www.crysys.hu

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
- Post-doc
  - Balázs Pejó, PhD
- PhD students
  - András Gazdag (cyber security of vehicles)
  - Máté Horváth (cryptographic obfuscation)
  - Dorottya Papp (program analysis, backdoor detection)
  - Szilvia Lestyán (privacy, machine learning)
  - Gergő Ládi (automated protocol reverse engineering)

+ associate members









Best known for ...

Home / News & Blogs / Zero Day

Hungarian Lab found Stuxnet-like Duqu malware

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

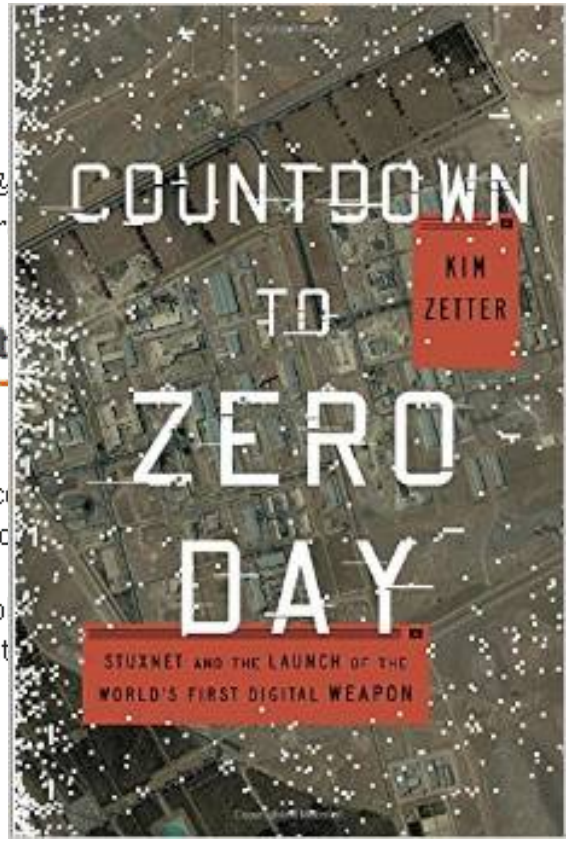
Summary: *The Laboratory of Cryptography and System Security (Cry*
confirmed its participation in the initial discovery of the Duqu cyber-sur

TO BE ON THE SAFE SIDE

Laboratory of Cryptography and Syst
Budapest University of Technology and Economics
Department of Telecommunications

A security lab attached to the Budapest University of Technology and Ec
come forward as the mystery outfit that found the Stuxnet-like "Duqu" c

According to Symantec's initial report on Duqu [PDF], the malware samp
an unnamed "research lab with strong international connections," a stat
speculation about the origins and intent of the threat.

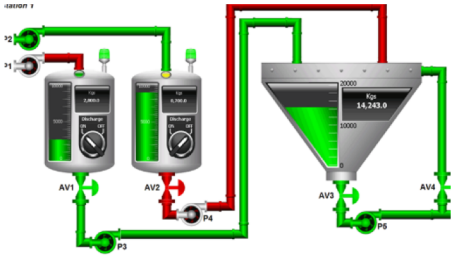


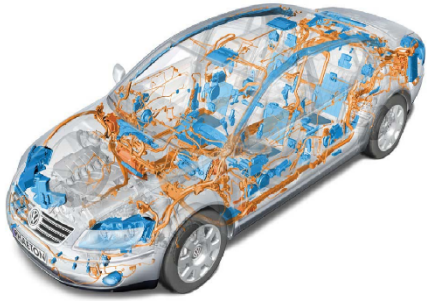
Activities

- research
  - security in cyber-physical systems, privacy-preserving technologies, economics of security and privacy
  - funding from H2020 ECSEL, H2020 IMI, Erasmus+, NKFIH (NKP, OTKA, VKE)
- 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)

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)
    3. IoT systems
  - embedded platform security, monitoring and attack detection, incident response, penetration testing





- privacy and anonymization
  - anonymization of large data sets, privacy issues in machine learning, privacy preserving computing

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

Why security of CPS is important?

https://www.youtube.com/watch?v=MK0SrxBC1xs

Our ”car hacking” project

> SC US
SC UK

Automakers urge Congress to limit regulation on 'Internet of Cars'

Strontium hacking team targets NATO members, political advisors

DATA CENTRE SOFTWAI

Security

Hackers
Audi airb

Just when V
pulls up

Buttyán stresse
software.

"It is not the spe
devices are typi

SOFTPEDIA® DESKTOP MOBILE WEB NEWS

Softpedia > News > Security

FLASH SALE: SpyShelter Premium 50% OFF

Audi Cars Hacked but Only Airbag System Affected

Start searching now...

Security researchers disable Audi TT airbags system

By Catalin Cimpanu 25 Oct 2015, 13:02 GMT

The trend of car-hacking revelations continues with three researchers from CrySys Lab and the Budapest University of Technology and Economics saying that they were able to quietly disable the airbags system on an Audi TT model.

Presenting their findings to The Register, the three explained that while their attack is not as glamorous as all the recent car-hacking cases from the past six months, their attack is more plausible to happen in real life.

That's because the attack relies on a zero-day exploit found in car mechanics software used to debug and fix cars sold by the Volkswagen Group. This software is built and sold by third-parties, not Volkswagen. Let's not put the blame on the company this time,

2 PHOTOS

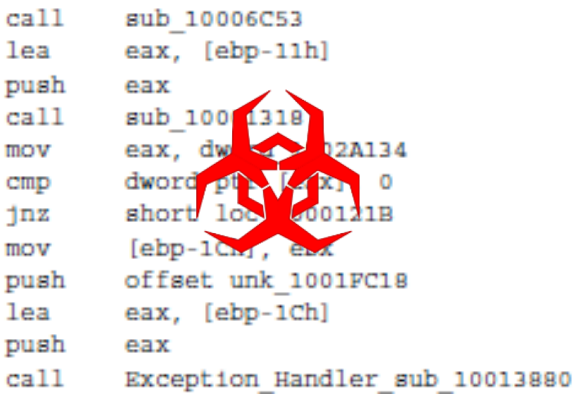
experiments were carried out during spring 2015

The researchers at work

Our ICS/SCADA testbeds

Other competencies

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



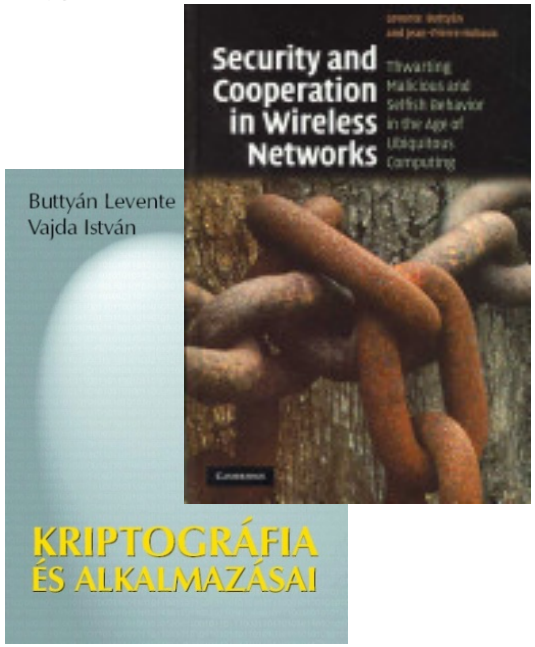
- applied cryptography
  - cryptographic protocols for secure communications and secure data storage
  - obfuscation of programs (theoretical)

Current projects

- Vehicle cyber security --» SECREDAS (H2020 ECSEL)
- ICS/SCADA security --» DIGMAN (NKFIH VKE), PIRAMID (IAEA)
- IoT security --» SETIT (NKFIH NKP)
- Privacy preserving machine learning --» MELLODDY (H2020 IMI)
- Cryptographic obfuscation (OTKA)
- IT security education --» ISSES (Erasmus+)

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

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 and Ukatemi Tech)
5. Dr. László Dóra (2011) (currently with Mongu for Teen, 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 BME-AUT, Budapest)
10. Dr. Gábor Pék (2015) (currently with Avatao, Hungary)

QuBit Conference
@QuBitCon

Follow

StartUp, Avatao, won the startup competition at our CyberSquare in Prague! Congratulations. Good job! #avatao #QuBit2017 @theavatao

avatao™

index SZABAD INDEX | ÖNKORMÁNYZATI VÁLASZTÁS 2019 | TÁMOGASS MINKET!

2019. 10. 03. csütörtök Helga | EUR 333,38 Ft ▼ GBP 374,08 Ft ▼ | 11 °C 16 °C | In English

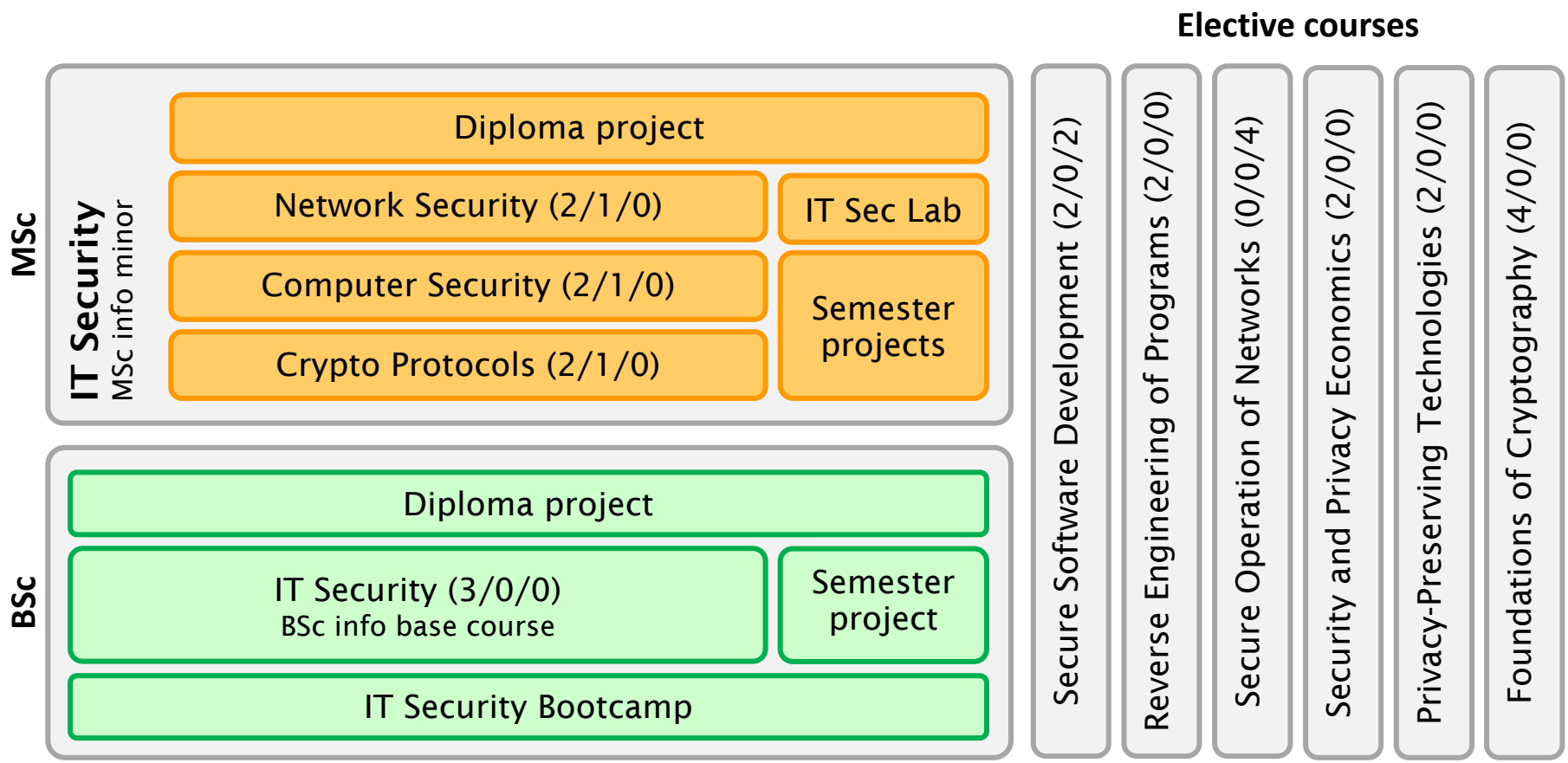
BELFÖLD KÜLFÖLD GAZDASÁG TECH-TUDOMÁNY KULT SPORT VÉLEMÉNY VIDEÓ FOTÓ 24 ÓRA

TECH-TUDOMÁNY | ITBN 2019 | KIBERBIZTONSÁG | PITCH | STARTUPVERSENY | OXO | CEU | MONGU

A tiniket biztonságos netezésre tanító app nyerte a kiberbiztonsági startupversenyt

MONGU for teen

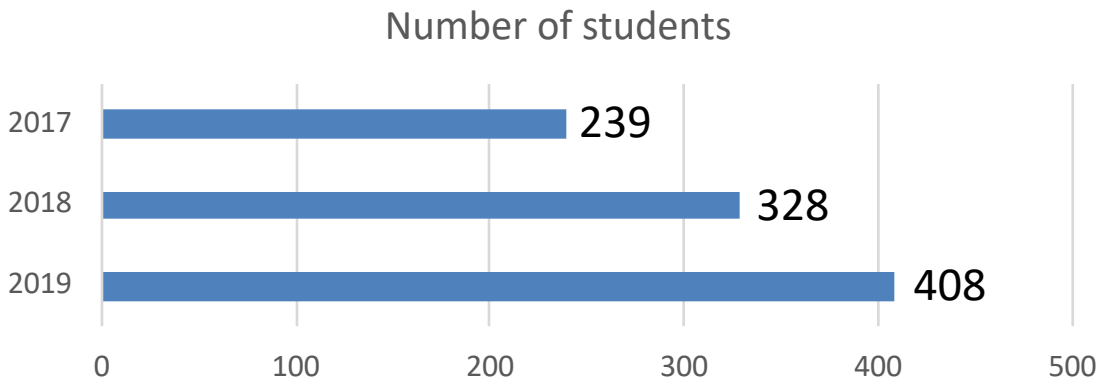
IT security education at BME (BSc, MSc)



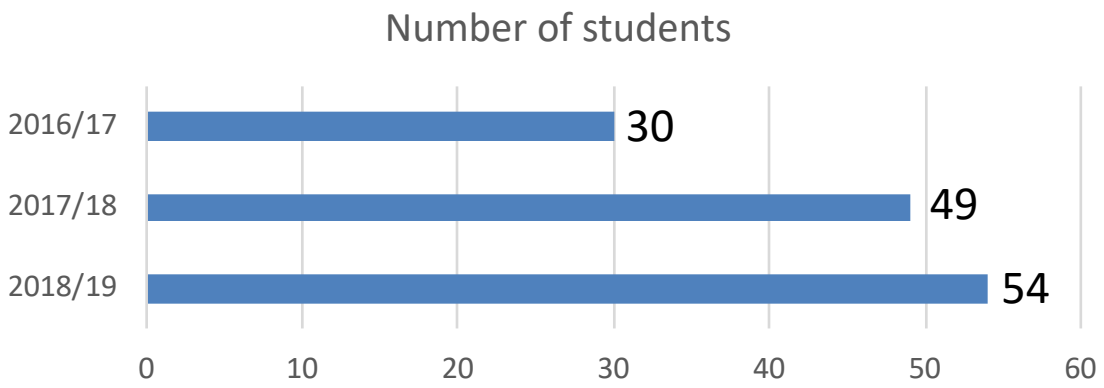
more info: http://www.crysys.hu/education/

Some statistics

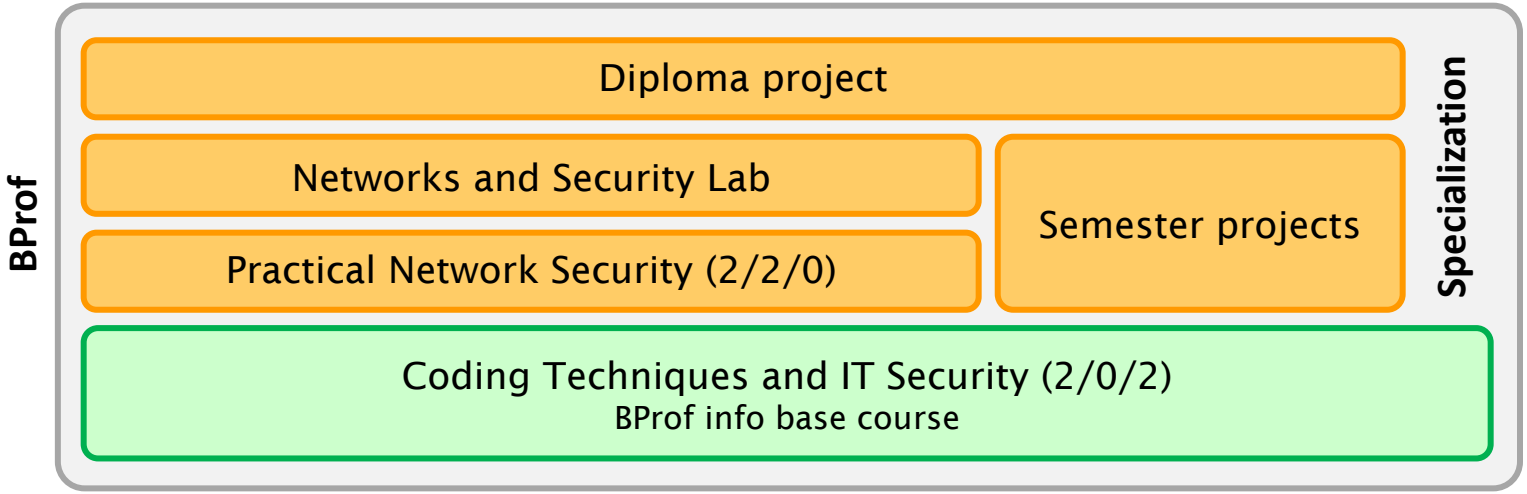
- BSc IT Security course



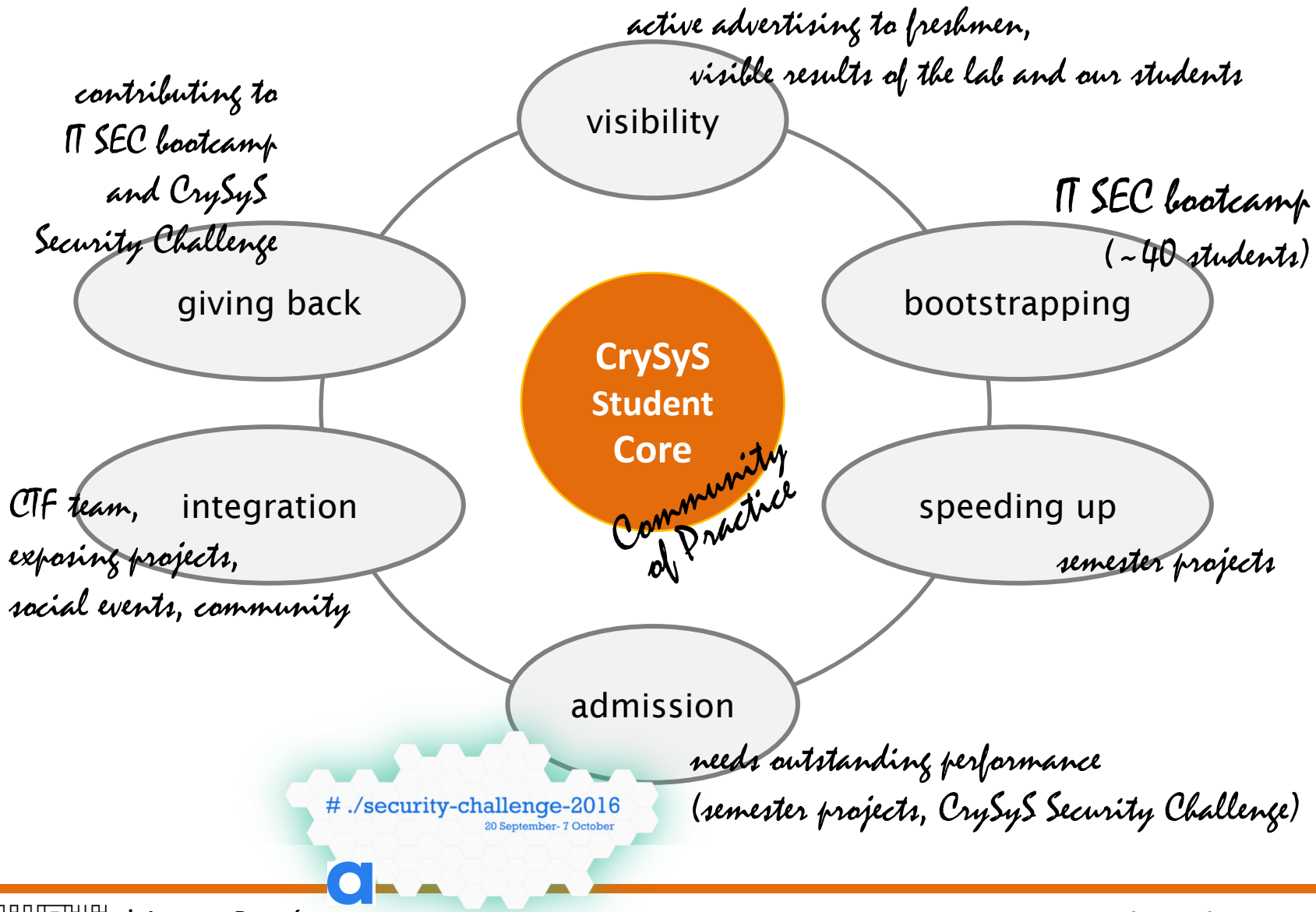
- MSc IT Security minor specialization



IT security education at BME (BProf)



Talent management



”Greatness isn’t born. It’s grown.”

ITcafé

index KÖRÚTI ROBBANTÁS | KVÓTANÉPSZAVAZÁS | HELPDESZKA | MIÉRTORSZÁG

2016. 09. 27. kedd
Adalbert

EUR: 307,75 Ft ▼
CHF: 282,53 Ft ▼

BELFÖLD KÜLFÖLD GAZDASÁG TECH TUDOMÁNY KULT SPORT VÉLEMÉNY VIDEÓ FOTÓ 24 ÓRA

TECH | HEKKER | HEKKELÉS | BME | DEFCON

Hírek » Biztonság rovat

Magyarok a legkomolyabb hekkerverseny döntőjében

Magyarok nyerték

index KÖRÚTI ROBBANTÁS | KVÓTANÉPSZAVAZÁS | HELPDESZKA | MIÉRTORSZÁG

2016. 09. 27. kedd
Adalbert

BELFÖLD KÜLFÖLD GAZDASÁG TECH TUDOMÁNY KULT SPORT VÉLEMÉNY VIDEÓ FOTÓ 24 ÓRA

májusban 284
ek (Capture The
a csapatok a
dszerekbe.

A világ legnagyobb hekkerversenyre megy a BME csapata

5 helyezett került
zottak a csapatok,
ersenyre.

A világ legrangosabb hekkertalálkozójára, a Las Vegsban megrendezett DEFCON 2016 konferenciára jutottak ki a BME Hálózati Rendszerek és Szolgáltatások Tanszék szakértői - ezt írják az egyetem Facebook-oldalán.

A CrySyS Lab csapata, a !SpamAndHex részt vehet a konferencia CTF versenyének döntőjén, a múlt hét végi selejtezőn ugyanis a tizedik helyen végzett a 276 résztvevőből.

Winners of iCTF 2014 (held in 2015)

!SpamAndHex in the DEFCON Final (2015, 2016, 2017)

coredump

iCTF 2019

Rank ▲	Team	Last Round Points	Total Score
1	Bushwhackers	1	98.67
2	WE_0WN_Y0U	0.67	83.75
3	[SPbCTF] Kappa	0.67	83.5
4	Hackerdom	0.67	80.58
5	STT	1	79.17
6	Tower of Hanoi	1	78.33
7	saarsec	0.67	77.42
8	NOPS	0	76.92
9	c0r3dump	0	76.58

c0r3dump

Academic team Budapest University of Technology and Economics

Website: https://www.crysys.hu/

Twitter: https://twitter.com/c0r3dumpCTF

0

Sign in to join the team.

Participated in CTF events

2019 2018

Overall rating place: **32** with **156.502** pts in 2019

Country place: **1**

Place	Event	CTF points	Rating points
3	WPICTF 2019	4056.0000	19.289*
14	SpamAndFlags Teaser 2019	574.0000	6.538
310	SwampCTF 2019	110.0000	0.361
127	Midnight Sun CTF 2019 Quals	307.0000	1.196
16	ENCRYPT CTF	3386.0000	19.535
16	VolgaCTF 2019 Qualifier	1826.0000	17.630
63	0CTF/TCTF 2019 Quals	604.0000	10.173
20	Teaser CONFidence CTF 2019	961.0000	10.060
9	UCSB iCTF 2019	76.5800	31.452

Spin-offs

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

- founded in 2012
- incident response, malware analysis, pentesting IT and OT systems, 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**

CloudSec Workshop, Pittsburgh, 2012

Tresorium: cryptographic file system for dynamic groups over untrusted cloud storage

István Lám[1,2], Szilveszter Szebeni [1,2], and Levente Buttyán [1,2]

[1]Tresorium Kft, Budapest, Hungary
[2]Laboratory of Cryptography and Systems Security (CrySyS), Budapest University of Technology and Economics, Hungary
[1]{*lam,szebeni*}*@tresorium.hu*, *buttyan@crysys.hu*

***Abstract*—In this paper, we present Tresorium, a cryptographic file system designed for cloud based data storage. In Tresorium, files are encrypted before they are uploaded to the cloud storage providers, therefore, not even the cloud storage providers can access the users' data. Yet, Tresorium allows the sharing files within a group of users by using an underlying group key agreement protocol. A key feature of Tresorium is that it handles changes in group membership and modification of files in an extremely efficient manner, thanks to the usage of so called key-lock-boxes and a lazy re-encryption approach. Finally, Tresorium supports an ACL-like abstraction, so it is easy to use. We describe Tresorium, and analyze its security and performance. We also present some simulation results that clearly show the efficiency of the proposed system.**

however, problematic. Firstly, if the cloud storage provider is compromised, an attacker can access every file in contempt of the ACL. Secondly, the administrators of the cloud storage provider can override the ACL settings, so they have access to the users' private files. Although ACL based systems may be implemented in more complex and secure way, the basic idea is still the same. To overcome these problems, authorization should not be done on the storage provider side. This leads us to the idea of cryptographic network file systems.

In cryptographic file systems there is no problem with an outside attacker or the curiosity of the administrators, because

tresorit

Encrypt. Sync. Share.

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

Tresorit raises €11.5 million in series B funding to help promote secure cloud collaboration

By James Bourne

04 September 2018, 15:03 p.m.
comment

Categories

Collaboration, Compliance, Security, Software

more info: https://tresorit.com/

avatao

Product Solutions Contact Careers About

Log In

Sign Up

Learn to build secure software

Acquire the right skills to implement and deploy secure applications.

Try our platform

Talk to a product specialist

https://avatao.com/

Discover paths

created by All sorted by alphabet

Paths | Challenges | Communities

OWASP Top 10 2017
by *Avatao Premium Community*
A list of the 10 Most Critical Web Application Security Risks
6%
Premium 20 | 5/79 | 215/5020

Web Security
by *Avatao Premium Community*
Common web application vulnerabilities
8%
Premium 11 | 3/37 | 175/2765

Smart Contract Security
by *Avatao Premium Community*
Known attack vectors and common anti-patterns in Solidity
0%
Premium 4 | 0/15 | 0/3610

Secure Coding in Java
by *Avatao Premium Community*
This path touches a wide range of security issues while programming in Java
0%
Premium 21 | 0/35 | 0/1350

Secure Coding in Python
by *Avatao Premium Community*
All you need to know about Python security
0%
Premium 7 | 0/31 | 0/1920

Secure Coding in C and C++
by *Avatao Premium Community*
Learn and understand how to write secure code in C and C++
0%
Premium 14 | 0/38 | 0/2365

DevSecOps
by *Avatao Premium Community*
Complete challenges and tutorials in the area of DevSecOps
0%
Premium 4 | 0/7 | 0/70

Reverse Engineering
by *Avatao Premium Community*
Disassembling is fun!
14%
Premium 7 | 4/28 | 190/4410

Secure Coding in C#
by *Avatao Premium Community*
This path touches some security issues while programming in .NET
0%
Premium 11 | 0/9 | 0/840

Mastering Cryptographic Engineering

by *Cryptography Engineering*

54% completed so far

Path

Details
Statistics
Challenges

Historical ciphers
- Trithemius cipher
- Breaking the Nihilist historical cipher
- Four-Square game
- Count and substitute

Stream ciphers
- Simple XOR cipher
- Fake Transaction
- One, Two, Buckle My Shoe

Block Encryption
- AES-CTR
- AES-CBC

Attacks on CBC
- Small Blocks
- Padding Oracle Attack

MAC functions
- XOR-MAC
- CBC-MAC
- CBC-MAC Forgery
- Final encryption is a real encryption

Secure Channels
- MAC-and-ENC protocol
- ENC-and-MAC protocol

Public Key Encryption
- Hybrid Encryption
- Hybrid Decryption
- Break RSA

Certificates
- Fake Andromeda

Four-Square game

Easy | 25 | Hints | 115
91

by Kamilla Toth

Tweet | Share

You have already solved this challenge. You don't need to solve it again, but you are free to do so.

Skill tags: Cryptography, Offensive

Description

The inspector of the military camp gets a letter from the second in command:

Uqzwhppahp pzywp tg outcdv pawaqqzk zaqzaaa. Luweaav ptn oivxazzovupwg aaq slv pqzxwq az rtn snpxgwpxspv. Ptn oboyqppwz xp upan xqzensr saxqzi ee nrxywkyqvy vk sli pwyqtlpgeqrlp. Cl pq yq weywywp, ttnz rtn negeywywp zqpqrosvlaa qrwgy upxwvl oe vgienv lz rtn etcwvlaa ywixqyywp ttn „Giwnyzi" vliivvy cslc. Slo yawgeznosq ls xzq imvcgiizv ptnnepsne slv yvuv vp ievlunqne yq yweonouzywvuo.B

The inspector knows that the encrypted text was generated with the four-square chiper, but unfortunately he lost his four-square matrices which would decrypt it. Help him to solve this problem!

Downloads
- *4square-help.pdf*
- *patterns.pdf*

Recommended readings
- *Four-square cipher (Wikipedia)*
- *Four-square cipher (GeocachingToolbox)*

Hints:

The plaintext squares contain the standard alphabet (letters are in the right order) and both i and j are in the same location (to reduce the alphabet size to 25). You may also find this document useful.

Hints

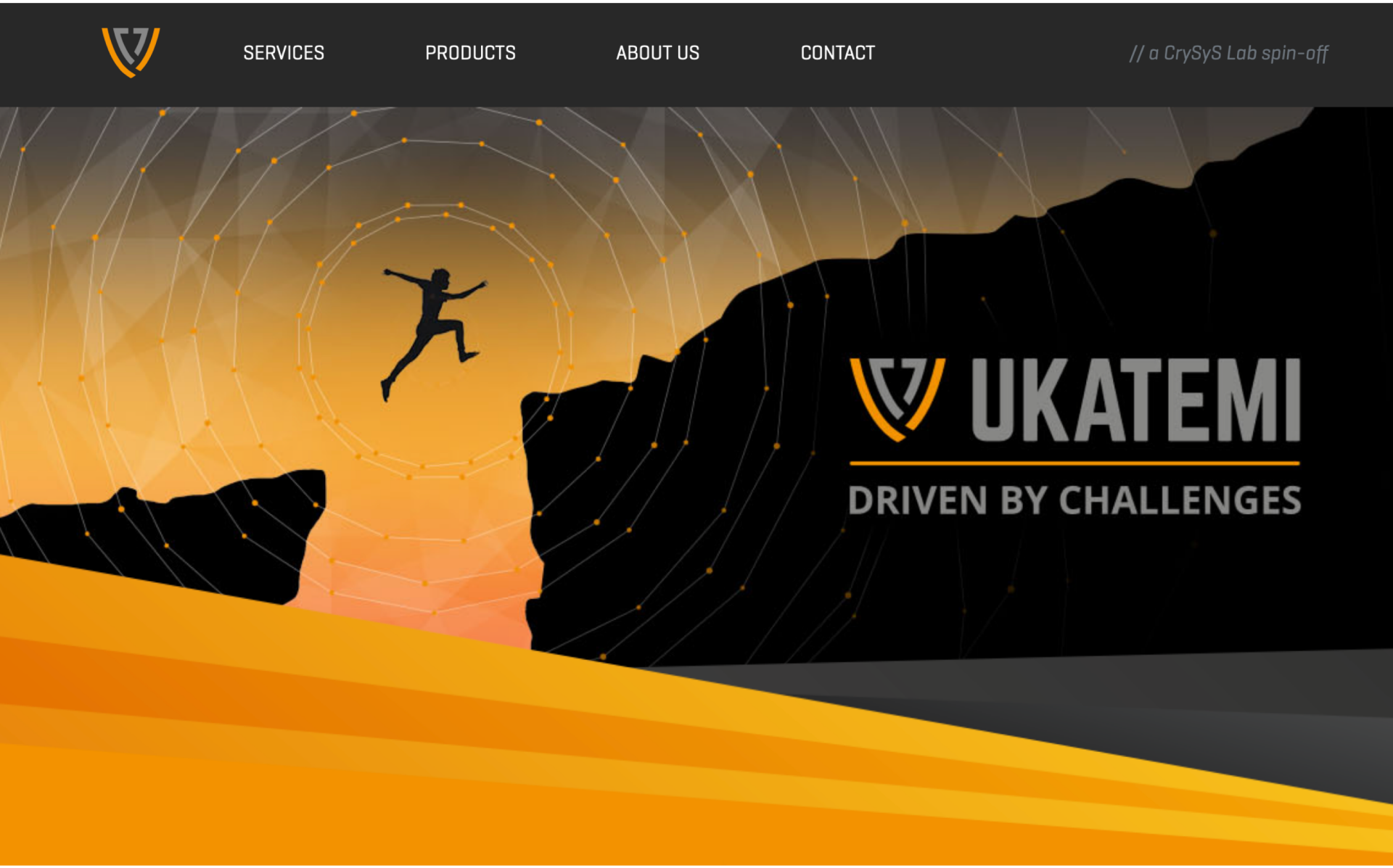
Guideline -10%

Submit your solution

Enter your acquired flag here...

Check solution

more info: https://www.youtube.com/watch?v=lJ88AO12TRI


SERVICES
PRODUCTS
ABOUT US
CONTACT
// a CrySyS Lab spin-off
UKATEMI
DRIVEN BY CHALLENGES

Key competencies and assets of Ukatemi

- Reverse engineering and malware analysis know-how
- Membership in trust based communities
- Own malware database with advanced search capabilities
- Penetration testing (ethical hacking) know-how
- Customized testing of security products
- Security of cyber-physical systems
  - ICS/SCADA (including nuclear facilities)
  - vehicles (CAN, V2X)
  - Internet of Things (e.g., smart meters)

Thanks!

Levente Buttyán
buttyan@crysys.hu