



# ncccn

P O R T A V E N T U R A 2 0 2 2



# Pwn2Own 2021

How to Win \$\$\$ at a Hacking Contest?

#CreatingValue

Cedric Halbronn

Alex Plaskett

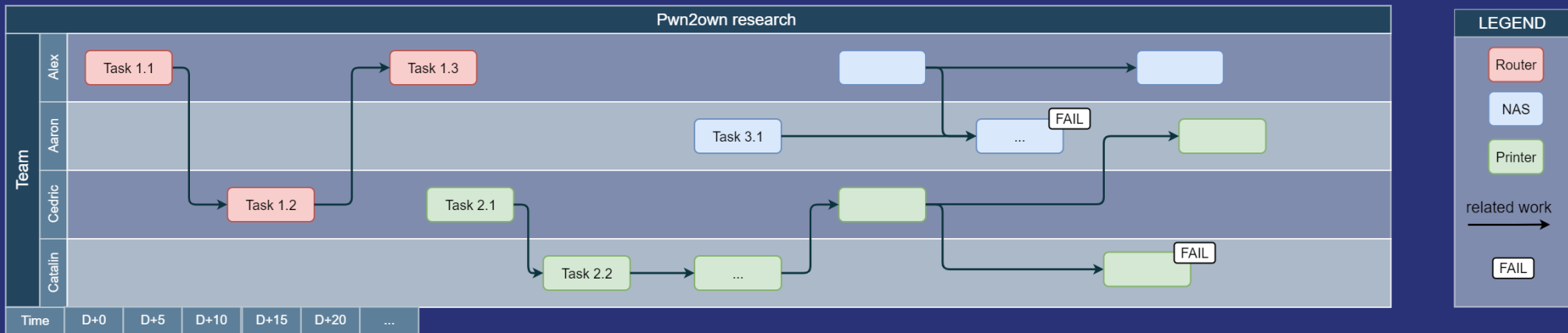
Aaron Adams

Catalin Visinescu

# Introduction

# Talk Overview and Aims

- Journey and process of competing at Pwn2Own Austin 2021
  - Behind the scenes work on getting an entry
- Both successes and failures
- Learnings
- Timelines



# Pwn2Own Overview

- Yearly vulnerability research competition held by ZDI (Trend Micro)
  - Pwn2Own Mobile (November) - competed
  - Pwn2Own Desktop (March)
  - Pwn2Own ICS (February)
- ZDI purchase vulnerabilities / exploits and provide directly to the vendors to fix the issues

# Rules

- No user interaction allowed
- No reboot allowed (?)
- Initial draw to determine the contestant attempts order
- Each contestant can only attempt one chain of bugs per category
  - Detailed later
- Rules per category in the competition (Network attacks / Sandbox escape / etc)
- No technical details allowed to be disclosed (until the issues are fixed)

# Agenda

- Target choice
- Vuln Research
- Competition
- Learning Experience



# Target Choice

# What Targets are Available?

- Some mobile phones are easier to exploit
- Printers are new to Pwn2Own (unknown security)

## Mobile phones

Target	Cash Prize	Master of Pwn Points
Samsung Galaxy S21	\$50,000 (USD)	5
Google Pixel 5	\$150,000 (USD)	15
Apple iPhone 12	\$150,000 (USD)	15

## Printers

Target	Cash Prize	Master of Pwn Points
HP Color LaserJet Pro MFP M283fdw	\$20,000 (USD)	2
Lexmark MC3224i	\$20,000 (USD)	2
Canon ImageCLASS MF644Cdw	\$20,000 (USD)	2

# What Targets are Available?

## NAS

Target	Prize	Master of Pwn Points
Synology DiskStation DS920+	\$40,000 (USD)	4
My Cloud Pro Series PR4100 from WD	\$40,000 (USD)	4
3TB My Cloud Home - Personal Cloud Storage from WD	\$40,000 (USD)	4
3TB My Cloud Home Personal Cloud from WD - firmware version 8.xx.xx-xxx (Beta)	\$45,000 (USD)	5

- NAS: previous research
  - Note: Western Digital is sponsor
- Routers have generally weaker security

## Routers

Target	Cash Prize	Master of Pwn Points
TP-Link AC1750 Smart Wi-Fi Router	WAN Side \$20,000 (USD)	2
	LAN Side \$5,000 (USD)	1
NETGEAR Nighthawk Wi-Fi Router (R6700 AC1750)	WAN Side \$20,000 (USD)	2
	LAN Side \$5,000 (USD)	1
Cisco RV340	WAN Side \$30,000 (USD)	3
	LAN Side \$15,000 (USD)	2
Mikrotik RB4011iGS+RM	WAN Side \$30,000 (USD)	3
	LAN Side \$15,000 (USD)	2
Ubiquiti Networks EdgeRouter 4	WAN Side \$30,000 (USD)	3
	LAN Side \$15,000 (USD)	2

# What Targets are Available?

## Speakers

Target	Cash Prize	Master of Pwn Points
Portal from Facebook	\$60,000 (USD)	6
Amazon Echo Show 10	\$60,000 (USD)	6
Google Nest Hub (2nd Gen)	\$60,000 (USD)	6
Sonos One Speaker	\$60,000 (USD)	6
Apple HomePod mini	\$60,000 (USD)	6

## TVs

Target	Cash Prize	Master of Pwn Points
Sony X80J Series - 43"	\$20,000 (USD)	2
Samsung Q60A Series - 43"	\$20,000 (USD)	2

## External disks

Target	Prize	Master of Pwn Points
1TB SanDisk Professional G-DRIVE ArmorLock SSD	\$40,000	4

- Lots of other targets
  - See later

# What NOT to Go For?

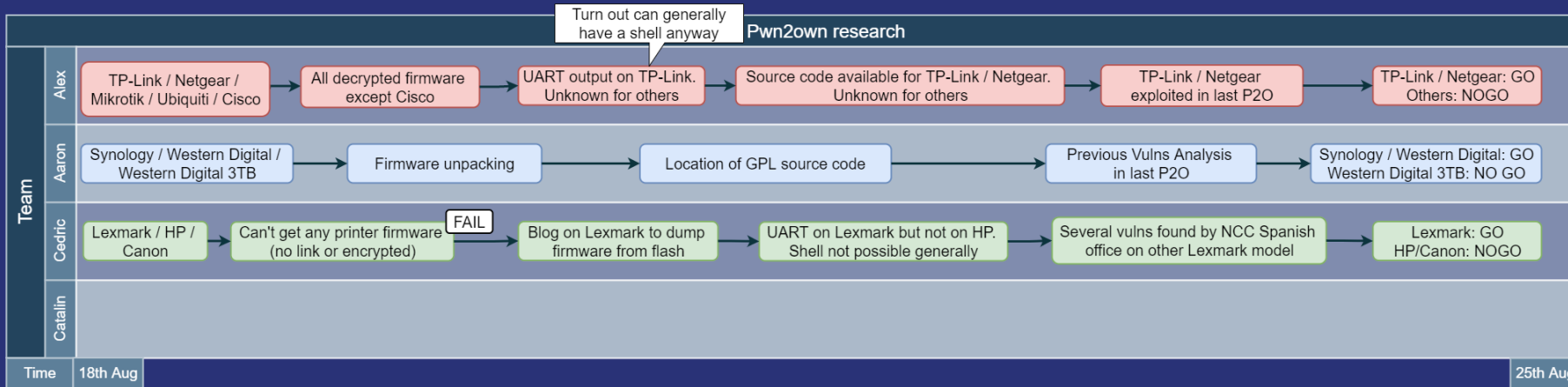
Gut feeling, experience and what we wanted to work on...

- External drive
  - Too low level and specific
- Televisions
  - Android based
- Home Automation
  - HomePod expected hard, unknown about other targets
- Mobile phones
  - Pixel/iPhone probably need huge time investment (a year?)
  - Samsung may have had potential but time constraints

# What to Go For?

- We only have 2.5 months to competition with no existing 0day
- Routers
  - Already had one available pre-pwn2own
  - Easier target
- NAS
  - Prize money seemed reasonable for expected difficulty
- Printers
  - First year at P2O, less researched?
  - Previous printer work and hardware team at NCC
- Useful to consultants?

# Initial Targets Choice



- Split 3 targets
  - Firmware unpacking
  - Debug capability
  - Source code analysis
  - Previous vulnerabilities?
- Reduced number of potential targets

# Selection Methodology

- E.g. printers

## P2O targets

Model	OS	decrypted firmware	UART output	interactive shell	JTAG	Logs in web interface	Bugs found
Lexmark MC3224i	Linux	No. known technique to dump firmware from flash,	Yes	No	No	Yes	several overflows in Web + 1 SNMP DoS + 2 info disclosure in Web + 3 others
Canon ImageCLASS MF644Cdw	?	? Firmware download requires a valid serial number	?	?	?	?	?
HP Color LaserJet Pro MFP M283fdw	RTOS?	No	No	No	No	Yes	2 XSS + 1 CSRF + several overflows in Web + several overflows in IPP

## Others

Vendor	OS	decrypted firmware	UART output	interactive shell	JTAG	Logs in web interface	Bugs found
Xerox	RTOS?	Yes	Yes	No	No	Yes	several overflows in IPP + several XSS + overflow in Google Cloud Print + overflow in Cookie field
Ricoh	RTOS?	Yes	Yes	Yes	No	Yes	overflow in HTTP + several overflows in Web + several overflows in IPP + 1 DoS in SNMP + overflow in LPD + DoS in LPD
Brother	RTOS?	Yes	No	No	No	Yes	1 heap overflow in IPP + 1 stack overflow in Cookie + 1 info disclosure in Web
Kyocera	Linux	No (only engineers)	No	No	No	Yes	1 path traversal in web + several overflows in web + several overflows in IPP + several XSS + integer overflow in web



# Attack Surface Mapping

- E.g. printers

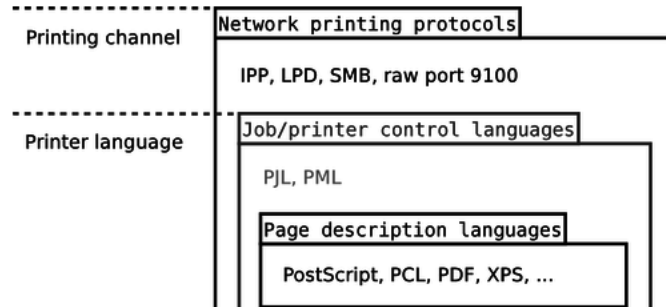
## In-scope

- Everything exposed over Ethernet, WiFi
- SNMP, FTP, NTP, Telnet, SLP (aka SRVLOC) (Service Location Protocol), TFTP, SMTP, etc. (management services)
- HTTP (web app logic or memory corruption bugs), SOAP/REST (web services used by mobile app or other software - information disclosure bugs, parameter sanitation bug), see [26](#) for methodology
- Wifi chip: probably hard target (see Project zero research from Gal [24](#))
- Raw service (TCP 9100), IPP, LPD, SMB (printer services i.e. printing channels)
  - PjL (Printer Job Language), PML (Printer Control languages) on top of printer services
    - PostScript (PS), PCL (Printer Command Language), PDF, XPS (Page Description Languages)
- AirPrint ([21](#) / [22](#) / [23](#) = extension to IPP)
- update process (if possible for p2o to manually ask for an update, and for us to arp spoofing, and there is no proper TLS configured (see [25](#)))

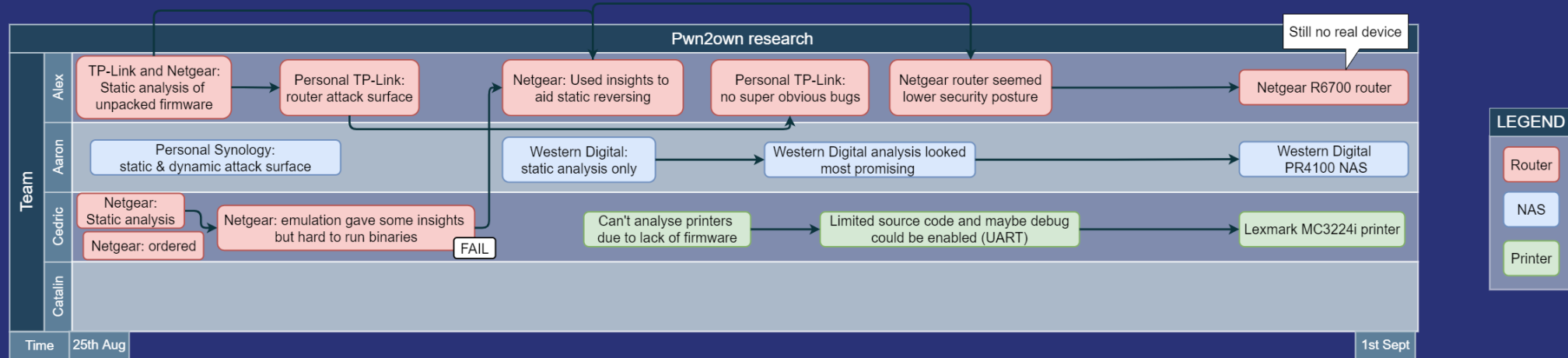
## Other ideas:

- Investigate mobile applications that allow printing on printers to see protocols used, etc.
- Are p2o targets are connected to the Internet? like if we could use a cloud service to pwn the devices? we could maybe ask them to set it up like that, if its a "normal" deployment

## Printer languages



# Final Targets Choice



- Static analysis vs dynamic analysis
  - Platform visibility
  - General code quality
  - Dangerous attack surface
- Ordered one Netgear

# Initial Analysis Summary (10 days total)



Netgear Router



Western Digital NAS

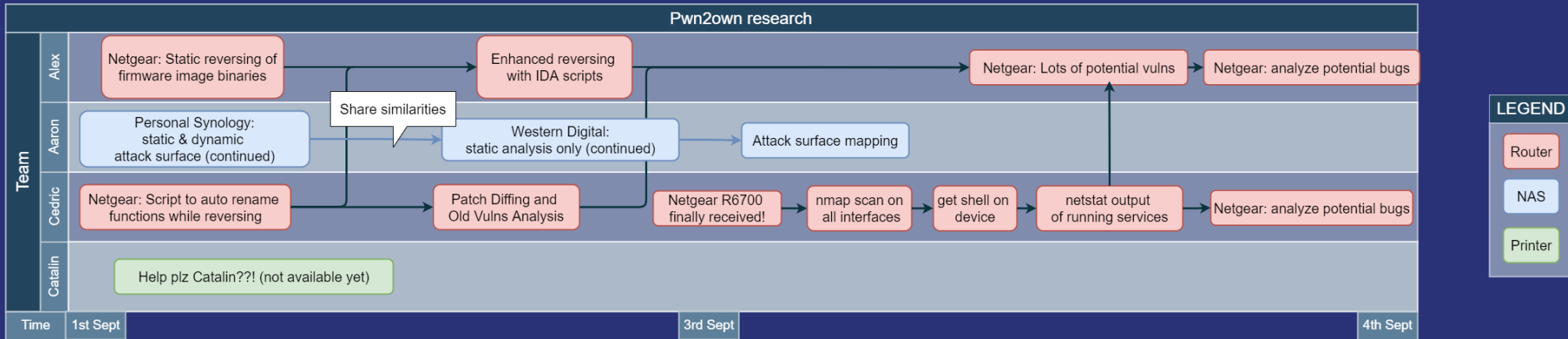


Lexmark Printer

- 2 months to go until the competition
- Now the real bug hunt kicks in!

# Vuln Research

# Primarily Static Analysis + Netgear Dynamic Analysis



- Focus on Netgear router and Western Digital NAS
- Attack surface
- Bug hunting (reversing + source code)
- Router received => dynamic analysis

# Netgear Batch of Bugs


Netgear R6700 KC\_PRINT Response\_Get\_Jobs Stack Overflows

#8 · created 9 months ago by

netgear

non-default

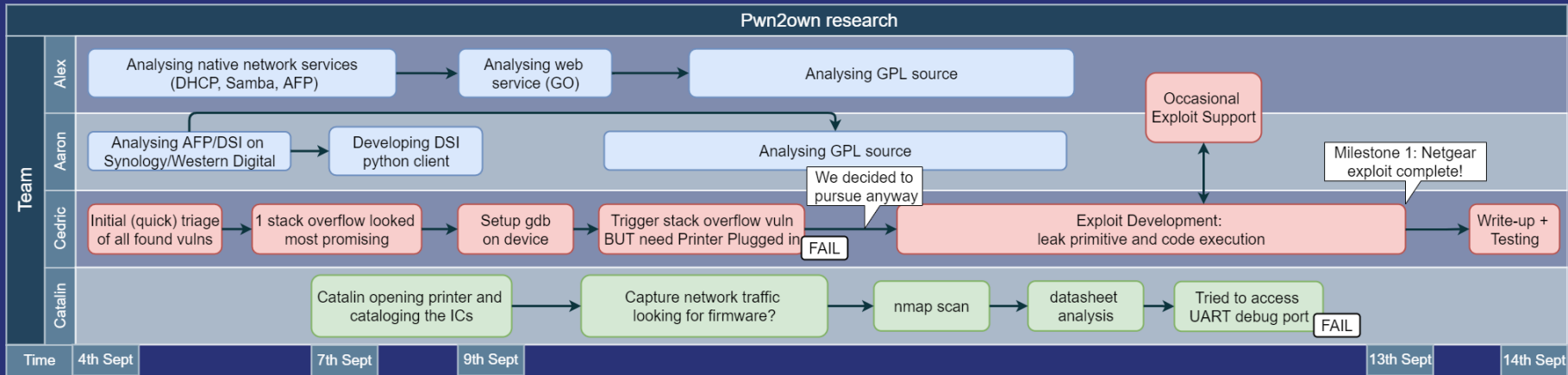
vulnerability

CLOSED  2

updated 9 months ago

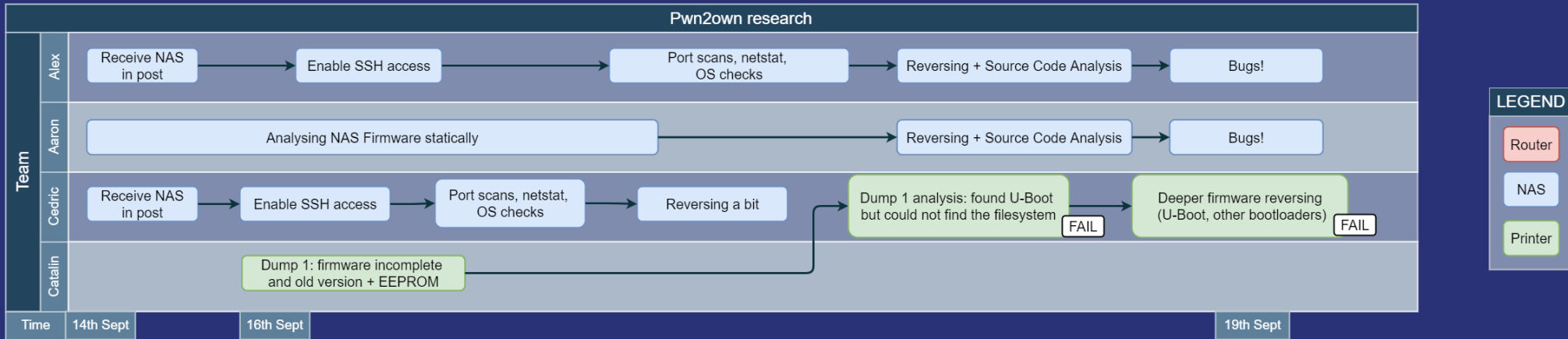
- Default services
- Network accessible and unauthenticated
- IPP blatantly looked exploitable with a stack overflow

# NAS Bug Hunting + Netgear Exploit Dev



- NAS: Bug hunting on external services (DHCP, Samba, AFP, Web)
- Router: Triage and exploitation of stack overflow vuln (COMPLETED)
  - Printer plugged-in requirement
- Printer: hardware familiarisation





# NAS Bug Hunting + Printer Firmware Dump



- NAS dynamic analysis and bug hunting
  - Enabling SSH
- Printer firmware dump (hardware)
- Printer firmware analysis: could not locate filesystem

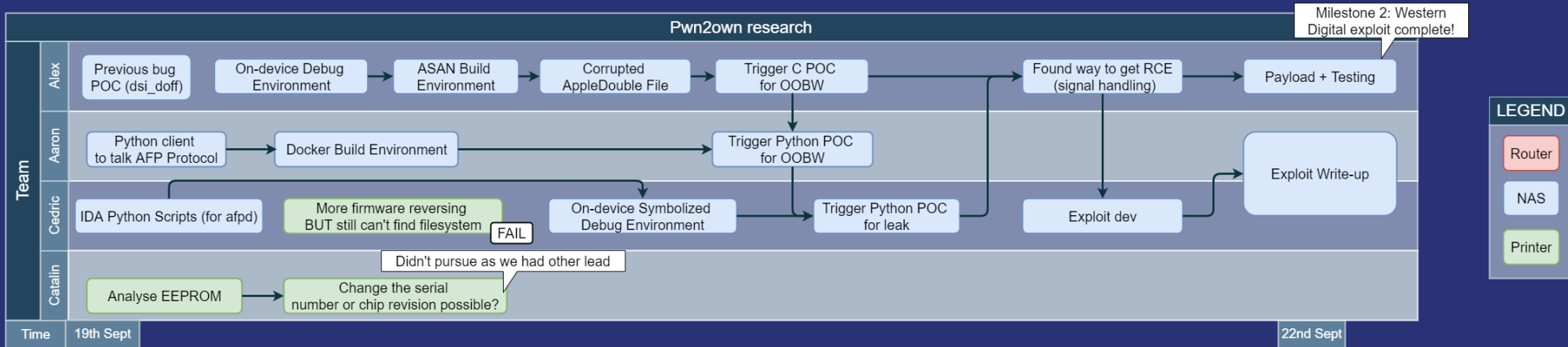


# Western Digital Batch of Bugs

WD My Cloud Pro PR4100 afpd ad_header_read_osx unchecked return value #21 · created 8 months ago by <span>vulnerability</span> <span>western digital</span>	CLOSED  7 updated 8 months ago
WD My Cloud Pro PR4100 afpd Stack Overflow #18 · created 9 months ago by <span>vulnerability</span> <span>western digital</span>	CLOSED  4 updated 8 months ago
WD My Cloud Pro PR4100 afpd OOB NULL Writes #17 · created 9 months ago by <span>vulnerability</span> <span>western digital</span>	CLOSED  2 updated 9 months ago
WD My Cloud Pro PR4100 login_check() always returns 1 #12 · created 9 months ago by <span>western digital</span>	CLOSED  6 updated 7 months ago

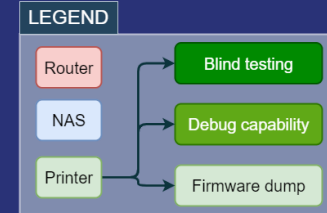
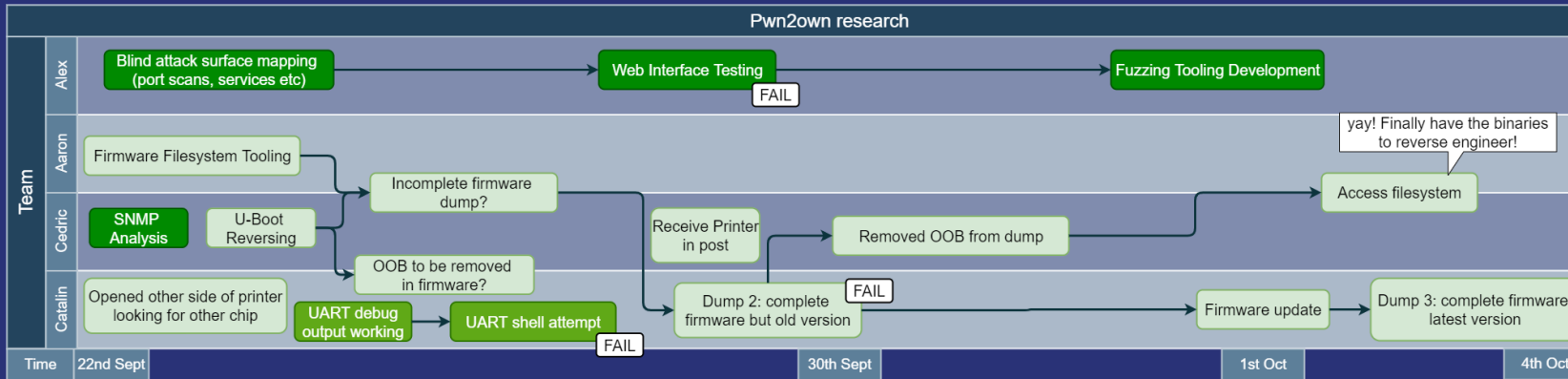
- Unchecked return value bug looked very interesting!
- Others don't look as interesting
  - OOB NULL write probably hard to exploit
  - Stack overflow was false positive
  - `login_check()` PHP was unreachable

# NAS Exploit Development



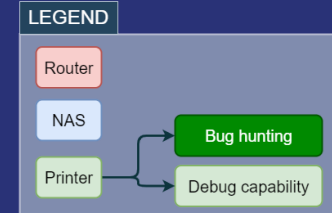
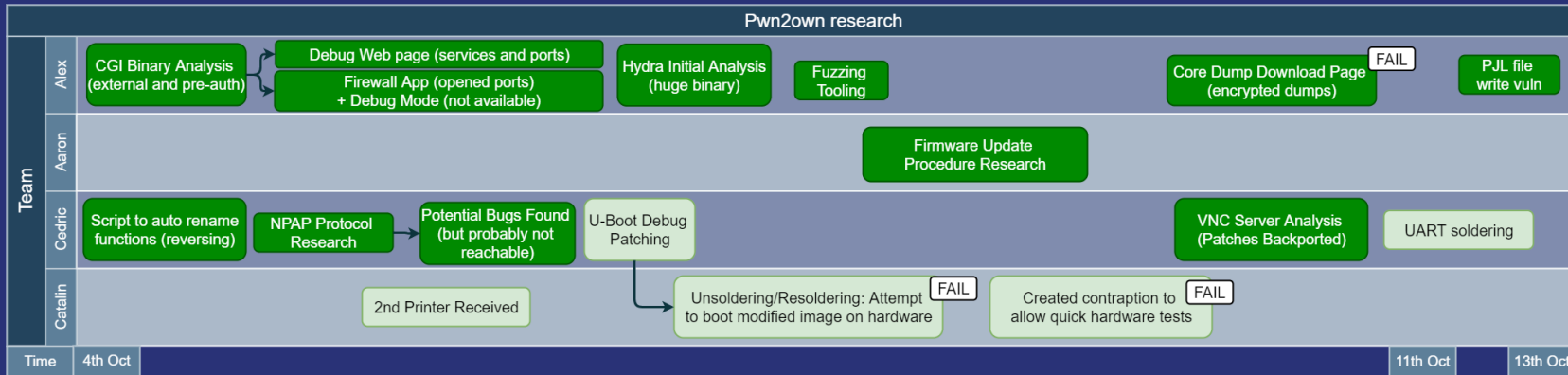
- NAS (Team work)
  - Trigger the bug
  - Library to speak the protocol
  - Debug environment
  - Exploit development (COMPLETED)

# Printer Attacks and Obtaining Filesystem



- Blind attacks
- Hardware debug output working
- Obtaining a complete firmware dump
  - \* Dump 2: more content
  - \* Dump 3: updated version
- Extracting filesystem (MILESTONE)

# Printer Bug Hunting and Platform Visibility



- Bug hunting on external services (reversing)
- Platform visibility
  - Debug web page
  - Core dump download page (encrypted)
- Simplify flash reprogramming without unsoldering
  - \* Attempt to get a shell with firmware patch
  - \* Check if secure boot is enabled

# PJL File Write Vuln


Lexmark MC3224 PJL LDLWELCOMESCREEN Insecure Temp File Creation

#37 · created 7 months ago by

Reported

lexmark

pwn2own

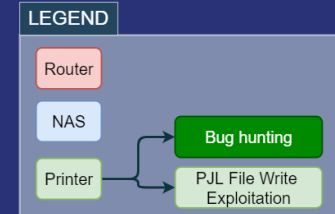
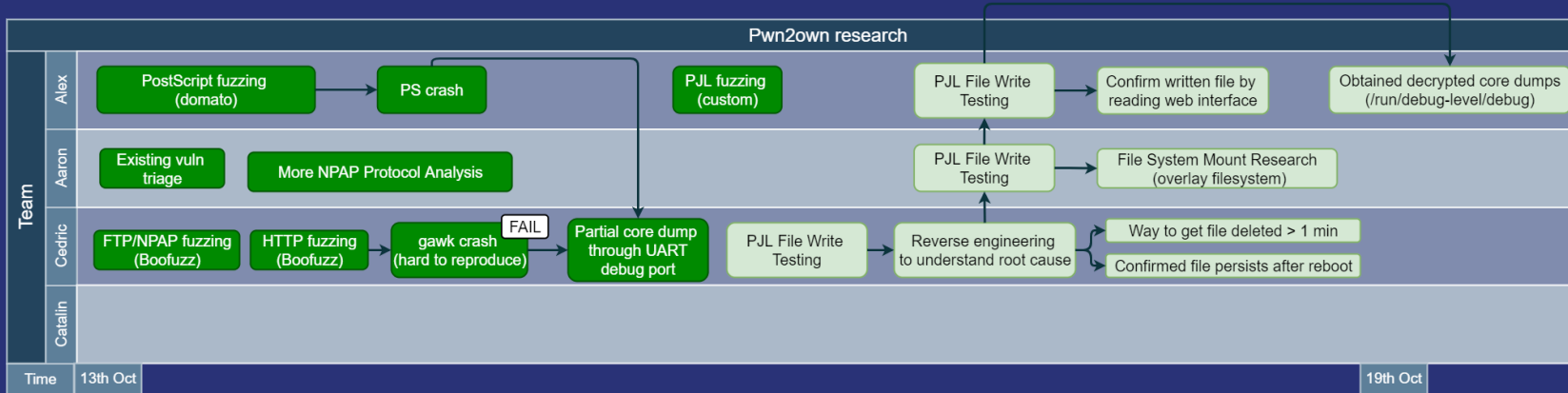
CLOSED  6

updated 7 months ago

- Blindly tested to write in lots of paths
- Couldn't overwrite existing files
- File deleted right after, not useful?

=> We tried to find more bugs due to lack of visibility

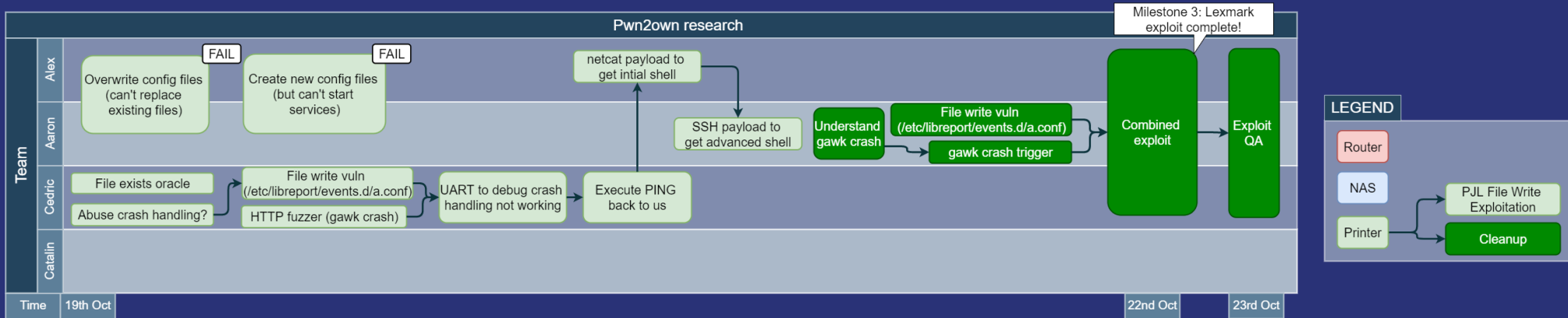
# Other Areas + PJL File Write Vuln



- Focus on other areas (fuzzing + static analysis)
  - PostScript crash + HTTP crash (gawk)
- Deep triage of PJP file write vuln
  - Reverse engineering
  - Filesystem constraints
  - Reading back file
- Use of PJP vuln to obtain decrypted core dumps



# PJL File Write Vuln Exploitation



- Tried different approaches to get code execution (config files, etc.)
- Got command execution
  - Found and abused crash handling
  - Trigger `gawk` crash with HTTP fuzzer
- Got shell on the printer (COMPLETED)
- Combined exploit + testing



# Exploit Packaging and Admin

MISC admin stuff

- Package write-ups of all bugs to ZDI
- Package exploits for distribution and test dependencies
- Write usage guides so ZDI can use the exploits
- Fill in forms and do paperwork for registration :)

We somehow make it for the registration in time

Event is on 2-4 Nov!!!

# Competition

# Competition

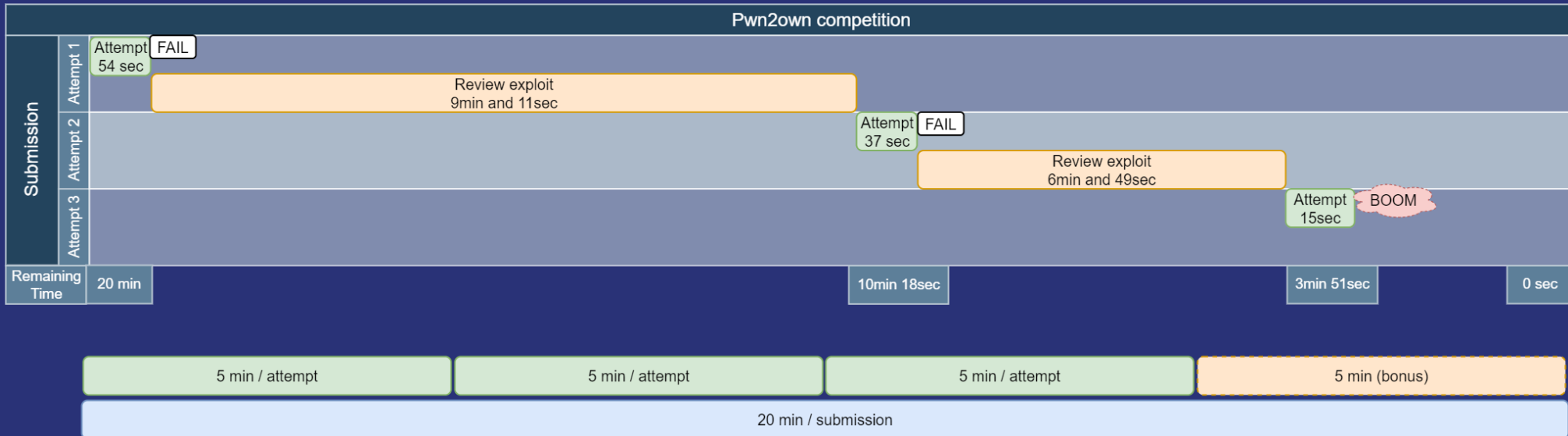
Quick recap on rules:

- 3 attempts
- 5 minutes per attempt
- All 3 attempts must be completed within 20 minutes

# Netgear Router

- A few weeks before the event, we asked them if they would accept our exploit
  - Requirement: connecting a printer to the router
    - We knew we might get rejected
    - Did not have a better bug candidate at time
  - Answer is no
    - Reported it to Netgear instead

# Western Digital NAS



Attempt 1 -> failed

- Manually reading file from SMB -> leak worked but script failed to read it
- Decided to add a `sleep()` before reading data

Attempt 2 -> failed

- Leak worked but failed to connect to shell during RCE part
- Decided to add a `sleep()` before connecting to shell

# Western Digital NAS - SUCCESS!



```
Terminal - root@ubuntu: /home/zdi/Downloads
id
uid=0(root) gid=0(root) euid=501(nobody) egid=1000(share) groups=1000(share)
pwd
/mnt/HD/HD_a2/Public/edg
```

# Western Digital NAS - Disclosure

- ZDI meeting
  - Unknown bug
- Western Digital meeting:
  - Unknown bug
  - Will be hard to fix since the bug is in netatalk open source project

NB. Removed netatalk entirely (AFP removed)

# Lexmark Printer

## First attempt

- Exploit worked, command exec and firewall disabled.
- However, no connection to SSH server.
- Had similar problems in testing pre-competition but assumed fixed.
- Modified exploit to start netcat as well as SSH.

## Second attempt

- ...



# Lexmark Printer - SUCCESS!

```
└─$ nc -v 192.168.1.10 1337
192.168.1.10: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.10] 1337 (?) open
id
uid=0(root) gid=0(root)
cat /Build.Info
075.281
17-Aug-21 10:28

Build Number: 14209
Persona: granite2-color
Image: core-image-highlevel-lite
build-bundle: GM.075.280-7-g9d69597
meta
meta-bsp
meta-bsp_3am_thre
meta-poky
meta-yocto-bsp      = "HEAD:5dabbae1203cdd72b9045179d4bc483f5666a46a"
meta-webserver
meta-networking
meta-oe
meta-python
meta-fileystems    = "HEAD:8760facba1bceb299b3613b8955621ddaa3d4c3f"
meta-lexmark       = "HEAD:ad7aa2b66d0c49f1be272f8fdd0122d4bbd0f919"
meta-granite       = "HEAD:cda562c41e77ba7b99d6ca192dad3fce775826ce"
meta-armada        = "HEAD:4fd14a06ba117531efbe1e5f1ee1030209bd2b4a"
meta-abrt          = "HEAD:a55df92c6fc027eef4148857371213462cb8bd8"
meta-rust          = "HEAD:abb625bac074f8e627ee6b5bf7934491804cf876"
meta-qt4           = "HEAD:8e791c40140460825956430ba86b6266fdec0a93"
meta-gplv2        = "HEAD:813b7d2b5573d8591c6cd8087b326f0a0703d6b9"
█
```

# Lexmark Printer - Disclosure

- ZDI meeting
  - Unknown bug
- Lexmark meeting:
  - Unknown bug
  - Gracefully handled disclosure and patched quickly!

# Learning Experience

# What to Learn From it

- Approach
  - Luck, instinct and being stubborn
  - Teamwork
  - Lazer focus + the grind
- Building knowledge base
- Going deep vs Going wide
  - Attack problems from different angles
  - More attack surface / more devices = more chance of finding impactful vulns
  - Fragmentation of effort problems
- Embedded (and probably SCADA) good place to start

# Overall Standing

- Happy with result

## Master of Pwn Standings

Contestant	Cash	Points
Synacktiv	\$197,500	20
DEVCORE	\$180,000	18
STARLabs	\$112,500	12
Sam Thomas	\$90,000	9
THEORI	\$80,000	8
Bien Pham	\$52,500	6.5
NCC Group	\$60,000	6
trichimtrich	\$40,000	5
Martin Rakhmanov	\$40,000	4
Flashback	\$33,750	3.75



# What's Next?

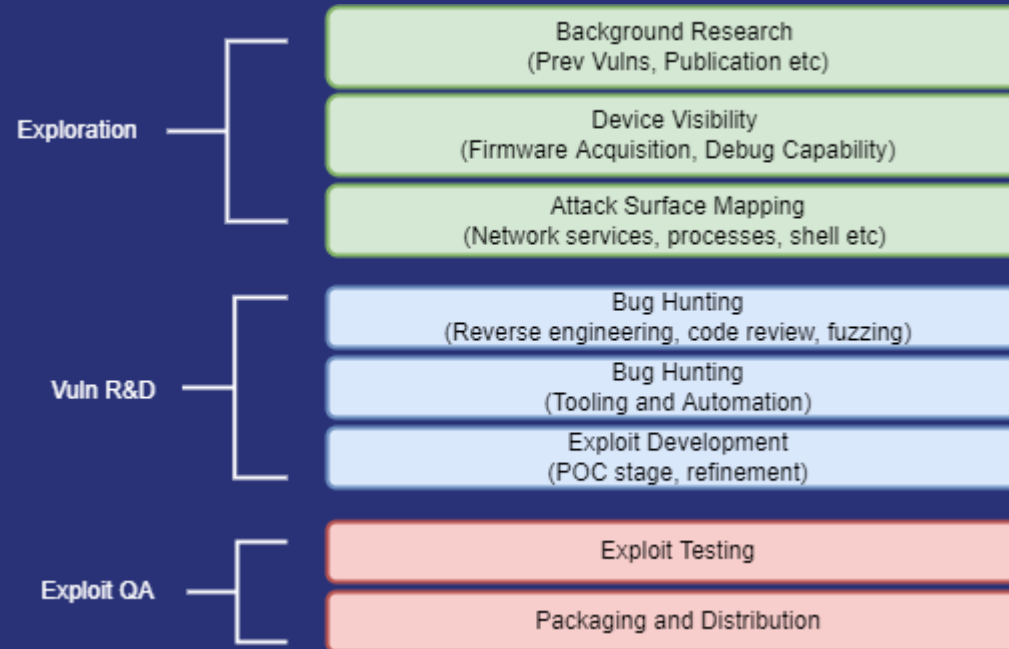
## Procedural Improvements

- Get at least one device per target
- Start on the preliminary tasks (firmware dumping, debug visibility etc) earlier
- Loop in more domain specialists (e.g. hardware/mobile etc)

## Technical Improvements

- Bug hunting automation tooling (fuzzing, reversing etc)
- Exploit testing capabilities (reliability etc)

# Generalised Methology



# Questions

Any questions?!?