Mentoring talent in IT security – A case study

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

dthis is joint work with Gábor Pék, Márk Félegyházi, and Boldizsár Bencsáth
### Team rating

<table>
<thead>
<tr>
<th>Place</th>
<th>Team</th>
<th>Country</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Plaid Parliament of Pwning</td>
<td></td>
<td>1789.884</td>
</tr>
<tr>
<td>2</td>
<td>Dragon Sector</td>
<td></td>
<td>1184.774</td>
</tr>
<tr>
<td>3</td>
<td>oops</td>
<td></td>
<td>1088.711</td>
</tr>
<tr>
<td>4</td>
<td>Shellophish</td>
<td></td>
<td>1019.307</td>
</tr>
<tr>
<td>5</td>
<td>iSpamAndHex</td>
<td></td>
<td>1015.489</td>
</tr>
<tr>
<td>6</td>
<td>dcua</td>
<td></td>
<td>917.887</td>
</tr>
<tr>
<td>7</td>
<td>Samurai</td>
<td></td>
<td>786.940</td>
</tr>
<tr>
<td>8</td>
<td>blue-lotus</td>
<td></td>
<td>783.061</td>
</tr>
<tr>
<td>9</td>
<td>217</td>
<td></td>
<td>769.190</td>
</tr>
<tr>
<td>10</td>
<td>Tasteless</td>
<td></td>
<td>766.784</td>
</tr>
</tbody>
</table>
What’s the magic secret to success?
The CrySyS Student Core
The CrySyS Student Core

- an invite-only group of students who are enthusiastic and who have already proved their aptitude for IT security

- how to get invited?
  - score among the best students at our CrySyS Security Challenge
  - provide an impressive performance during a student semester project
Operation of the Core

- weekly meetings (including the holiday seasons)
  - a member presents work he has done recently
  - joint preparation for CTF games
    - discuss tutorials and write-ups
    - solve challenges from previous years
Operation of the Core

- members really enjoy to be part of the Core
  - develop unique knowledge and skills
  - feel good in a social sense
  - have independence and responsibility
Operation of the Core

- faculty members minimize their control on the Core
  - attract and prepare interested students
  - advise the selection of new Core members
  - acquire financial support for the operation of the group
The Core is a *community of practice*

”a group of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly”  -- Etienne Wenger, 1991

1. a shared domain of interest
2. joint activities and information sharing
3. development of a shared ”repertoire of resources”
Efficiency by *situated learning*

"learning that takes place in the same context in which it is applied"

- learning through the relationships between people (in a community of practice)
- learning by doing (under some supervision)
- better understanding
- more efficient for hands-on skills (than lectures)
Sustainability needs a program

- visibility
- bootstrapping
- speeding up
- admission
- integration
- giving back
Sustainability needs a program

- we get in touch with students early in their curriculum
- we create igniting moments
  - raise interest in IT security
  - give the necessary force and endurance for diligent practice
Sustainability needs a program

- starting an activity in IT security is difficult
  - too much information available
  - experimenting may be illegal
- we organize a bootcamp
  - a set of selected topics
  - lot of hands-on exercises
Sustainability needs a program

- we provide opportunities for further development
  - **avatao** challenges
  - possibility for newbies to join the !SpamAndHex CTF team
  - involvement in projects

visibility

bootstrapping

speeding up

admission

integration

giving back
Sustainability needs a program

- we demand performance for admission to the Core
  - students feel that they achieved something
  - it is a privilege to belong to the group

visibility
bootstrapping
speeding up
admission
integration
giving back
Sustainability needs a program

- usually an organic process
- we ask newcomers to give a talk on their special know-how
  - creates their status in the group
  - helps engaging in discussions and building relationships
- new members are involved in the CTF activity

visibility

bootstrapping

speeding up

admission

integration

giving back
Sustainability needs a program

- Core members actively participate in training aspiring students
  - supervising bootcamp sessions
  - developing challenges for the annual CrySyS Sec Challenge

visibility
bootstrapping
speeding up
admission
integration
giving back
Success is measurable

DefCon CTF finalist (2015, 2016)

- UCSB iCTF 2013
- EKOPARTY CTF 2015
- UCSB iCTF 2014
- HITCON CTF 2015 Final
- Nuit du Hack CTF Finals 2014
- CONFidence CTF 2015
- ASIS CTF Quals 2015
- ASIS CTF Finals 2015
- Hack.lu CTF 2015
- RuCTFE 2015
- RuCTF Finals 2016
- Belluminar 2016
avatao offers hands-on IT security exercises for people to sharpen their skills

the most recent spin-off from the CrySyS Lab
avatao – on-line IT security exercises

Mastering Computer Security

Oh My Secure Sums

by Gabor Acs-Kurucz

Skill tags
Secure C Programming

Description
Your task is to securely sum those integers and check an error occurred. You don't need to implement this automatically upon submission.

The function gets a string that contains those integers separated by spaces, and if an error occurred, then the function should return NULL.

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.
avatao – advantages

- convenient for students
  - no need to install anything, it just works
  - potential solutions can be submitted and there’s immediate response
  - if something goes wrong, just re-start any time the exercise
  - many exercises have a step-by-step solution guide

- offers great opportunities for teachers
  - no need for infrastructure to set up and maintain
  - there are already 250+ exercises (and growing)
  - it takes just a few minutes to create a new path
  - can be used for homeworks, lab exercises, exams, CTFs, ...
  - free access by contributing new content
Conclusions

- IT security courses in the university curriculum are designed for the average students
- Special attention is needed to identify outstanding students, make them interested in IT security, and help them grow their talent
Conclusions

- our program is based on
  - the CrySyS Student Core
  - 6 steps to ensure sustainability

- we heavily use avatao as a tool
  - in the ignition, bootstrapping, speeding up, admission, and giving back phases

- our success is measurable

- our blueprint can be copied
Laboratory of Cryptography and System Security (CrySyS Lab)  
Department of Networked Systems and Services  
Budapest University of Technology and Economics  
www.crysys.hu