Introducing the CrySyS Lab

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

Mission

- internationally recognized, **high quality research** on security and privacy in computer systems and networks
- **teaching** IT security and applied cryptography in the context of university courses, laboratory exercises, and student semester projects
- provision of **consulting** services without compromising the general academic objectives

Current members

- faculty members
  - Levente Buttyán, PhD, habil, Associate Professor (head of the lab)
  - Boldizsár Bencsáth, PhD, Assistant Professor
  - Márk Félegyházi, PhD, Assistant Professor
  - Tamás Holczer, PhD, Assistant Professor
  - Gergely Ács, Phd, Assistant Professor (from fall 2016)
  - Gergely Biczók, Phd, Assistant Professor (from fall 2016)

- PhD students
  - Dorottya Papp (security assurance in cyber-phyiscal systems)
  - András Gazdag (forensic analysis in cyber-physical systems)
  - Máté Horváth (cryptographic obfuscation)

+ associate members

+ CrySyS Student Core
  - 12-16 talented students and alumni working with us permanently

+ students working on diploma and semester projects

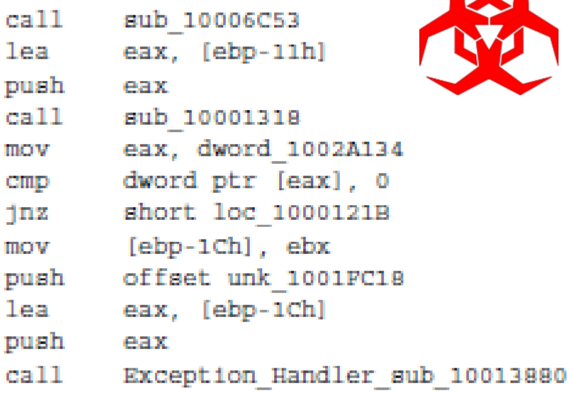
Technical competence

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

- security in cyber-physical systems
  - industrial automation and control systems, in-vehicle embedded networks and devices
  - vulnerability assessment, security assurance, anomaly detection, incident response, forensic analysis

Technical competence

- malware analysis
  - static and dynamic program analysis, reverse engineering, memory forensics
  - involvement in the analysis of multiple high profile targeted malware (APT)



```
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
```

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

- privacy enhancing techniques
  - anonymization of large data sets

Selected EU projects

SeVeCom – Secure Vehicle Communications (www.sevecom.org)
(EU STREP, 2006-2008)

UbiSec&Sens – Ubiquitous Sensing and Security (www.ist-ubisecsens.org)
(EU STREP, 2006-2008)

WSAN4CIP – Wireless Sensor Networks for Critical Infrastructure Protection
(EU STREP, 2009-2011)

EU-MESH – Enhanced, Ubiquitous, and Dependable Broadband Access using MESH Networks (www.eu-mesh.eu)
(EU STREP, 2008-2010)

CHIRON – Cyclic and Person Centric Health Management (www.chiron-project.eu) (ARTEMIS IP, 2010-2012)

Some results on targeted malware analysis

- Duqu (October 2011)
  - discovery, naming, and first analysis of Duqu

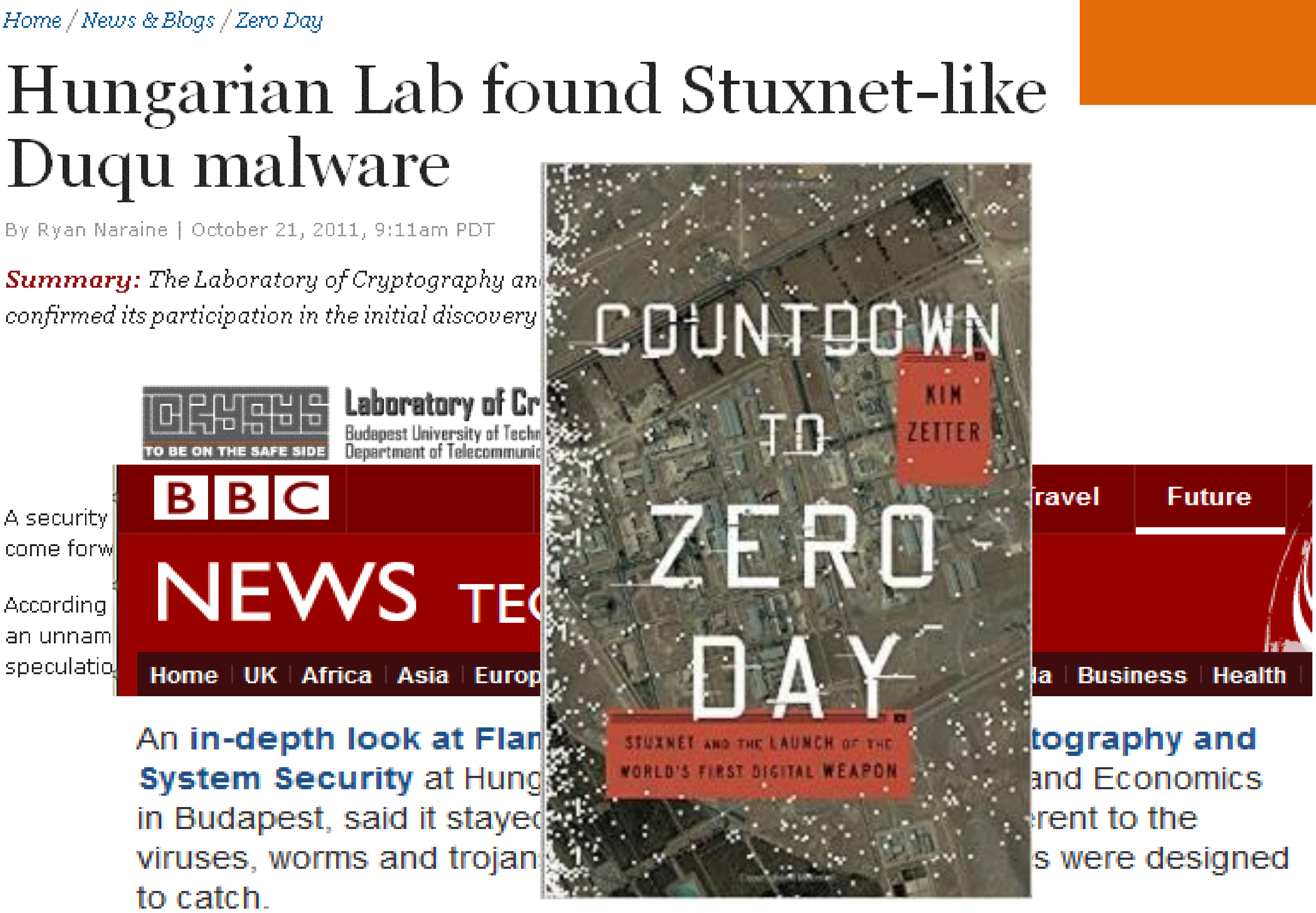
    striking similarities to **Stuxnet**, but different mission (info-stealer)
  - identification of the dropper component

    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
- Duqu 2.0 (June 2015)
  - detailed comparison with the original Duqu

    recovering signs of common origin



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 an*
confirmed its participation in the initial discovery

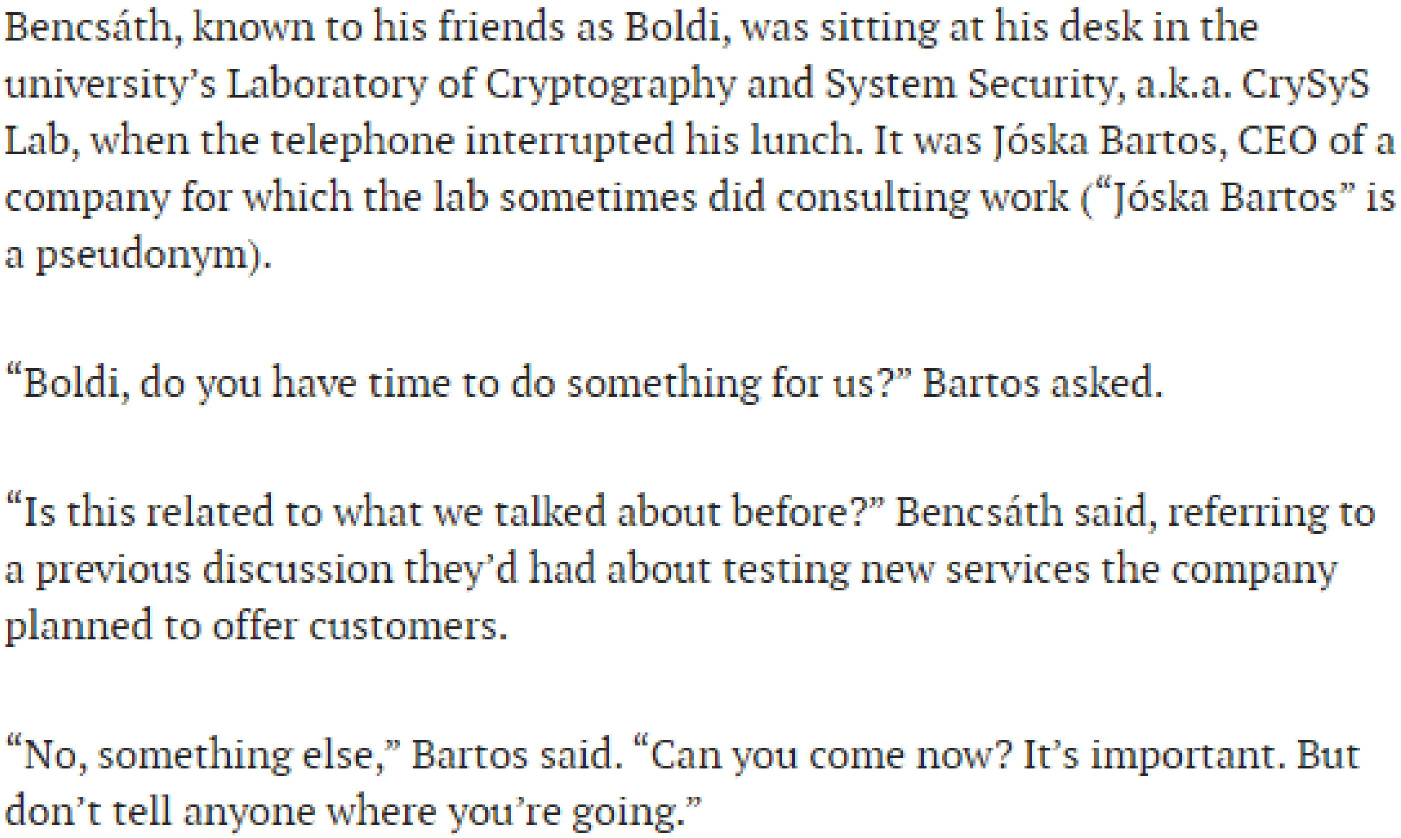
CrySyS
TO BE ON THE SAFE SIDE
Laboratory of Cr
Budapest University of Techn
Department of Telecommunic

A security
come forw

According
an unnam
speculatio

An **in-depth look at Flan** **tography and**
System Security at Hung and Economics
in Budapest, said it stayed rent to the
viruses, worms and trojan s were designed
to catch.

Excerpt from the book



Bencsáth, known to his friends as Boldi, was sitting at his desk in the university's Laboratory of Cryptography and System Security, a.k.a. CrySyS Lab, when the telephone interrupted his lunch. It was Jóska Bartos, CEO of a company for which the lab sometimes did consulting work ("Jóska Bartos" is a pseudonym).

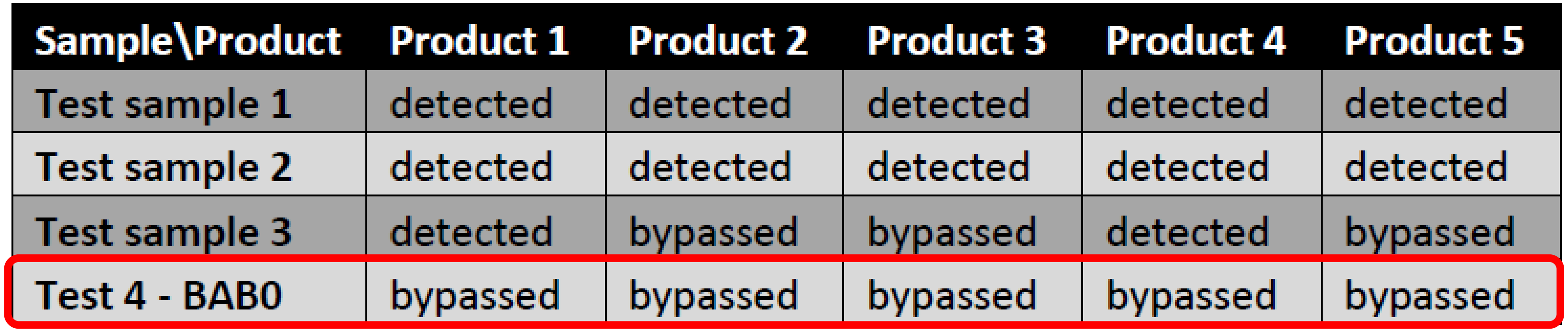
"Boldi, do you have time to do something for us?" Bartos asked.

"Is this related to what we talked about before?" Bencsáth said, referring to a previous discussion they'd had about testing new services the company planned to offer customers.

"No, something else," Bartos said. "Can you come now? It's important. But don't tell anyone where you're going."

Recent research projects

- testing APT detection tools
  - new tools specially developed to detect unkown malware (e.g., FireEye, Cisco SourceFire, Palo Alto's WildFire)
  - how good they are?
  - we tested them with custom developed samples
    - all test samples implemented RAT functionality
    - remote C&C communication via back-connect



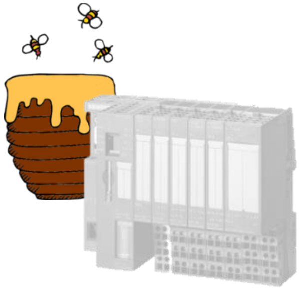
Sample\Product	Product 1	Product 2	Product 3	Product 4	Product 5
Test sample 1	detected	detected	detected	detected	detected
Test sample 2	detected	detected	detected	detected	detected
Test sample 3	detected	bypassed	bypassed	detected	bypassed
Test 4 - BAB0	bypassed	bypassed	bypassed	bypassed	bypassed

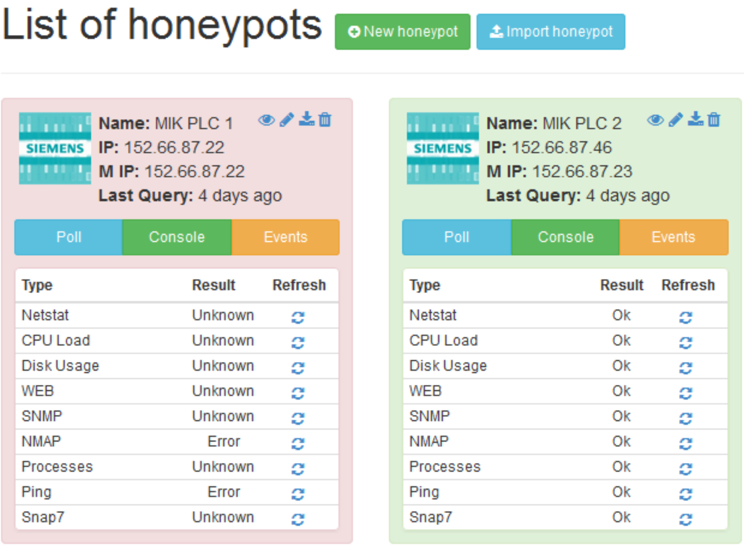
Recent research projects

- Repository of Signed Code (funded by ONRG)
  - advanced attackers (APTs) started to use malware signed with compromised keys or fake certificates
    - Stuxnet, Duqu, Flame, ...
  - standard signature verification procedures cannot identify compromised keys and fake certificates
  - ROSCO is a large database where we collect signed objects
  - ROSCO can augment the standard signature verification workflow with additional services that help to detect compromised keys, fake certificates, and signed malware
    - notify key owner when a new object signed with a specific key is seen
    - provide reputation information on signers and signed code
  - available for testing at rosco.crysys.hu

Recent research projects

- design and development of a PLC honeypot
  - a decoy system that apears to be a real PLC
  - allows for the observation of attacker steps
  - our honeypot simulates a Siemens Simatic 300 PLC
  - high interaction level (set values can be read back)
  - special attention to make it indistinguishable from a real PLC
  - web based honeypot management system





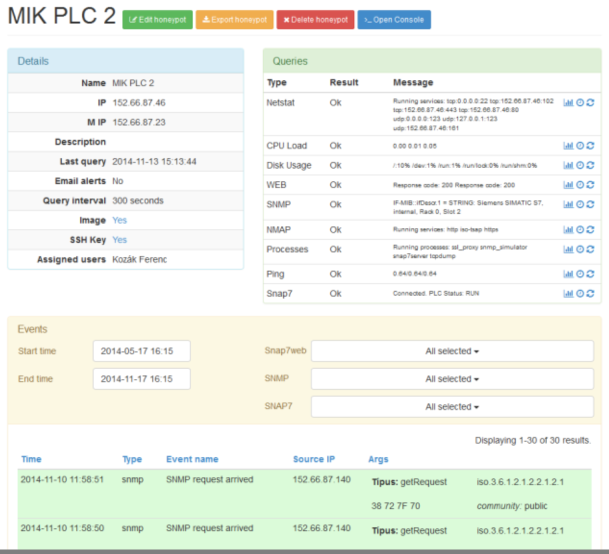
List of honeypots

Name: MIK PLC 1
IP: 152.66.87.22
M IP: 152.66.87.22
Last Query: 4 days ago

Type	Result	Refresh
Netstat	Unknown	⟳
CPU Load	Unknown	⟳
Disk Usage	Unknown	⟳
WEB	Unknown	⟳
SNMP	Unknown	⟳
NMAP	Error	⟳
Processes	Unknown	⟳
Ping	Error	⟳
Snap7	Unknown	⟳

Name: MIK PLC 2
IP: 152.66.87.46
M IP: 152.66.87.23
Last Query: 4 days ago

Type	Result	Refresh
Netstat	Ok	⟳
CPU Load	Ok	⟳
Disk Usage	Ok	⟳
WEB	Ok	⟳
SNMP	Ok	⟳
NMAP	Ok	⟳
Processes	Ok	⟳
Ping	Ok	⟳
Snap7	Ok	⟳



MIK PLC 2

Details

Name	MIK PLC 2
IP	152.66.87.46
M IP	152.66.87.23
Description	
Last query	2014-11-13 15:13:44
Email alerts	No
Query interval	300 seconds
Image	Yes
SSH Key	Yes
Assigned users	Kozák Ferenc

Queries

Type	Result	Message
Netstat	Ok	Running services: tcp:0.0.0.0:22 tcp:152.66.87.46:102 tcp:152.66.87.46:443 tcp:152.66.87.46:80 udp:0.0.0.0:123 udp:127.0.0.1:123 udp:152.66.87.46:161
CPU Load	Ok	0.00 0.01 0.05
Disk Usage	Ok	/:10% /dev:1% /run:1% /run/lock:0% /run/shm:0%
WEB	Ok	Response code: 200 Response code: 200
SNMP	Ok	IF-MIB::ifDescr.1 = STRING: Siemens SIMATIC S7, internal, Rack 0, Slot 2
NMAP	Ok	Running services: http iso-tsap https
Processes	Ok	Running processes: ssl_proxy snmp_simulator snap7server tcpdump
Ping	Ok	0.64/0.64/0.64
Snap7	Ok	Connected. PLC Status: RUN

Events

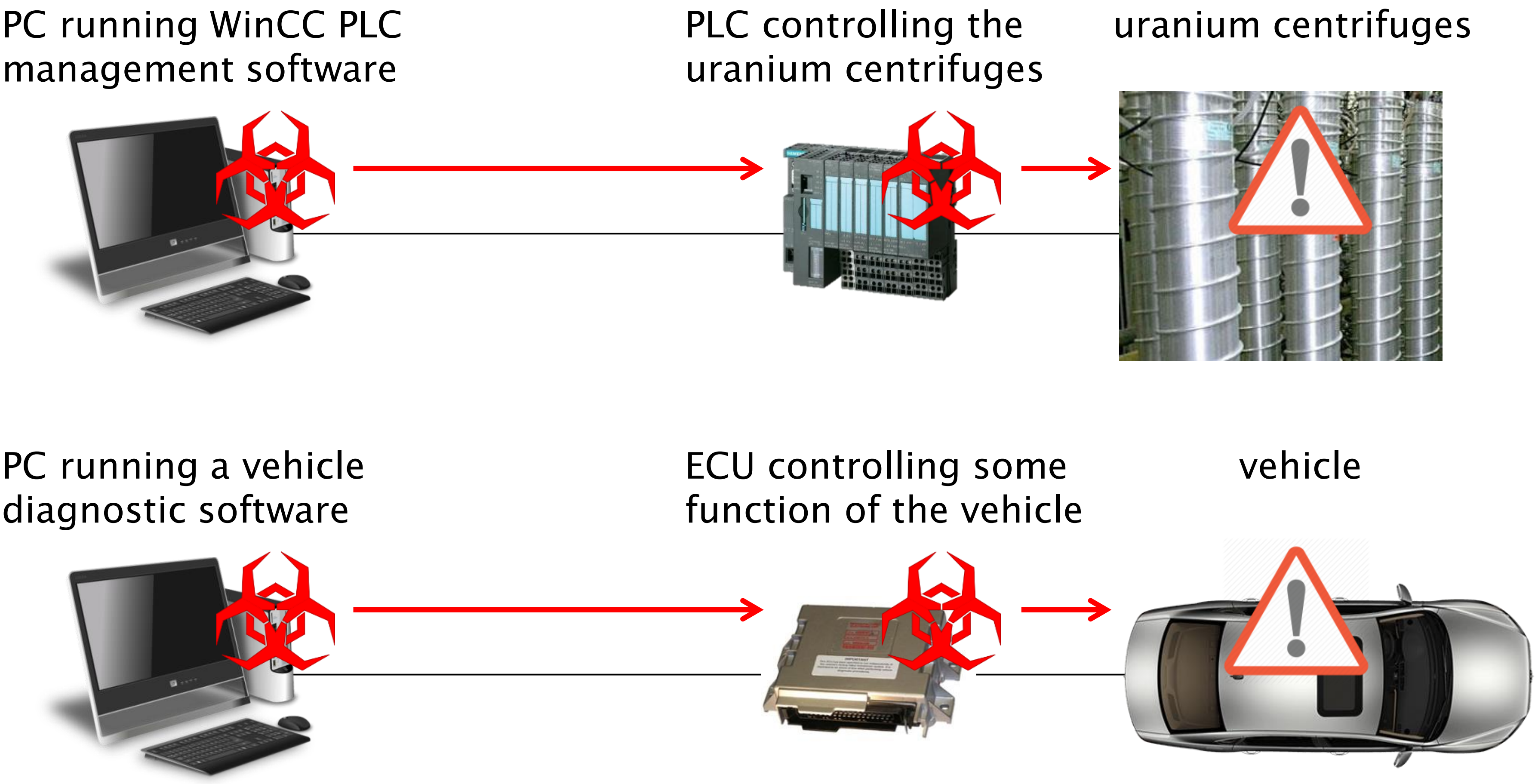
Start time: 2014-05-17 16:15
End time: 2014-11-17 16:15
Snap7web: All selected
SNMP: All selected
SNAP7: All selected

Displaying 1-30 of 30 results.

Time	Type	Event name	Source IP	Args	
2014-11-10 11:58:51	snmp	SNMP request arrived	152.66.87.140	**Tipus:** getRequest 38 72 7F 70	iso.3.6.1.2.1.2.2.1.2.1 *community:* public
2014-11-10 11:58:50	snmp	SNMP request arrived	152.66.87.140	**Tipus:** getRequest	iso.3.6.1.2.1.2.2.1.2.1

Recent research projects

- hacking cars in the style of Stuxnet



PC running WinCC PLC management software

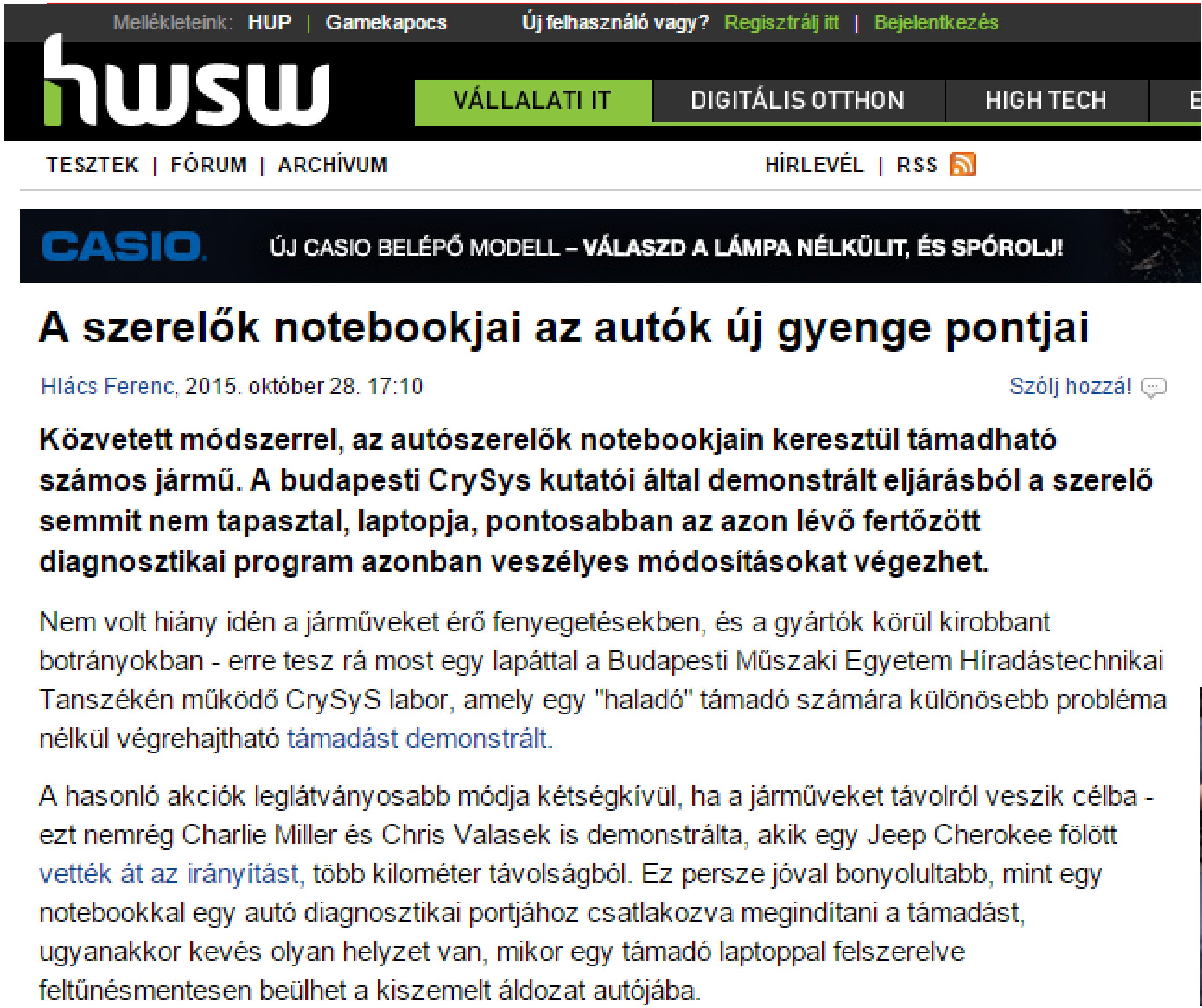
PLC controlling the uranium centrifuges

uranium centrifuges

PC running a vehicle diagnostic software

ECU controlling some function of the vehicle

vehicle


Mellékleteink: HUP | Gamekapocs
Új felhasználó vagy? Regisztrálj itt | Bejelentkezés
hwsw
VÁLLALATI IT
DIGITÁLIS OTTHON
HIGH TECH
E
TESZTEK | FÓRUM | ARCHÍVUM
HÍRLEVÉL | RSS

CASIO ÚJ CASIO BELÉPŐ MODELL – VÁLASZD A LÁMPA NÉLKÜLIT, ÉS SPÓROLJ!

A szerelők notebookjai az autók új gyenge pontjai

Hlács Ferenc, 2015. október 28. 17:10

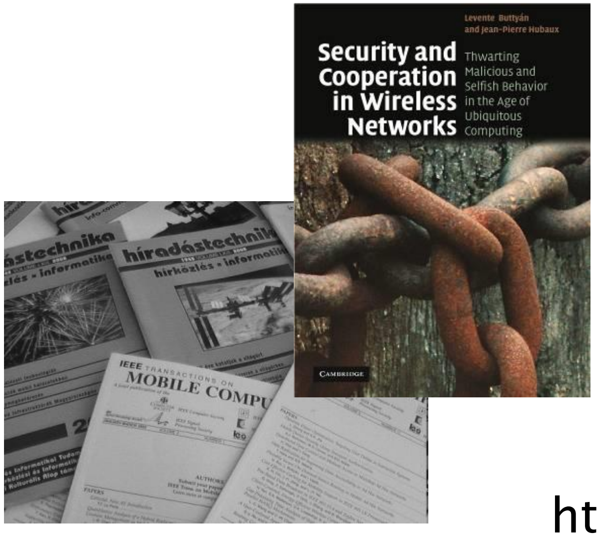
Közvetett módszerrel, az autószerelők notebookjain keresztül támadható számos jármű. A budapesti CrySys kutatói által demonstrált eljárásból a szerelő semmit nem tapasztal, laptopja, pontosabban az azon lévő fertőzött diagnosztikai program azonban veszélyes módosításokat végezhet.

Nem volt hiány idén a járműveket érő fenyegetésekben, és a gyártók körül kirobbant botrányokban - erre tesz rá most egy lapáttal a Budapesti Műszaki Egyetem Híradástechnikai Tanszékén működő CrySyS labor, amely egy "haladó" támadó számára különösebb probléma nélkül végrehajtható támadást demonstrált.

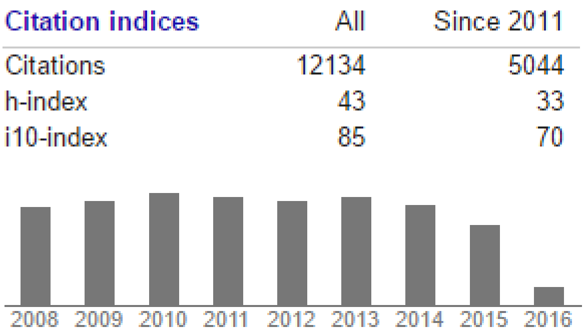
A hasonló akciók leglátványosabb módja kétségkívül, ha a járműveket távolról veszik célba - ezt nemrég Charlie Miller és Chris Valasek is demonstrálta, akik egy Jeep Cherokee fölött vették át az irányítást, több kilométer távolságból. Ez persze jóval bonyolultabb, mint egy notebookkal egy autó diagnosztikai portjához csatlakozva megindítani a támadást, ugyanakkor kevés olyan helyzet van, mikor egy támadó laptoppal felszerelve feltűnésmentesen beülhet a kiszemelt áldozat autójába.

Publications

- 7 books
- 10 book chapters
- 80 journal papers
- 120 conference papers
- 2 Internet Drafts
- 5 patents

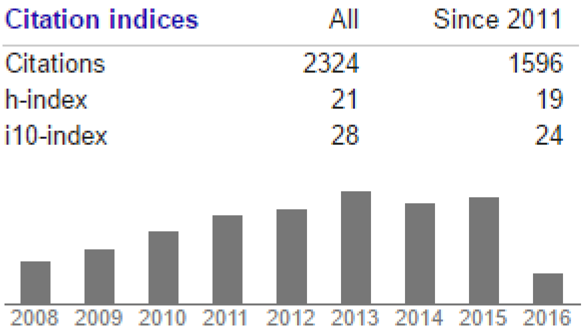

Levente Buttyán and Jean-Pierre Hubaux
Security and Cooperation in Wireless Networks
Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing
CAMBRIDGE
híradástechnika
hírközlés · informatika
IEEE TRANSACTIONS ON MOBILE COMPU

Levente Buttyán



Citation indices	All	Since 2011
Citations	12134	5044
h-index	43	33
i10-index	85	70

Márk Félegyházi



Citation indices	All	Since 2011
Citations	2324	1596
h-index	21	19
i10-index	28	24

papers available online at:
http://www.crysys.hu/research/publications/

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 at University of Lanceshire, UK)
- Dr. Áron Lászka (2014) (currently with UC Berkeley, USA)
- Dr. Gábor Gulyás (2015) (currently with INRIA Rhones-Alpes, France)
- Dr. Gábor Pék (2015) (currently with Avatao and CrySyS Lab)

Spin-offs started from the CrySyS Lab

tresorit

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

Ukatemi
advanced threat
mitigation technologies

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

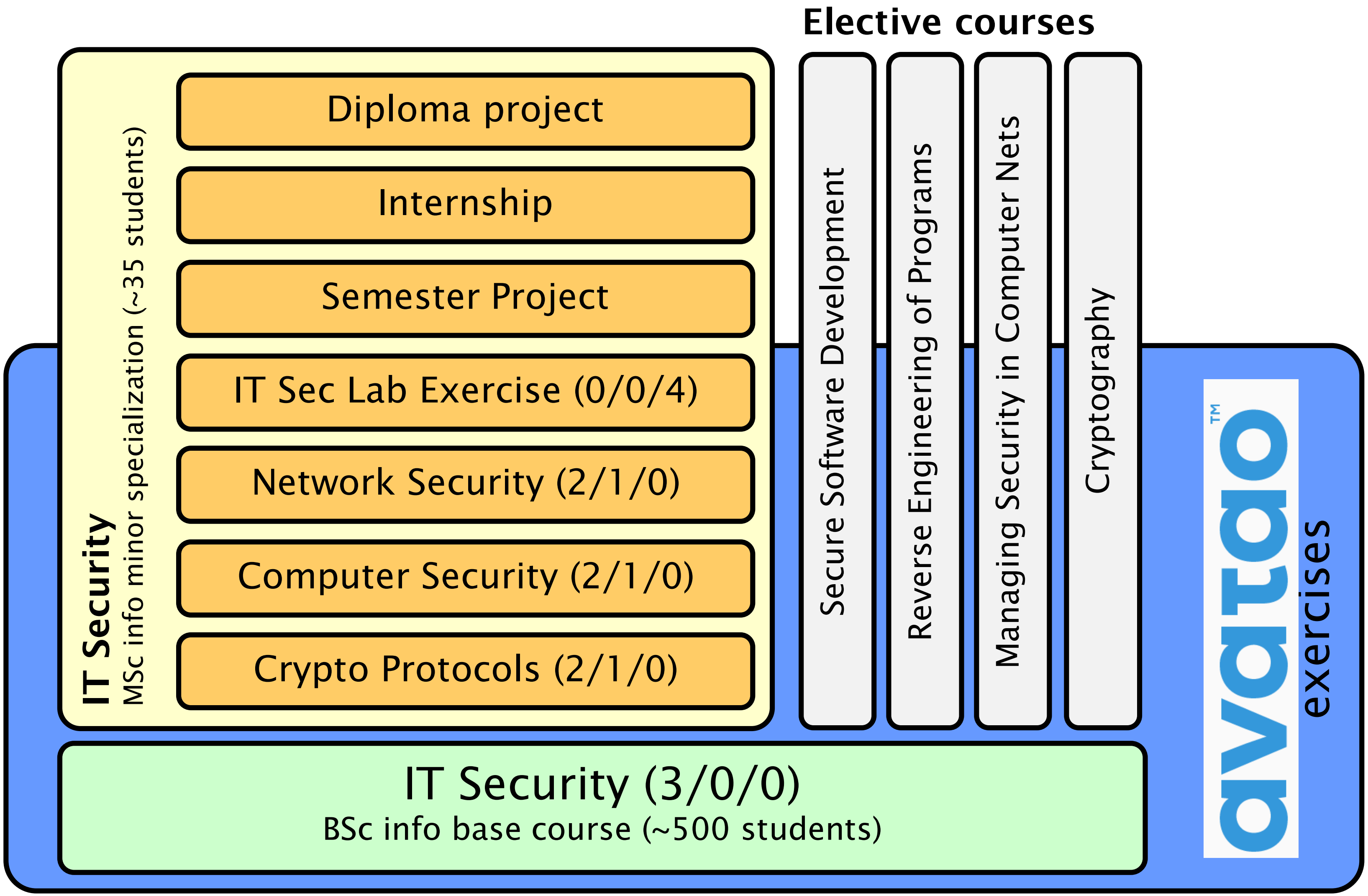
IT-SEC Expert
www.it-sec.hu

- founded in 2012
- malware analysis training, cyber security exercises

avatao™

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

IT security education at BME



Elective courses

- Secure Software Development
- Reverse Engineering of Programs
- Managing Security in Computer Nets
- Cryptography

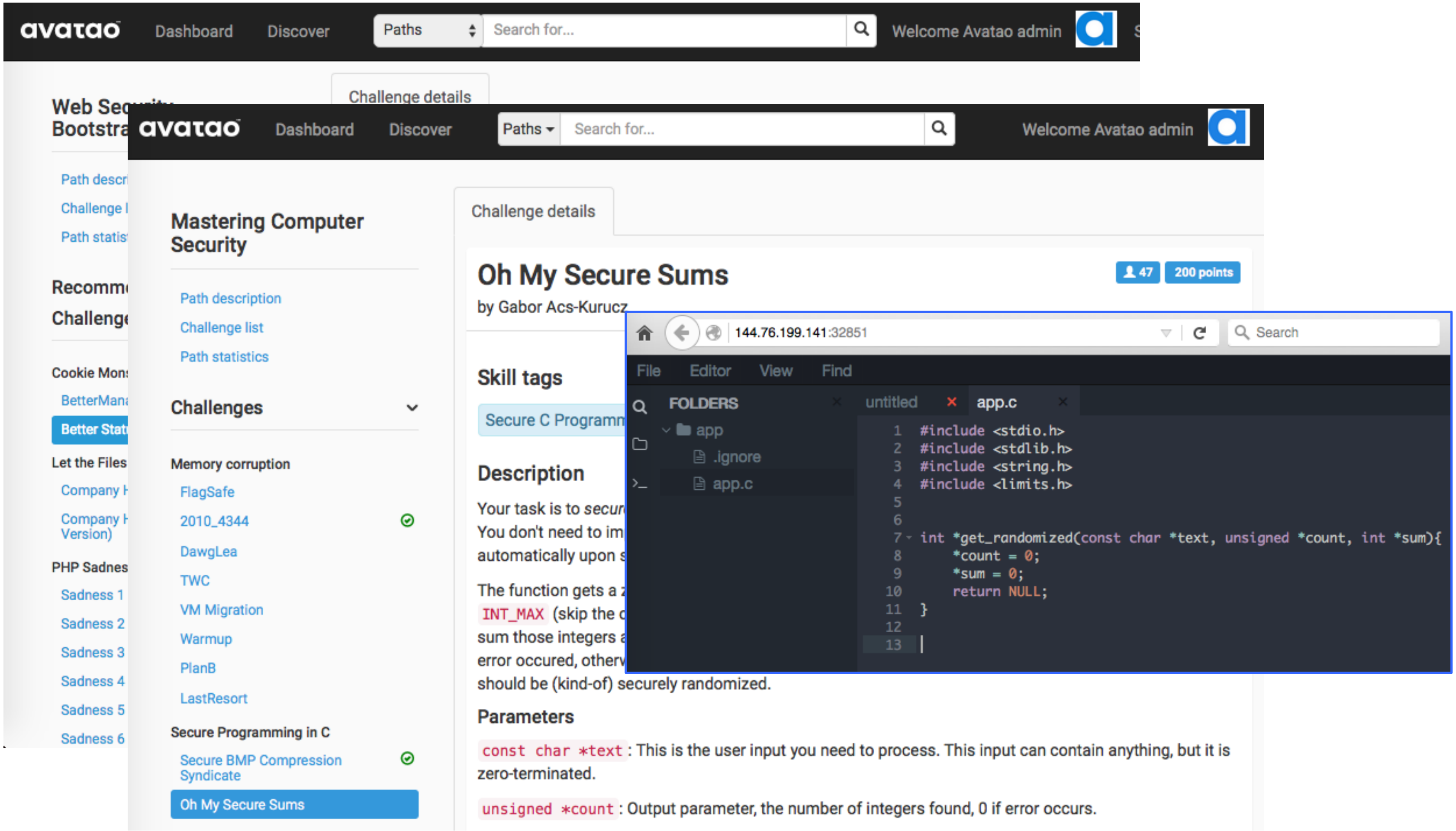
IT Security
MSc info minor specialization (~35 students)

- 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)

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

avatao™ exercises

avatao – on-line IT security exercises



Oh My Secure Sums

by Gabor Acs-Kurucz

Skill tags

Secure C Programm

Description

Your task is to *secur*
You don't need to im
automatically upon s

The function gets a z
`INT_MAX` (skip the c
sum those integers a
error occured, otherw
should be (kind-of) securely randomized.

Parameters

`const char *text` : This is the user input you need to process. This input can contain anything, but it is zero-terminated.

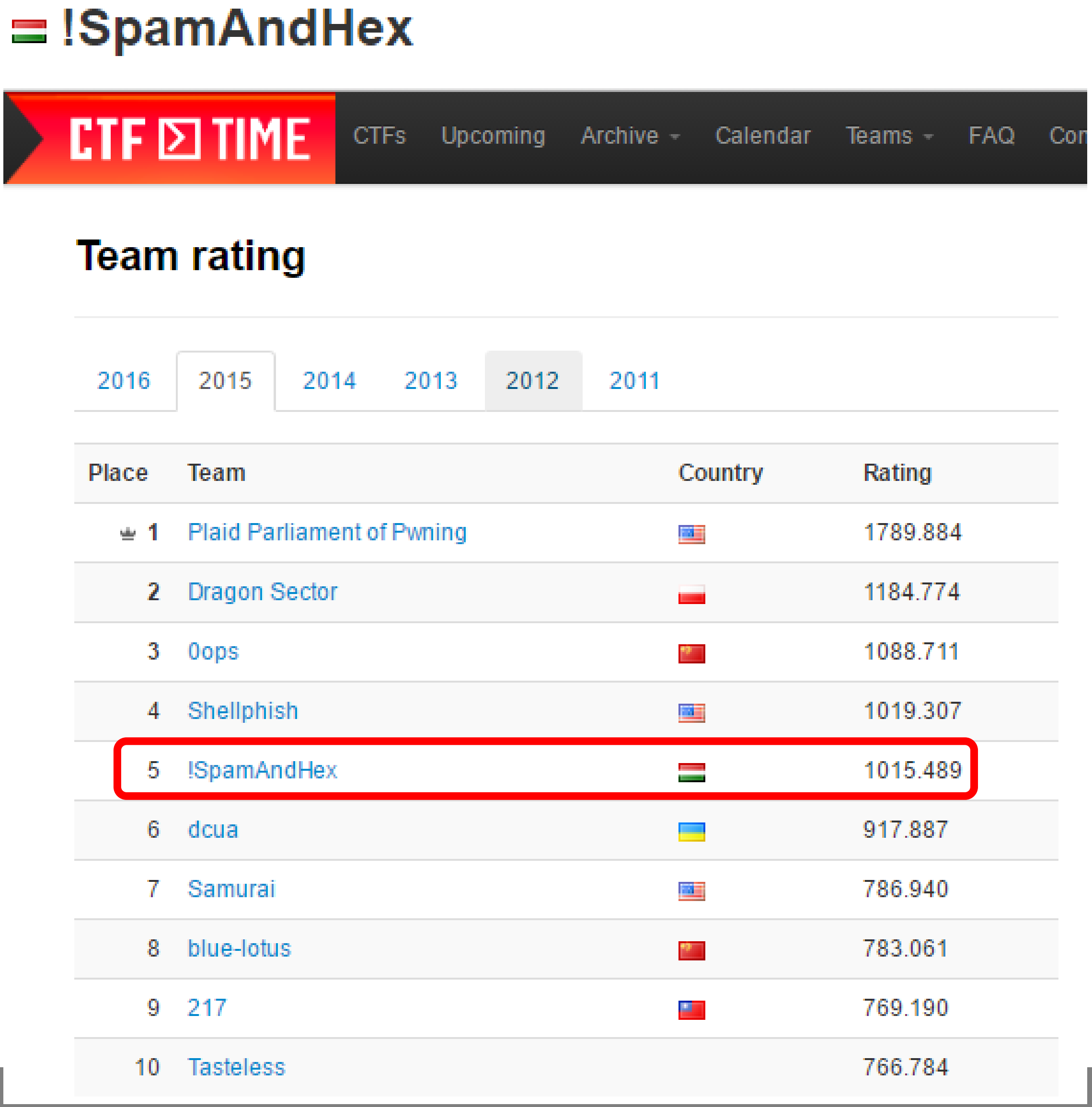
`unsigned *count` : Output parameter, the number of integers found, 0 if error occurs.

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <limits.h>


int *get_randomized(const char *text, unsigned *count, int *sum){
    *count = 0;
    *sum = 0;
    return NULL;
}

```

Talent management

- CrySyS Student Core
  - invite-only group of talented students, community of practice
  - sharing specialized knowledge, improving hacking skills, participation on CTF competitions (→ !SpamAndHex team)
  - 12-16 students and alumni, regular meetings
- annual CrySyS Security Challenge
  - from 2011, always in the fall semester
  - best performing students are invited into the Student Core
- CrySyS IT Security Bootcamp
  - preparation for the CrySyS Sec Challenge and more
  - supervised exercise sessions using avatao
  - appr. 30 students (in spring semester)

!SpamAndHex



🇭🇺 !SpamAndHex

Team rating

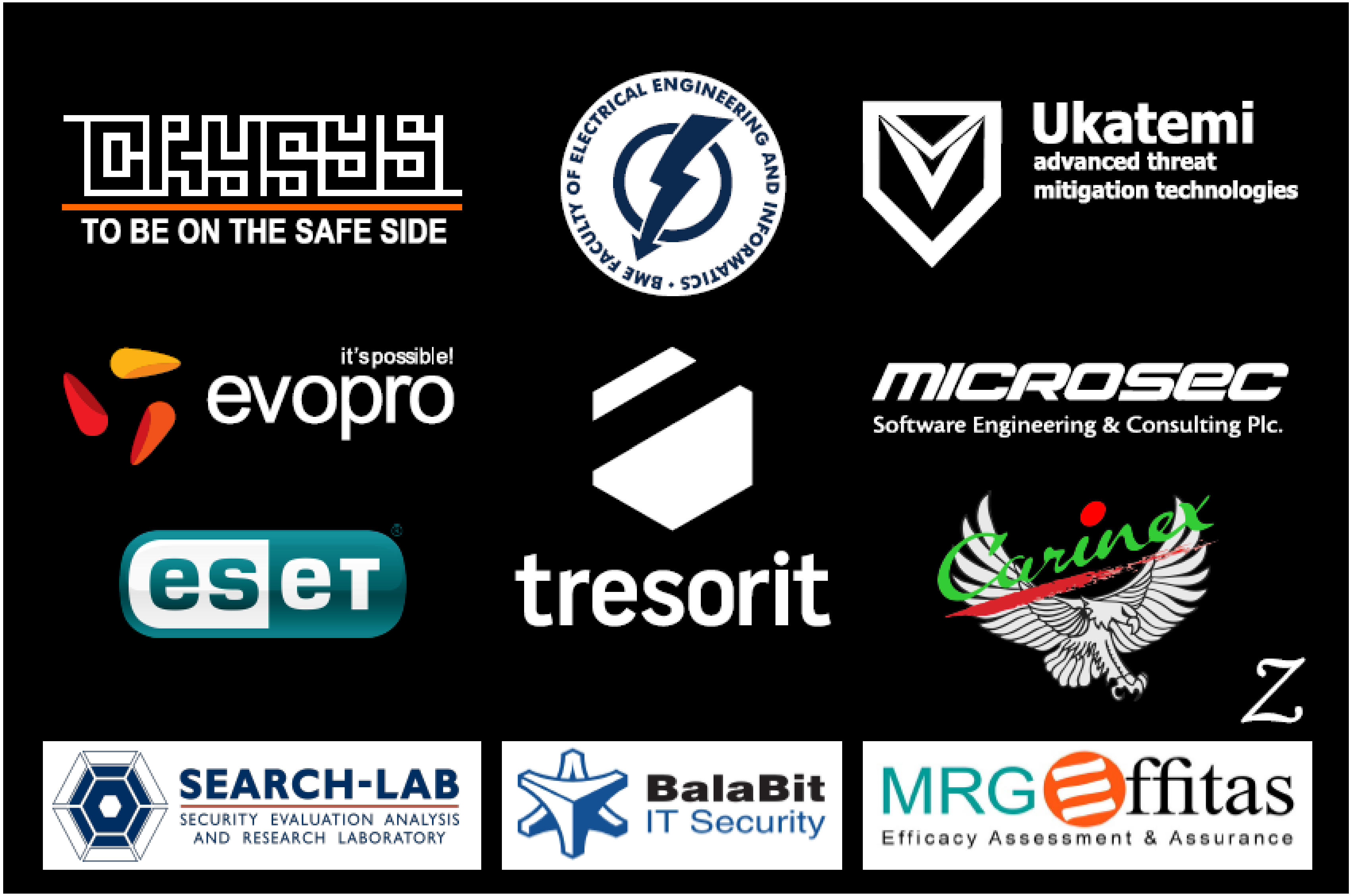
2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Plaid Parliament of Pwning	🇺🇸	1789.884
2	Dragon Sector	🇵🇱	1184.774
3	0ops	🇨🇳	1088.711
4	Shellphish	🇺🇸	1019.307
5	!SpamAndHex	🇭🇺	1015.489
6	dcua	🇺🇦	917.887
7	Samurai	🇺🇸	786.940
8	blue-lotus	🇨🇳	783.061
9	217	🇹🇼	769.190
10	Tasteless		766.784

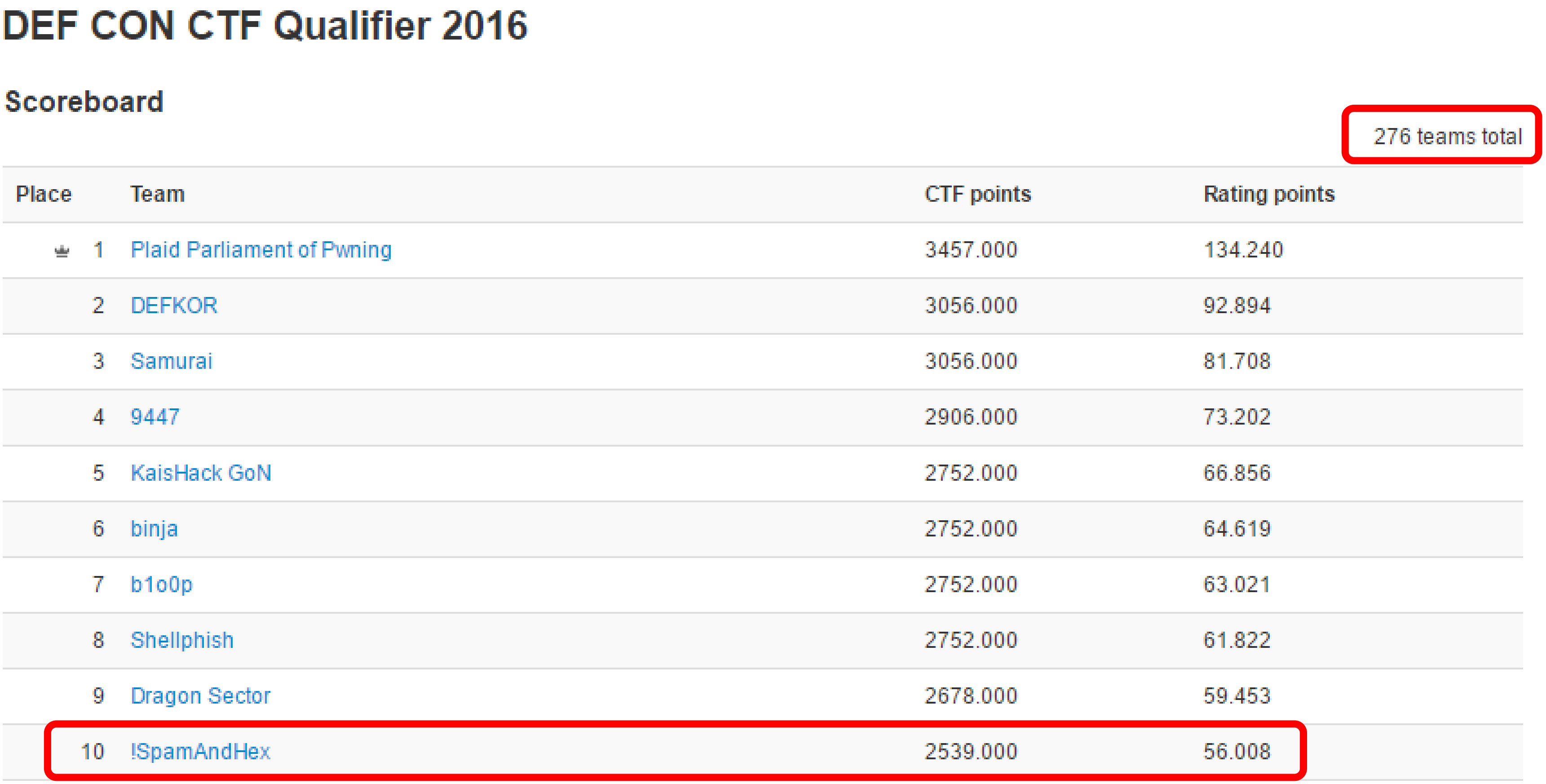
Winners of iCTF 2014 (March 2015)

Qualified for DEFCON 2015 CTF Finals

Sponsors of our DEFCON CTF team in 2015



Qualified for DEFCON 2016 CTF Finals !!!



DEF CON CTF Qualifier 2016

Scoreboard

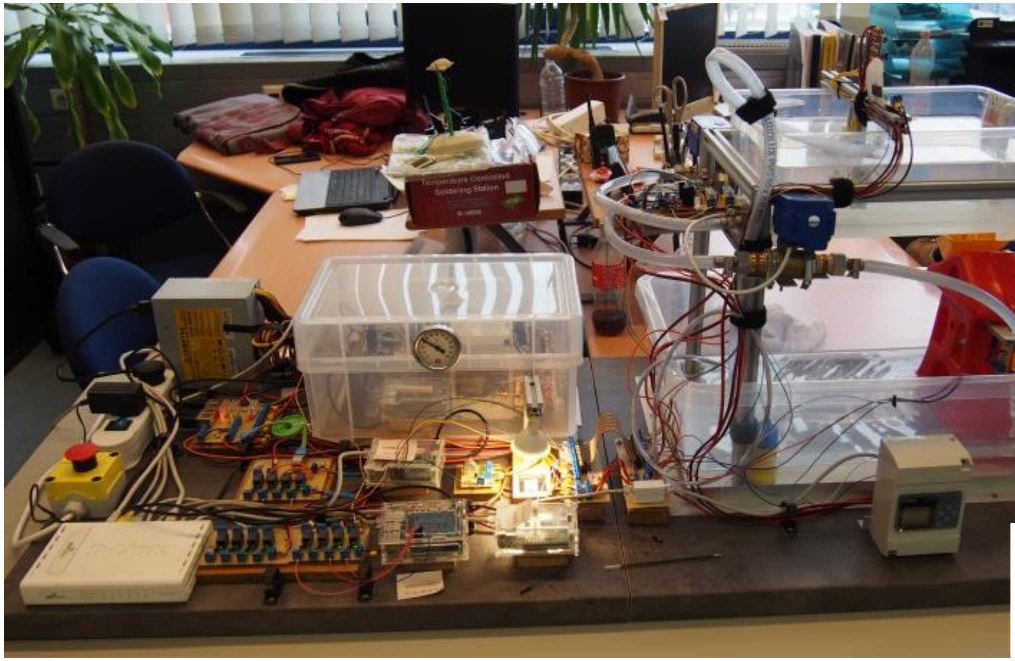
276 teams total

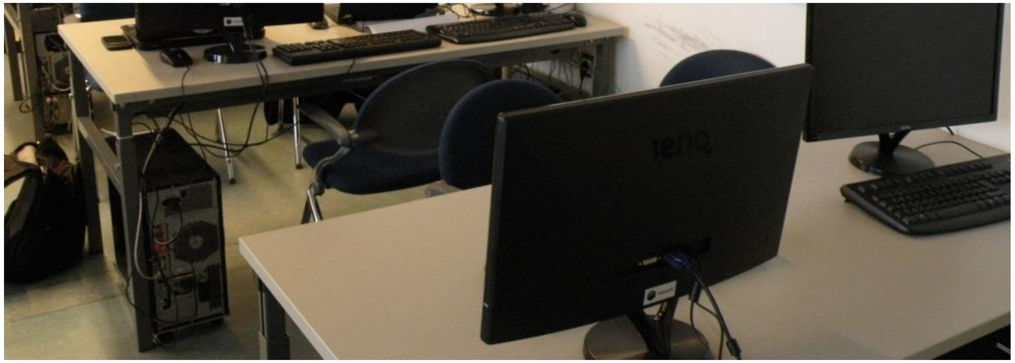
Place	Team	CTF points	Rating points
♛ 1	Plaid Parliament of Pwning	3457.000	134.240
2	DEFKOR	3056.000	92.894
3	Samurai	3056.000	81.708
4	9447	2906.000	73.202
5	KaisHack GoN	2752.000	66.856
6	binja	2752.000	64.619
7	b1o0p	2752.000	63.021
8	Shellphish	2752.000	61.822
9	Dragon Sector	2678.000	59.453
10	!SpamAndHex	2539.000	56.008

Sponsors of our DEFCON CTF team in 2016

HUNITYDEFENSE
HUNGARIAN CYBER SECURITY CONSORTIUM
CRYSYS
www.crysys.hu
BME FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS
tresorit
dimension data
TMSI
MICROSEC
Software Engineering & Consulting Plc.
SYMMETRIA MAGYARORSZÁG
Információ Integritás Kft.
SOPHOS
eset
MRG Effitas
Efficacy Assessment & Assurance
SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY
BalaBit
IT Security

Our infrastructure





We are thankful to ...

it's possible!
evopro

SIEMENS

MICROSEC

tresorit

BalaBit
IT Security

IBM®

MRG Effitas
Efficacy Assessment & Assurance

Possible forms of collaboration

- get involved in teaching
  - invited lectures in different courses
  - full elective course
- offering projects for students
  - semseter project
  - diploma project (BSc – 1 semester, MSc – 2 semesters)
  - internship (6-8 weeks)
- offering exercises
  - building some laboratory exercises on the partner’s product
  - contributing exercises to avatao
- scolarships to students and to faculty
- R&D projects
  - duration can be 6-12 months (with possibility to expand if needed)
  - close collaboration with industry partner
  - faculty engagement improves students’ productivity
- sponsoring
  - talent management (Student Core, !SpamAndHex team, IT Security bootcamp, CrySyS Sec Challenge)
  - infrastructure (student PCs, servers, software licenses)

www.crysys.hu

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