Journey to the West

Gábor Pék, PhD

CrySyS Lab, Department of Networked Systems and Services

Budapest University of Technology and Economics

Journey to the West – the old way

*Journey to the West is a Chinese novel published in the **16th** century during the Ming dynasty and attributed to Wu Cheng'en.*

It is one of the Four Great Classical Novels of Chinese literature (Wikipedia)

by Shizao

http://sites.psu.edu

Vocabulary

- CTF – Capture The Flag competition
- Pwn
- ROP
- Jeopardy
- Stack pivoting
- One-gadget-RCE
- Canary
- I/O redirection
- Information leakage
- Attack & Defense
- Brute-forcing ASLR

Back to the Future

- ## CrySyS SecChallenge
  - Annual competition for (mainly) BME students
  - Dates back to 2011
  - Web, forensics, binary reversing, exploitation, cryptography challenges

- ## avatao
  - In 2014 we started to build our cloud-based exercise platform
  - Hosts CrySyS SecChallenge, too
  - Allow students to practice on real challenges 24/7

- ## CrySyS Student Core
  - Invite-only group of exceptionally talented students
  - Founded in April 2013
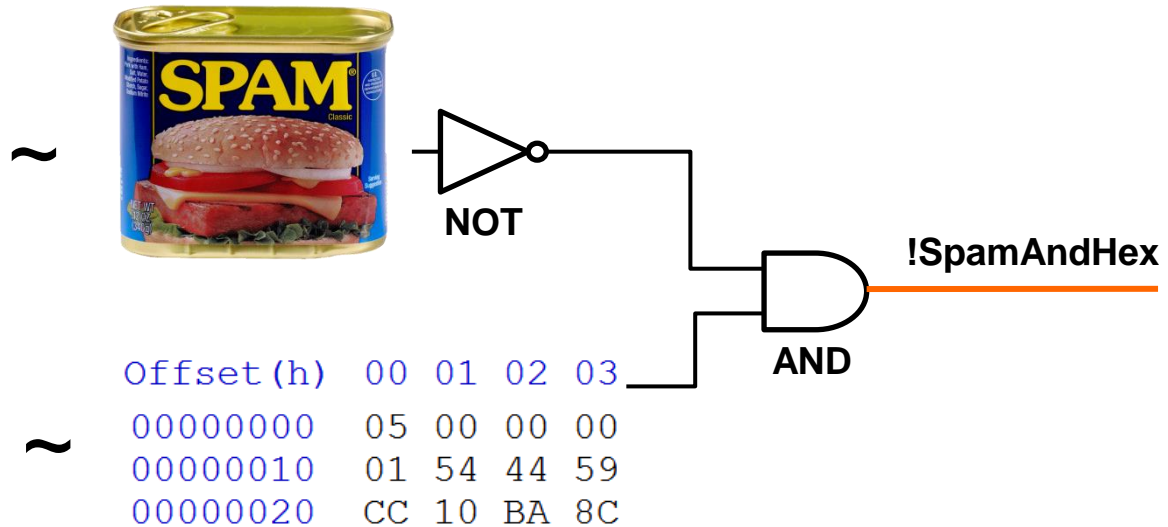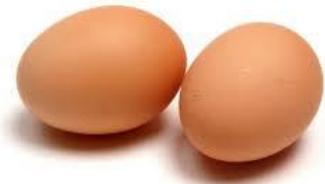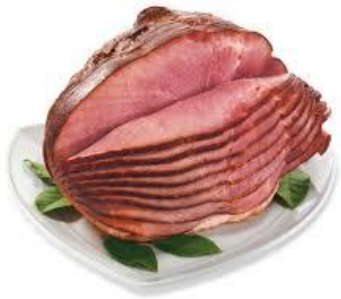
CrySyS Student Core

- Invite-only group
  - Best students from CrySyS SecChallenge
  - Best students from student projects
  - The most active members from CTF games

- Weekly meetings with different topics
  - Preparing for CTFs
  - Invited and internal talks (cryptography, system security, etc)
  - Eating pizza and having fun ☺

!SpamAndHex

- **Members of the CrySyS Student Core**
  - formed the *!SpamAndHex CTF team* to participate at international hacking competitions.

- **Since then, the !SpamAndHex team**
  - *won* various competitions (e.g., UCSB iCTF 2014, ASIS CTF)
  - and qualified for the *DEFCON 2015 Finals* (out of >4000 teams)!!!

- **Currently (as of November 13, 2015)**
  - we are ranked as the *4th best team* in the global toplist of CTFtime (out of >7000 teams)!!!

Giving birth to !SpamAndHex

- Ingredients


```
Offset(h)   00 01 02 03
00000000    05 00 00 00
00000010    01 54 44 59
00000020    CC 10 BA 8C
```

NOT

AND

!SpamAndHex

!SpamAndHex evolution

- ## 2013
  - Participated at 4 CTFs
  - Position 56
  - Overall score: 212
- ## 2014
  - Participated at 28 CTFs
  - Position 14
  - Overall score: 574
- ## 2015
  - Participated at 30 CTFs
  - **Position 4**
  - Overall score: 861

Team rating

2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
♔ 1	Plaid Parliament of Pwning	🇺🇸	1525.387
2	Dragon Sector	🇵🇱	941.207
3	0ops	🇨🇳	912.046
4	!SpamAndHex	🇭🇺	861.156
5	Shellphish	🇺🇸	814.069
6	dcua	🇺🇦	721.580
7	Samurai	🇺🇸	664.020
8	blue-lotus	🇨🇳	653.284
9	Gallopsled	🇩🇰	646.089
10	217	🇹🇼	611.410

DEFCON 2015 Qualifier

- **DEFCON CTF Qualifier**
  - The "Hacker World Championship"
  - More than 4000 teams
- **48 hours**
- **Wide range of challenges**
  - Pwning
  - Coding
  - Web
  - Misc
  - Crypto
- **Qualification for the Final**
  - Winners of 4 other CTFs
  - The best 11 teams from the Qualifier

PPP	57
DEFKOR	57
9447	57
Gallopsled	53
HITCON	46
blue-lotus	45
SpamAndHex	**44**
CORNDUMP	43
0ops	42
0daysober	42
Dragon Sector	42
Shellphish	42
LC↯BC	41
Mostly Inexperienced Beginner Hackers	40
Samurai	39
KAIST GoN	39
Alternatives	36
Eat, Sleep, Pwn, Repeat	34
Routards	34
binja	32
WhatTheBird	32
Blunt Instrument	32
tasteless	30
int3pids	27
0x8F	26

!SpamAndHex @ DEFCON 2015 Finals

- ## 15 Teams
  - USA, China, *Hungary*, Poland, International, Switzerland, …
- ## Attack & Defense
  - Binary reversing and exploitation
  - Various architectures and platforms (e.g., Windows 10 ARM)!

- ## Team t-shirt

- ## Without our *sponsors* it would had been impossible to participate!
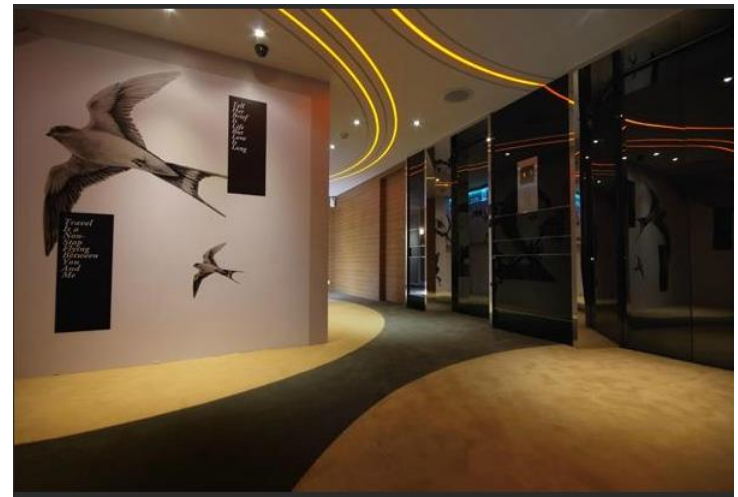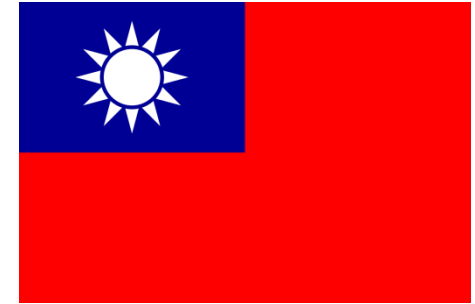
Journey to the East

- We qualified for HITCON CTF Finals!
- 4 players/team
- Attack & Defense
- Taiwan, December 5-6, 2015
- Free hotel reservation @ Forward Hotel in Taipei

Conclusion

- CTFs are fun and educational

- Deep understaing of IT security is required

- There are various ways to go
  - No needle in the haystack to solve a challenge

- Good people make a team rock!
  - Determination is mandatory!!!

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

contact:

Gábor Pék, PhD
Associate Member, Team leader of CrySyS Student Core
gabor.pek@crysys.hu