mission

The Laboratory of Cryptography and System Security (aka CrySyS Lab, Budapest) is committed

- to carry out internationally recognized, high quality **research on security and privacy in computer networks and systems**, and
- to **teach network and system security, privacy, and applied cryptography** in the context of university courses, laboratory exercises, and different student projects.

The lab also provides consulting services upon request, including ethical hacking and security audits, design of secure protocols and system architectures, technical assistance in incident response, malware analysis, threat evaluation, and risk management.

We strongly believe in problem driven, project oriented research, therefore, we put emphasis on participating in R&D projects, where we collaborate with industrial partners and academic institutions, and maintain strong international connections.

members

Faculty members

Dr. Levente Buttyán, associate professor, head of the lab
Dr. Boldizsár Bencsáth, assistant professor
Dr. Márk Félegyházi, assistant professor
Dr. Tamás Holczer, assistant professor

PhD students

Gábor Gulyás (research on privacy)
Gábor Pék (research on malware detection and secure virtualization)

Associate members

Gábor Molnár, Ukatemi Technologies
Tamás Koczka, Tresorit
János Szurdi, Carnegie Mellon University
Dr. István Vajda, BME-HIT

+ members of the **CrySyS Student Core**
+ students working on their semester or diploma projects

current teaching

Our current courses include some base courses given to a large population of students, a set of focused courses given in the context of the MSc Specialization on Security of Communication Systems, and a set of elective courses:

Base course on Computer Networking:
:: Computer Networking (Info BSc, in German) (M. Félegyházi)

Base courses on Information Security:
:: Information Security (Info MSc) (I. Vajda, L. Buttyán, B. Bencsáth)
:: Information Security (EconInfo MSc) (I. Vajda, L. Buttyán, B. Bencsáth)

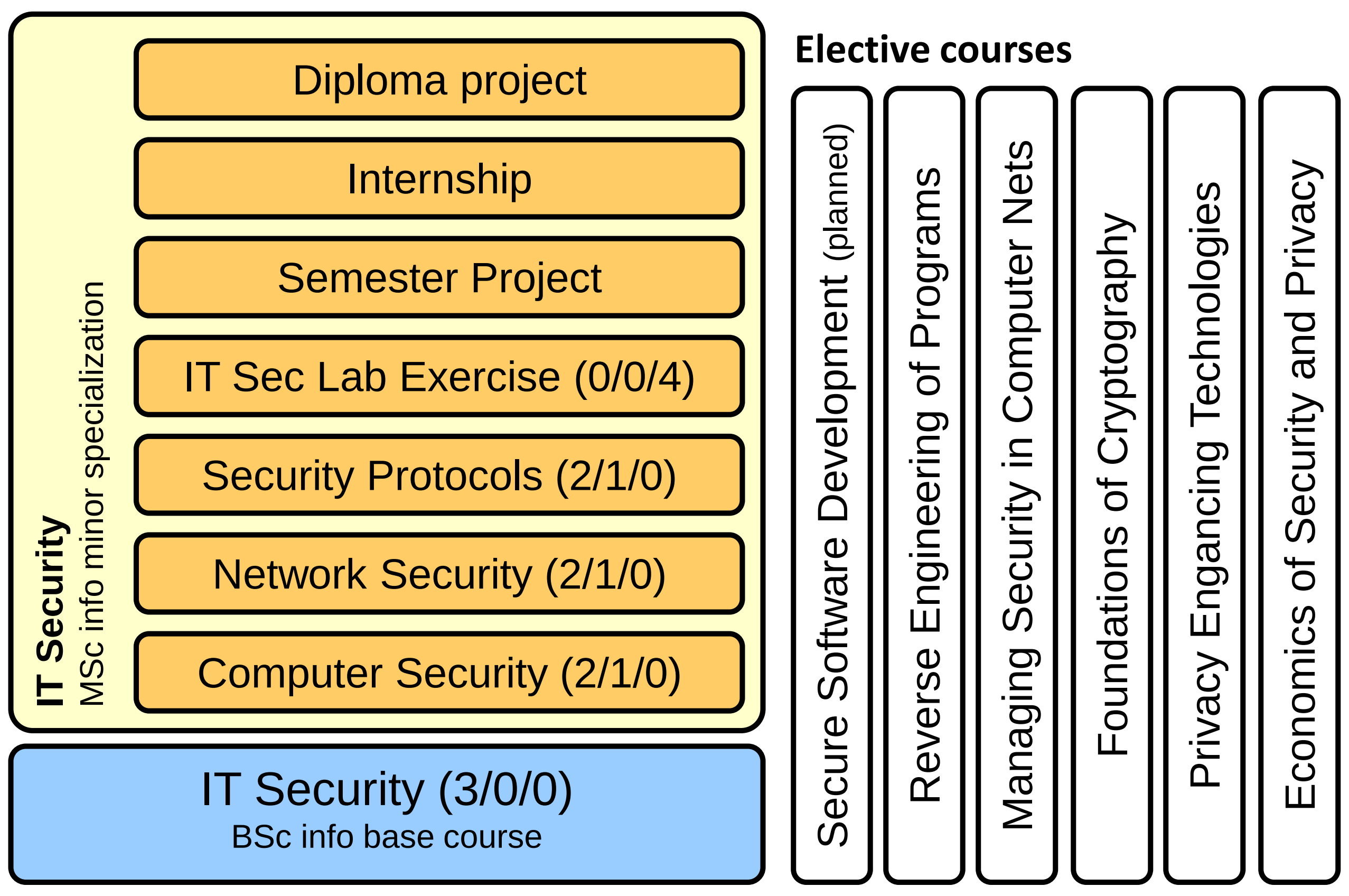
Special on Security of Communication Systems:
:: Cryptography and its applications (I. Vajda)
:: Security protocols (L. Buttyán)
:: Foundations of secure e-commerce (L. Buttyán)
+ laboratory exercises, semester and diploma projects

Elective courses:
:: Network security in practice (B. Bencsáth)
:: Economics of security and privacy (M. Félegyházi)
:: Privacy enhancing technologies (G. Gulyás)
:: Managing security in computer networks (M. Félegyházi, T. Holczer)

We also supervise a large number of laboratory exercises, as well as student semester and diploma projects. Our students won 1st, 2nd, and 3rd prizes multiple times on the annual student scientific conference (TDK) organized by the university.

future teaching

As of 2015, we start teaching according to the freshly re-designed BSc and MSc programs of the Faculty of Electrical Engineering and Computer Science. In these new programs, we will teach a BSc base course on IT Security and we will run an MSc minor specialization on IT Security with courses on Computer Security, Network Security, and Security Protocols. A number of elective courses on special aspects of security and privacy will complement the mandatory courses of the minor. With this new educational structure, all teaching of IT security at BME will be concentrated within the CrySyS Lab.



IT Security
MSc info minor specialization

Diploma project
Internship
Semester Project
IT Sec Lab Exercise (0/0/4)
Security Protocols (2/1/0)
Network Security (2/1/0)
Computer Security (2/1/0)

IT Security (3/0/0)
BSc info base course

Elective courses

Secure Software Development (planned)
Reverse Engineering of Programs
Managing Security in Computer Nets
Foundations of Cryptography
Privacy Engancing Technologies
Economics of Security and Privacy

talent management

We pay special attention to attract and work with students interested in IT security. To discover talented students, we organize the annual **CrySyS Security Challenge**, which is a hacking contest with exciting problems to solve. For students, the Sec Challenge provides a platform for „learning by doing"; for us, it is a vehicle to discover the best students in hacking.

Those who achieve an outstanding result in the Sec Challenge are invited to join the **CrySyS Student Core**, which is an invite only club, where young IT security professionals discuss ideas, expand their knowledge, prepare for international hacking contests, socialize, and amuse themselves. The Student Core, which has around a dozen members, also helps us in teaching activities, as well as in the organization of the annual CrySyS Sec Challenge.

Student Core members often team up to participate on international hacking contests (e.g., Capture-the-Flag games) under the team name of **!SpamAndHex**. They have achieved extraordinary results at many occasions:

:: CSAW 2013: 12th position out of 1378 teams
:: iCTF 2013: 2nd position out of 123 teams
:: PlaidCTF 2014: 17th position out of 867 teams
:: DefCon 2014 qualifier: 24th position out of 402 teams
:: Pwnium CTF 2014: 13th position out of 912 teams

and currently maintain the precious 20th position in the general ranking of all CTF teams around world.

PhD graduates

We strongly encourage students who have affinity for research to join us as PhD students and participate in our research projects.

In the past ten years, the following persons obtained their PhD degree in the lab and received the **CrySyS Steel Ring for PhD Graduates**:

:: Dr. István Zsolt Berta (2005) (currently with Citi Bank, Hungary)
:: Dr. Péter Schaffer (2009) (currently with Ernst&Young, Luxemburg)
:: Dr. Gergely Ács (2009) (currently with INRIA Rhones-Alpes, France)
:: Dr. Boldizsár Bencsáth (2010) (currently with CrySyS Lab, Budapest)
:: Dr. László Dóra (2011) (currently with Citi Bank, Hungary)
:: Dr. Tamás Holczer (2013) (currently with CrySyS Lab, Budapest)
:: Dr. Vinh Thong Ta (2014) (currently with INRIA Lyon, France)
:: Dr. Áron Lászka (2014) (currently with Vanderbilt University, USA)

past projects

In the past, our research focused on security and privacy in wireless embedded networks (such as sensor networks, vehicular networks, mesh networks, RFID systems) as well as on economics of security. We have been involved in a number of **international projects**:

SeVeCom
Secure Vehicle Communications (www.sevecom.org)
(EU STREP, supervised by L. Buttyán)

UbiSec&Sens
Ubiquitous Sensing and Security (www.ist-ubisecsens.org)
(EU STREP, supervised by L. Buttyán)

WSAN4CIP
Wireless Sensor Networks for Critical Infrastructure Protection (www.wsan4cip.eu)
(EU STREP, supervised by L. Buttyán)

EU-MESH
Enhanced, Ubiquitous, and Dependable Broadband Access using MESH Networks (www.eu-mesh.eu)
(EU STREP, supervised by L. Buttyán)

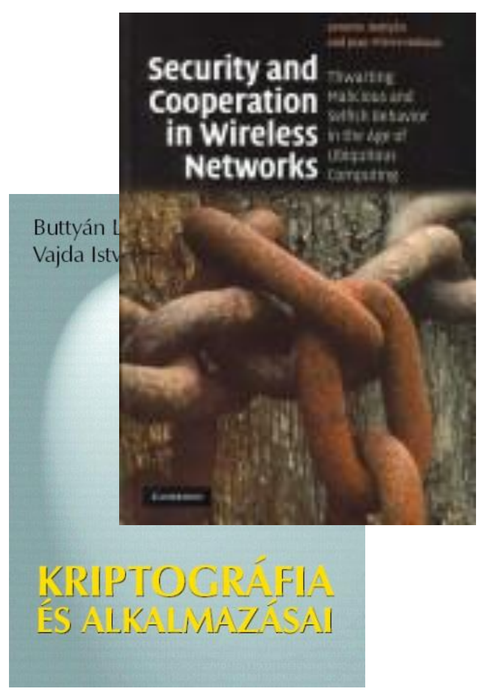
CHIRON
Cyclic and Person Centric Health Management
(www.chiron-project.eu)
(ARTEMIS IP, supervised by L. Buttyán and R. Schulz)

Some **national projects** in the past:
Smart Card Based Electronic ID (HUNEID), Security and Privacy in Ubiquitous Computing, Mobility Supporting Security Architectures

publications

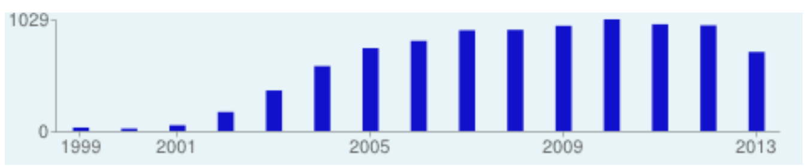
In the academic research community, the quality of research is often measured in terms of number and quality of publications, as well as in terms of number of independent citations. We are proud of our colleagues who have strong publication records and are outstanding according to the above measures. Our colleagues published:

7 books
10 book chapters
~80 international journal papers, including
:: 12 papers in IEEE Transactions
:: 2 papers in ACM Computing Surveys
~120 international conference papers
:: mostly IEEE and ACM
2 Internet Drafts
5 patent submissions

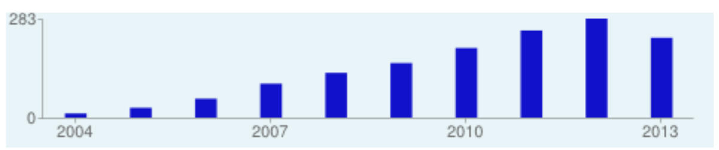

Security and Cooperation in Wireless Networks
Buttyán L
Vajda Ist
KRIPTOGRÁFIA ÉS ALKALMAZÁSAI

According to Google Scholar, the total number of independent citations to our papers is ~11000. The statistics of the most cited authors are the following:

Levente Buttyán
:: citations: 10430
:: h-index: 40



Márk Félegyházi
:: citations: 1373
:: h-index: 18



targeted malware

In the recent past, our laboratory participated in a number of investigations, aiming at identifying and analyzing targeted malware samples that were used for the purpose of cyber espionage:

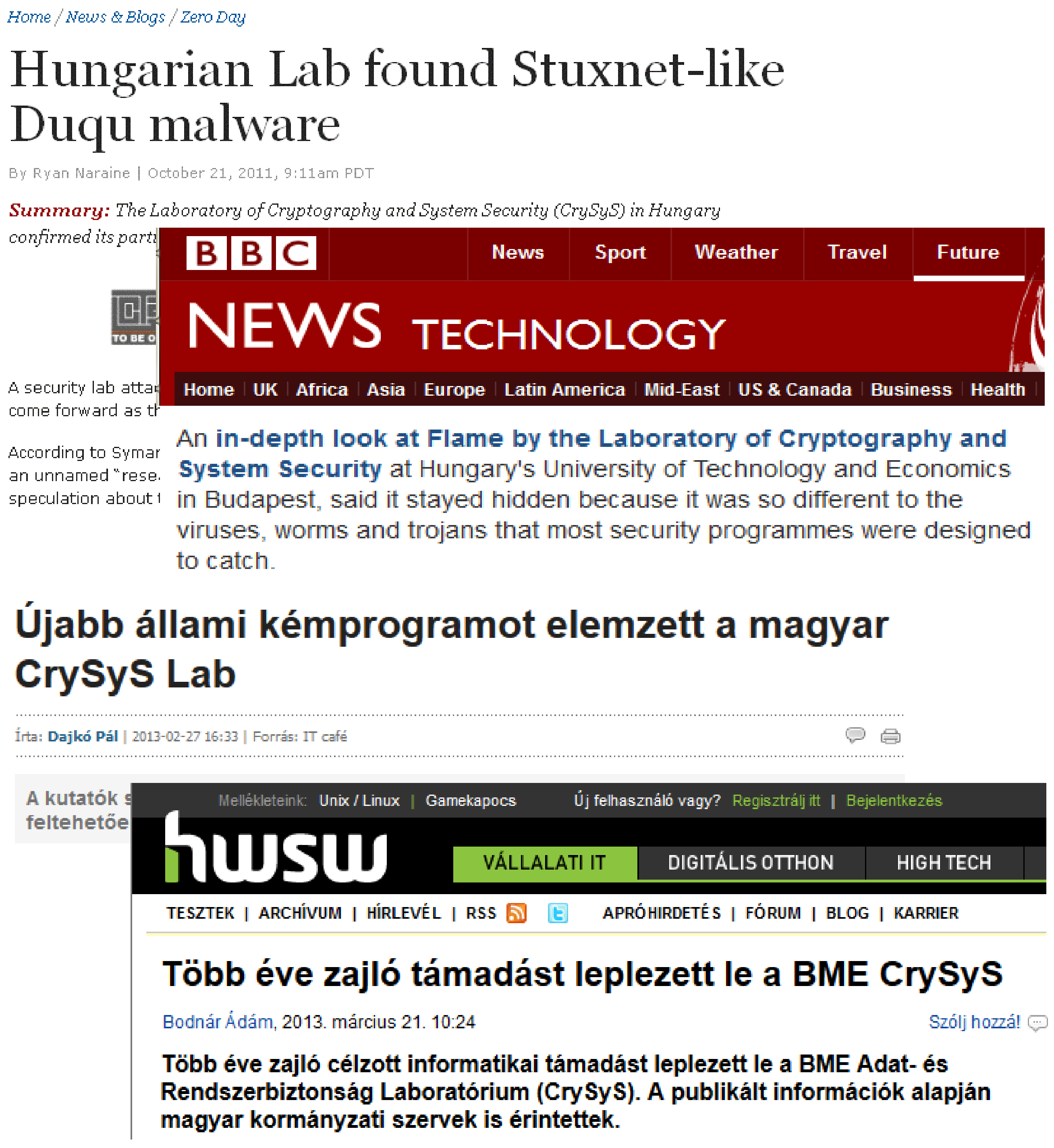
Duqu [October 2011]
:: discovery, naming, and first detailed analysis of Duqu
striking similarities to Stuxnet, but different mission (espionage)
number of known victims is ~20
:: identification of the dropper
0-day Windows kernel exploit (in embedded font parsing)
:: development of the Duqu Detector Toolkit
open source, heuristic anomaly detector
detects Duqu and Stuxnet

Flame [May 2012]
:: first detailed technical analysis of Flame (aka Flamer)
another info-stealer used in the Middle-East
uses a fake certificate to appear as a Windows Update proxy
needed MD5 hash collision attack

Miniduke [February 2013]
:: first detailed technical analysis in collaboration with Kaspersky
yet another infostealer targeting governmental entities and human right organizations in Europe

TeamSpy [March 2013]
:: strong involvement in the investigation efforts and first detailed technical analysis of the malicious toolkit named TeamSpy
set of malicious spying tools that have been used in multiple attack campaigns against high-profile targets

media coverage



Home / News & Blogs / Zero Day

Hungarian Lab found Stuxnet-like Duqu malware

By Ryan Naraine | October 21, 2011, 9:11am PDT

Summary: The Laboratory of Cryptography and System Security (CrySyS) in Hungary confirmed its parti

A security lab atta
come forward as th

According to Symar
an unnamed "rese.
speculation about t

An **in-depth look at Flame by the Laboratory of Cryptography and System Security** at Hungary's University of Technology and Economics in Budapest, said it stayed hidden because it was so different to the viruses, worms and trojans that most security programmes were designed to catch.

Újabb állami kémprogramot elemzett a magyar CrySyS Lab

Írta: Dajkó Pál | 2013-02-27 16:33 | Forrás: IT café

A kutatók s
feltehetőe

Mellékleteink: Unix / Linux | Gamekapocs
Új felhasználó vagy? Regisztrálj itt | Bejelentkezés
hwsw
VÁLLALATI IT
DIGITÁLIS OTTHON
HIGH TECH
TESZTEK | ARCHÍVUM | HÍRLEVÉL | RSS
APRÓHIRDETÉS | FÓRUM | BLOG | KARRIER

Több éve zajló támadást leplezett le a BME CrySyS

Bodnár Ádám, 2013. március 21. 10:24
Szólj hozzá!

Több éve zajló célzott informatikai támadást leplezett le a BME Adat- és Rendszerbiztonság Laboratórium (CrySyS). A publikált információk alapján magyar kormányzati szervek is érintettek.

recent projects

In recent years, the world has witnessed a series of high-profile targeted attacks against various targets, including organizations that operate industrial control systems and critical infrastructures. Our work focuses on the development of new methods that help detecting such targeted attacks and recovering from them. In particular, our main objective is to minimize the time during which a successful attack remains undetected. To reach this goal, we design and develop new system and network monitoring approaches based on honeypots, and new methods for detecting previously unidentified malware.

Security of Critical Infrastructures

:: national funding (NFÜ), 2013-2014
:: CrySyS Lab's task:
- security monitoring of industrial networks
- malware analysis framework

Security of Smart Energy Systems (SecSES)

:: EIT ICT Labs project, Smart Energy Systems action line, 2013
:: consortium partners: Siemens, KTH
:: CrySyS Lab's task:
- development of a PLC honeypot

Framework for Security Monitoring in Critical Infrastructures

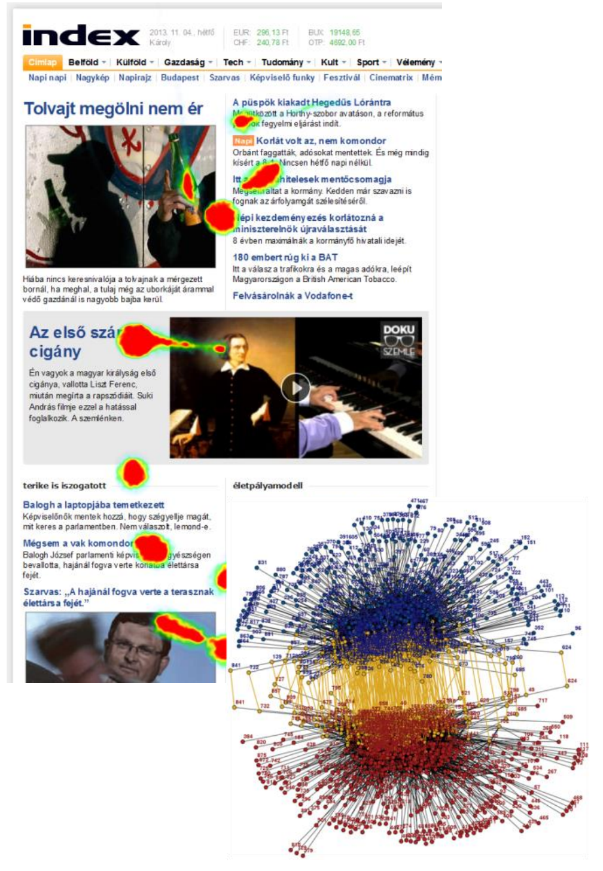
:: EIT ICT Labs project, Smart Energy Systems action line, 2014
:: consortium partners: Siemens, KTH
:: CrySyS Lab's task:
- threat intelligence gathering using the PLC honeypot developed earlier

recent projects

We believe that privacy is a basic human right that should be taken seriously. Today, privacy concerns are not limited to physical surveillance of the population, but they also include issues such as identifying and tracking the behavior of users in cyber space. Our projects aim at understanding the power of existing on-line tracking techniques in different contexts (e.g., web, social networks), and proposing better privacy enhancing mechanisms.

Mouse behavior tracking as a personal identification tool
Our goal is to analyze to what extent mouse heat maps and mouse behavior tracking can be used against personal privacy, and to propose countermeasures.

Pervasive on-line tracking
We aim at quantifying the extent to which web bug based online tracking can invade the privacy of the Hungarian web users.



>>> **spythebug.pet-portal.eu**

De-anonymization of anonymized social network data
We study the performance of existing de-anonimization algorithms in the context of social networks, improve their performance, and develop better anonymization techniques.

TO BE ON THE SAFE SIDE

Laboratory of Cryptography and System Security :: CrySyS Adat- és Rendszerbiztonság Laboratórium (CrySyS Lab)
Budapest University of Technology and Economics :: Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)
Department of Networked Systems and Services :: Hálózati Rendszerek és Szolgáltatások Tanszék (HIT)

>>> **www.crysys.hu**

industry relations

We continuously try to align our research and teaching efforts with the interests of the IT industry, and hence, we maintain strong relationships with many industrial partners. Due to space limitations, we cannot list all of them here, so we list only those partners that we have recently developed good relationships with:

MICROSEC   ERICSSON   KÜRT INFORMATION MANAGEMENT
GOV CERT MAGYARORSZÁG NBSZ   MRG Effitas Efficacy Assessment & Assurance   evopro it's possible!
tresorit   SOPHOS   BalaBit IT Security
Microsoft   KASPERSKY lab   Symantec.

Consulting is an important part of our activities, as it helps us to keep our knowledge up-to-date and extend our practical know-how. Our consulting works range from ethical hacking type of activities through the development of specific security mechanisms to complete security architecture design. There is also lot of interest in our incident response and malware analysis know-how and capabilities. In addition, we provide customized security training to industrial partners.

spin-offs

tresorit

www.tresorit.com

Tresorit was started as a student project in the CrySyS Lab and it evolved into a spin-off thanks to the talent and devotion of the students, István Lám and Szilveszter Szebeni, who designed the Tresorit architecture. Tresorit is a cloud based encrypted data storage system that allows for secure sharing of information within closed user groups. In Tresorit, data is encrypted on the client side before it is uploaded into the cloud, hence, users do not need to trust the cloud storage provider.

Ukatemi advanced threat mitigation technologies

www.ukatemi.com

We founded Ukatemi Technologies to address the problems of targeted cyber attacks. Ukatemi provides malware threat intelligence services and technical assistance in incident response, and it performs malware analysis and security auditing.

AVATAO knowledge you need

www.avatao.com

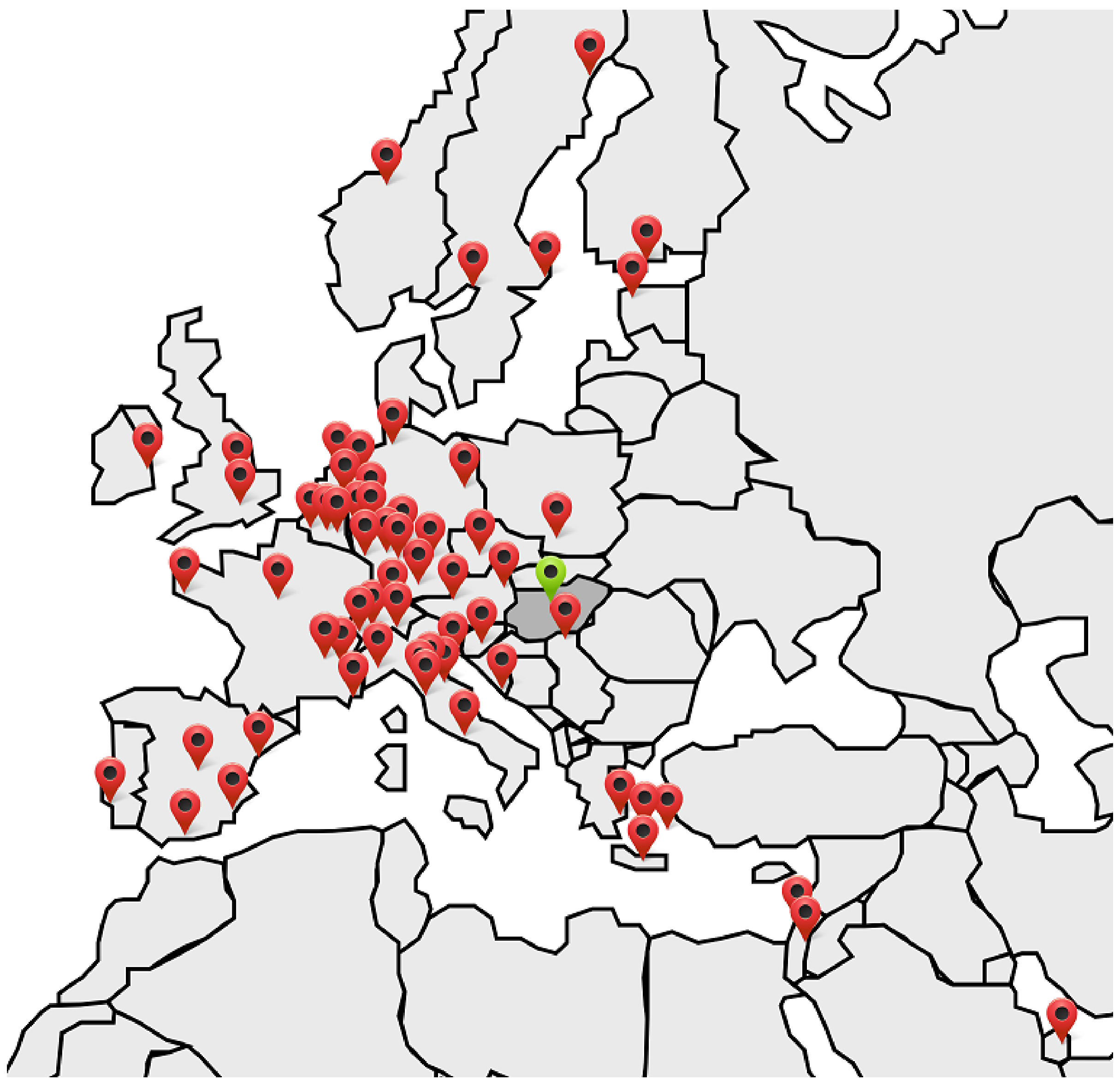
Avatao is an e-learning platform for IT professionals offering custom-tailored learning paths and detailed analytics about the learning process. Avatao helps users acquiring desired skills by guiding them through a series of hands-on exercises and challenges.

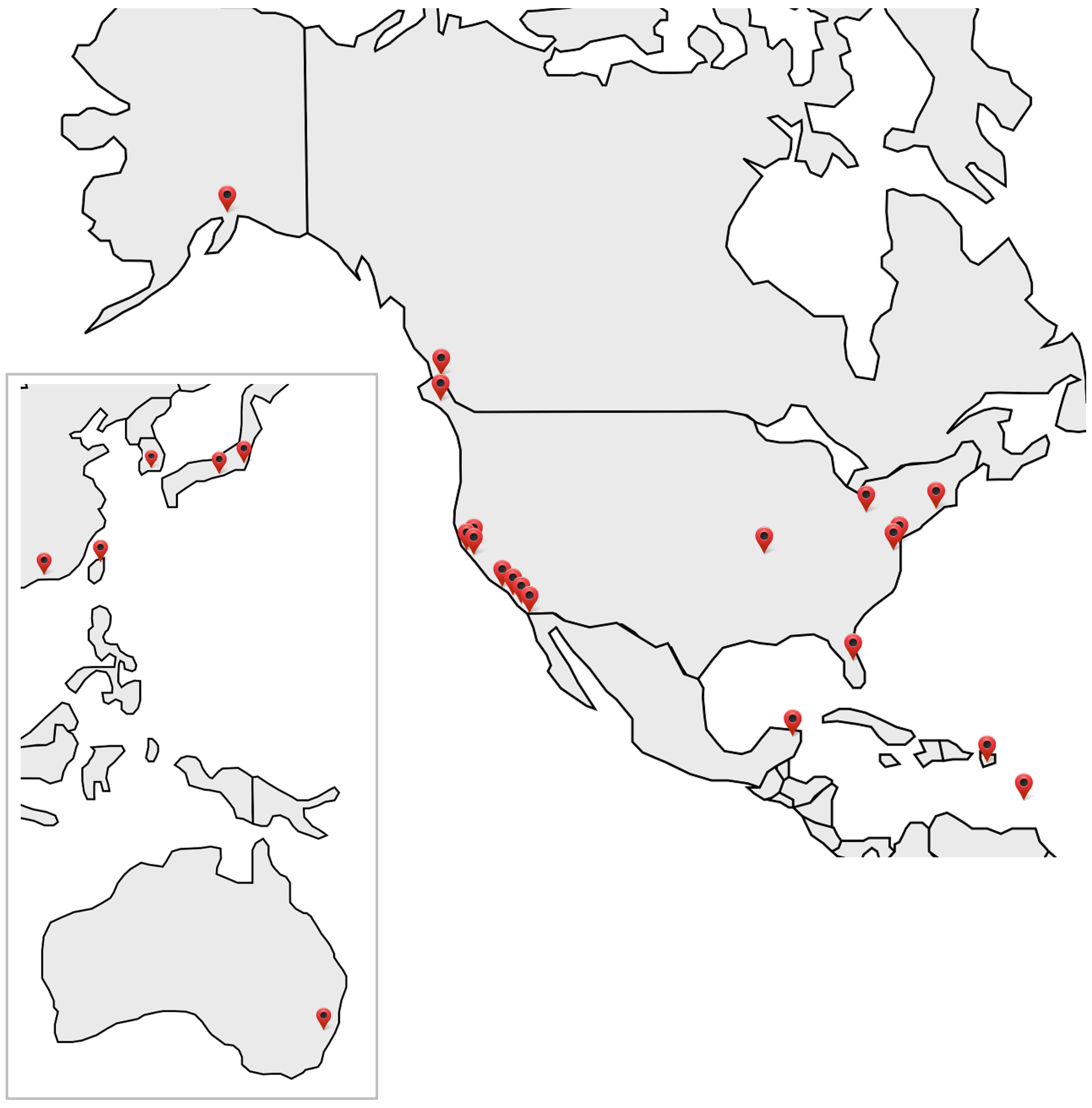
IT-SEC Expert www.it-sec.hu

IT-SEC Expert is a non-profit company specialized in industry oriented research and training in the field of IT security.

globe-trotting

We are lucky to travel to many places in the world for different project meetings and conferences. All together, members of the lab visited more than 80 cities, some of them multiple times, during the past 10 years.





communities

CrySyS Alumni Network

We try preserving the contact to and keeping track of our former students and colleagues. For this reason, we created the CrySyS Alumni Network, which mainly consists of those persons who did their diploma or PhD projects in the lab. Currently, the CrySyS Alumni Network has around 100 members. PhD graduates are distinguished alumni who receive the CrySyS Steel Ring which has the lab logo and the date of graduation graved in it.

CrySyS Student Core

The CrySyS Student Core is an invite only, self-study group, where students expand their knowledge, discuss ideas, prepare for international hacking contests, socialize, and in general, have fun. Only students with outstanding achievements are invited in the Student Core, typically those who achieved high ranking in our annual hacking contest, the CrySyS Security Challenge. Currently, the Student Core has around a dozen members. Junior members are still active students, while senior members are former students who still actively participate in the life of the Student Core.

!SpamAndHex hacking team

Ad hoc subsets of the CrySyS Student Core occasionally team up to participate in international hacking contests under the team name of !SpamAndHex

contacts

If you are a student interested in our work, or perhaps even wish to join our lab, then you can get in touch with us in many ways:

:: visit our web site at **www.crysys.hu**
   (scan QR code in the bottom-right corner)
:: read our blog at blog.crysys.hu
:: find and follow us on Facebook, Twitter, and LinkedIn
:: we still read regular e-mail
:: if we are in our room, we usually pick up the phone too
:: or simply jump into the lab or our offices personally.

You find the e-mail addresses, phone numbers and room numbers of the faculty members below:

Levente Buttyán	buttyan@crysys.hu	463 1803	IE.433
Boldizsár Bencsáth	boldi@crysys.hu	463 3422	IE.433
Márk Félegyházi	mfelegyhazi@crysys.hu	463 2047	IE.418
Tamás Holczer	holczer@crysys.hu	463 2047	IE.418

CrySyS TO BE ON THE SAFE SIDE

Laboratory of Cryptography and System Security :: CrySyS Adat- és Rendszerbiztonság Laboratórium (CrySyS Lab)
Budapest University of Technology and Economics :: Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)
Department of Networked Systems and Services :: Hálózati Rendszerek és Szolgáltatások Tanszék (HIT)

www.crysys.hu