FIRMWARE
REVERSE
ANALYSIS
KONSOLE
RED
BALLOON
SECURITY
WHO AM I
WHAT DO I DO
WHO AM I
WHAT DO I DO
WHO AM I
WHAT DO I DO
WHO AM I

WHAT DO I DO

PAST PUBLICATIONS:

• **Pervasive Insecurity of Embedded Network Devices.** [RAID10]

• **A Quantitative Analysis of the Insecurity of Embedded Network Devices.** [ACSAC10]

• **Killing the Myth of Cisco IOS Diversity: Towards Reliable Large-Scale Exploitation of Cisco IOS.** [USENIX WOOT 11]

• **Defending Legacy Embedded Systems with Software Symbiotes.** [RAID11]

• **From Prey to Hunter: Transforming Legacy Embedded Devices Into Exploitation Sensor Grids.** [ACSAC11]
WHO AM I

WHAT DO I DO

Past Embedded Tinkerings:

• Interrupt-Hijack Cisco IOS Rootkit
Interrupt-Hijack Rootkit
[Blackhat USA 2011]

- 2nd-stage: Exception Hijack and IOMEM Snooping

- The (MIPS) ERET, or Exception-Return is an Architecture Invariant
- ISR Entry Point is a Binary Invariant, Typically Found at 0x600080180, etc
- Can just hijack entry point, but there is an interior motive

Interrupt-Hijack shellcode frees us from the tyrannies of the watchdog timer.
Perpetual, stealthy execution!
5th Year Ph.D. Candidate
Intrusion Detection Systems Lab
Columbia University
Co-Founder and CEO
Red Balloon Security Inc.
www.redballoonsecurity.com

Past Embedded Tinkering:
• Interrupt-Hijack Cisco IOS Rootkit
• HP LaserJet Printer Rootkit

Who am I
What do I do

7.27.2012
frak.redballoonsecurity.com

a@redballoonsecurity.com
HP-RFU Vulnerability
HP LaserJet 2550 Rootkit

[28c3]

1. Reverse Proxy
   Printer -> Attacker

2. Reverse Proxy
   Printer -> Victim

3. Attacker -> Server
   Via Reverse Proxy

4. Win: Reverse Shell
   Server -> Kitteh

Attacker

Firewall

Network Printer

Server

7.27.2012
frak.redballoonsecurity.com
a@redballoonsecurity.com
WORKFLOW

[Cisco IOS ROOTKIT]
WORKFLOW
[Cisco IOS ROOTKIT]
[HP LaserJet Rootkit]
[Software Symbiotes for Routers, Phones, Printers]
Unpacking Process

- Parse Package
- Manifest
- Decrypt, Compress

- Known Algorithm or Proprietary Algorithm?
- Record
- Encrypted?
- Record
- Compressed?
- Record
- Checksummed?
- Record
- Digitally Signed?

- Known Format or Proprietary Format?
- Sub-Record / FileSystem
- Extraction

- Original Binary Firmware Image

Firmware Analysis

Firmware Modification
Unpacking Process

Known Algorithm or Proprietary Algorithm?

Record

Encrypted?

Record

Compressed?

Record

Checksummed?

Digitally Signed?

Known Format or Proprietary Format?

Sub-Record / FileSystem Extraction

Original Binary Firmware Image

Firmware Analysis

Firmware Modification
**ORIGINAL BINARY FIRMWARE IMAGE**

**UNPACKING PROCESS**

**PARSE PACKAGE MANIFEST**

**DE(crypt,compress)**

- **RECORD ENCRYPTED?**
- **RECORD COMPRESSED?**
- **RECORD CHECKSUMMED?**
- **RECORD DIGITALLY SIGNED?**

**KNOWN ALGORITHM OR PROPRIETARY ALGORITHM?**

**SUB-RECORD / FILESYSTEM EXTRACTION**

**KNOWN FORMAT OR PROPRIETARY FORMAT?**

**FIRMWARE ANALYSIS**

**FIRMWARE MODIFICATION**
Modified Binary Firmware Image

Repacking Process

Firmware Analysis

Firmware Modification
MODIFIED BINARY FIRMWARE IMAGE

REPACKING PROCESS

RE-\{CRYPT,COMPRESS\}, RECALCULATE CHECKSUM, ETC

REGENERATE PACKAGE MANIFEST

KNOWN ALGORITHM OR PROPRIETARY ALGORITHM?

RE-PACK MODIFIED SUB-RECORD / FILE SYSTEM

KNOWN FORMAT OR PROPRIETARY FORMAT?

RECORD ENCRYPTED?
RECORD COMPRESSED?
RECORD CHECKSUMMED?
RECORD DIGITALLY SIGNED?

FIRMWARE ANALYSIS

FIRMWARE MODIFICATION
REASONS WHY ANG STAYS HOME ON FRIDAY NIGHT
REASONS WHY ANG STAYS HOME ON FRIDAY NIGHT
REASONS WHY ANG STAYS HOME ON FRIDAY NIGHT
Reasons why Ang stays home on Friday night

Payload Development
Payload Design
Payload Testing

7.27.2012
frak.redballoonsecurity.com
a@redballoonsecurity.com
REASONS WHY ANG STAYS HOME ON FRIDAY NIGHT

PAYLOAD DESIGN
PAYLOAD DEVELOPMENT
PAYLOAD TESTING

STARE
@
BINARY
BLOB

7.27.2012
frak.redballoonsecurity.com
a@redballoonsecurity.com
Such Mystery!
THIS PART
This part is important
FIRMWARE

EVERSE

NALYSIS

ONSOLE

[BETTER LIVING THROUGH SOFTWARE ENGINEERING]
UNPACKING ENGINE

- HP-RFU Module
- Cisco IOS Module
- Cisco-CNU Module
- XYZ-Format Module

Modification Engine

REPACKING ENGINE

- HP-RFU Module
- Cisco IOS Module
- Cisco-CNU Module
- XYZ-Format Module

Analysis Engine
Device/Vendor Dependent

UNPACKING ENGINE

REPACKING ENGINE

Modification Engine

Analysis Engine
UNPACKING ENGINE

MODIFICATION ENGINE

REPACKING ENGINE

ANALYSIS ENGINE

Device/Vendor Agnostic
Device/Vendor Dependent

**UNPACKING ENGINE**

Device/Vendor Agnostic

**MODIFICATION ENGINE**

**ANALYSIS ENGINE**
Device/Vendor Dependent

UNPACKING ENGINE

REPACKING ENGINE

Device/Vendor Agnostic

Modification Engine

Analysis Engine
F R A K

IRMWARE EVERSE NALYSIS ONSOLE

[BETTER LIVING THROUGH SOFTWARE INTEGRATION]
FRAK

[Better Living Through Software INTEGRATION]
F R A K

FIRMWARE  REVERSE  ANALYSIS  CONSOLE

[BETTER LIVING THROUGH SOFTWARE INTEGRATION]

7.27.2012  frak.redballoonsecurity.com  a@redballoonsecurity.com
F R A K

FIRMWARE   REVERSE   ANALYSIS   ONSOLE

[BETTER LIVING THROUGH SOFTWARE INTEGRATION]

MORE INTEGRATION ON THE WAY
Firmware analysis console

7.27.2012
frak.redballoonsecurity.com

Available Commands
- unpacker_add | u
- help
- firmware_analyze | fa | analyze
- firmware_remove | ur
- firmware_import | fi | import
- firmware_unpack | fp | export
- firmware_export | fx | export
- cut
- modifier_remove | mr
- toggle_debug | db
- exit
- show_panels
- firmware_load | rl
- packer_list | pl
- analyze_grov | as
- analyze_add | aa
- packer_add | ps
- firmware_modify | fn | modify
- firmware_grov | fs
- modifier_list | ml
- set_panels
- firmware_pack | tp | pack
- modifier_add | aa
- clear
- ?
- toggle_verbose | vb
- unpacker_list | ul
- analyzer_list | al
- toggle_auto_analysis | auto

Last Cwd: / Last Status: command not found
Firmware Reverse Analysis

Unpack, Analyze, Modify, Repack: Cisco IOS

test_img = "..//test-data/cisco-ios/c7200-a3jk9s-mz.124-25d.bin"
fmoObj = FirmwareObject(fName=test_img)
fmoObj.registerUnpacker(FrankUnpackerFactory.giveUnpacker("cisco-ios-unpacker"))
fmoObj.unpack()
childObj = fmoObj.getFirmwareObj("/1")
childObj.registerUnpacker(FrankUnpackerFactory.giveUnpacker("generic-unzip-unpacker"))
childObj.unpack()

meat = fmoObj.getFirmwareObj("/1/0")
meat.registerModifier(FrankModifierFactory.giveModifier("cisco-ios-showversion-modifier"))
meat.modify()

childObj.registerPacker(FrankPackerFactory.givePacker("pkzip-packer"))
childObj.pack()

fmoObj.registerPacker(FrankPackerFactory.givePacker("cisco-ios-packer"))
result = fmoObj.pack()

print "tada!"
Without FRAK!
STARE @ BINARY BLOB

PAYLOAD DEVELOPMENT
PAYLOAD TESTING
PAYLOAD DESIGN

{ WITH FRAK! }
ENOUGH TALK DEMO TIME

• Packer/Repacker for Cisco IOS, HP-RFU
• Automagic Binary Analysis
• IDA-Pro Integration
• Entropy-related Analysis
• Automated IOS/RFU Rootkit Injection
Loading a Cisco IOS firmware image into FRAK.

Notice FRAK's auto-analysis modules detects a high entropy binary with an MIPS executable header. Hmmm!
Entropy map of firmware image.

White: high entropy data
Black: low entropy data

Small low random header and footer.

Large amount of random data.

Hmm!
Unpacking image with the cisco-ios unpacker module.

Unpacker yields 3 new records. Notice the auto-analysis output.

Record One: small executable section. Entropy 4.5 (0 - 8)
Record Two: large binary with pkzip header. Entropy 7.8
Record Three: small footer. just a few bytes
Entropy map of header.

Look familiar?

Let’s unpack the middle pkzip record.

cmd: unpack /1 generic-unzip
Unpacking record /1 with the generic-unzip unpacker.

Unpacker yields one record.
Auto-analysis finds a large MIPS ELF executable. Hurray!
Entropy map of unzipped record.

Does the structure look familiar?
IDA Integration using the idainteractive analyzer module.

All IDA automation can be integrated into FRAK as analyzer modules.
Let's have some fun.

Find a string inside the main unpacked executable and replace it.

Use the string-finder analyzer module.
Analysis Results

- lastFlushDir: /tmp/tmp3fCXsBc7200-a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
- this_p-end: 57466171
- elf: 32-bit MSB executable, cisco 7200, 1 (SYSV)
- this_p-loc: 57465397
- type: CODE
- avg-entropy: 5.34211649312
- this_p-start: 57465396
- this_p-size: 775
- target-pattern: This product contains
- isa: MIPS

String-finder analyzer module yields the following:

pattern found at offset: 57465397

string containing offset starts at: 57465396

containing string length: 775

(assuming c-style null-terminated string)
Modify the main executable image using the string-replace-file modifier module.

Input:
replace_offset
replace_filename
replace_overrun

Will replace the contents of a string starting at replace_offset with contents of replace_filename. Has an option to exceed the length of the original string.
7.27.2012
frak.redballoonsecurity.com

replace_filename

/Users/angcui/cave/RBS/frak/trunk/frak-console/src/johnface

a3jk9s-mz.124-25d.bin/UNPACKED/unpacked_1/UNPACKED/unpacked_0
7200, 1 (SYSV)

ngcui/cave/RBS/frak/trunk/frak/extern/idap/idapython/idainteractive.py /tmp/tmp3fCXs8c7200-a
/UNPACKED/unpacked_0/ORIGINAL/C7200-A3.BIN

Running analyzer: string-finder-analyzer
<urwid.command_map.CommandMap object at 0x1005a9f10> Noneng firmwareObj at path: /1/0 with analyzer: string-finder... -)
Modified!

Notice the ** next to record /1/0.

Let's repack and test!

1: Repack record /1 with the pkzip packer module

2: Repack record / with the cisco-ios packer module

3: Export firmware tree to file system
I wonder what the Johnface file contained. Hrm...

Let’s fire up Dynamips and find out.
FRAK is still WIP. For Early Access

Contact

frak-join@lists.redballoonsecurity.com
FRAK is still WIP. For Early Access

Contact
frak-join@lists.redballoonsecurity.com

FRAK Page: http://frak.redballoonsecurity.com
FRAK is still WIP. For Early Access

Contact
frak-join@lists.redballoonsecurity.com

FRAK Page: http://frak.redballoonsecurity.com

Thank you DARPA Cyber Fast Track!