Introducing the CrySyS Lab

Levente Buttyán
Laboratory of Cryptography and System Security (CrySyS)
Budapest University of Technology and Economics
Department of Networked Systems and Services
www.crysys.hu

Current members

- faculty members
  - Levente Buttyán, PhD, Associate Professor (head of the lab)
  - Boldizsár Bencsáth, PhD, Assistant Professor
  - Márk Félegyházi, PhD, Assistant Professor
  - Tamás Holczer, PhD, Assistant Professor
  - István Vajda, DSc, Professor (affiliate)
- PhD candidates
  - Gábor Gulyás (privacy in social networks, identity separation techniques)
  - Áron Lászka (robustness of network toplogies, optimization problems, game theory)
  - Gábor Pék (security of virtualized systems, malware analysis)
- CrySyS Student Core
  - 10-12 talented students working with us permanently

\+ students working on diploma and semester projects

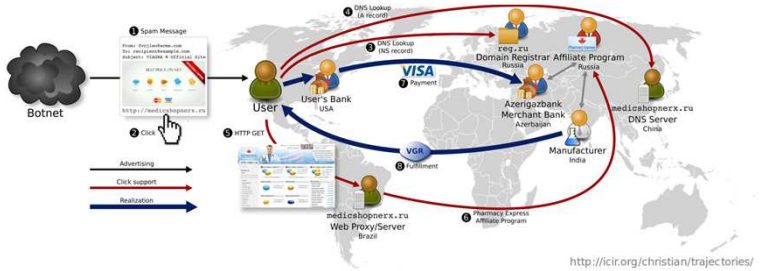
Mission

- internationally recognized, **high quality research** on security and privacy in computer networks and systems
  - problem driven, project oriented research → we are committed to establish and participate in R&D projects, in which we collaborate with industrial and other academic partners
- **teaching** network and system security, privacy, and cryptography in the context of university courses, laboratory exercises, and student semester projects
- provision of **consulting** services without compromising the general academic objectives

Research areas in the past

- **security and privacy in wireless embedded networks**
  - sensor networks, body mounted sensor networks, mesh networks, car-to-car communications, RFID systems
  - secure communications, secure routing, secure distributed data storage, location privacy, private authentication, privacy preserving cluster head election

- **economics of security**
  - game theoretic models of strategic behavior, incentive compatible security architectures, quantitative risk management, cyber insurance



Project highlights

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

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

WSAN4CIP – Wireless Sensor Networks for Critical Infrastructure Protection
(EU STREP, supervised by L. Buttyan)

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

CHIRON – Cyclic and Person Centric Health Management
(ARTEMIS IP, supervised by L. Buttyan and R. Schulz)

Current research

- **detection and analysis of unknown targeted malware**
  - static and dynamic program analysis, reverse engineering, rootkit detection
  - Windows, Android

```
call    sub_10006C53
lea     eax, [ebp-11h]
push    eax
call    sub_10001318
mov     eax, dword_1002A134
cmp     dword ptr [eax], 0
jnz     short loc_1000121B
mov     [ebp-1Ch], ebx
push    offset unk_1001FC18
lea     eax, [ebp-1Ch]
push    eax
call    Exception_Handler_sub_10013880
```

Highly visible recent results

- Duqu (October 2011)
  - **discovery, naming, and first 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 (Feb 2013)
  - **detailed technical analysis with Kaspersky**
- TeamSpy (Mar 2013)
  - **first detailed technical analysis**

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 participation in the initial discovery of the Duqu cyber-surveillance Trojan.*

A security
come forw

According
an unnam
speculatio

ITcafé

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

RENDSZERGAZDA vagy? Segítsd munkánkat, vegyél részt az ITPRO 201

IBM Storwize® V3700 4,2 TB adat-tárhellyel most

Több éve zajló támadást leplezett le a BME CrySyS

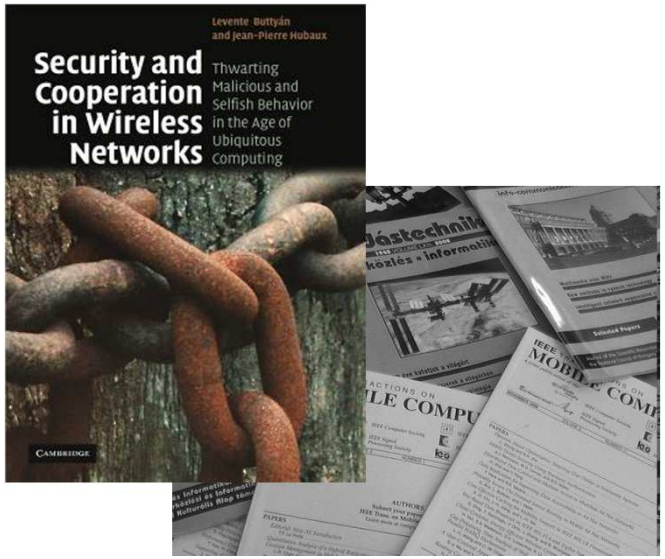
Bodnár Ádám, 2013. március 21. 10:24 Szólj hozzá!

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

A Nemzeti Biztonsági Felügyelet riasztása nyomán kezdett vizsgálódásba a BME CrySyS, a folyamat eredménye egy információgyűjtő kártevő leleplezése lett. A publikát adatok alapján a támadók feltehetően évek óta több hullámban hajtottak végre információgyűjtő tevékenységet, magyar kormányzati szervek mellett orosz iparvállalat, közel-keleti elektronikai cég, oroszországi követségek, illetve francia és belga kutatóintézetek is érintettek az incidensekben.

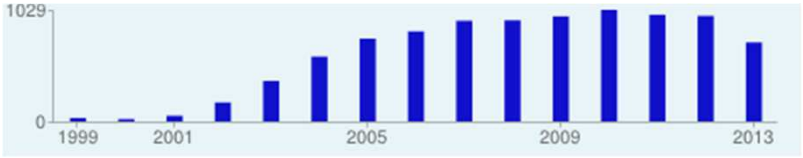
Publications between 2003 and 2013

- 5 books
- 4 book chapters
- ~25 journal papers
  - including 7 IEEE Transactions
- ~60 conference/workshop papers
- 2 Internet Drafts
- 2 patent submissions



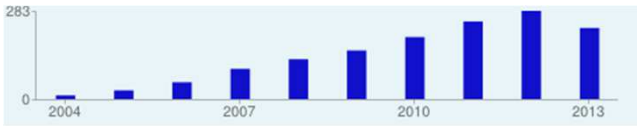
Citations of Levente Buttyán:

	All	Since 2008
Citations	9550	5623
h-index	39	31
i10-index	66	60



Citations of Márk Félegyházi:

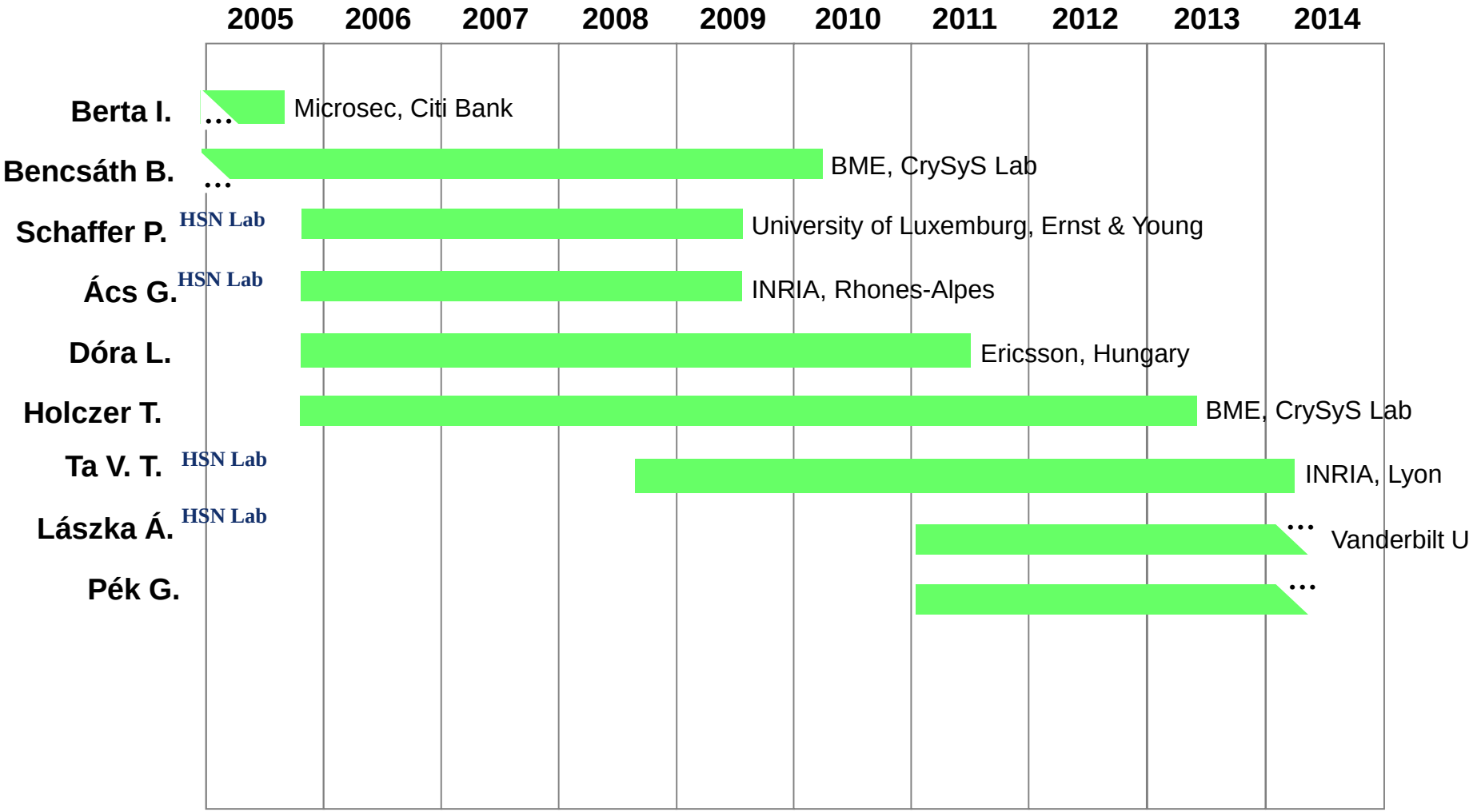
	All	Since 2008
Citations	1452	1245
h-index	17	16
i10-index	20	20



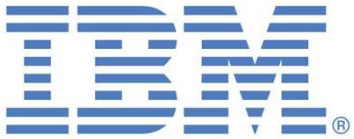
International collaborations

- EPFL, Switzerland (Prof. Jean-Pierre Hubaux)
- University of Twente, The Netherlands (Prof. Frank Kargl)
- KTH, Sweden (Prof. Panagiotis Papadimitratos, Prof. György Dán)
- NEC Laboratories, Germany (Dr. Dirk Westhoff)
- IHP, Germany (Prof. Dr. Peter Langendoerfer)
- INRIA Rhone-Alpes (Dr. Claude Castelluccia)
- University of Münster, Germany (Prof. Rainer Böhme)
- Eurecom, France (Dr. Davide Balzarotti)
- University of Rome 3 (Dr. Roberto Di Pietro)
- …
- University of Washington, Seattle (Prof. Radha Poovendran)
- University of California, Berkeley (Prof. Jean Walrand)
- ICSI, Berkeley (Prof. Vern Paxson)
- …

PhD graduates



Consulting and industry relations



Spin-offs

IT-SEC Expert
www.it-sec.hu

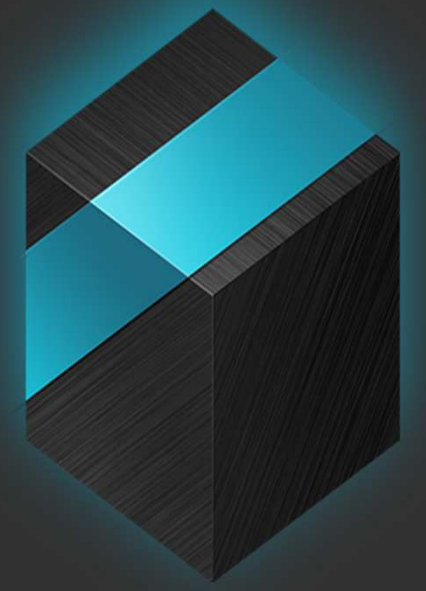
industry oriented research,
development, and training

Ukatemi
advanced threat mitigation technologies

agile incident response
malware threat intelligence

tresorit

encrypted data storage in the cloud



tresorit

[redacted]ot. Sync. Share.

Everything is encrypted before
upload. You're in control.

Ukatemi

Ukatemi Technologies
Threat Intelligence Services

© 2013 Ukatemi Technologies Ltd.

Teaching

- Base course in Computer Networking
  - Computer Networking (Info BSc German, Computernetzwerke) (M. Félegyházi)
- Base courses in Information Security
  - Information Security (Info MSc, Adatbiztonság) (I. Vajda, L. Buttyán, B. Bencsáth)
  - Information Security (GaIn MSc, Adatbiztonság) (I. Vajda, L. Buttyán, B. Bencsáth)
- Special on Security of Communication Systems
  (Hírközlő rendszerek biztonsága MSc informatikus szakirány)
  - Cryptography and its applications
    (Kriptográfia és alkalmazásai) (I. Vajda)
  - Security protocols
    (Biztonsági protokollok) (L. Buttyán)
  - Foundations of secure e-commerce
    (A biztonságos elektronikus kereskedelem alapjai) (L. Buttyán)
  - \+ laboratory exercises, semester and diploma projects
    (all members)

Teaching

- Elective courses
  - Network security in practice
    (Hálózatbiztonság a gyakorlatban) (B. Bencsáth)
  - Economics of security and privacy
    (A biztonság és a privátszféra védelmének közgazdaságtana) (M. Félegyházi)
  - Privacy enhancing technologies
    (Privátszféra erősítő technológiák) (G. Gulyás)
  - Administrating security in computer networks
    (Számítógéphálózatok biztonságos üzemeltetése) (M. Félegyházi, T. Holczer)

- Student projects
  - semester, diploma, TDK, ...

Working with talented students

- CrySyS Security Challenges: http://www.crysys.hu/security-challenges.html
  - 2011, 2012, 2013
- CrySyS Student Core
- Capture the Flag (CTF) hacking contests
  - iCTF 2011: 36/87
  - iCTF 2012: 23/98
  - CSAW 2013: 12/1378 (2/490)
  - **iCTF 2013: 2/123**

Questions?

www.crysys.hu