w w w . c r y s y s . h u

Introducing the CrySyS Lab

Levente Buttyán, PhD

Laboratory of Cryptography and Systems Security

Department of Networked Systems and Services

Budapest University of Technology and Economics

buttyan@crysys.hu

Members

- faculty members
  - Levente Buttyán, PhD, habil, Associate Professor (head of the lab)
  - Boldizsár Bencsáth, PhD, Assistant Professor
  - Tamás Holczer, PhD, Assistant Professor
  - Gergely Biczók, PhD, Assistant Professor
  - Gergely Ács, PhD, Assistant Professor

- PhD students
  - Dorottya Papp (security assurance in cyber-phyiscal systems)
  - András Gazdag (forensic analysis in cyber-physical systems)
  - Máté Horváth (cryptographic obfuscation)
  - Szilvia Lestyán (privacy, machine learning)
  - Gergő Ládi (automated protocol reverse engineering)

+ associate members
  - Márk Félegyházi, PhD, avatao.com
  - Gábor Pék, PhD, avatao.com
  - István Vajda, DSc, Professor

Best known for …

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.*

CRYSYS
TO BE ON THE SAFE SIDE

Laboratory of Cryptography and System Security
Budapest University of Technology and Economics
Department of Telecommunications
www.crysys.hu

A security lab attached to the Budapest University of Technology and Economics in Hungary has come forward as the mystery outfit that found the Stuxnet-like "Duqu" cyber-surveillance Trojan.

According to Symantec's initial report on Duqu [PDF], the malware sample was passed along by an unnamed "research lab with strong international connections," a statement that led to speculation about the origins and intent of the threat.

Publications and citations

- 7 books
- 10 book chapters
- 80+ journal papers
- 140+ conference papers
- 2 Internet Drafts
- 5 patents
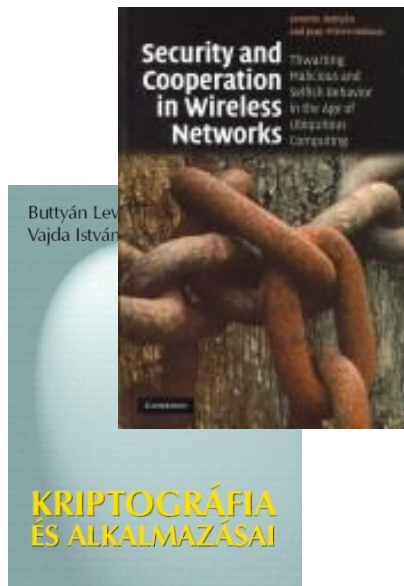
	All	Since 2012
Citations	13781	5210
h-index	48	36
i10-index	96	77

	All	Since 2012
Citations	751	683
h-index	11	9
i10-index	11	9

	All	Since 2012
Citations	1038	749
h-index	11	10
i10-index	12	11

	All	Since 2012
Citations	2900	1839
h-index	24	21
i10-index	32	29

Activities

- **research**
  - security in cyber-physical systems, privacy-preserving technologies, economics of security and privacy
  - funding from EIT Digital, Erasmus+, H2020 ECSEL, and national funding agencies

- **teaching**
  - IT security program at the BME
  - Applied Cryptography at the Aquincum Institute of Technology
  - special training sessions and cyber security exercises for industrial partners

- **talent management**
  - PhD students
  - CrySyS Student Core

- **consulting**
  - for IAEA, HAEA, and private companies
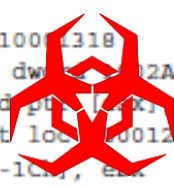
Research areas

- **security in cyber-physical systems**
  - application areas:
    1. industrial automation and control systems (including Industry 4.0)
    2. in-vehicle embedded networks and devices (including connected and autonomous cars)
  - attack detection, incident response, forensic analysis, software security assurance

- **privacy and anonymization**
  - anonymization of large data sets, applications of machine learning, privacy impact analysis

- **economics of security and privacy**
  - applications of game theory for analyzing strategic behavior, risk management
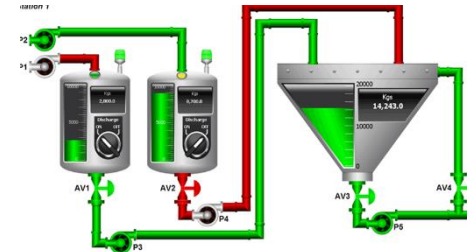
Other competencies

- malware analysis
  - static and dynamic program analysis, reverse engineering
  - analysis of targeted malware (APT)
  - custom testing of anti-malware solutions

```
call     sub_10006C53
lea      eax, [ebp-11h]
push     eax
call     sub_100   318
mov      eax, dw        2A134
cmp      dword          0
jnz      short loc   0011B
mov      [ebp-1C ],
push     offset unk_1001FC18
lea      eax, [ebp-1Ch]
push     eax
call     Exception_Handler_sub_10013880
```

- applied cryptography
  - cryptographic protocols for secure communications and secure data storage
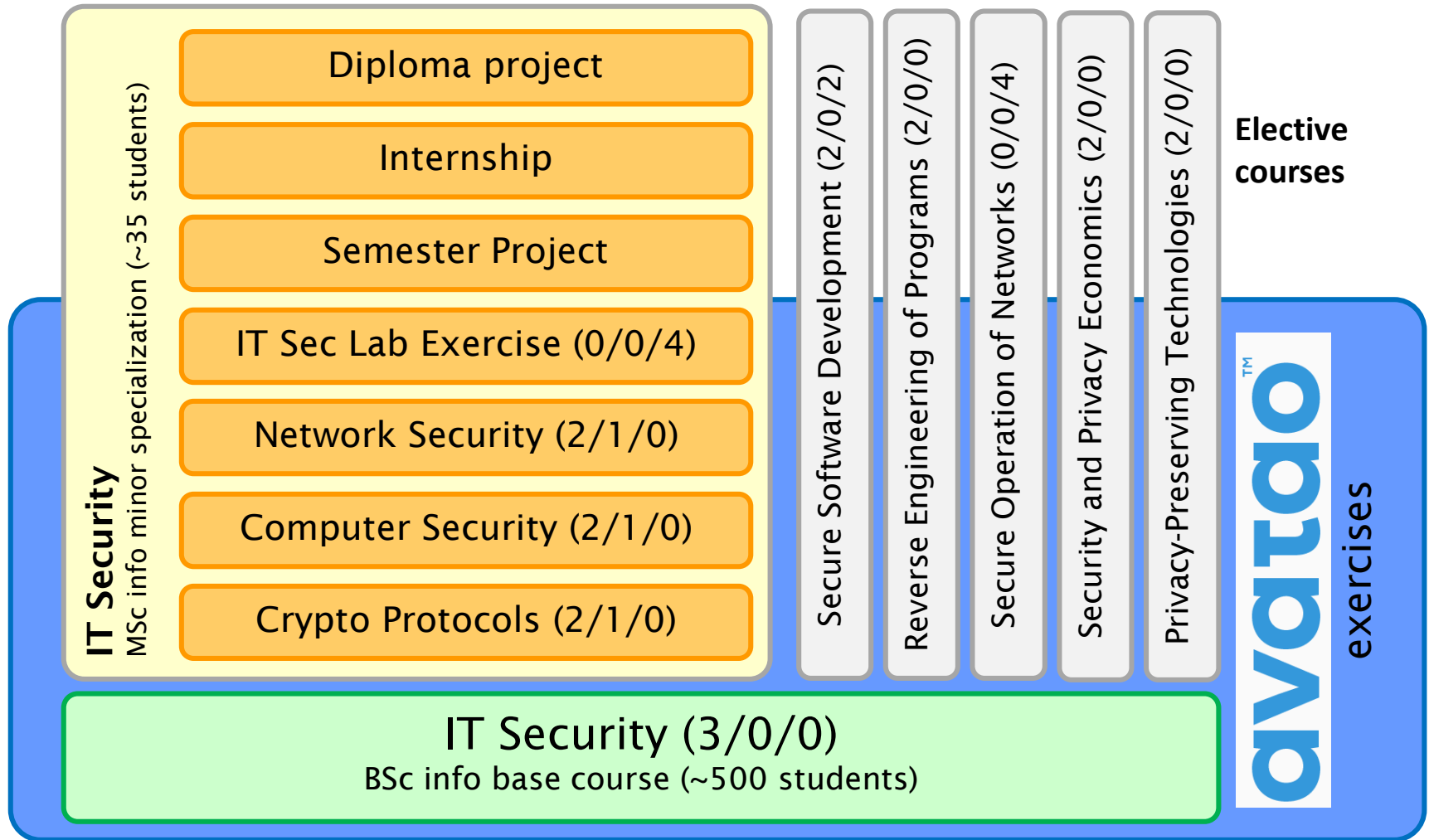 - obfuscation of programs

```
03003802  996CB7BA  0EG0161B  G0021C06
BA7CE203  G0030200  01208600  37D14D00
1B7125G0  024FG002  53D03C00  AD722500
!BD03C00  887525C1  01A07700  37D14D00
.B7125G0  024FG002  53D03C00  AD722500
BD03C00  887525C1  4F553     53414247
F4F3D41  4242434E  3D4A6     6469204
.6C2F4F  553D4553  414       4F3D414
.425604  00313F30   424 01   0003424
003042  4CG        024E4E4F  00B1D3.
?254F1  21    09   8833B0CC  2957EE
.3ECAA  CB3EE8EF  DF038D7F  A14217
2AA4D  04143B75  4F571C83  535C04
7DED9  B57C659E  C820EE07  FA49F
.96DB  7D7F743D  9A36DD29  454E0
014D  410800C8  9A54E072  5A14C
```

PhD graduates

1. Dr. István Zsolt Berta (2005) (currently with Citi Bank, Hungary)
2. Dr. Péter Schaffer (2009) (currently with Ernst&Young, Luxemburg)
3. Dr. Gergely Ács (2009) (currently with CrySyS Lab, Budapest)
4. Dr. Boldizsár Bencsáth (2010) (currently with CrySyS Lab, Budapest)
5. Dr. László Dóra (2011) (currently with Citi Bank, Hungary)
6. Dr. Tamás Holczer (2013) (currently with CrySyS Lab, Budapest)
7. Dr. Vinh Thong Ta (2014) (currently at University of Lanceshire, UK)
8. Dr. Áron Lászka (2014) (currently with University of Houston, USA)
9. Dr. Gábor Gulyás (2015) (currently with INRIA, France)
10. Dr. Gábor Pék (2015) (currently with Avatao, Hungary)

IT security education at BME

IT Security — MSc info minor specialization (~35 students)

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

Elective courses:
- Secure Software Development (2/0/2)
- Reverse Engineering of Programs (2/0/0)
- Secure Operation of Networks (0/0/4)
- Security and Privacy Economics (2/0/0)
- Privacy-Preserving Technologies (2/0/0)

avatao exercises

IT Security (3/0/0) — BSc info base course (~500 students)

more info: http://www.crysys.hu/education/

Talent management

active advertising to freshmen,
results of the !Spam and Hex CTF team

contributing to
IT SEC bootcamp
and CrySyS
Security Challenge

IT SEC bootcamp
(~40 students)

visibility

giving back

CrySyS Student Core

Community of Practice

bootstrapping

CTF team,
exposing garage projects

integration

speeding up

semester projects

admission

./security-challenge-2016
20 September- 7 October

outstanding performance
(semester projects, CrySyS Security Challenge)

Winners of iCTF 2014 (held in 2015)

Qualified for DEFCON Final in 2015, 2016, 2017

Spin-offs

- founded in 2011
- sharable encrypted data storage in the cloud
- web site: **www.tresorit.com**

- founded in 2012
- cyber incident response, malware analysis, malware threat intelligence, exploit mining, and more ...
- web site: **www.ukatemi.com**

- founded in 2014
- on-line platform for IT security exercises, support for recruitment, on-borading, continuous training, university education, CTF-like competitions, ...
- web site: **www.avatao.com**

Thanks!

Levente Buttyán

buttyan@crysys.hu