

Cyber@UC Meeting 31

Hardware Hacking

If You're New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- Stay updated through our weekly emails and **SLACK**



Announcements


- Happy late Halloween
- **October 27/28th** was the **ACM** programming challenge
- **CharitEweek** from Nov. 13th-Nov. 17th
- **Red team** against Franco's Class! *Nov. 27th*
- Reached out to **P&G** again for a tour of their **cybersecurity operations center**
- **Logo Design** Competition





Weekly Content Committee Session

Reaper

- First spotted in September
 - Based off of Mirai, but no longer relies on cracking weak passwords
 - Enslaves vulnerable IoT devices and creates a botnet network
 - Contains vulnerabilities for Dlink, Netgear, Linksys, Goahead, JAWS, AVTECH, Vacron
 - Believed to have already infected 2 million devices, growing 10k/day
 - Mirai only needed 100k devices infected to take down the DNS provider Dyn in a massive DDOS attack
 - The author is still modifying its code
- 

Reaper (continued)

- There are warnings of another vulnerability called IoTroop that is believed to be adding devices to the same botnet and has infected over 100k devices
- Mirai was a botnet that took down almost a million routers back in November 2016

<https://thehackernews.com/2016/11/mirai-router-offline.html>

<https://thehackernews.com/2017/10/iot-botnet-malware-attack.html>



DUHK

- Stands for “Don’t Use Hard-coded Keys”
- Uses a cryptographic implementation vuln to allow attackers to recover encryption keys that secure VPN connections
- This is the third crypto vuln seen just this month, KRACK, ROCA
- Affected vendors include Cisco, Fortinet, TechGuard
- DUHK exploits an outdated pseudorandom number gen algorithm that works with a hard coded seed key
- Some vendors store the secret seed value hard-coded into their source code
- By using a state recover attack, man-in-the-middle attackers who know the seed value can know the input values for the PRNG

Hardware Hacking

Hardware Hacking Example

- Stuxnet
 - Equivalent to DDOS for hardware
 - Targeted PLCs
 - Iran's Nuclear Program Targeted
- Cause Centrifuges to tear themselves apart
 - Believe to have Destroyed 1/5th of them



← Simple Centrifuge



Breakout Session

Hardware Hacking Topics

- IO exploitation
- Firmware Reverse Engineering
- Coldboot Attacks
- FPGA/ASIC Reverse Engineering (Silicon Dye Analysis)
- PCB RE
- Power Analysis



Breakout Session

- Has this ever been done
- Who would perform this exploit
- Why would it be done
- If you wanted to do it. What would you do it on.

