DEVCORE
SECURITY
CONSULTING

Your printer is not your printer ! - Hacking Printers at Pwn2Own

Angelboy


angelboy@chroot.org


@scwuaptx

Whoami

- Angelboy
  - Researcher at DEVCORE
  - Ex-CTF Player
    - HITCON / 217
  - Chroot
  - Pwn2Own
    - 2020 Tokyo/2021 Austin
  - Co-founder of pwnable.tw
  - Speaker
    - HITB GSEC 2018/AVTokyo 2018/VXCON/HITCON

PWNABLE.TW

DEVCORE SECURITY CONSULTING

Agenda

- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

Agenda

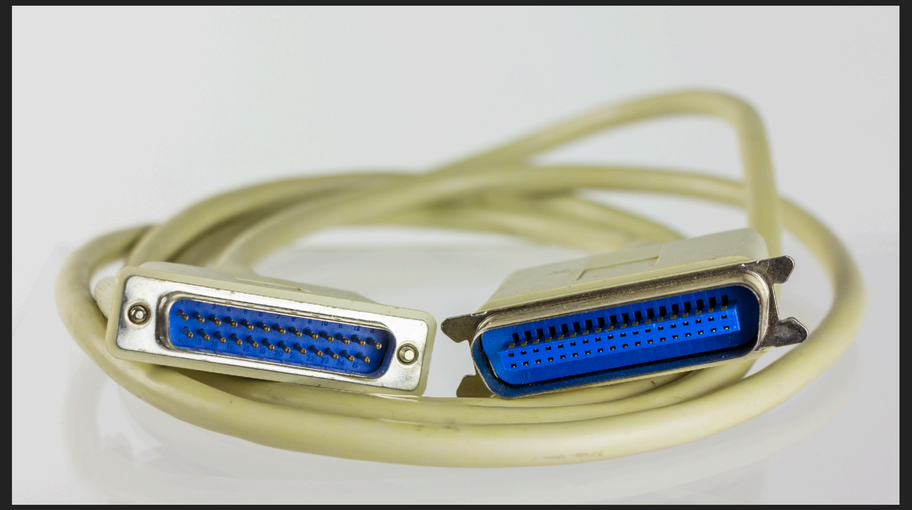
- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

DEVCORE SECURITY CONSULTING

Introduction

Printer

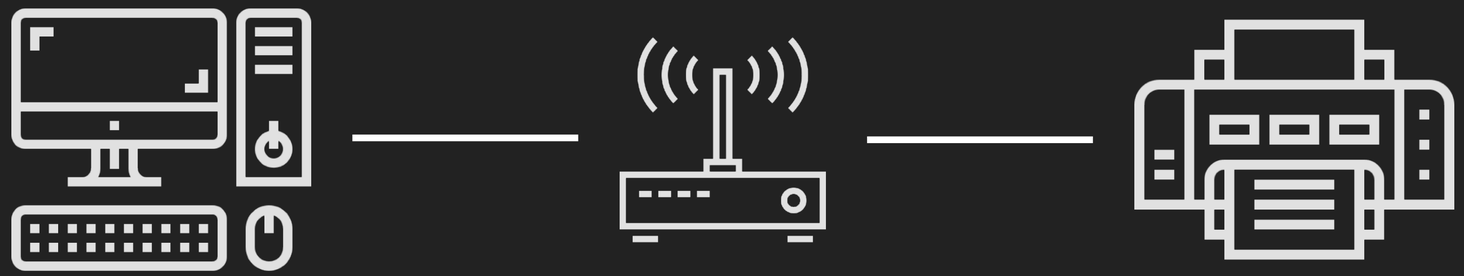
- In the early days
  - to use the printer, it was necessary to
    - Use IEEE1284 or USB to connect to the Computer
    - Install Printer driver before printing
- Usually only a single printer feature



Introduction

Printer - IoT

- Nowadays
  - Printer can provide a variety of services which make printer not only more convenient but also closer to IoT
    - It can be found immediately when connected to intranet



DEVCORE SECURITY CONSULTING

image: Flaticon.com

Introduction

Printer - IoT

LPD Printing:	Enabled
LPD Banner Page Printing:	Enabled
FTP Printing:	Disabled
9100 Printing:	Enabled
Bonjour:	Enabled
IPP Printing:	Enabled
IPPS Printing:	Enabled
AirPrint:	Enabled
SLP:	Enabled
WS-Discovery:	Enabled
WS-Print:	Enabled
WS-Scan:	Enabled
SNMP:	Enabled
LLMNR:	Enabled

Printing is also easier

https://images.plurk.com/2UhjPCQFrPya3pxKLeEdK9.jpg

Angel boy+ 分享 10 年前

今天在幫系上老師看網路印表機問題的時候 結果他突然吐出這幾張紙來 @@ 這..... 顆顆

19 1

DEVCORE SECURITY CONSULTING

Motivation

Introduction

Motivation

- Intranet
  - Printer is one of the most common devices in the intranet

Introduction

Motivation

- Intranet
  - Printer is one of the most common devices in the intranet
  - Good target to hide our actions

Introduction

Motivation

- Intranet
  - Printer is one of the most common devices in the intranet
  - Good target to hide our actions
  - Sometimes integrate with Active Directory

Introduction

Motivation

- Pwn2Own 2021 Austin

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

%0Acat%20/etc/passwd

`ls`

We thought they were trivial at first, but ...

; /bin/usr/id ;

DEVCORE SECURITY CONSULTING

RTOS
(Real-Time Operating System)

Challenge Accept !


DEVCORE
SECURITY
CONSULTING
Lexmark
Canon

DEVCORE SECURITY CONSULTING

We will focus on Canon and HP in this talk

Agenda

- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

Analysis

- At the beginning, we thought we need to ……

DEVCORE SECURITY CONSULTING

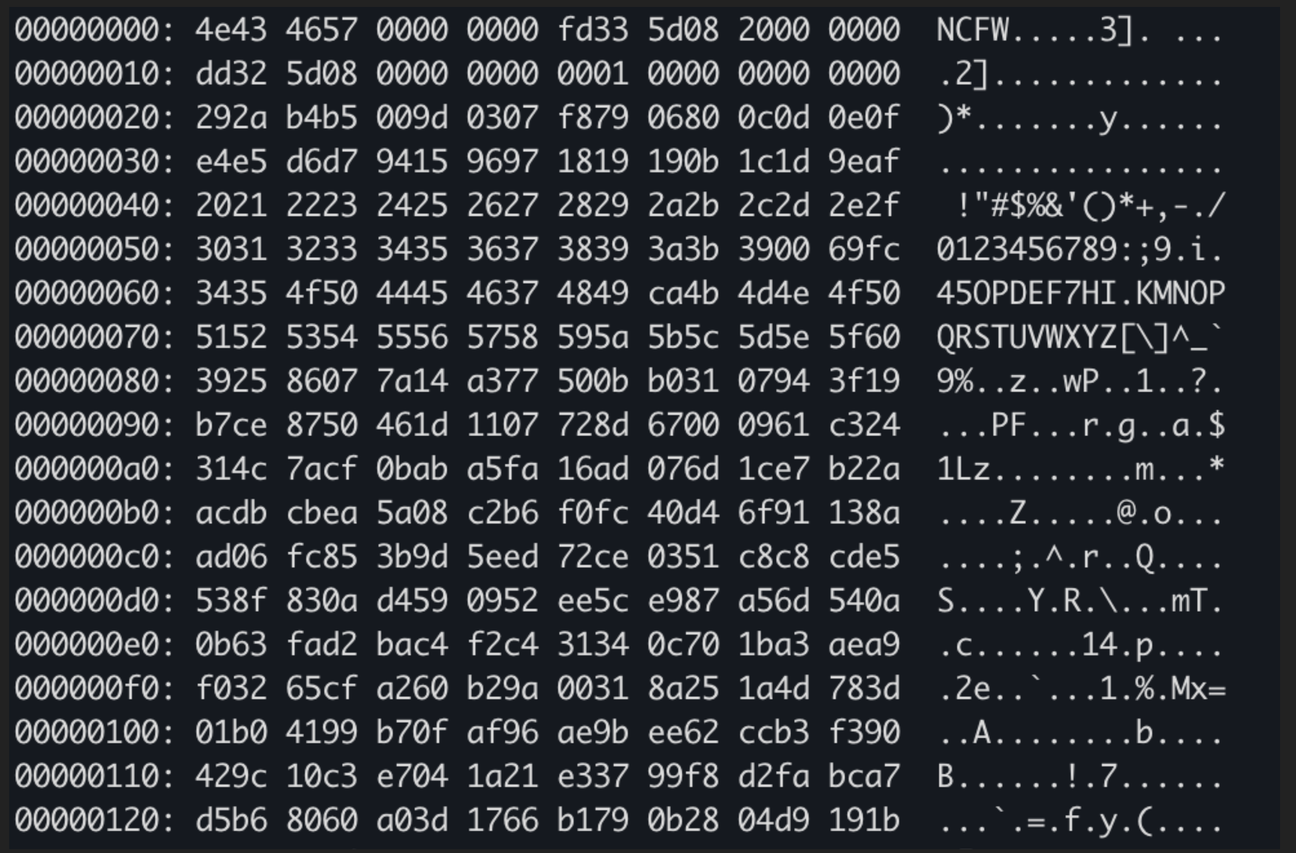
In fact, we didn’t tear down any of them !

Canon

Analysis

Canon - Firmware Extract

- Firmware version v6.03
  - From Canon official
- At the beginning, we use binwalk
  - But the firmware is obfuscated
  - We cannot use IDA directly



Analysis

Canon - Firmware Extract

- We also try some previous works
  - TREASURE CHEST PARTY QUEST: FROM DOOM TO EXPLOIT
    - by Synacktiv
  - Hacking Canon Pixma Printers – Doomed Encryption
    - by Contextis research

Analysis

Canon - Firmware Extract

- We also try some previous works
  - TREASURE CHEST PARTY QUEST: FROM DOOM TO EXPLOIT
    - by Synacktiv
  - Hacking Canon Pixma Printers – Doomed Encryption
    - by Contextis research
- But it cannot extract the firmware :(

Analysis

Canon - Firmware Extract

- We can find some information from obfuscated firmware

Size Magic

```
00000000: 4e43 4657 0000 0000 fd33 5d08 2000 0000  NCFW....3]. ...
00000010: dd32 5d08 0000 0000 0001 0000 0000 0000  .2].............
00000020: 292a b4b5 009d 0307 f879 0680 0c0d 0e0f  )*.......y......
00000030: e4e5 d6d7 9415 9697 1819 190b 1c1d 9eaf  ................
00000040: 2021 2223 2425 2627 2829 2a2b 2c2d 2e2f   !"#$%&'()*+,-./
00000050: 3031 3233 3435 3637 3839 3a3b 3900 69fc  0123456789:;9.i.
00000060: 3435 4f50 4445 4637 4849 ca4b 4d4e 4f50  45OPDEF7HI.KMNOP
00000070: 5152 5354 5556 5758 595a 5b5c 5d5e 5f60  QRSTUVWXYZ[\]^_`
```

We decide to use this patten to search other firmwares without obfuscated

Analysis

Canon - Firmware Extract

- We need to download other firmwares from Canon official website
  - Original firmware download URL is

https://pdisp01.c-wss.com/gdl/WWUFORedirectTarget.do?id=MDQwMDAwNDc1MjA1&cmp=Z01&lang=EN

Analysis

Canon - Firmware Extract

https://pdisp01.c-wss.com/gdl/WWUFORedirectTarget.do?id=MDQwMDAwNDc1MjA1&cmp=Z01&lang=EN

040000475205

Analysis

Canon - Firmware Extract

https://pdisp01.c-wss.com/gdl/WWUFORedirectTarget.do?id=MDQwMDAwNDc1MjA1&cmp=Z01&lang=EN

040000475205

Type

Pdf,firmware …

Ordinal Number

Other model

Version

Firmware version

DEVCORE SECURITY CONSULTING

Analysis

Canon - Firmware Extract

- We can list all versions of firmware
  - V2.01
  - V4.02
  - V6.03
  - V9.03 !?
  - V10.02 !?

But all versions are obfuscated 😭

Let’s download all models

Analysis

Canon - Firmware Extract

- About 130G
- grep NCFW and some plaintext

```
Binary file ./_win-wg7800-ust-fw-v0311.exe.extracted/win-wg7800-ust-fw-
v0311/WG7800series_V0311.exe matches
Binary file ./_MF8080Cw_FirmwareUpdateTool_V1006_KOR.exe.extracted/mf8000c_v1006 for
windows.exe matches
Binary file ./_win-wg7800-ust-fw-v0461.exe.extracted/win-wg7800-ust-fw-
v0461/WG7800series_V0461.exe matches
Binary file ./_win-wg7000-ust-fw-v0257.exe.extracted/win-wg7000-ust-fw-
v0257/WG7000series_V0257.exe matches
```

Analysis

Canon - Firmware Extract

- WG7000 Series is not obfuscated !
  - We analyze the firmware of WG7000 to find the key function

```
1  char *__fastcall sub_41AB68A8(char *result, unsigned int size, char a3)
2  {
3    unsigned int i; // r3
4    unsigned int v4; // r4
5
6    for ( i = 0; i < size; ++i )
7    {
8      v4 = (unsigned __int8)(result[i] - (a3 + i) - 1);
9      result[i] = ~((2 * v4) | (v4 >> 7));
10   }
11   return result;
12 }
```

Analysis

Canon - Firmware Extract

- Try to use the same function to deobfuscate the firmware of MF644CDW
  - Bingo !

```
00000520: 17f9 0120 10bd 0000 496e 7661 6c69 6420  ... ....Invalid
00000530: 4f70 6572 6174 696f 6e00 0000 4469 7669  Operation...Divi
00000540: 6465 2042 7920 5a65 726f 0000 4f76 6572  de By Zero..Over
00000550: 666c 6f77 0000 0000 556e 6465 7266 6c6f  flow....Underflo
00000560: 7700 0000 496e 6578 6163 7420 5265 7375  w...Inexact Resu
00000570: 6c74 0000 5349 4746 5045 3a20 4172 6974  lt..SIGFPE: Arit
00000580: 686d 6574 6963 2065 7863 6570 7469 6f6e  hmetic exception
00000590: 3a20 0000 10b5 0146 02a0 00f0 d9f8 0120  : .....F.......
000005a0: 10bd 0000 5349 4752 5452 4544 3a20 5265  ....SIGRTRED: Re
000005b0: 6469 7265 6374 3a20 6361 6e27 7420 6f70  direct: can't op
000005c0: 656e 3a20 0000 0000 10b5 0128 05d0 0021  en: .......(...!
000005d0: 03a0 00f0 bdf8 0120 10bd 09a1 f8e7 0000  ....... ........
000005e0: 5349 4752 544d 454d 3a20 4f75 7420 6f66  SIGRTMEM: Out of
000005f0: 2068 6561 7020 6d65 6d6f 7279 0000 0000   heap memory....
00000600: 3a20 4865 6170 206d 656d 6f72 7920 636f  : Heap memory co
00000610: 7272 7570 7465 6400 10b5 0021 02a0 00f0  rrupted....!....
00000620: 97f8 0120 10bd 0000 5349 4750 5646 4e3a  ... ....SIGPVFN:
00000630: 2050 7572 6520 7669 7274 7561 6c20 666e   Pure virtual fn
00000640: 2063 616c 6c65 6400 0b46 0146 1846 00f0   called..F.F.F..
```

Plaintext message

Analysis

Canon - Firmware Analysis

- Image Base Address
  - We spent some time looking for image base address of firmware
    - rbasefind

```
0x40b00000: 9800
0x40aff000: 8771
0x40b01000: 8176
0x40afe000: 8143
0x40afd000: 8026
0x40afa000: 7861
0x40afb000: 7796
0x40b02000: 7791
0x40afc000: 7756
0x40af9000: 7681
```

Analysis

Canon - Firmware Analysis

- Original base is 0x40b00000
- It doesn’t seem to be the correct base

```
sub_41AE51A0(6, "%s: called, len=%d.\n", (const char *)&loc_4489AC08, *a3);
if ( a1[46] < 0x20u )
{
  sub_41AE51A0(5, "%s: auth header creation.\n", (const char *)&loc_4489AC08);
```

```
ROM:4489AC08 loc_4489AC08                            ; DATA XREF: sub_41C24A3
ROM:4489AC08                                         ; sub_41C24A38+40↑o ...
ROM:4489AC08                 ANDEQ          R0, R0, R0
ROM:4489AC0C                 ANDEQ          R0, R0, R0
ROM:4489AC10                 ANDEQ          R0, R0, R4
ROM:4489AC14                 ANDEQ          R0, R0, R2
ROM:4489AC18                 ANDEQ          R0, R0, R4
ROM:4489AC1C                 ANDEQ          R0, R0, R4
ROM:4489AC20                 ANDEQ          R0, R0, R1
ROM:4489AC24                 ANDEQ          R0, R0, R3
ROM:4489AC28                 ANDEQ          R0, R0, R1
ROM:4489AC2C                 ANDEQ          R0, R0, R4
ROM:4489AC30                 ANDEQ          R0, R0, R8
ROM:4489AC34                 ANDEQ          R0, R0, R4
ROM:4489AC38                 ANDEQ          R0, R0, R1
ROM:4489AC3C                 ANDEQ          R0, R0, R7
```

Should be strings

Analysis

Canon - Firmware Analysis

- Image Base Address
  - We can find a correct function and debug message to adjust to the correct offset
    - We found the base is 0x40affde0

Analysis

Canon - Firmware Analysis

```
18  debugprintf(6, "%s: called, len=%d.\n", aReadsigneddata, *a3);
19  if ( a1[46] < 0x20u )
20  {
21    debugprintf(5, "%s: auth header creation.\n", aReadsigneddata);
22    v8 = (*(int (**)(void))(*(_DWORD *)(a1[2] + 76) + 68))();
23    debugprintf(6, "%s: lenRead %d.\n", aReadsigneddata, v8);
```

DEVCORE SECURITY CONSULTING

Analysis

Canon - Firmware Analysis

- Canon MF644CDW
  - OS - DryOSV2
    - Customized RTOS by Canon
  - ARMv7 32bit little-endian
  - Linked with application code into single image
    - Kernel
    - Service
    - ...

HP

DEVCORE SECURITY CONSULTING

Analysis

HP - Firmware Extract

- Relatively easy
  - Binwalk -Z
    - Take about 3 - 4 days
    - It will get correct firmware !
  - Other part is similar to Canon

Analysis

HP - Firmware Analysis

- HP - MFP M283fdw
  - OS
    - RTOS - Modify from ThreadX/Green Hills
  - ARM11 Mixed-endian
    - Code - little-endian
    - Data - Big-endian

Agenda

- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

Attack Surface

- Nowadays, there are many services that are enabled by default on the printer

Service	Port	Description
RUI	TCP 80	Web interface
PDL	TCP 9100	Page Description Language
PJL	TCP 9100	Printer Job Language
IPP	TCP 631	Internet Printing Protocol
LPD	TCP 515	Line Printer Daemon Protocol
SNMP	UDP 161	Simple Network Management Protocol

Attack Surface

- Nowadays, there are many services that are enabled by default on the printer

Service	Port	Description
SLP	TCP 427	Service Location Protocol
mDNS	UDP 5353	Multicast DNS
LLMNR	UDP 5355	Link-Local Multicast Name Resolution
…	…	…

Attack Surface

- After we evaluate the overall architecture, we decide to focus on service discovery and DNS series of services
  - SLP
  - mDNS
  - LLMNR

Such protocols implemented by manufacturer themselves are often prone to vulnerabilities

Agenda

- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

Hacking Canon Printer

Hacking printers at Pwn2Own

Service Location Protocol

- SLP is a service discovery protocol that allows computers and other devices to find services in local area network

Hacking printers at Pwn2Own

Canon - SLP

- SLP Architecture without Directory Agent

Hacking printers at Pwn2Own

Canon - SLP

- SLP Architecture without Directory Agent

Hacking printers at Pwn2Own

Canon - SLP

- SLP Architecture without Directory Agent

Hacking printers at Pwn2Own

Canon - SLP

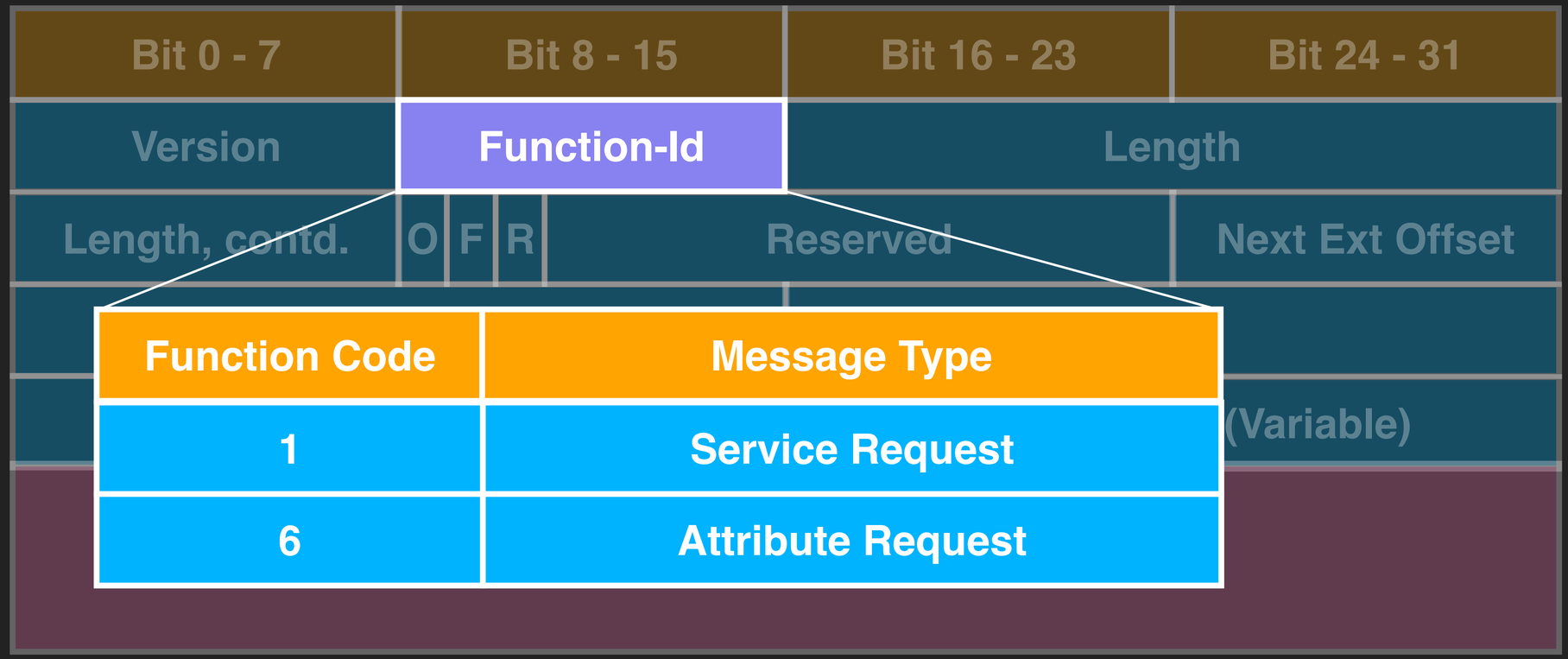
- SLP Packet Structure

Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
Version	Function-Id	Length	
Length, contd.	O F R	Reserved	Next Ext Offset
Next Ext Offset, contd.		XID	
Language Tag Length		Language Tag (Variable)	
Payload (Variable)			

Hacking printers at Pwn2Own

Canon - SLP

- Canon only implemented service request and attribute request



Hacking printers at Pwn2Own

Canon - SLP

- Attribute Request (AttrRqst)
  - Allow a User Agent to discover attributes of given service (by supplying its URL) or for entire device type

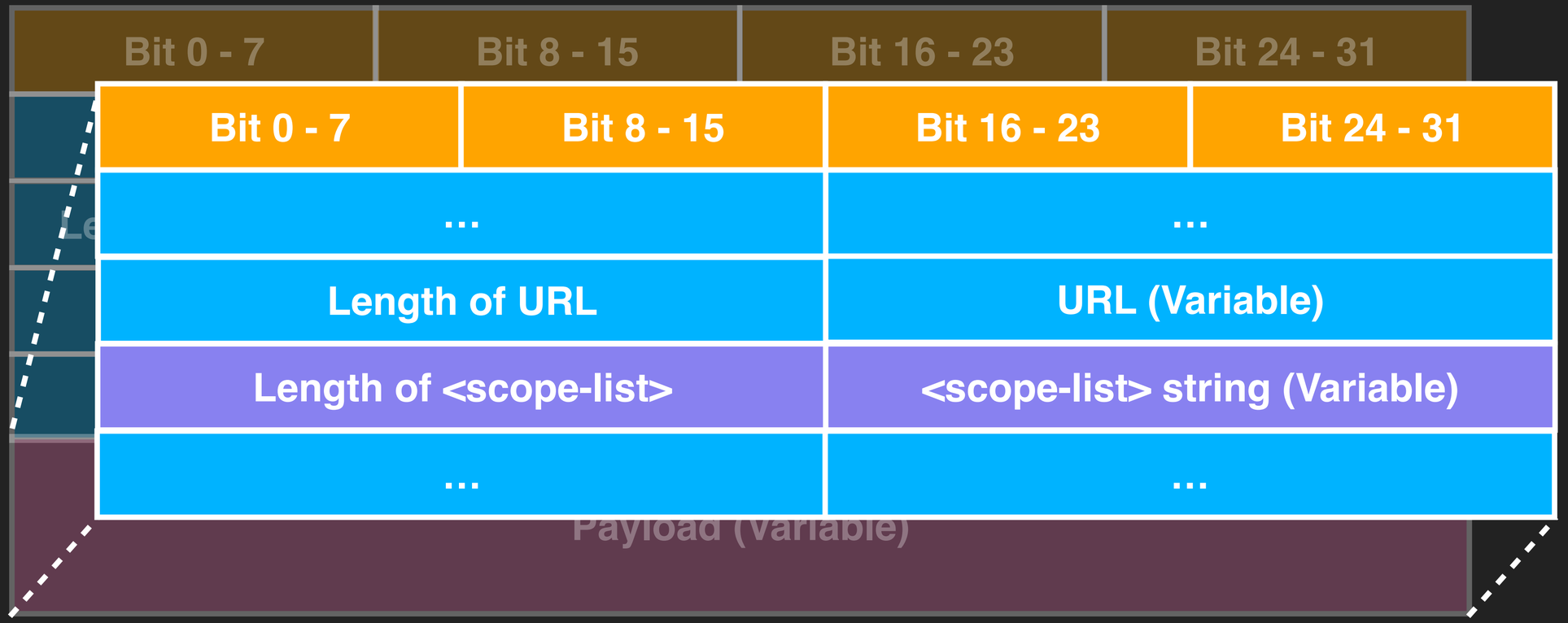
```
The attribute Request:

  URL         = service:printer:lpr://igore.wco.ftp.com/draft
  scope-list  = Development
  Lang. Tag   = de
  tag-list    = resolution,loc*

receives the Attribute Reply:

  (location-description=13te Etage),(resolution=res-600)
```

https://www.ietf.org/rfc/rfc2608.txt

Hacking printers at Pwn2Own

Canon - SLP

- Attribute Request (AttrRqst)



https://www.ietf.org/rfc/rfc2608.txt

Hacking printers at Pwn2Own

Canon - Vulnerability

- There is a stack overflow when Canon is parsing the body of AttrRqst
  - It will convert escape character to character

Hacking printers at Pwn2Own

Canon - Vulnerability

- There is a stack overflow when Canon is parsing the body of AttrRqst

```
int parse_scope_list(...){
    char destbuf[36];
    unsigned int max = 34;
    parse_escape_char(...,destbuf,max)
}
```

Hacking printers at Pwn2Own

Canon - Vulnerability

- There is a stack overflow when Canon is parsing the body of AttrRqst

```
int parse_escape_char(...){
    for(int i = 0 ; i < datalen ;i++){
        if(data[i] == '\\'){  //escaping case
            ...
            destbuf[outlen] = value;
        }else {
            if(outlen <= max){
                goto error;
            }
            destbuf[outlen] = data[i];
        }
        outlen++;
    }
}
```

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

Canon - Vulnerability

- There is a stack overflow when Canon is parsing the body of AttrRqst

```
int parse_escape_char(...){
    for(int i = 0 ; i < datalen ;i++){
        if(data[i] == '\\'){  //escaping case
            ...
            destbuf[outlen] = value;
        }else {
            if(outlen <= max){
                goto error;
            }
            destbuf[outlen] = data[i];
        }
        outlen++;
    }
}
```

Although there is validation in normal case

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

Canon - Vulnerability

- There is a stack overflow when Canon is parsing the body of AttrRqst

```
int parse_escape_char(...){
    for(int i = 0 ; i < datalen ;i++){
        if(data[i] == '\\'){  //escaping case
            ...
            destbuf[outlen] = value;
        }else {
            if(outlen <= max){
                goto error;
            }
            destbuf[outlen] = data[i];
        }
        outlen++;
    }
}
```

No validation in escaping case

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

Canon - Exploitation

- Protection
  - No Stack Guard
  - No DEP
  - No ASLR

image: Flaticon.com

Hacker Friendly :)

We just need to find a buffer to store our shellcode and return to it

Hacking printers at Pwn2Own

Canon - Exploitation

- BJNP
  - A service discovery protocol designed by Canon
  - Exploited by Synacktiv
  - It will store session data on the global buffer

Hacking printers at Pwn2Own

Canon - Exploitation

- Exploit Step

Hacking printers at Pwn2Own

Canon - Exploitation

- Exploit Step
  - Use BJNP to store our shellcode on a global buffer

Hacking printers at Pwn2Own

Canon - Exploitation

- Exploit Step
  - Use BJNP to store our shellcode on a global buffer
  - Trigger stack overflow in SLP and overwrite return address

Hacking printers at Pwn2Own

Canon - Exploitation

- Exploit Step
  - Use BJNP to store our shellcode on a global buffer
  - Trigger stack overflow in SLP and overwrite return address
  - Return to the global buffer

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

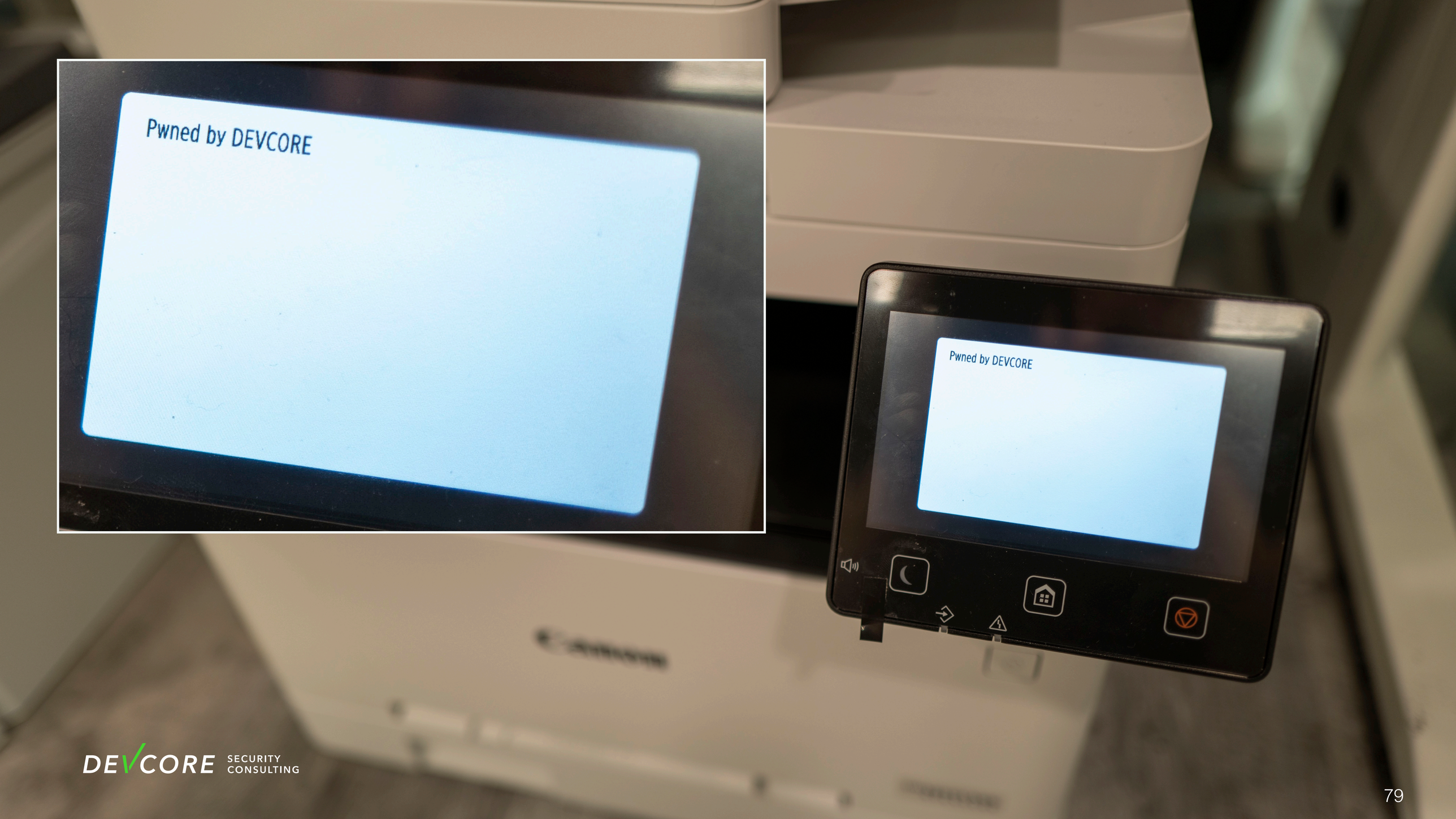
- Require you to prove that you have pwned the target
  - In terms of printer, we choose to print "DEVCORE logo" on the LCD screen at first

But we spent a lot of time looking for it ...

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

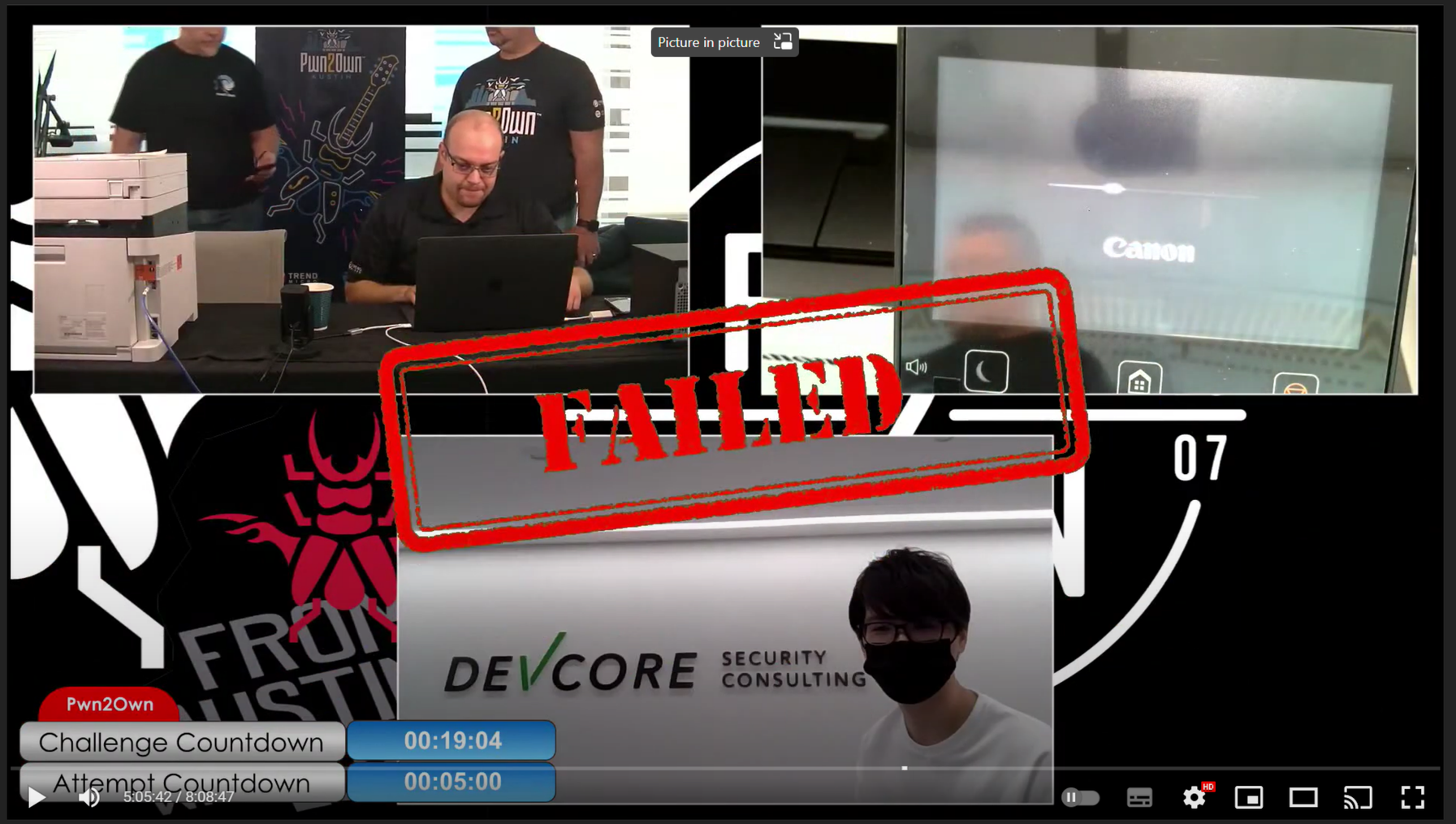
- Require you to prove that you have pwned the target
  - In terms of printer, we choose to print "DEVCORE logo" on the LCD screen
  - In the end, due to time constraints, we finally only chose to print the message on the screen


Pwned by DEVCORE
Pwned by DEVCORE

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

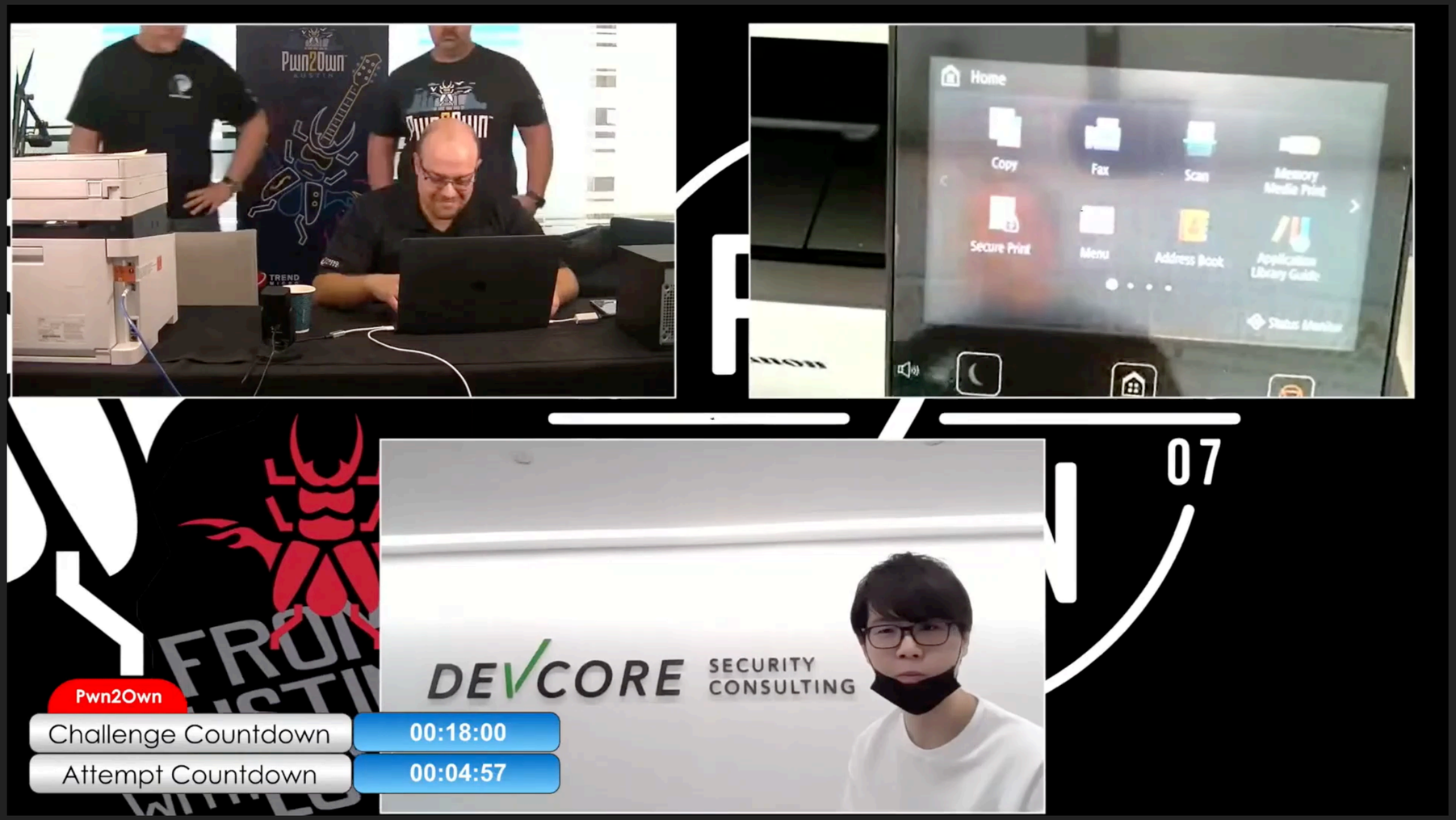
- First try



Hacking printers at Pwn2Own

Pwn2Own Austin 2021

- Second try



http://youtu.be/vQbQImZ3XRw?t=18405

Hacking printers at Pwn2Own

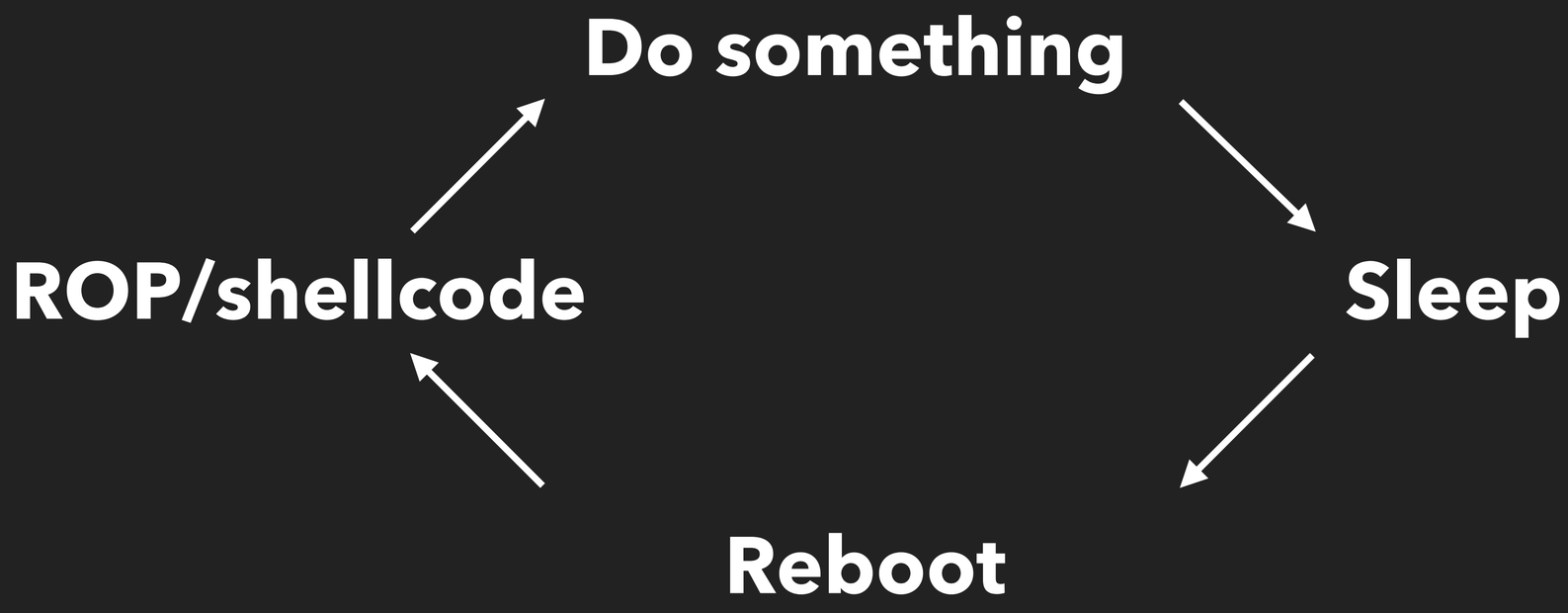
Canon - Exploitation

- Debugger ?
  - If we want to debug it, we need to have a debug console
    - Need to teardown the printer
  - Use an old exploit to install customized debugger
    - Need to downgrade the printer

Hacking printers at Pwn2Own

Canon - Exploitation

- But we are too lazy, we just use sleep debug to debug it :)



Hacking HP Printer

Hacking printers at Pwn2Own

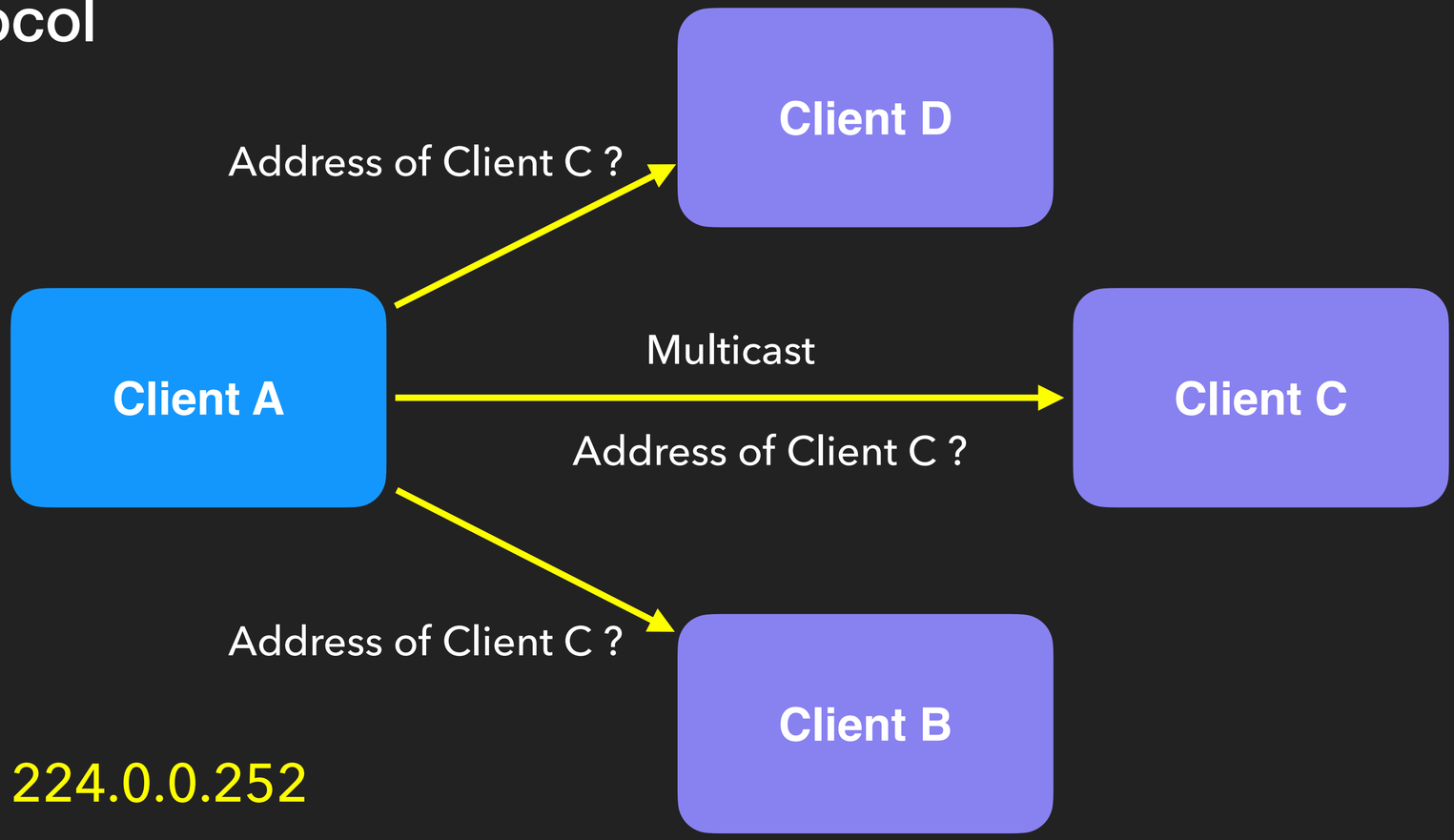
Link-Local Multicast Name Resolution

- LLMNR is very similar to mDNS. It provides base name resolution on the same local link

Hacking printers at Pwn2Own

HP - LLMNR

- LLMNR protocol

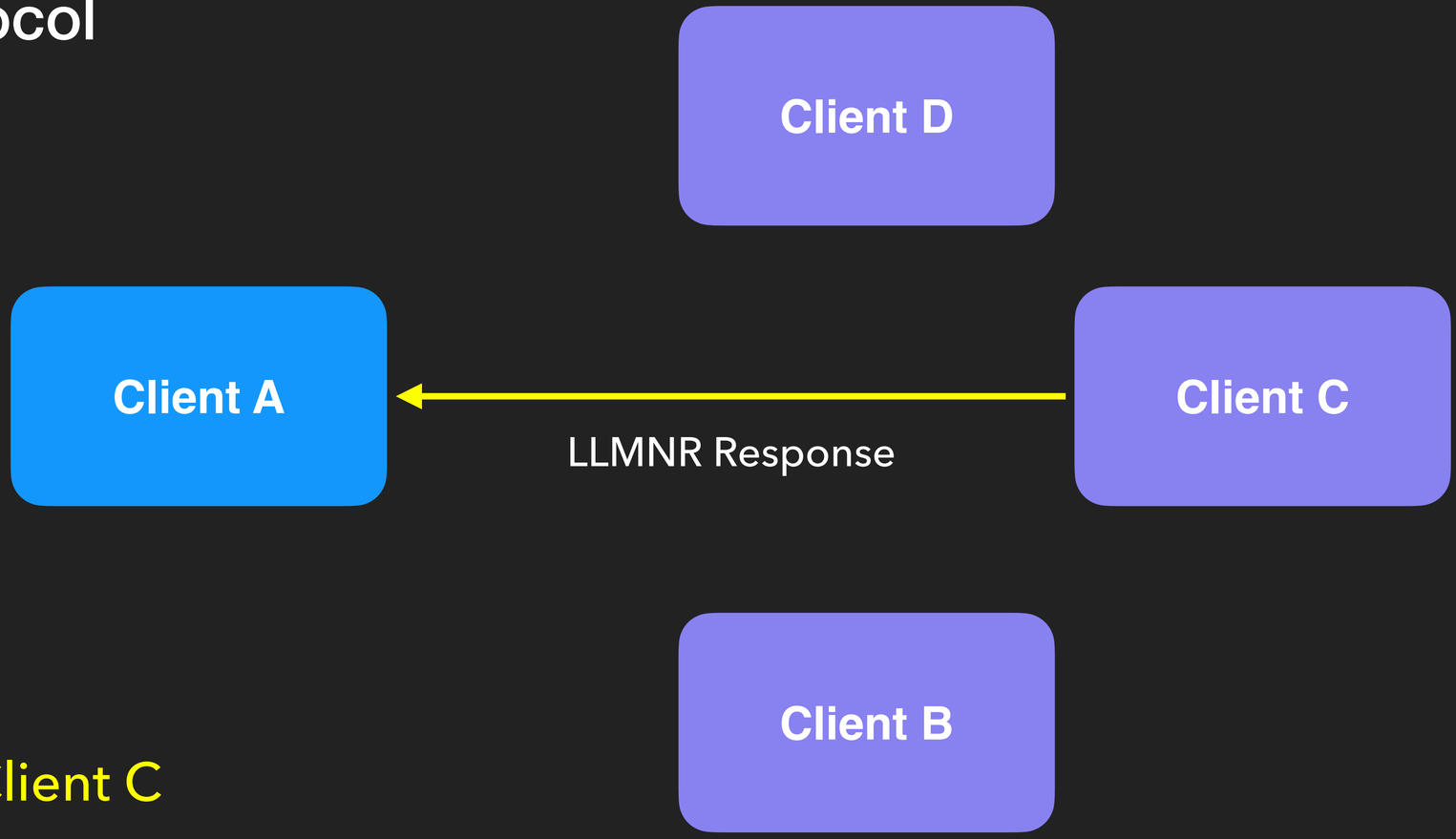


Send requests to 224.0.0.252

Hacking printers at Pwn2Own

HP - LLMNR

- LLMNR protocol



Response from Client C

Hacking printers at Pwn2Own

HP - LLMNR

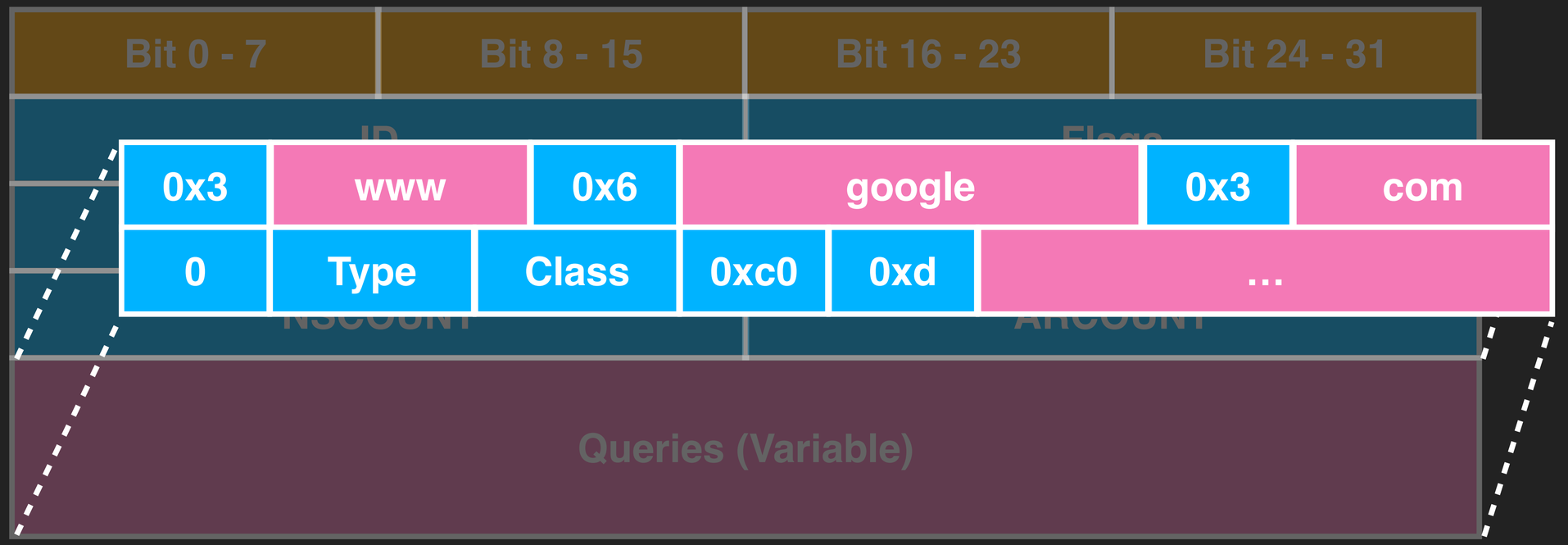
- LLMNR Header (Base on DNS header format)

Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
ID		Flags	
QDCOUNT		ANCOUNT	
NSCOUNT		ARCOUNT	
Queries (Variable)			

Hacking printers at Pwn2Own

HP - LLMNR

- LLMNR queries use the same format as DNS query



Hacking printers at Pwn2Own

HP - Vulnerability

- There is a stack overflow when LLMNR is parsing the queries

```
int llmnr_process_query(...){
    char result[292];
    consume_labels(llmnr_packet->qname,result,...)
    ...
}
```

Hacking printers at Pwn2Own

HP - Vulnerability

- There is a stack overflow when LLMNR is parsing the queries

```
int __fastcall consume_labels(char *qname, char *dst, int llmnr_packet)
{
  while ( 1 )
  {
    labels_length = qname[idx++];
    if(!labels_length)
        break;
    ...
    while(labels_length > 0){
      val = qname[idx++];
      labels_length = (char)(labels_length - 1);
      dst[v4++] = val;
    }
    ...
  }
}
```

Fixed size buffer on stack

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

HP - Vulnerability

- There is a stack overflow when LLMNR is parsing the queries

```
int __fastcall consume_labels(char *qname, char *dst, int llmnr_packet)
{
  while ( 1 )
  {
    labels_length = qname[idx++];
    if(!labels_length)
        break;
    ...
    while(labels_length > 0){
      val = qname[idx++];
      labels_length = (char)(labels_length - 1);
      dst[v4++] = val;
    }
    ...
  }
}
```

Without any length verification

DEVCORE SECURITY CONSULTING

We tried to exploit it in the similar way as Canon, but ...

Hacking printers at Pwn2Own

HP - Exploitation

- Protection
  - No Stack Guard
  - XN (DEP)
  - Memory Protect Unit (MPU)
  - No ASLR

image: Flaticon.com

Hacking printers at Pwn2Own

HP - Exploitation

- Some limits in this vulnerability
  - We can only overflow about 0x100 bytes
  - Null terminated
  - XN(DEP) and MPU
    - Preventing us from executing shellcode

image: Flaticon.com

Hacker not Friendly ?

Can be bypassed ?

How to implement it ?

image: Flaticon.com

Hacking printers at Pwn2Own

HP - Exploitation

- Let's delve into HP RTOS

Hacking printers at Pwn2Own

HP - Exploitation

- Let's delve into HP RTOS
  - Linked with application code into single image

Hacking printers at Pwn2Own

HP - Exploitation

- Let's delve into HP RTOS
  - Linked with application code into single image
  - Many tasks run
    - in a single address
    - in kernel-mode

MMU

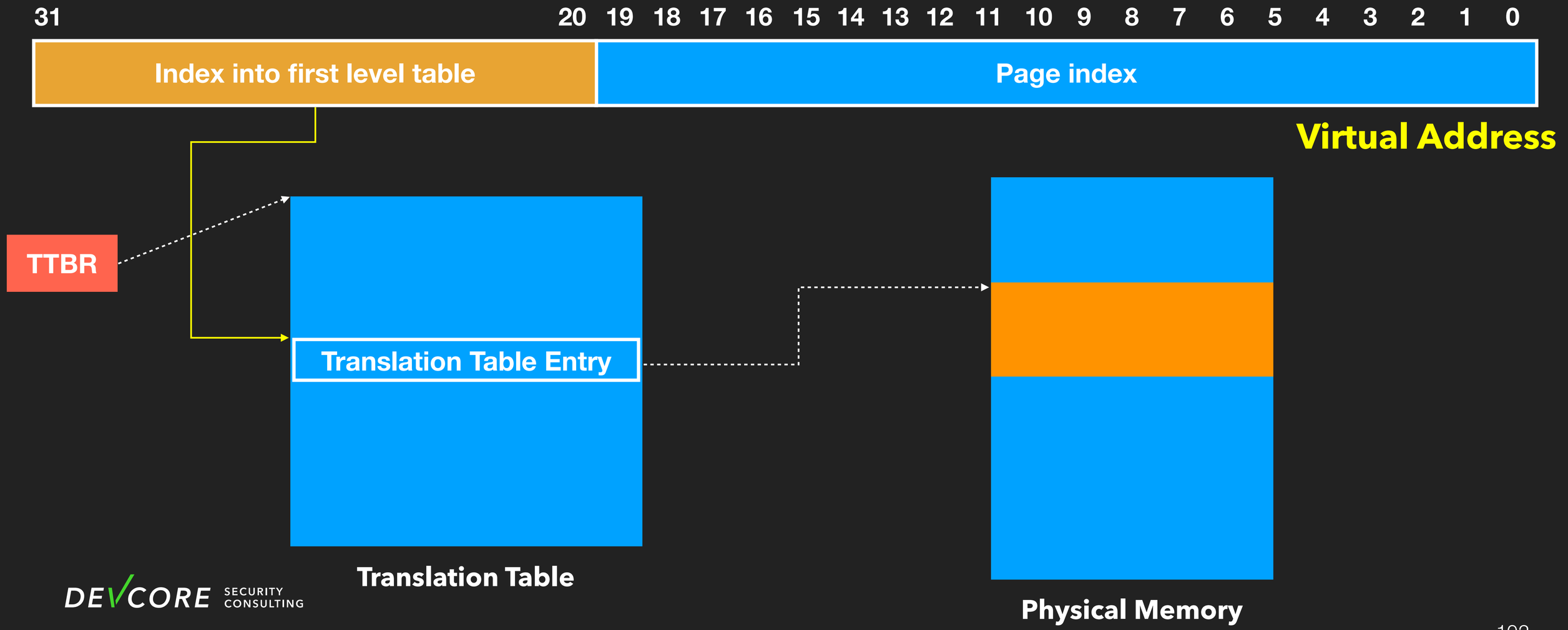
Hacking printers at Pwn2Own

HP - Exploitation

- MMU in HP M283fdw
  - Use one-level page table translation
    - Translation table entry for translating a 1MB section
  - Translation table is located at 0x4003c000

Hacking printers at Pwn2Own

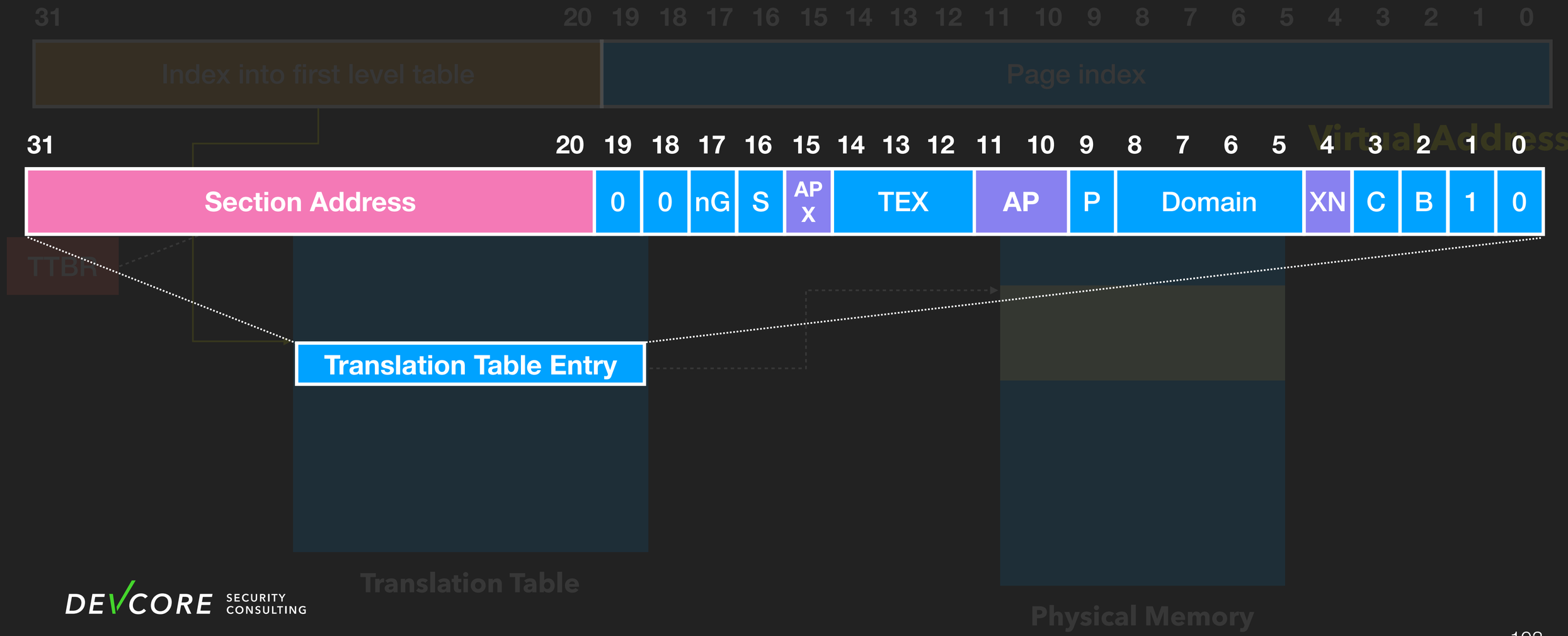
HP - MMU



DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

HP - MMU



Hacking printers at Pwn2Own

HP - Exploitation

- MMU in HP M283fdw
  - Translation table is on known address
    - We can bypass XN through modifying translation table entry !

Hacking printers at Pwn2Own

HP - Exploitation

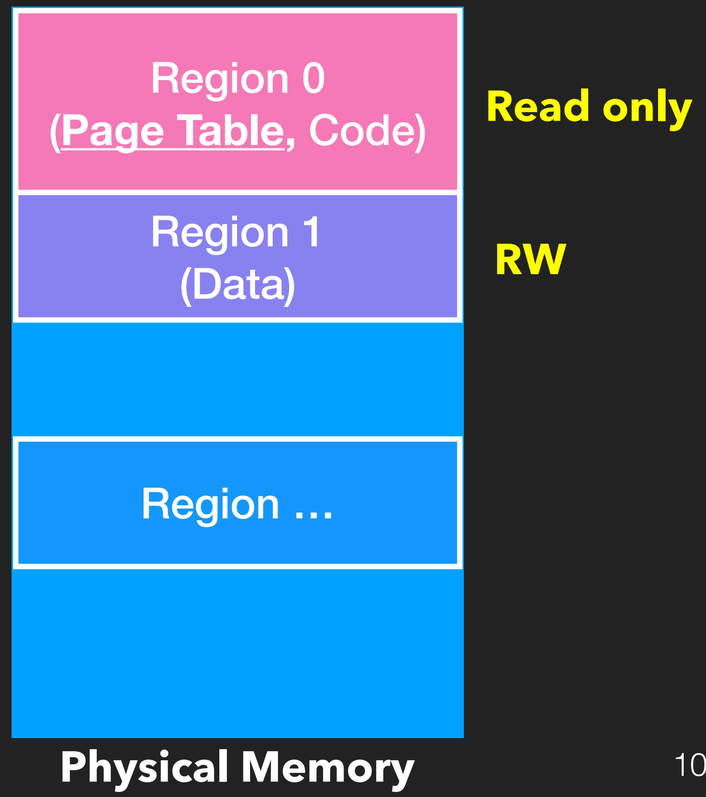
- MMU in HP M283fdw
  - Translation table is on known address
    - We can bypass XN through modifying translation table entry !
    - But it's protected by Memory Protection Unit(MPU)

MPU

Hacking printers at Pwn2Own

HP - Exploitation

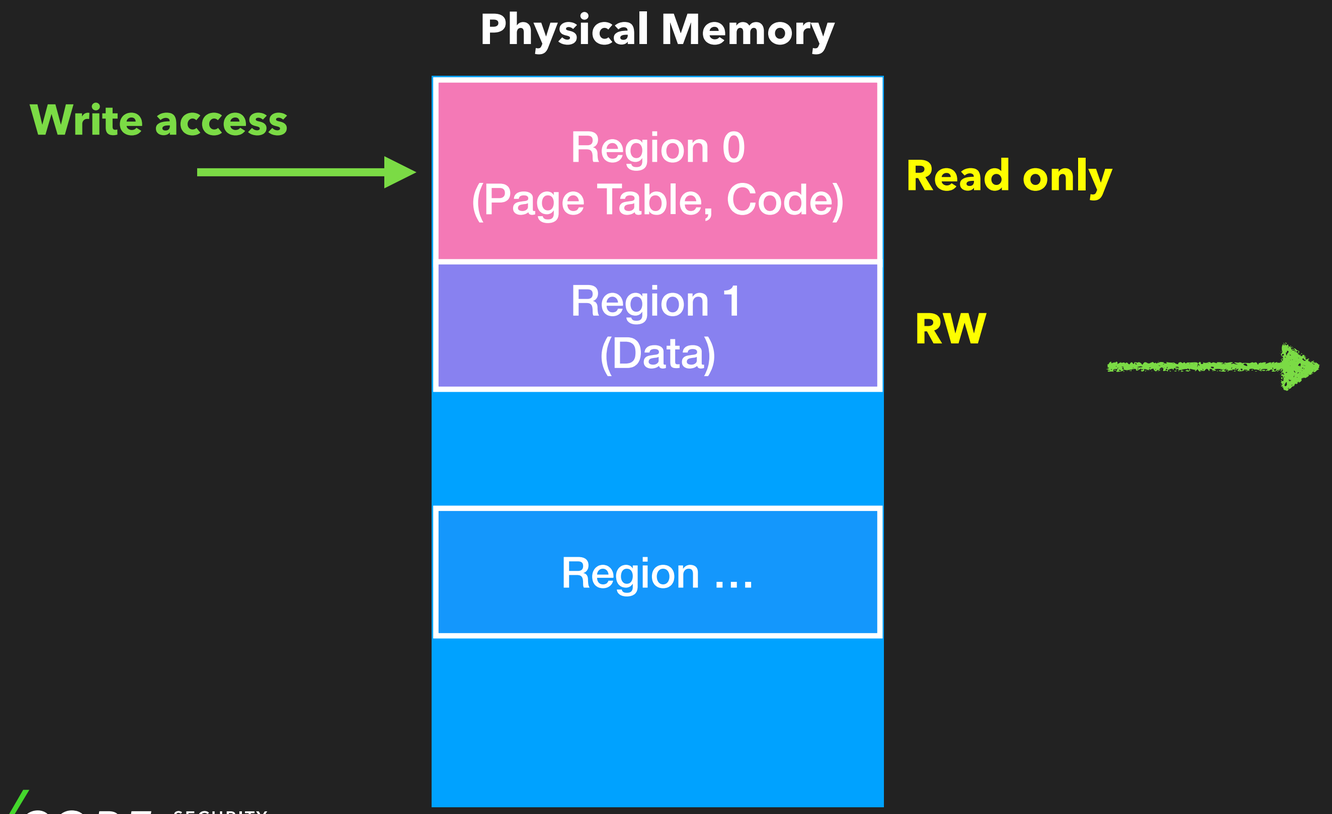
- Memory Protection Unit
  - The MPU enables you to partition memory into regions and set individual protection attributes for each regions
    - Enable when booting



Hacking printers at Pwn2Own

HP - Exploitation

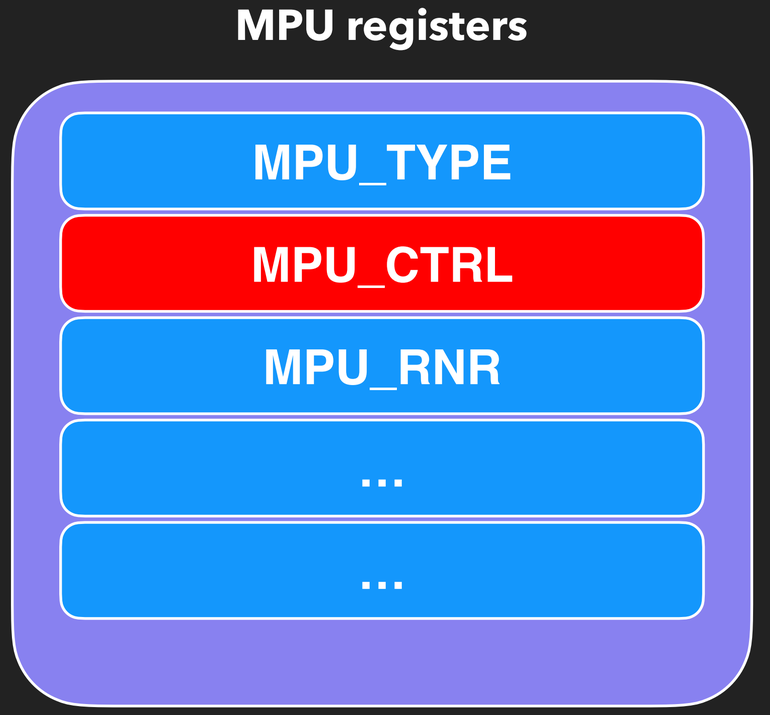
- Memory Protection Unit



Hacking printers at Pwn2Own

HP - Exploitation

- Memory Protection Unit
  - The MPU is configured by a series of memory mapped register in System Control Spaces
    - MPU_CTRL 0xE0400304



We can easily use ROP to overwrite it with 0 to disable MPU

Hacking printers at Pwn2Own

HP - Exploitation

- After we disable MPU and overwrite translation table entry
  - We can modify any code page
    - Modify the code of LPD(Line Printer Daemon) in order to read our payload to specific address
      - Convert LPD to Debug Console

Hacking printers at Pwn2Own

HP - Exploitation

- After we disable MPU and overwrite translation table entry
  - We must invalidate
    - Translation Lookaside Buffer
    - D-cache and I-cache

Hacking printers at Pwn2Own

HP - Exploitation

- Exploit Step
  - Trigger stack overflow in LLMNR and overwrite return address

Hacking printers at Pwn2Own

HP - Exploitation

- Exploit Step
  - Trigger stack overflow in LLMNR and overwrite return address
  - ROP to disable MPU

Hacking printers at Pwn2Own

HP - Exploitation

- Exploit Step
  - Trigger stack overflow in LLMNR and overwrite return address
  - ROP to disable MPU
  - ROP to modify translation table entry

Hacking printers at Pwn2Own

HP - Exploitation

- Exploit Step
  - Trigger stack overflow in LLMNR and overwrite return address
  - ROP to disable MPU
  - ROP to modify translation table entry
  - ROP to modify code of LPD

Hacking printers at Pwn2Own

HP - Exploitation

- Exploit Step
  - Trigger stack overflow in LLMNR and overwrite return address
  - ROP to disable MPU
  - ROP to modify translation table entry
  - ROP to modify code of LPD
  - Use LPD to read our shellcode and jump to shellcode

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

- Require you to prove that you have pwned the target
  - Originally, we just wanted to print the message on the LCD screen

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

- Require you to prove that you have pwned the target
  - Originally, we just wanted to print the message on the LCD screen
  - But luckily, we later saw that a little bit like the DEVCORE logo can be printed
    - Just modify the string and trigger printer test

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

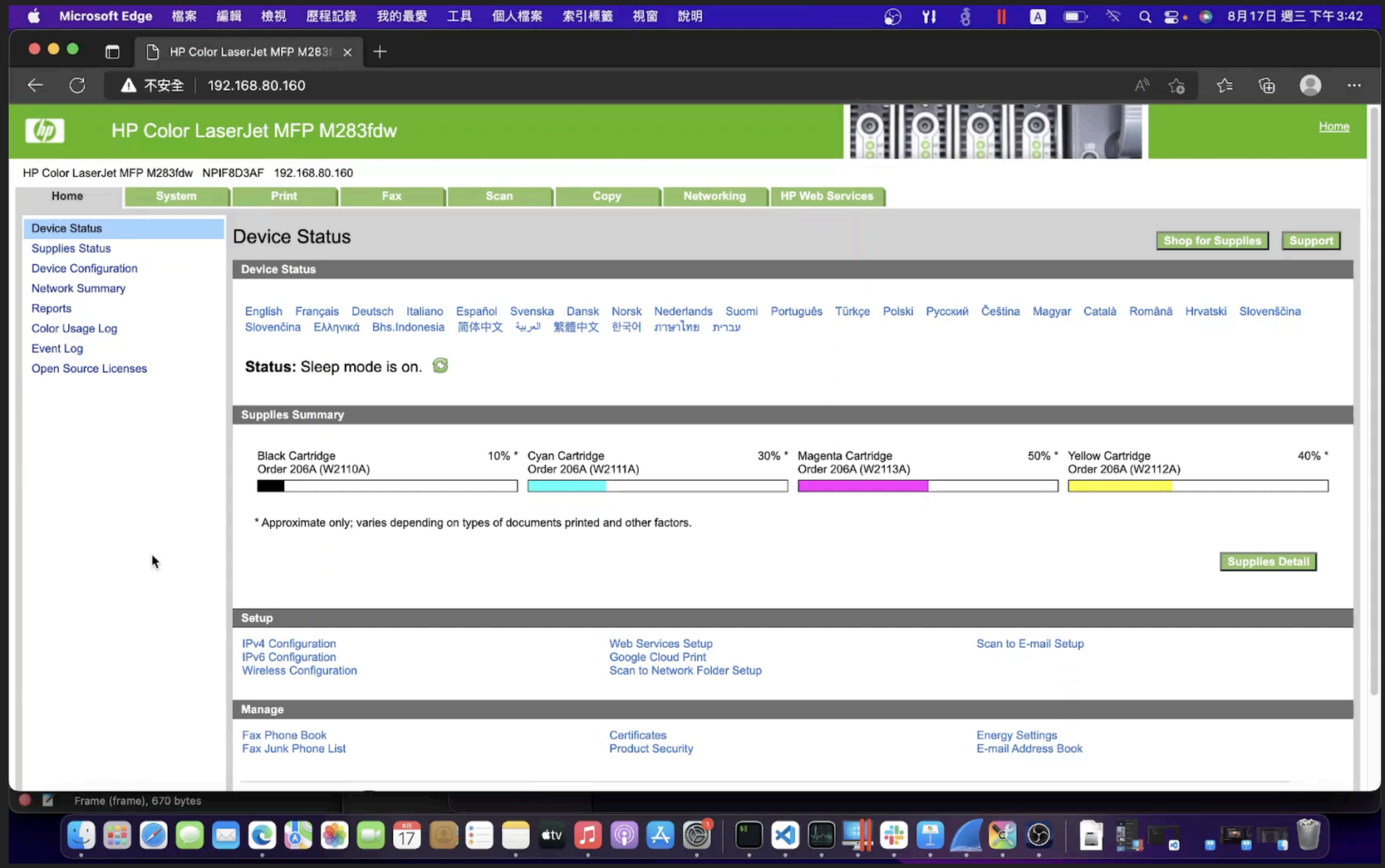
- First try

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

Pwn2Own Austin 2021

- Debug Console



Hacking printers at Pwn2Own

Pwn2Own Austin 2021

- Result

DEVCORE SECURITY CONSULTING

Hacking printers at Pwn2Own

Exploitation

- After we have code execution
  - We can
    - Steal Credential
    - Lateral movement
      - Hard to detect
    - …

Agenda

- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

Mitigation

- Update
  - Canon and HP printer have been patched, please update to the latest

Mitigation

- Update
  - Canon and HP printer have been patched, please update to the latest
- Disable unused service
  - The attack surface of printer is too huge
    - Many services are opened by default

Mitigation

- Update
  - Canon and HP printer have been patched, please update to the latest
- Disable unused service
  - The attack surface of printer is too huge
    - Many services are opened by default
- Firewall

Agenda

- Introduction
- Analysis
- Attack Surface
- Hacking printers at Pwn2Own
- Mitigation
- Conclusion

Conclusion

- Discovery and DNS series services are weak in printer
- Printer is still a good target for red team

Reference

- https://labs.withsecure.com/assets/BlogFiles/Printing-Shellz.pdf
- https://foxglovesecurity.com/2017/11/20/a-sheep-in-wolfs-clothing-finding-rce-in-hps-printer-fleet/
- https://research.checkpoint.com/2018/sending-fax-back-to-the-dark-ages/

Thank you for listening

 @scwuaptx