A CRYSYS LABORRÓL
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

- PhD students
  - Dorottya Papp (security and safety co-design)
  - András Gazdag (forensic analysis of embedded systems)
  - Máté Horváth (cryptographic obfuscation)

- associate members

+ CrySyS Student Core
  - 12-15 talented students and alumni working with us permanently

+ students working on diploma and semester projects
Technical competence

- **Design of security mechanisms and privacy enhancing solutions 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, firmware integrity, incident response, forensic analysis
Technical competence

- **detection and analysis of unknown targeted malware**
  - static and dynamic program analysis, reverse engineering, memory forensics, rootkit detection
  - multiple platforms (Windows, Linux, Android)

- **applied cryptography**
  - cryptographic protocols for secure communications, secure data storage, and code obfuscation

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

By Ryan Naraine | October 21, 2011

Summary: The Laboratory confirmed its participation in the investigation.

A security come forward.

According an unnam speculation:

An in-depth System Se in Budapest viruses, work to catch.

...
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.”
Spin-offs

- **tresorit**
  - founded in 2011
  - sharable encrypted data storage in the cloud
  - web site: [www.tresorit.com](http://www.tresorit.com)

- **Ukatemi**
  - founded in 2012
  - malware threat intelligence, cyber incident response
  - web site: [www.ukatemi.com](http://www.ukatemi.com)

- **IT-SEC Expert**
  - founded in 2012
  - industry oriented research, development, and training
  - web site: [www.it-sec.hu](http://www.it-sec.hu)

- **AVATAO**
  - founded in 2014
  - talent management system with personalized learning paths and hands-on exercises
  - web site: [www.avatao.com](http://www.avatao.com)
Teaching

**IT Security MSc info minor specialization**

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

**IT Security (3/0/0)**

BSc info base course

**Elective courses**

- Secure Software Development (planned)
- Reverse Engineering of Programs
- Managing Security in Computer Nets
- Foundations of Cryptography
- Privacy Enhancing Technologies
- Economics of Security and Privacy

**Avatao on-line exercises**
Talent management

- annual CrySyS Security Challenges
  [http://www.crysys.hu/security-challenges.html](http://www.crysys.hu/security-challenges.html)

- CrySyS Student Core
  invite-only self-study group of talented students
  - appr. 15 students and alumni (every Thursday, 6pm-8pm)

- CrySyS Novice Group
  preparation for the Sec Challenge and more...
  - appr. 30 students (every Wednesday, 5pm-7pm)
<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Plaid Parliament of Pwning</td>
</tr>
<tr>
<td>2</td>
<td>oops</td>
</tr>
<tr>
<td>3</td>
<td>Dragon Sector</td>
</tr>
<tr>
<td>4</td>
<td>Glopshot</td>
</tr>
<tr>
<td>5</td>
<td>!SpamAndHex</td>
</tr>
<tr>
<td>6</td>
<td>blue-lotus</td>
</tr>
<tr>
<td>7</td>
<td>dcue</td>
</tr>
<tr>
<td>8</td>
<td>217</td>
</tr>
<tr>
<td>9</td>
<td>HITCON</td>
</tr>
<tr>
<td>10</td>
<td>Samurai</td>
</tr>
<tr>
<td>11</td>
<td>Tasteless</td>
</tr>
<tr>
<td>12</td>
<td>0daysober</td>
</tr>
</tbody>
</table>

Overall rating place: 5 with 537.216 pts in 2015

<table>
<thead>
<tr>
<th>Place</th>
<th>Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Camp CTF 2015</td>
</tr>
<tr>
<td>11</td>
<td>DEF CON CTF 2015</td>
</tr>
<tr>
<td>3</td>
<td>WhiteHat Contest 10</td>
</tr>
<tr>
<td>4</td>
<td>PoliCTF 2015</td>
</tr>
<tr>
<td>3</td>
<td>CONFidence CTF 2015</td>
</tr>
<tr>
<td>7</td>
<td>DEF CON CTF Qualifier 2015</td>
</tr>
<tr>
<td>4</td>
<td>ASIS CTF Quals 2015</td>
</tr>
<tr>
<td>8</td>
<td>VolgaCTF 2015 Quals</td>
</tr>
<tr>
<td>7</td>
<td>Teaser CONFidence CTF 2015</td>
</tr>
<tr>
<td>10</td>
<td>PlaidCTF 2015</td>
</tr>
<tr>
<td>1</td>
<td>UCSB iCTF 2015</td>
</tr>
</tbody>
</table>
CrySyS Sec Challenge 2015


sec2015.crysys.hu
ÖNLAB PROJEKTEKRŐL
modern operating systems require digital signature on system software before it is installed

advanced attackers (APTs) may use malware signed with compromised keys or fake certificates

- kernel drivers used by Stuxnet and Duqu were signed with compromised keys of otherwise legitimate hardware manufacturers
- Flame appeared to be a signed Windows update; certificate chain contained a fake certificate that looked like a valid Microsoft certificate

standard signature verification procedure does not allow for detecting key compromise and fake certificates

we developed ROSCO, a large repository of signed objects

ROSCO provides basic services such as
- checking if a signed object is known and when it was seen first time
- checking what else the signer of the object signed in the past
- alerting the owner of a key K if an object signed with K is uploaded to the repository
Example: signer reputation service

com.harvesters.linkupwow
Example: signer reputation service

com.harvesters.linkupwow

1/47

virus total
Example: signer reputation service

what else has ivan signed?

- com.androidemu.harvemm1
- com.androidemu.harvespmxd
- com.androidemu.harvedragon3
- com.harvesters.linkupwow
- ...

ivan
Example: signer reputation service

- com.androidemu.harvemm1
- com.androidemu.harvespmxd
- com.androidemu.harvedragon3
- com.harvesters.linkupwow
- ivan

23/55
23/51
23/54
22/50
...

virus total
Example: signer alert service

https://....

comodo
Example: signer alert service
Student project proposals

- **MOBILE CLIENTS (ON MULTIPLE PLATFORMS) FOR ROSCO**
  The task of the student is to develop a mobile client for ROSCO for any of the popular mobile platforms. The mobile client should communicate with the ROSCO back-end (a JSON interface is available), upload information about signed certificates and programs that have been downloaded to the mobile device, and receive and visualize related reputation information to the mobile user. The user interface should be intuitive and easy to use. The client should also be prepared for handling user privacy preferences.

- **BROWSER BASED CLIENTS FOR ROSCO**
  The task of the student is to develop a browser plug-in that works as a client for ROSCO for any of the main browser platforms. The plug-in should communicate with the ROSCO back-end (a JSON interface is available), upload information about signed certificates and programs that have been downloaded by the browser, and receive and visualize related reputation information to the user. The user interface should be intuitive and easy to use. The client should also be prepared for handling user privacy preferences.

- more projects: [http://crysys.hu/student-projects.html](http://crysys.hu/student-projects.html)
A TÁRGYRÓL
Gyakorlatok

- két kurzus: G1, G2
- G1 → G2 (kb. 15 ember)
  - levél Mahóné Novák Krisztának (novak@hit.bme.hu)
  - Subject: VIHIMA06
  - Body: név, neptun, "a G2 kurzus az XYZ felvett tárgyammal ütközik,"
  - határidő: szeptember 14, hétfő
  - aki nem küld levelet, azt áttehetjük a G2 kurzusra

- gyakorlatok demó jellegűek
- néhány gyakorlatra érdemes gépet hozni esetleg, ezt majd előtte jelezzük
Követelmények

- **Szorgalmi időszakban:**
  - 2 db nagy házi projekt
    » memory corruption
    » secure coding
  - Avatao platformon keresztül
    » regisztrációról comment mezőbe: VIHIMA06-2015
  - órák végén ellenőrző kérdések

- **Vizsgaidőszakban:**
  - szóbeli vizsga
  - óra végi ellenőrző kérdésekre adott válaszok beszámítanak
Lehetőségek

- Avatao feladatok megoldását értékeljük
  - SecChallenge vagy csak úgy

- Avatao feladatok készítését is értékeljük
Fontosabb linkek

- IT biztonság mellékspecializáció
  - [http://www.crysys.hu/it-sec/](http://www.crysys.hu/it-sec/)

- Számítógép-biztonság (VIHIM06) tárgy weboldala
  - [http://www.hit.bme.hu/~buttyan/courses/BMEVIHIMA06/](http://www.hit.bme.hu/~buttyan/courses/BMEVIHIMA06/)
  - elérhető a mellékspecializáció oldaláról is
  - elérhető a [www.crysys.hu](http://www.crysys.hu) oldal felől is

- Avatao kihívások (gyakorlatok):
  - [https://avatao.com/](https://avatao.com/)
  - regisztráció oldalon comment mezőbe: VIHIMA06-2015

- labor weboldala:
  - [www.crysys.hu](http://www.crysys.hu)

- CrySyS Student Core oldala:
  - [http://core.crysys.hu/](http://core.crysys.hu/)