has participated on the consortium formation as well as project application development. Besides other activities TPEB has mediated the involvement of the Czech SME, Monet+, in the consortium.

Consortium

The consortium has been developed to include strong research institutions, R&D companies as well as end-users to represent the full supply chain across the areas of interest.

Participant No *	**Participant organisation name**	**Country**
1 (Coordinator)	The University of Sheffield	UK
2	Transport for London	UK
3	Bristows LLP	UK
4	Brno University of Technology	CZ
5	NXP Semiconductors Austria GmbH	AT
6	Hyperion Systems (Consult Hyperion)	UK
7	CISC Semiconductor GmbH	AT
8	University of Surrey	UK
9	Technology Platform Energy Security (CZ)	CZ
10	SmartO	FR
11	MIRA	UK
12	Monet+	CZ
13	Astutim Ltd	UK

In the end the consortium includes partners from the UK (7), Czech Republic (3), Austria (2), and France (1). The engagement of the Czech institutions has been coordinated and with the exception of Brno Technical University negotiated by TPEB.

The aim of the project

The economic, health and quality of life benefits of the continuing and forecast proliferation of ICT technologies in the environment, healthcare and in various infrastructures would be seriously undermined if current cybersecurity approaches are not challenged. Add to this the fact that quantum computing is in not too far horizon and would lead to a whole re-think of the concept of traditional cryptography for cybersecurity. For systems using wireless communications methods and which have low resources in terms of cryptographic security,

computational capability, or available electrical power, the limitations could me even more serious and even prohibitive.

This proposal aims at delivering a step change in cybersecurity for constrained environments by enabling an adaptive approach to cybersecurity that is implemented in real time; end-to-end security techniques for low resource wireless ICT systems will be developed which are capable of adaptively responding to their environment in order to mitigate security risks. Utilizing the unique expertise available from the consortium members, we will consider a novel approach to end to end security that combines both cryptography-based security with physical layer security in an adaptive way that can be deployed in real-time within ICT environments characterised by stringent low resource requirements, in particular in terms of low energy. These environments are seen to be the most challenging from the technical aspects and the most rewarding in terms of future impact. The results of the investigation will be applied to real-life applications in in-built and automotive environments.

Specific objectives:

- To investigate and determine how the physical radio frequency (RF) environment, such as a building or vehicle, can be dynamically changed in order maximize security and minimise user risk in wireless systems.
- To investigate how to make cryptography-based security scalable with low resource and deliver the required primitives and protocols to support it.
- To develop techniques that combine physical layer security with scalable cryptography-based security to achieve adaptive security in resource constrained environments.
- To validate the concept of adaptive security in real-life applications
- To design and develop low resource wireless ICT systems which are capable of adaptively responding to their environment in order to mitigate security risks.
- To demonstrate platform independent methods for provable security against physical attacks.

Specified objectives of the project

Scientific objectives/measure of success

S01 - Scalable, low resource cryptography primitives combined with secure protocols to enable an adaptive approach to security in resource constrained environments / Simulation and implementation results showing the improved performance for intended applications published in a peer reviewed conference or journal paper.

S02 - Adaptive cryptographic protocols for authentication and key management / Simulation and implementation results showing the improved performance for intended applications published in a peer reviewed conference or journal paper.

S03 - Formal analysis of existing and newly devised cryptographic protocols. The analysis will also identify shortcomings in these protocols / Simulation and implementation results showing the improved performance for intended applications published in a peer reviewed conference or journal paper.

S04 - To assess and develop techniques to dynamically control RF propagation within the built environment to reduce the probability of successful eavesdropping and denial of service attacks in wireless ICT systems / Simulation and experimental demonstration with results published in a peer reviewed conference or journal paper.

S05 - Design and retro-fitting mechanisms to further develop wireless friendly buildings in which counter measures are to attacks on wireless ICT devices are inherent within the structure / Simulation and experimental demonstration with results published in a peer reviewed conference or journal paper.

S06 - Counter measures implemented in the radio front end of wireless devices to maintain resilience to interception / Simulation and experimental demonstration/with results published in a peer reviewed conference or journal paper.

Technical objectives/measures of success

T01 - Design and implementation of a test platform to investigate the security and privacy implications of the above whereby counter measures are used both at radio frequency (RF) and cryptographic layers as appropriate / Details of experimental trial results.

T02 - Perform system level integration of adaptive RF and cryptographic technique / Details of experimental trial results.

T03 - Perform system level validation using enhanced contactless payment and RFID ticketing systems, within realistic environments including a London Underground tube station / Details of experimental trial results.

Impact objectives/measures of success

I01 - New cybersecurity framework for low resource wireless ICT / Adoption of adaptive security in wireless ICT infrastructure of the future, resulting in economic benefit to stakeholders in the EU.

I02 - Development of legal frameworks and precedence / Adoption of legal frameworks providing confidence in ICT infrastructure in terms of security and privacy.

I03 - Contributions to international standards / Partners will ensure dissemination of results to relevant standard bodies including ISO/IEC JTC1 SC06 (NFC), ISO/IEC JTC1 SC17 (Smart Cards) and ISO/IEC JTC1 SC31 (RFID).

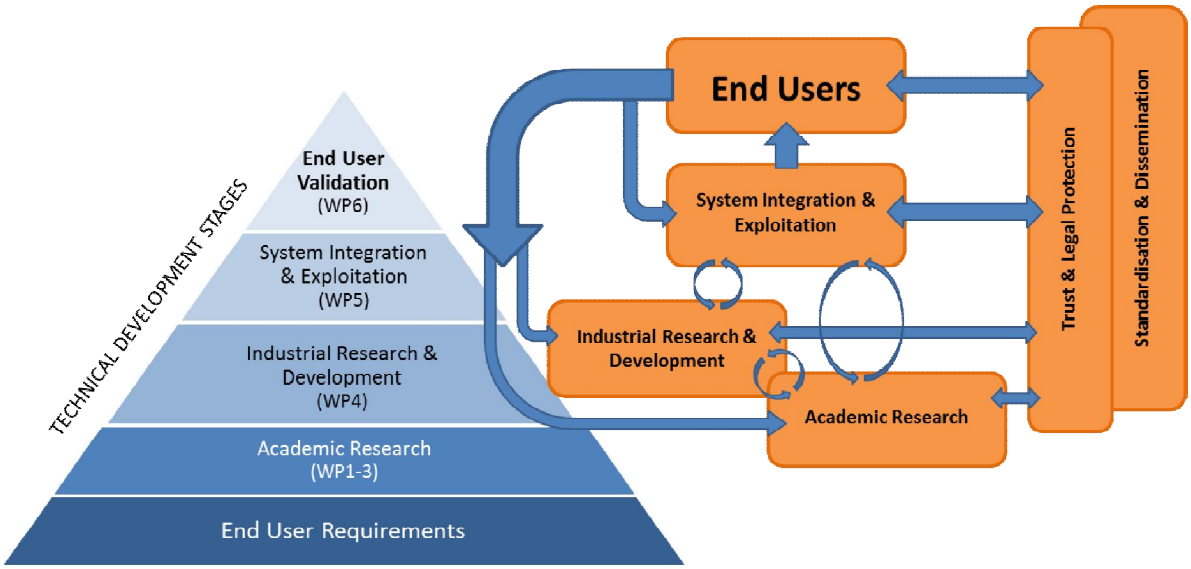
The proposal has been related to Cybersecurity and Trustworthy ICT by considering how the threats, vulnerabilities and risks associated with the fast evolution of ICT technology and its widespread adoption can be mitigated for the lifespan of the application it supports.

The proposal focuses on designing and developing a range of end-to-end security techniques for low resource wireless ICT systems which are capable of adaptively responding to their environment in order to mitigate security risks. The cosortium will consider practical and economically viable solutions addressing how the physical RF environment can be dynamically changed in order maximize the associated cybersecurity security and minimise user risk in wireless systems.

Additionally, this proposal spans both the cryptography and the security-by-design for end-to-end-security themes and addresses key challenges within each theme in the context of low resource smart environments. The idea is to apply novel and generic cybersecurity solutions to specific technologies in order to validate their effectiveness in real-world scenarios.

A holistic approach to end-to-end security involving all stakeholders

Security-by-design paradigms will be developed and tested, providing end-to-end security, across all hardware and software layers of a low resource wireless ICT system and throughout the associated business supply-chain.



Adaptive RF environments:

The project proposes to develop solutions for dynamically reconfigurable environments, and to develop solutions that decrease the security risks associated with improper use or misconfiguration, which will be identified through formal analysis as a robust method for testing and validation.

- Design and retro-fitting mechanisms to further develop wireless friendly buildings in which counter measures are to attacks on wireless ICT devices are inherent within the structure;

- Counter measures implemented in the radio front end of wireless devices to maintain resilience to interception.

Adaptive Security:

The project will implement low resource cryptographic primitives which can adapt to the environment in which they are used. The consortium aims to develop solutions that improve end-to-end security, even taking into account foreseeable improvements in attacker hardware and computational capabilities. The project will apply novel and generic cybersecurity solutions to specific technologies in order to validate their effectiveness in real-world scenarios.

- hybrid techniques of combining both scalable cryptography and adaptive RF solutions;

- Cross-layer design for threat mitigation.

Platform independent primitives

The proposal endeavours to provide platform independent solutions for low resource wireless cryptographic devices, which are threat aware and also contain self-adaptive security to be used within highly connected, complex environments, with dense and interoperable networks. For example the cryptography primitives implementations would develop portable modular solutions either as software codes for embedded platforms or portable hardware platforms such as HDL for ASIC and FPGA platforms.

Practical validation

The proposed technology will be validated in realistic application scenarios, including near field communication (NFC) used in contactless payment transactions, and radio frequency identification (RFID) taking commuter transportation (London Transport) and automotive as example scenarios.

Low resource secure scalable cryptography

The project will demonstrate a net increase in cryptographic performance, or reduction in power consumption or resource usage, compared to state-of-the-art cryptographic approaches.

- Optimised security and privacy vs resource usage trade-offs.

The challenges for the project

This project provides a technological and commercial framework to mitigate the inherent threats, vulnerabilities and risks in low resource wireless ICT systems. It addresses the fundamentally urgent questions of how can we guarantee security by technological design to offer maximum protection for such systems and their users.

Therefore we aim to provide fully integrated end-to-end security across all layers in environments whereby the RF channel can be incorporated into the system and modified to provide an additional layer of security beyond what is currently available in systems. This will be achieved by adaptively changing the radio frequency (RF) channel or transmission at the physical layer, and thereby producing an environment which can be optimised to offer a dynamic level of security and resilience depending on the current threat. By adapting to the external environmental RF conditions and monitoring for threat, it is proposed that a higher level of security can be achieved than by cryptographic solutions alone. This offers systems designers a third line of defence, building on existing protocols and cryptographic solutions with a smart environment and adaptive physical layer (PHYSmart). Further to this we will investigate hybrid techniques of combining both cryptography and adaptive RF solutions which will go beyond the state-of-the-art for wireless ICT security.

Cybersecurity challenges in low resource wireless ICT systems.

Here we present a range of cybersecurity challenges which occur in low resource wireless ICT systems. These provide a focus for the fundamental research and give a background to why a successful project outcome will be important to the ICT community. By developing solutions to meet these challenges we aim to validate the concept of increased security through use of an adaptive physical environment.

RFID challenge

RFID is increasingly used in the supply chain and logistics. According to IDtechEx in 2013 a total of 3 billion UHF RFID tags are sold with 2 billion used for garment tagging. However, a more diverse products range contain RFID tags today., than in previous years. For example Microsofts Surface has an embedded RFID tag in order ensure transport safety. When a surface product is assembled an embedded RFID tag with contact interface is programmed with a unique key. Each time the Surface is powered up this RFID tag's key is read and the Microcontroller compares its key with the key in the RFID tag through a certain algorithm. Only if the key in the RFID tag matches the criteria the Surface enables operation Otherwise, otherwise it is locked. Before shipment the key in the RFID tag is erased and consequently anyone steeling the Surface product will not be able to operate it. When the Surface arrives at its final destination the key on the RFID tag is restored by use of an RFID reader that gets the key from the Surface vendors data base and the Surface can be operated. A downside of this approach is that the RFID tag may be identified by anyone with an UHF RFID reader and therefore a pickpocket may quickly know whether someone has an RFID tag in its rucksack. The work in this project will address methods on how this could be resolved using currently

developed new UHF RFID air interface standards and crypto standards. Furthermore, we will carry out research on system concepts resulting in solutions that ensure product safety, deft prevention and privacy while still best utilizing the possible advantages in the supply chain.

NFC challenge

Contactless payments, using near field communication (NFC) as their enabling technology are at a point where the number of such payment terminals available in retail outlets are increasingly on the rise. At the same time, mobile handsets supporting NFC are becoming widely available. These emulate contactless cards to allow the user to make small transactions in a matter of seconds, thus reducing queues and inconveniences with small change. Though NFC was first introduced in 2003 by defining its operation through the International Standards Organisation (ISO), the release of products supporting contactless payments did not gain momentum until around 2007. Banks and card issuers in the UK have only adopted contactless payments in the past few years. The standards, including ISO14443 and ISO10373, were implemented with regards to designing and testing NFC devices with respect to their defined functionality. These standards do not address security risks associated with making transactions wirelessly, which are dependent on the design of NFC antennas, the radio propagation in the surrounding environment at the frequency of operation (13.56MHz), as well as the encryption in the transaction protocols used. Another potential risk factor is the integration with the Europay, MasterCard and Visa (EMV) payment protocols, which were designed for contact payments (chip and PIN), predating NFC. The NFC wireless interface introduces attack methods that were not possible when the protocols were designed.

Our approach to this research considers known issues in NFC contactless payments illustrated in Figure 3. Particular attention is paid to the capability of radio frequency (RF) devices to mount such attacks, where previous experiments have not been sufficiently conclusive. For a denial of service attack, previous research has considered how “bogus” NFC tags can be placed in the vicinity of a payment device so as to occupy the wireless link and prevent its ability to make a transaction [1]-[3]. We will investigate a different attack vector, where a relatively high powered radio source at the NFC operating frequency in the vicinity of one or more contactless payment terminals can effectively jam the wireless channel. Large metallic objects in the vicinity or even the building structure, given that its size is resonant at HF wavelengths, could be used as an antenna to radiate a high power source resulting in denial of service. Therefore suitable building solutions are required to minimise the likelihood of successful attacks.

Eaves dropping a contactless payment transaction can be achieved by use of a covert antenna such as wire about 5m in length coiled around a rucksack. Such an antenna could also be used in an active attack to interrogate a mobile device even when not in use and collect information (also known as “skimming”). A further opportunity is a “man in the middle” attack [4], where the attacker can intercept a transaction so the user and the device think they are communicating with each other, while in reality they are both communicating with the attacker acting as the man in the middle. It has been established through our preliminary work

and other work [5, 6] that successful interrogation and eavesdropping depends on the characteristics of the antennas and also on the background radiation in the high frequency (HF) band used, for example from radio broadcasting and nearby electrical devices. However, work to date considers only standard antennas at close distances to show they are able to eavesdrop or interrogate in proximity [5]-[7], while no conclusive results have been published regarding what covert antennas can be used and under what conditions, yet preliminary measurements at UNIS have shown such antennas as in Figure 3 can be readily used at distance. We will also take comprehensive measurements to model the HF background noise in different locations (e.g. buildings with different designs, outdoors and underground) using realistic covert antenna designs. This will allow us to determine at what distances eavesdropping or interrogation is feasible based on the magnetic field strengths used in NFC standards. We will also investigate how 'artificial background noise' could be created in order to jam eavesdroppers.

Knowledge of the propagation characteristics of HF signals within buildings from signal sources within or outside the building is therefore important from the point of view of this project. Whilst such propagation characteristics have been extensively investigated at higher frequencies (e.g. mobile telephony) no significant investigations appear to have taken place within the HF band that have been reported in the literature. Preliminary measurements undertaken at the University of Leicester indicate that for a transmitter located outside a building, signal strengths at similar distances from the antenna can vary between 1-2dB to more than 35dB lower inside than outside. The variation within the building is complex and requires thorough investigation to relate the signal strength to building structure, and to quantify the effects for different building types.

Though a major proportion of this project will be concerned with RF and microwave communications (including structural engineering with regards to the built environment) and digital signal processing, it is not sufficient to only ascertain under which conditions negligibly low bit error rates are achieved. Even with non-zero error rates, there may still be a risk to security and privacy from an attacker who can aggregate information from multiple transactions or public sources. This project will make such analysis based on real measurements of the surrounding radio environment, using realistic radio equipment accessible to an attacker. Furthermore, we will also consider any flaws in the standard protocols using formal analysis [8], taking into consideration the possibility of performing active attacks such as spoofing messages and responses. With regards to denial of service attacks, we will not only consider what levels of RF power can be used to achieve this, but also in what (more efficient) ways it can be achieved, such as transmitting well-timed short sequences to discreetly corrupt a transaction or by otherwise abusing the protocols to disable a payment terminal.

Automotive challenge

Historically, vehicles were independent mechanical systems that were subject only to physical security threats (i.e. break-ins). However, modern vehicles are now reliant on electronic

control systems, and these increasingly interact via in-vehicle networks in order to achieve higher levels of functionality than can be provided by a collection of stand-alone sub-systems. Furthermore, wireless interfaces are becoming ever more common in vehicles in order to enable a wide range of applications. These include e-Call, electronic tolling, remote keyless entry (RKE), tyre pressure monitoring systems (TPMS), remote diagnostics [9], wireless flashing of software upgrades, V2X communications (i.e. vehicle-to-vehicle/infrastructure), integration with smartphones [10] and other nomadic devices, and in-vehicle wireless networks (e.g. Bluetooth and Wimax). This rapidly expanding attack surface will make the vast numbers of vehicles, as well as roadside infrastructure and the wider transport systems that they participate in, potentially vulnerable to malicious and nuisance attacks unless steps are taken to identify and mitigate such threats from the outset [11, 12].

Although many of these applications are still emerging, RKE has been common for some time and TPMS has been mandatory passenger cars and similar vehicles since 2007 in the USA [13], and since 2012 in the EU [14]. The possibility of using wireless relay techniques to extend the range of RKE systems, and so achieve the more traditional criminal goal of gaining physical access to the vehicle, is described in [15]-[17]. Attacks against vehicle systems by exploiting security vulnerabilities in the wireless communications of TPMS are described in [18], which reports that eavesdropping on TPMS transmissions can be achieved at ranges of up to 10 m with a simple omnidirectional antenna, rising to 40 m with a basic amplifier, and potentially even greater distances using a directional antenna. Simulations of attacks on the FlexRay protocol [19] and CAN bus [20] have also been reported as methods to gain access to vehicle sub-systems, and a conclusion of the experimental studies outlined in [21] is that, for current vehicles, achieving access to almost any sub-system can also provide access to almost all of the other sub-systems.

The automotive environment presents particular difficulties, in that it involves large-scale, decentralized, and constantly changing wireless networks. Furthermore, the vehicle nodes may change their position, and hence their channel characteristics, very rapidly, while both eavesdroppers and more active threat agents may move equally rapidly. However, cyber security attacks on vehicles are particularly critical as they may have operational impacts that could lead to significant safety consequences, for both vehicle occupants and other road users, as well as possible financial and privacy implications. Thus, cyber security considerations are becoming an increasingly important aspect of functional safety analysis for vehicles.

TPEB´s Involvement

Apart from contributing to the formation of the consortium and to the formulation of the project application, in case the project is supported TPEB would play the following roles. Thanks to its nature connecting the research sphere with the comercial sector and state administration TPEB will be responsible for exploitation and dissemination activities, which also involve a development of supporting business strategies. Additionally, TPEB will co-organise several public events including the major demonstrative conference taking place in Prague by the end of the project. Finally, TPEB will also provide essential expertise in

standardisation and certification through the expert basis of the Office for Standards, Metrology, and Testing.

More specifically from the project perspective, TPEB will be involved in three work packages dealing with consortium management, exploitation and dissemination processes and activities, and analysis of the standardisation needs and development of the standardisation strategy.

Advanced Wireless Technologies for Clever Engineering (ADWICE)

The project Advanced Wireless Technologies for Clever Engineering (ADWICE) is aimed at creating a strong partnership between the research centre of Sensor, Information and Communication Systems (SIX, Czech Republic) and various institutes at the Faculty of Engineering and Information Technologies (ETIT) of the Vienna University of Technology (Technische Universität Wien –TUW, Austria). QS World University Rankings ranks TUW on position 91 among engineering faculties worldwide. The partnership will result in the transfer of excellence in research from TUW to SIX.

TPEB´s role is defined to stimulate multiplying effects due to its intensive cooperation with SIX. The idea is to link relevant companies and other stakeholders with the research and innovation activities resulting from the cooperation between the institutions in the Czech Republic and Austria. In this sense TPEB will contribute to the formulation of upcoming project proposals and consortia formation as well as support the dissemination and exploitation of the outcomes coming from the *teaming* cooperation.

Technologie sledování prvků kritické infrastruktury

V rámci této kapitoly bude představen projekt **OPTIMUS – Bringing Order to Chaos during Massive Victim CBRN Incidents**, který mimojiné počítá i s využitím technologických prvků UAV a UGV. Z obecného hlediska je projekt komplexní a propojuje všechny čtyři oblasti projektu energetická a kybernetická bezpečnost.

OPTIMUS – Bringing Order to Chaos during Massive Victim CBRN Incidents

TPEB has cooperated on the preparation of the project proposal which was successfully submitted under the call DRS 2 2014 H2020. TPEB has participated on the consortium formation as well as project application development. Besides other activities while working on the application TPEB started cooperation with the Faculty of Military Health of the University of Defence, Czehc Republic, Military Research Institute, Center for Biological Protection in Techonin, and National Institute for Nuclear, Chemical, and Biological Protection

Consortium

The consortium has been developed to include strong research institutions, R&D companies as well as end-users to represent the full supply chain across the areas of interest. The special emphasis has been put on the end-users since the project counts with the pilots introducing the applicability of the technology developed within the project.

Participant No *	**Participant organisation name**	**Acronym**	**Country**
Technology providers			
1	EXUS	EXUS	GR
2	MORPHO	MPH	FR
3	Universidad Politécnica de Valencia	UPV	ES
4	DIGINEXT	DXT	FR
5	Telespazio Iberica	TPZ	ES
6	Stiftelsen SINTEF	SINTEF	NO
7	ADITESS Advanced Integrated Technology solutions and Services	ADIT	CY
8	TELESTO	TEL	GR

9	Centre Suisse d'Electronique et de Microtechnique	CSEM	CH
10	VECSYS	VECS	FR
11	CANBERRA FRANCE	CANB	FR
12	National Research Council of Italy, Institute of Biomedicine and Molecular Immunology, Palermo	IBIM	IT
13	Crisisplan	CPLAN	NL
14	Commissariat à l'énergie Atomique et aux Energies Alternatives – Laboratoire d'Electronique et des Technologies de l'Information	CEA	FR
15	EULAMPIA Advanced Technologies	EUL	GR
16	INTEC INDUSTRIE-TECHNIK	INTEC	GE
17	PROENGIN	PROEN	FR
Ethical, Social and Legal beneficiaries			
18	Eticas Research & Consulting	ETICAS	ES
19	Vrije Universiteit Brussel	VUB	BE
Expert End-users			
20	Helse Stavanger HF, Stavanger University Hospital - RAKOS	SUH	NO
21	Assistance Publique-Hospitaux de Paris	SAMU	FR
22	Centre for Security Studies	KEMEA	GR
23	Centre de Coordinación Operativa de Catalunya, Departament d'Interior, Generalitat de Catalunya	INT	ES
24	Sistema d'Emergències Mèdiques	SEM	ES
25	Technology Platform – Energy Security	TPEB	CZ
26	Czech Republic-Ministry of Defence- University of Defence	UDB	CZ
27	Military Research Institute	VVU	CZ
28	National Institute for NBC Protection	SUJCHBO	CZ

The Aim of the Project

The risks of terrorist acts using CBRN materials have been for a long time part of the EU´s strategic culture. The EU CBRN Action Plan highlighted the need for coordinated action to prevent, detect, prepare, and respond to CBRN incidents, and the need to put in place new

systems and technologies dealing with multiple 'all hazard' threats to society and critical national infrastructure.

The focus has been largely put on the processes linked with prevention and detection of, and response to CBRN threats. OPTIMUS intends to fill in the gap in a less investigated area of the first response after a CBRN incident. More specifically, OPTIMUS technology focuses on the assessment and treatment of victims on the spot facing CBRN-related attack or accidents. Several current events (f.e. the case of ebola) apparently show a relevancy of this endeavor as well as a need on the part of the medical rescue services to be well prepared and equipped. Therefore OPTIMUS aims at offering a unified system of detection, traceability, triage and individual monitoring of victims on the field which would also be adaptable on all types of hazards and environment hit by the incident.

OPTIMUS project intends to focus on both innovative technologies and related operational processes. More precisely the project is organised along four strategic pillars

Pillar 1: OPTIMUS and its stakeholders

To become successful OPTIMUS innovations have to be tested and later accepted by the targeted stakeholders. Therefore the consortium has been joined a strong group of relevant stakeholders across Europe (while others supported the project through the Letters of Interest) who will be in a permanent interaction with the development team under the coordination of CPLAN. More specifically, OPTIMUS will organize several tests and pilots throughout the project as well as module and system assessment and validation campaigns before the practical pilot demonstrations. Additionally, the consortium will provide a thorough analysis of Pre-Commercial Procurement Scenarios on CBRN response systems.

Pillar 2: OPTIMUS and the Emergency Health Services Operations

Given its nature and potential deployment OPTIMUS will have to effectively address the complex system of crisis management mechanisms. The proposing consortium has already pinpointed the stages in the provision of triage, medical follow-up and hospitalization in which, OPTIMUS can intervene with clear benefit towards, the citizens, the field operatives and the overarching crisis management and search and rescue mechanisms. More specifically, OPTIMUS project will introduce innovative solutions for contamination detection, pre-hospitalisation processes (blood droplet sampling), on field diagnostic processes, or victims´ monitoring.

Pillar 3: OPTIMUS and Technological Excellence

OPTIMUS is centered around innovative technologies in the area of CBRN post-event management. The aim of the project is to design, develop, integrate and deliver a European-wide, end-to-end congruent prototype, to facilitate CBRN-related detection, traceability, triage and individual monitoring of victims providing more effective service in saving the lives of citizens at risk, ensuring minimal casualties among first responders and triage crews, improving drastically the response of the civil authorities and health systems by optimizing the use of the available resources, minimizing the contamination expansion through agile, real-time control, and downsizing the cost of CBRN operations.

Therefore, OPTIMUS will define a full architecture and integrate the necessary technological backbone, designed to provide intelligent data fusion with big-data enablement, seamless interconnection and interoperability between the different system elements and layers eliminating data ambiguity. Peer-to-peer information processing will enable access in a ubiquitous manner by all involved actors. OPTIMUS with its modular and open structure ensures that non-functional requirements like IT security (confidentiality, integrity, and availability), performance, maintainability and serviceability, usability, intra- and inter-operability, testability and cost efficiency, will be fulfilled. OPTIMUS will be based on approved, generally accepted and mature technologies. OPTIMUS will also exploit ICASS platform, a test supporting tool for pre-evaluating and pre-assessing the applicability of all new concepts and technologies introduced within OPTIMUS before being implemented. An enormous advantage is the repeatable and reproducible execution of test runs under approximately the same preconditions. Thus, if the test-object facilitates it, fully automated test runs are feasible. ICASS is independent and executable on every conventional hardware/software system, resource efficient while operating as a stand-alone application. OPTIMUS' technical work is organised along three (3) delivery axes.

Specifically:

A. Victim-specific technologies, systems and services.

- On the spot victim's condition estimate and detection

o A comprehensive diagnosis on the field based on the combination of different sources of information (environmental contamination level, point of care diagnostic tools, handheld CBRN devices, etc.).

o Rapid recording of victim's signs and symptoms, such as respiration rate and systolic blood pressure, directly in the hot zone, using rapidly deployable cooperative body sensors and innovative speech to text applications.

o Automatic and Fast determination of victim's condition based on the execution of the appropriate triage Protocol (START, SORT, etc) electronically via FRs, ergonomically designed to be adapted to extreme working conditions, Information Management Units.

- Biometric identification

o Establish unique victim's identity via rapid collection of victim's biometrics.

o Modality specific: contactless capturing of fingerprint, 3D face and iris on mobile device.

o Ergonomic methodology for minimising time of on-site intervention.

o Unique identifier derived of biometric template generation.

o Encryption of victim's information (biometric, medical etc.), for privacy purposes (Template protection).

- Individual victim monitoring

o Creating a unique medical e-file for each victim from the very beginning of the hospitalization process (hot zone).

o Engaging simple and cost effective electronic tagging system for rapid association of victim's ID with his/her corresponding e-file.

o On the field personalized health monitoring systems to improve medical personnel efficiency in large-scale events, supporting several levels of monitoring, from simple medical triage to real-time un-assisted monitoring of individual victim's vital signs, enabling a dynamic triage approach.

• Victim's population flow tracking

o Determining number and movement flows of (potential) victims via state of the art video analytic methods applied to various video streams originating from cameras installed in UAVs and UGVs as well as CCTV infrastructure.

o Rapid deployment of virtual fencing solutions based on optical fibre technology capable of monitoring the traffic around the polluted area, providing the position and the contamination level of contaminated objects crossing the fence and remotely measuring with high precision the contamination level of specific points of interest. (Obj. fulfilled: D5.3.1)

B. The OPTIMUS centralised operations management system.

• Delivering an advanced Common Operational Picture, tailored to the needs of operations managers by making use of advanced approaches for the simulation and visualization of operations.

• Optimizing the use of available resources (human, infrastructure, medical care units etc.) throughout the generation of optimum crisis management strategies.

• Generation of hospitalization guidelines, FRs early warnings and accurate estimations on crisis evolvement, to improve crisis management and response while reducing risk of cross-contamination between affected and non-affected victims.

C. OPTIMUS as part of an overarching Search and Rescue System.

A System-of-Systems based on the OPTIMUS integrated approach for the performance of triage operations, able to cope with diverse use cases (C,B,R,N), threats and to leverage on existing infrastructure.

• Implement a proper mechanism that will ensure security of private data. OPTIMUS will boast an increased level of security for its constituents, meaning that it will be designed in such a manner to keep its potential vulnerability to a minimum, safeguarding the integrity of the channels and exchanged data. A security by design approach will be put in place to ensure that this critical objective is met.

• Interoperable communications fabric. A resilient and seamless communication platform integrated to the mechanisms already in place, able to support the proper and timely delivery of the gathered data to the different system entities. OPTIMUS will leverage telecommunications networks/systems that are already used in SaR systems in Europe.

• Uniform data exchanges that will enable information sharing across multiple channels, supporting and sustaining the optimal decision making process for key stakeholders.

- Mobile Emergency Operations Centre (MEOC). A concept brought forward since it is currently being adopted in European SaR systems, since its successful demonstration in E-SPONDER (coordinated by EXUS). It provides a common operational picture of the situation as well as a communication bridge between the first responders that operate in the field and the main, remotely located EOC (usually located at Civil Protection Headquarters).

- Cooperative unmanned platforms. The use of COTS mini-UAVs, under the aero-modelling concept bearing proper payloads fulfils the demand of accurate and timely data provision. Through the application of cooperative control algorithms to deliver mini-UAV swarms the OPTIMUS operational capabilities will be further enhanced.

- Perform real-time micro & macro-scale environmental contamination mapping. Use of state-of-the-art sensors (preferably as part of the civil protection threat detection infrastructure) in a cooperative manner will allow full knowledge of the extent and type of contamination in an area by creating contamination maps, that prevent & secure the FRs from unwanted exposure to hazardous substances during the course of their mission.

- Threat propagation predictive models and simulations. This will be a complementary asset that will allow the timely prediction about how an event may evolve & how this might may pose risks of contamination to the citizens.

- FR Health monitoring system: This is a successfully demonstrated concept from E-SPONDER […]. In this case OPTIMUS will be able to monitor the health of FRs on the field in real-time and to seamlessly inform them on any mission-related update.

- Portable Information Management Units: This is the heart of main actors' terminal units (based on E-SPONDER). It provides its bearer with situational awareness (interface, maps, sensor readings etc.), while it manages and processes all the received data. It provides a visual interface to be used by the main actors, hardware interfaces to interconnect and integrate the rest of the mobile system modules and finally the software interfaces necessary for the real-time extraction of the information from the rest of the subsystems of their terminal unit.

Pillar 4: OPTIMUS and the European Society

OPTIMUS will deliver a system that will be capable of improving the detection, traceability, triage and individual monitoring of victims after a mass CBRN incident while developing a set of procedures and technologies that are compliant with privacy and data protection regulations, promote an ethical approach to crisis management and adhere to the principles of responsible research and innovation. This all requires that issues of acceptability, desirability, data management and ethics will be addressed as well as issues relating to policy, training, technology and societal impact will be explored and developed.

OPTIMUS Concept and Approach

OPTIMUS reflects the complexity and diversity of the parameters affecting the response in CBRN incidents and intends to improve most of the solutions and processes in various phases. The main phases of operations can be summarized as follows:

A. Event Identification.

B. Preliminary Situation awareness.

C. On-site Situation awareness assessment and Infrastructure deployment.

D. Initialization of search and rescue operations including hot spot evacuation and on the spot victim's triage.

E. Initialization of medical/decontamination follow-up and victim's monitoring.

F. Completion of victim's triage and initialization of victim's hospitalization processes.

G. Provision of medical treatment.

H. Site decontamination/restoration and remediation.

From this perspective OPTIMUS will mainly address the phases D-F through the creation of an anthropocentric and effective response platform incorporating (improved) technologies and standard operating procedures.

Training, Validation, Pilots and Demonstration

The validation of the OPTIMUS platform will be periodically conducted at the premises of KEMEA's Police Training Centre at Markopoulo, Athens (former 2004 Olympic Shooting Grounds). Within existing infrastructure, a field testing ground will be set up simulating all three operational zones (hot-warm-cold). Specialized CBRN personnel from Hellenic Police, Fire Service and the National Ambulance Service will contribute in the manning of testing field. In this way, all parts of the OPTIMUS project will be tested in real operational environment in order to identify gaps and technical malfunctions of the integrated procedures and systems incorporated.

Chemical incident in Norway

This pilot simulates a chemical train accident in Norway. A freight train collides with a bus on an unsecured crossing. The train, carrying chemicals including ammonia and acrylonitrile, derails and catches on fire. One of the carts begins to leak. The nearby water is potable water for the municipality and risks becoming infected. An unknown number of passengers were onboard the bus. They are believed to be severely injured or dead. The pilot will test procedures, technology on triage and coping with the incidents, observing the injured persons in several stages, such as in the hot zone, decontamination, transportation to the hospital, and within the hospital itself. The coping on-scene is vital, and technology and procedures of situation assessment, cooperation and leadership will be tested. The pilot will take place in the Western part of Sandnes, near Ganddal station. This location is ca. 200m from the incident, ca. 3 km from the nearest Fire and Ambulance Station, and ca. 4 km from the city Centre and the nearest police station. Aprox. 250 persons will participate, consisting of members of the fire department (30), police (30), ambulance service (30), Stavanger University Hospital (40), Civil Defense (30), NGO (20), Joint Rescue Coordination Centre South Norway, Stavanger (5), Helicopter Squadron (6), air ambulance (3), municipalities and doctors watch Centre (50), County administration (5) and Norwegian CBRN Centre (3). OPTIMUS is expected to provide technological tools to assess the severity and extent of the spread and type of chemical agents, to facilitate the protection of first responders and civilians, and to improve the triage and management of the affected people.

Biological incident in the Czech Republic

A group of tourists went to South-western China, visiting the "authentic" and rural places (e.g. local markets) and sampling local food. By the end of the tour about 10 members of the group started to experience mild symptoms of upper respiratory infection, such as mild fever, muscular and joint pains, sore throat and dry cough. On the day of departure their symptoms worsened. Two members experienced fever of 38 C and higher and severe cough. During the flight back the cough worsened even more and the patients progressed towards a respiratory in sufficiency. During the flight the attendants recognized more than 20 passengers altogether having some kind of respiratory symptoms and reported a suspicion of a transmissible disease. According to the IATA rules, their suspicion was reported to the ground personnel, who alerted the Department of Public Health (DPH). After the arrival to the airport in Prague, the passengers showing any of the symptoms were isolated in the designated isolation room. The DPH evaluated both the epidemiological and clinical data and, based on that, declared a suspicion of highly communicable disease and alerted the integral rescue system. Due to the fast progression of the disease and a relatively short incubation time, a ricin poisoning cannot be ruled out.

The pilot test will take place in the Department of Biological Defense in Techonin, CZ, with nearly 100 participants, both civilian and military. These include DPH officials (3), Fire Brigade (13), Mobile Bio-Transport from the CZ Army (4), Medical Rescue Unit (6), Dept of Biological Defense (6), Specialized Hospital staff (8), Military Health Sciences staff personnel (10) and students (20), Police (2), Military Police (2) and observers (10). OPTIMUS tools will be used for ricin detection; monitoring and identification of patients in the individual transport isolation devices; monitoring and transfer of the individual patient`s data to the commanding personnel; GPS monitoring of the patients and contaminated waste; communication with the Specialized Hospital; monitoring of the vital data by the hospital physician; and prioritization of transport of the individual patients based on the severity of their symptoms.

Radiological incident in Spain

This case involves a container containing scrap metal and a radioactive device. The container gets stolen by a small group of delinquents, who want to sell the metal on the black market. An old tele-therapy device (which is radioactive), coming from a country with minimal control over high radioactive sources, is dismantled by the thieves and part of the Cs-137 salt is released into one of their backyards, situated in a suburb of Barcelona. Radioactive material spreads throughout the neighborhood due to strong winds. Four days later one of the thieves is diagnosed with severe radiation exposure by hospital staff, who call civil protection authorities and warn them of a possible radiological emergency in the neighborhood where the patient lives. Some 5,000 inhabitants have to be checked for contamination, which results in panic amongst civilians. Health emergency services, radiological experts, fire fighters and other first responders work together on site. In the end 200 persons are contaminated (180 externally, 20 externally and internally). INT manages the incident according to the emergency plan for radiological emergencies, which was approved by the Catalan regional government and validated by the Spanish Nuclear Safety Council. OPTIMUS is expected to provide technological tools to assess the severity and extent of the radiological contamination, to facilitate the protection of FRs & civilians, and improve the triage & management of the affected people.

Nuclear/ Radiological incident in France

SAMU will conduct a pilot test based on a nuclear/radiological event within the OPTIMUS project. This drill simulates a bomb explosion in a French train station while passengers are boarding a train, resulting in many victims. Radiological material is detected. Ca. 500 persons will take part in this drill, consisting of 200 victims, first responders (50 firemen/rescuers), out of hospital medical responders from SAMU (50), SAMU hospital medical responders (15), police officers/gendarmes (20), and several other services such as workers on the train station, the French society of railway (SNCF), and city employees for electricity and gas services (30). The drill will take place in a railway station on French territory. All actions are performed according to the ORSEC plan (rules into force on the French territory). All state services are coordinated by the civil defense zone; health actions will be coordinated by the regional health agency and zonal SAMU coordination will be performed by SAMU de PARIS. The medical actions, such as victim categorization, extraction and transportation, decontamination, and other medical treatments including hospital care will be tested during the simulation, making use of the OPTIMUS devices and techniques which will be evaluated according to the demands of the leaders involved in the project.

TPEB´s Involvement

In case the project gets supported TPEB will step in performing exploitation and dissemination role connected with the initiatives linked particularly with the end-users. TPEB will also organise several workshops in EU institutions and NATO. Additionally, TPEB will also offer experts from the Office for Standards, Metrology, and Testing from the Defence Standardisation, Codification, and Government Quality Assurance Authority assessing the current standardisation landscape and suggesting and developing both civil and military standardisation strategies.

Koordinace aktivit v rámci inovačního managementu (projekt na obecné úrovni spojující všechny čtyři oblasti)

1st Workshop on Coordinating the EU R&D&I initiatives in the area of security in Visegrad

Project Description

The aim of the project is to stimulate V4 cooperation in the area of H2020 research and innovation projects in the field of SECURITY. The intention is to bolster awareness about the H2020 potential particularly among the enterprises with R&D capabilities. After organizing the initial event the project should result in the permanent V4 innovative management structure which would enhance cooperation while utilizing regional proximity in establishing consortia applying for H2020 projects.

The statistics of the V4 countries´ involvement in the previous Framework Programmes show that there is a growing ability of the research institutions to participate on or even lead European consortia. However, the awareness about the H2020 potential among the enterprises with R&D capabilities is rather low. This is particularly problematic since after the evaluation of the Framework Programmes operated during the last EU budgetary period the European Commission has underlined that H2020 projects should be oriented on tangible innovations and technologies that would be directly put in practice. Needless to say that external support for R&D sector in all V4 countries is of their vital interest.

The project has two interlinked goals. Firstly, the consortium will organize the workshop where the consortium members and H2020 SECURITY National Points of Contact (see the Letters of Support attached to this application) will share national experience with and outline the cooperative potential for the V4 enterprises and research institutions. The discussion will be also enriched by invited guest speakers from the European institutions that have a great experience with EU security-related programmes (ISPRA, TNO, DELTA). The event should bolster awareness and instigate the interest among the companies to invest their energy into EU innovative projects.

Secondly, following the event the consortium members will establish a permanent cooperative platform aiming for building strong regionally based consortia providing relevant partnerships or even leadership roles in projects applications for H2020.

The primary target groups are enterprises with R&D potential and research institutions operating in the field of security that could largely benefit from the H2020 projects. However, it should be also stressed that the support for R&D initiatives is repeatedly declared by the governments and included in various strategic documents. At the same time all V4 countries have a great potential in raising their profiles in the EU (research) initiatives. Last but not least national security is becoming more and more technologically demanding while it is essential for all V4 countries to utilize their own potential and not only follow the technological developments of the more developed part of the EU. The support provided by

the National Points of Contact confirms that V4 regional cooperation is potentially meaningful and effective.

Consortium

TPEB is the PPP platform involved in several project applications including three H2020 projects dealing with access control, CBRN detection and hospitalization guidelines, and digital security. BHE belongs among the most successful Hungarian companies utilizing the EU R&D projects support in the security-related areas. It is a strong case of successful company developing its R&D potential through innovative projects. Warsaw University of Technology is the Polish top technical school having large experience with international research projects. The university represents the research pole in our intentionally diverse consortium. Addsen is the most efficient Slovak institution capitalizing on the experience with more than 25 applications and 7 supported project under the FP 7 scheme.

Future expectations

The ultimate aim of the project is to stimulate regional cooperation among the relevant stakeholders resulting in increasing number of H2020 (security) and potentially other EU RDI-oriented projects applications. The consortium assumes that other efficient partners will join the permanent platform, which should be run through a common website and projects-related cooperative meetings. In this sense the project is oriented the long-term future cooperation. Through supporting the initial activity the Visegrad Fund would remain one of the founding pillars of the permanent platform.

Projekt Zajištění vzdělávacích a podpůrných služeb včetně e-learningu

Projekt se zaměřoval na poskytnutí komplexního vzdělání v energetice a přidružených oblastech souvisejících s kritickou infrastrukturou. Role TPEB byla spojena s organizací a koordinací odborných kurzů v této oblasti, které by byly vyučovány na členských institucích TPEB (především Vysoké škole báňské v Ostravě a Vysokém učením technickém v Brně. Vzhledem ke vzdělávacímu charakteru a v daném segmentu k expertním školením byl projekt zcela v souladu s dlouhodobým posláním TPEB.

Další aktivity a výsledky III. etapy

Projektový Kulatý stůl

Dne 26. června 2014 pořádala Technologická platforma Energetická bezpečnost ČR kulatý stůl v hotelu Troja, Trojská 1/2232 na Praze 8. Kulatého stolu se zúčastnili členové platformy včetně representantů GŘ ZHS gen. Svobody a plk. Chalupy a hosté z ÚNMZ pan ředitel Kratochvíl a Ing. Kubeš a Technologického centra Akademie věd České republiky Ing. Hillerová. Cílem kulatého stolu byla prezentace výsledků II. etapy projektu Energetická a kybernetická bezpečnost ČR. Současně byly presentovány aktivity TPEB ČR za období prvního půlroku 2014.

Dále byly představeny podané a plánované projekty, jak tuzemské, tak zahraniční, které TPEB ČR, ve spolupráci se svými členy a tuzemskými a zahraničními partnery realizuje. Manažer projektu, JUDr. Richard Hlavatý a členové realizačního týmu (doc. Ing. Jindřich Ploch, CSc., Prof. Dr. Ing. Zbyněk Raida, Ph.D. a PhDr. Vít Střítecký, M.Phil., Ph.D.) informovali o průběhu příprav těchto projektů a o možnostech dalšího zapojení členů platformy využitím spolupráce s realizačním týmem projektu na přípravě, zpracování a podání projektové žádosti, vytvoření nebo zapojení do konsorcií, získání kontaktů z jiných zemí a vytipování a prověření potencionálních partnerů.

V rámci kulatého stolu vystoupila také Ing. Eva Hillerová, která prezentovala aktivity Technologického centra Akademie věd v souvislosti s aktuálním programem Horizont 2020, kde je technologické centrum národním kontaktním místem pro českou republiku a účastníci kulatého stolu byli seznámeni s poradenstvím pro instituce a firmy, které technologické centrum v této souvislosti nabízí a poskytuje.

Dalším bodem programu byla informace o přípravě konference v rámci realizace projektu v Poslanecké sněmovně Parlamentu České republiky na téma " Úloha a možnosti TPEB ČR v oblasti průmyslové energetické a kybernetické bezpečnosti a ochrany kritické infrastruktury „„ která se bude konat v září 2014.

Účast na zahraničních fórech

Vedoucí projektu, JUDr. Richard Hlavatý, se v květnu 2014 na pozvání European Organisation of Security, se kterou TPEB dlouhodobě spolupracuje, zúčastnil konference skupiny Archimedes s názvem "Establishing a European Network of National Organisations for Security" pořádané řeckým předsednictvím v Radě EU v Aténách. TPEB presentovala za Českou republiku aktivity v oblasti energetické a kybernetické bezpečnosti a ochrany kritické infrastruktury. Jedním z cílů setkání bylo vytvoření konsorcií pro projekty Horizont 2020 – Security a podávání společných projektů a jejich prosazování pro komerční využití. V návaznosti na toto jednání TPEB vstoupila do jednoho projektového konsorcia (OPTIMUS)

a další připravuje. Podobné jednání absolvoval dr. Hlavatý ve sejný měsíc také DG JRC v Ispře.

Účast na domácích konferencích a podobných akcích

Dr. Hlavatý zastupoval TPEB na mezinárodní konferenci **Kybernetická bezpečnost a současné komunikační technologie**, která se konala 30. ledna v Brně. Cílem konference, které se zúčastnilo více než 100 odborníků z celého světa, bylo prezentovat aktivity v oblasti kybernetické bezpečnosti v evropských zemích, na českých univerzitách a v českých firmách. Konference měla ambici pootevřít dveře vzájemné spolupráci všech uvedených subjektů, kde v dané oblasti hraje TPEB stále významnější roli.

Dr. Hlavatý zastupoval TPEB na velkém česko-německém cvičení, jehož hlavním pořadatelem byla společnost ČEPS, a.s., člen TPEB. Unikátní společné mezinárodní **bezpečnostní cvičení DRILL 2014**, které proběhlo 16. 9. 2014 v blízkosti státních hranic nedaleko Hory sv. Šebestiána, vyzkoušelo spolupráci více než 200 profesionálů z obou zemí. Společně se podíleli na náročné realizaci stavby náhradního přeshraničního elektrického vedení, které spojuje sítě společností ČEPS a 50Hertz. Cvičení DRILL 2014 simulovalo extrémní situaci, kdy může dojít k selhání některé technické části elektrické sítě, například k pádu stožáru. Krizovou situaci, kterou scénář cvičení připravil, řešili desítky odborníků z energetických společností ČEPS a 50Hertz. Povolány byly dva vrtulníky. Zasahoval zde vrtulník Policie ČR, který pomáhal hasit požár v blízkosti vedení. Vrtulník Armády ČR pak kvůli nepřístupnému terénu dopravoval části konstrukce nových stožárů na místo stavby. Při vztyčování stožárů asistovaly tři jeřáby. Celá akce se neobešla bez desítek zásahových vozů záchranných složek obou zemí.

Dr. Hlavatý také vystoupil na konferenci **Most energetika 2014**, která se konala pod záštitou Ministerstva průmyslu a obchodu. Ročník 2014 se zabýval hlavně významem a praktickým dopadem Státní energetické koncepce ve vazbě na Státní surovinovou politiku ČR, energetickou a kybernetickou bezpečností a významem domácích surovin na pozadí politické krize na Ukrajině. Dr. Hlavatý na konferenci prezentoval vize a aktivity TPEB ve vazbě na právě řešené projekty.

Zástupci TPEB se v dalších týdnech zúčastní konferencí *Cybersecurity 2014*, kterou organizuje společnost IDG Czech Republic, a.s. společně se společnostní Microsoft a XX. ročníku konference *SmartWorld*, kterou organizuje společnost Monet+, která vstoupil do jedné z projektových žádostí v rámci programu H2020.

Budoucí aktivity a výhled do IV. Etapy

Jak už bylo několikrát zmíněno, TPEB bude nadále pokračovat v aktivním formování výzkumných, vývojových a inovativních konsorcií a podávání projektových žádostí. Stáe ještě v rámci III. etapy došlo k přípravě několika projektů, které budou podány v návaznosti na výzvy.

TAČR

Vývoj a aplikace metod behaviorální analýzy při fyzické ochraně letišť a dalších objektů kritické infrastruktury

Cíl projektu:
Na základě cílů, definovaných v „Národním bezpečnostním programu“ ministerstva dopravy České republiky, je žádoucí vytvořit podmínky pro dosažení zvýšení efektivity bezpečnostních kontrol na letištích využitím nově koncipované metodiky přípravy pracovníků bezpečnostních kontrol. Předpokladem úspěšné realizace je navázání výzkumu na poznatky ukončeného evropského projektu „Behaviorální modelování pro bezpečnost na letištích“ BEMOSA (Behavioral Modelling for Security in Airports) a jejich důsledné rozpracování do konkrétních cílu pro provozní praxi.

Specificky se bude jednat o:

- sestavení standardizovaného výcvikového programu pro pracovníky bezpečnostních kontrol na letišti (s možností aplikace i na další objekty kritické infrastruktury). Zpracovaný výcvikový program bude orientován jako součást národního bezpečnostního programu výcviku (NBPV) s možností aplikace i do jiných zemí do členských států EU.

- vývoj a aplikace softwaru pro identifikaci primárních vlastností uchazeče o pracovní pozici pracovníka bezpečnostní kontroly na letišti

- návrh technologií vhodných pro aplikaci do systému pro behaviorální analýzu cestujících před vlastním provedením bezpečnostní kontroly, včetně jejich funkčních ověření v provozu

Cílem projektu tedy bude vytvoření komplexního návrhu pro kvalifikovaný výběr a výcvik pracovníků schopných provádět analýzu chování cestujících pro potřeby perspektivních kontrolních bezpečnostních stanovišť (Checkopoint of the Future) na provozní úrovni letišť v Evropě a České republice na takové úrovni, aby se navrhovaná metoda mohla stát standardem pro členské státy EU případně i pro další státy.

Problematiku kvalifikovaného výběru a výcviku bezpečnostních pracovníků pak rozpracovat do úrovně použitelné i v jiných oblastech, využívajících bezpečnostní kontrolu osob, zejména i u jiných módů osobní dopravy a dalších objektů kritické infrastruktury. Novost navrhovaného řešení spočívá v očekávané změně přístupu bezpečnostních pracovníků k

prováděnému procesu kontroly a tím i k očekávanému zvýšení míry bezpečnosti při provádění bezpečnostních kontrol. Projekt předpokládá vytvoření výcvikového programu pracovníků bezpečnostní kontroly začleněním behaviorální analýzy. Po vytvoření adekvátního výcvikového programu, jeho ověření v praxi bude tento program předložen k certifikaci a začlenění do NBPV jako standard pro výcvik vybraných pracovních pozic na letištích a obdobných institucí. Aplikace principu behaviorální analýzy tak vytváří podmínky pro zabezpečení dosažení mnohem vyšší úrovně okamžitéhohodnocení potenciálních hrozeb a rizik. Prioritní oblast řešení projektu bude zaměřená na bezpečnost těch částí infrastruktury a zdrojů, zejména v oblasti dopravy a dalších kritických zařízení, ve kterých musí být pokryta bezpečnostobyvatelstva prostředky a postupy, zahrnujícími ochranu před organizovanou kriminalitou, extremizmem a terorizmem.

Kybernetické zabezpečení malé a střední firmy

Projekt bude koordinován ze strany TPEB a bude směřovat d programu TAČR Epsilon, podprogramu *Znalostní ekonomika*.

Abstrakt: Hrozbám kybernetických útoků a souvisejícímu ohrožení kritických infrastruktur je kvůli jejich vzrůstající intenzitě věnována stále větší pozornost. Kvalitní zabezpečení si však mohou zajistit pouze velké a ekonomicky silné firmy. V případě malých firem pak není zabezpečení proti kybernetickým hrozbám dostatečné. Proto chceme v rámci předkládaného projektu vypracovat metodický rámec, který malým a středním firmám umožní zvýšit svou kybernetickou bezpečnost vhodnou organizací zabezpečení infrastruktury, eliminací chyb a úmyslného poškození kybernetické ochrany vlastními zaměstnanci. Metodický rámec bude implementován formou modulární softwarové aplikace.

H2020

Přestože lze očekávat více projektových žádostí, v rámci třetí etapy TPEB vstoupila do konsorcia, které s jistotou odpoví na projektovou výzvu DS-2-2014: Digital Security: Cybersecurity, Privacy, and Trust – ACCESS CONTROL.

Cíl projektu Access Control

The project will cover the design, development and implementation of strong access-control technologies for critical infrastructures such as power plants, airports and datacenters. The project will include extensive evaluation of available smart-card and smart-phone platforms and their security analysis including side-channel analysis. On proven hardware, cryptographic authentication protocols based on provable security principles will be implemented. New approaches based on contemporary cryptography will be applied. The supporting software, necessary for system integration into existing systems will be

implemented and tested. The resulting system will be evaluated by security experts and verified and deployed in real-life infrastructures with high security demands.

COST – European Cooperation in Science and Technology

TPEB v rámci III. etapy iniciovala práci na programu Akce COST, která slouží k vytváření sítí vzájemné spolupráce mezi výzkumnými subjekty Evropské Unie a zemí, které k iniciativě COST přistoupily (např. Švýcarsko, země bývalé Jugoslávie, Kanada, USA). Akce je vždy zaměřena na určité výzkumné téma. Financovány jsou společné workshopy, stáže mladých vědců, letní školy a další aktivity mezinárodní mobility. Samotný výzkum financují ze svých zdrojů samotné země iniciativy COST. V případě České republiky je výzkum financován v rámci programu COST CZ, který administruje Ministerstvo školství, mládeže a tělovýchovy (MŠMT).

Jelikož každou Akci COST typicky tvoří 40 až 60 výzkumných subjektů (univerzity, výzkumné ústavy, firmy), jsou tyto Akce jedinečnou platformou k vytváření konsorcií mezinárodních projektů a spoluprací. Financována je vždy účast nevýše dvou účastníků z jedné členské země COST.

Seznam běžících Akcí COST je dostupný na adrese http://www.cost.eu/domains_actions. Komunikační systémy přitom mají vlastní doménu *Information and Communication Technologies* (ICT). Komunikační technologie se rovněž objevují v Akcích, které zasahují do více domén (tzv. *Trans-Domain Actions*, TD).

Pokud má český subjekt zájem připojit se k běžící Akci COST, postupuje podle pokynů uvedených na webové stránce http://www.msmt.cz/vyzkum-a-vyvoj/jak-podat-projekt-cost. Je-li soulad plánovaného výzkumu kompatibilní s Akcí COST, MŠMT požádá českého velvyslance v Bruselu o podpis Memoranda o porozumění, čímž je přidružení k Akci COST oficiálně potvrzeno.

Z běžících Akcí COST přitom k výzkumu bezpečnostních aplikací, ochraně kritických infrastruktur, ochraně obyvatelstva a souvisejícím tématům přispívají:

- **TD10**01 | Novel and reliable optical fiber sensor systems for future security and safety applications
  15 November 2010 - 14 November 2014
- **IC11**06 | Integrating biometrics and forensics for the digital age
  14 March 2012 - 13 March 2016
- **TD12**02 | Mapping and the citizen sensor
  28 November 2012 - 27 November 2016
- **IC12**04 | Trustworthy manufacturing and utilization of secure devices
  12 December 2012 - 11 December 2016

- **IC12**06 | De-identification for privacy protection in multimedia content 26 March 2013 - 25 March 2017
- **IC13**04 | Autonomous control for a reliable internet of services 14 November 2013 - 13 November 2017
- **IC13**06 | Cryptography for secure digital interaction 07 April 2014 - 06 April 2018
- **IC14**02 | Runtime verification beyond monitoring 26 September 2014 - 14 May 2018
- **IC14**03 | Cryptanalysis of ubiquitous computing systems 26 September 2014 - 13 May 2018
- **IC14**04 | Multi-paradigm modelling for cyber-physical systems 26 September 2014 - 13 May 2018