2003 - 2013

A decade of experience in IT security research

CrySyS Lab, Budapest

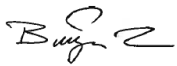
Laboratory of Cryptography and System Security
Budapest University of Technology and Economics
Department of Networked Systems and Services

preface

After spending 6 years in the Swiss Federal Institute of Technology - Lausanne, I came home and joined the Budapest University of Technology and Economics on the 1st of January 2003 with strong intentions to establish an internationally recognized research laboratory in the field of IT security. I was lucky that my colleague, Prof. István Vajda, who led the E-biz Lab at that time, welcomed me and my ideas, and we founded the Laboratory of Cryprography and System Security, or shortly CrySyS Lab, together with the PhD students of the E-biz Lab. I introduced a new way of thinking in the lab, a different approach to research, focusing on the quality of publications that we produce and increasing our visibility internationally. There were other lucky circumstences: Hungary joined the EU in 2004, and I have been invited into new research projects funded by the EU. These projects provided resources that let our young laboratory grow and develop at the beginning.

Now, 10 years later, we can say that we achieved our initial goals: the CrySyS Lab has become well-known and recognized both within our country and internationally. Our current and former colleagues are all well-established and respected members of the IT security research community. We have worked hard for the success, and it was not always easy. But we always had strong determination and internal motivation to overcome the difficulties and to produce first class results by pushing our performance to its limits. I am proud of each member of the lab and the results that we achieved together during the last 10 years.

I am also deeply indepted to a number of people and organizations that helped and supported us. I am grateful to the former and current Heads of the Department, Prof. László Pap and Prof. Sándor Imre, respectively, for supporting me personally, and the CrySyS Lab as a whole right from the beginning. I gratefully acknowledge the financial support that we received from Ericsson through the HSN Lab in the form of long-term scholarships provided to 4 of our PhD students. I am also thankful to KPMG and Microsec for their support that allowed us to improve our computing infrastructure, as well as to Evopro, Kürt, and Sophos for sponsoring the CrySyS Security Challenge and our iCTF team. Many thanks go to our industry partners, colleagues and students with whom we worked together in the last 10 years in various contexts. And finally, we apologize to our families for spending more time on our work than they might have been expected.



Levente Buttyán
Head of the CrySyS Lab

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 cryptography in the context of university courses, laboratory exercises, and different student projects.

The lab also provides consulting services upon request, including ethical hacking, design of secure protocols and system architectures, 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.

in IT security research >>> 2013

CrySyS
TO BE ON THE SAFE SIDE

members

Dr. István Vajda
Dr. Levente Buttyán
Boldizsár Bencsáth
István Zsolt Berta
Gergely Ács
Péter Schaffer
László Dóra
Tamás Holczer
László Csik
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
PhD
PhD
PhD
PhD
PhD
PhD

members

László Czap

Ta Vinh Thong

Dr. Márk Félegyházi

Dr. Amit Dvir

Áron Lászka

Gábor Pék

Gergely Kótyuk

Gábor György Gulyás

János Szurdi

in IT security research >>> 2013

CrySyS

TO BE ON THE SAFE SIDE

projects

In the last decade, our research focused on security and privacy in wireless and mobile networks (sensor networks, vehicular networks, mesh networks), economics of security, and detection and analysis of targeted malware. We have been involved in a number of international and national 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)

Other projects:
Dependable Security with Enhanced Reconfigurability (DESEREC), Biologically Inspired Networks and Services (BIONETS), Virus Center, Smart Card Based Electronic ID (HUNEID), Security and Privacy in Ubiquitous Computing, Strong User and Device Authentication in Mobile Environments, Mobility Supporting Security Architectures, Secure Streaming in Mobile Environments.

targeted malware

In the passed two years, our laboratory participated in a number of investigation efforts, aiming at identifying and analyzing targeted malware samples that were used for the purpose of espionage in cyber warfare activities:

Duqu [October 2011]

discovery, naming, and first detailed analysis of Duqu
:: striking similarities to Stuxnet, but different mission (info-stealer)
identification of the dropper component
:: 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 sKyWIper)
:: another info-stealer, but more complex than Duqu (unusually large size)

Miniduke [February 2013]

first detailed technical analysys in collaboration with Kaspersky Labs
:: yet another infostealer targeting governmental entities and human right organizations

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 different targets, inlcuding high profile ones

globe-trotting

We were lucky enough 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.

globe-trotting

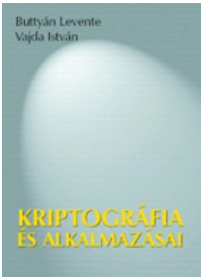
in IT security research >>> 2013

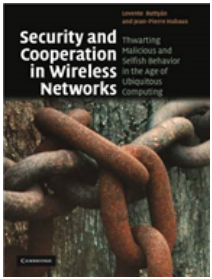
TO BE ON THE SAFE SIDE

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 that our laboratory has a very strong publication record and stands high according to the above measures:

- 5 books
- 4 book chapters
- ~20 international journal papers
  - :: including 7 IEEE Transactions and 1 ACM Computing Surveys
- ~60 international conference papers
  - :: mostly IEEE and ACM
- 2 Internet Drafts
- 2 patent submissions





According to Google Scholar, the total number of independent citations to our papers is ~9600. As of March 2013, the h-index of Levente Buttyán is 38 and the h-index of Márk Félegyházi is 15.

In addition, our visibility in the research community and among IT security practitioners has been greatly increased recently by an extensive media coverage of our work on the analysis of various targeted malware attacks.

spin-offs

tresorit

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 desgined 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. More information and the product itself are available at **www.tresorit.com.**

Ukatemi

advanced threat mitigation technologies

We founded Ukatemi Technologies to address the problems of targeted cyber attacks against critical infrastructures and industrial control systems. The company provides advanced monitoring, incident response, and malware threat intelligence services. In monitoring, we focus on rapid detection of break-ins with advanced techniques that go beyond traditional intrusion detection. Our forensic analysis services help our clients to identify the main causes of an incident, and to understand what went wrong and why, whereas our malware intelligence services help them to understand the impact of the incident, and the motivations of the attackers. More information is available at **www.ukatemi.com.**

IT-SEC Expert

www.it-sec.hu

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

industry relations

We have always maintained strong relationships with various industrial partners, because we continuously try to align our research and teaching efforts with the interests of the IT industry. Within our projects, we collaborated with many partners from Hungary and abroad during the past ten years. The following set of company logos is far from being complete, we included only those partners with whom we had some collaboration in the last couple of years. In particular, we do *not* include our industrial partners in EU projects and companies that contracted us for consulting.

Consulting is an important part of our activities, as it helps us to keep ourselves up-to-date and extend our practical know-how. Our consulting works range from ethical hacking type of activities through development of specific security mechanisms to complete security architecture design. There is also lot of interest in our malware analysis know-how and capabilities. We build in the experiences that we gain during consulting into our courses, laboratory exercises, and into the annual CrySyS Security Challenge, a competition that we organize for our students (see education activities). We also provide customized security training to industrial partners.

We have been teaching courses on security and privacy at the Budapest University of Technology and Economics. Our courses inlcude 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)

:: Administrating 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 our university.

We pay special attention to attract and work with students talented in IT security. In particular, we organized two IT security contests for students, where they had to solve problems related to reverse engineering, network log analysis, compromising different network based services, and breaking into systems and obtaining root privileges, etc. We also recruited and led the student hacking teams of the university at the international Capture The Flag (iCTF) competitions of 2011 and 2013.

We maintain a large alumni network, and try to stay in touch with our former students.

timeline

2003

- CrySyS Lab founded
- first project funded by OTKA
- Virus Flags project
- looking for potential PhD students
- 6 journal and 7 conference papers
- beginning of the Special on Security of Infocommunication Systems
- new book on Cryptography and Its Applications

2004

- start working with potential PhD students Gergely Ács, Péter Schaffer, Tamás Holczer, and László Dóra
- OTKA project, HUNEID project
- 3 journal and 9 conference papers
- 3 TDK projects, 17 semester projects

2005

- submission of 4 successful EU project proposals
- MIK security project starts
- Istvan Zsolt Berta defends his thesis and receives the PhD degree
- 5 journal and 7 conference papers
- 7 diploma projects
- 5 new PhD students join the lab: G. Ács, L. Csik, L. Dóra, T. Holczer, P. Schaffer
- purchase of 4 MicaZ sensor motes

2006

- Márk Félegyházi joins the lab as an associate member
- Levente Buttyán is promoted Associate Professor
- a plethora of new projects: UbiSecSens, Sevecom, BIONETS, DESEREC, MobileSEC (w/ E-group), MESSENGER
- OTKA and MIK projects continue
- 2 book chapters, 9 journal and 7 conference papers
- 16 semester and 3 diploma projects

2007

- Ta Vinh Thong joins as a student and wins first prize at the TDK
- 7 projects running in parallel, LOT OF WORK!
- successful new proposal EU-MESH
- graphical password experience with ~180 students
- new book on Security and Cooperation in Wireless Networks
- 3 journal and 10 conference papers
- we teach Security on BSc and MSc in Hungarian and in English at BME, and in Révkomárom, Slovakia
- 13 semester and 8 dilpoma projects

2008

- Ta Vinh Thong and László Czap join as new PhD Students, Gábor Pék joins as BSc student
- successful completion of UbiSecSens, Sevecom, DESEREC, and our MIK and MobileSEC projects
- successful new EU proposal WSAN4CIP
- new project EU-MESH starts
- 6 journal and 3 conference papers
- 8 diploma, 3 TDK projects (2 first prizes!)

timeline

2009

- new project WSAN4CIP starts, EU-MESH continues
- successful completion of BIONETS
- 6 journal and 5 conference papers
- 3 members defend their theses and receive the PhD (G. Ács, P. Schaffer, Boldizsár Bencsáth)
- educational reform: new Special on Security of Communication Systems
- we teach a base course on Security in the MSc program, and 4 courses in the Special, 6 diploma projects

2010

- István Lám and Szilveszetr Szebeni join as student, start working on encrypted filesystems, and win first prize at the TDK
- Amit Dvir joins the lab as a post doc
- successful completion of EU-MESH, WSAN4CIP continues, CHIRON starts
- 5 journal and 9 conference papers
- 5 diploma projects
- László Dóra defends his thesis and obtains the PhD degree

2011

- Márk Félegyházi joins as a faculty member, Levente Buttyán becomes the Head of the Lab officially
- Gábor Pék, Áron Lászka, and Gergely Kótyuk join as new PhD students
- successful completion of WSAN4CIP, CHIRON continues
- 2 Internet Drafts, 1 patent, 4 journal and 10 conference papers
- many unsuccesful attempts for EU grants
- Duqu discovered, intensive media coverage
- first CrySyS Security Challenge,
- first participation at the iCTF competition
- Tresorit launched

2012

- CHIRON project continues
- Flame analyzed, intensive media coverage
- 8 conference and 3 journal papers (including one on the cousins of Stuxnet)
- many invitations from various places to give talks on targeted attacks (Cancun, Washington DC, London, Amsterdam, Grenoble, Erlangen, Balatonőszöd, ...)
- successful national project proposals with a research focus on critical infrastructure protection
- spin-offs IT-SEC Expert and Ukatemi Technologies started
- Gábor Gulyás joins the lab

2013

- new NFÜ project on Protecting Critical Infrastructures from Targeted Attacks starts
- János Szurdi joins the lab temporarily
- Miniduke analysis, media coverage
- TeamSpy analysis, media coverage
- second CrySyS Security Challenge
- second participation at the iCTF competition

in IT security research >>> 2013

CrySyS
TO BE ON THE SAFE SIDE

More information is available at

www.crysys.hu