Intro to System Security

Focus Areas and Call to Actions

System security

- Hands-on and practical
- Network security
- Wireless security
- Protocol security
- Software security
- OS security
- Web security
- Database security
- Cloud security
- Mobile security
- IoT/embedded security

Vulnerable environments and CTF

- Plenty of environments to play with
- https://www.vulnhub.com/
- Let's systematically
  - Have infrastructure
  - Setup them
  - Play with them
  - Fix/Maintain/Develop them
  - Writeup them

Web security and OWASP

- WASAC (by Juho)
- VulnHub and CTF Environments
- OWASP Top 10
- OWASP Tools and Environments

Reverse Engineering and Emulation

- Tools
  - Radare2
  - Angr.io
  - QEMU
- Improving architectures support
- Improving binary formats support
- Adding more analysis modules

Exploits and Shell Codes

Tools

- Metasploit
- Shell-Storm
- ExploitDB

Adding more architectures

Adding more OSes

Adding more payloads

Highly configurable payloads and exploits

Software Defined Radios

Tools

- USRP
- RTL-SDR
- HackRF

Sniffing

Protocol decoding and decrypting

Advance RSA/DSA/HTTPS cracking experim.

Tools

CADO-NFS

GGNFS

msieve

Optimal use of HPC infrastructure

Improve the tools and their setup

Target 512 bits -> 768 bits :-O

Cleanup the Internets of short/cracked keys

Many other topics/directions

- Hardware hacking skills
  - Memory dumps
  - Hardware glitching
- IoT/embedded
- CCTV
- Password tools

Call to actions

PROPOSE/SUBMIT TALKS HAVING HANDS-ON AND DEMOS

PROPOSE TO LEAD AN "IMPLEMENTATION" WORKSHOP

DON'T BE SHY, LET'S MEET AND LEARN CYBERSECURITY TOGETHER

"JySec Algorithm"

COOL
SECURITY IDEA

TOOLS

EXPERIMENTS

COMMUNITY
& SHARING

FUN

REPEAT