Killing the Myth of Cisco IOS Diversity

Towards Large-Scale Exploitation of Cisco IOS

ANG CUI
ANG@CS.COLUMBIA.EDU
COLUMBIA UNIVERSITY INTRUSION DETECTION SYSTEMS LAB

PROF. SALVATORE J. STOLFO | SAL@CS.COLUMBIA.EDU
JATIN KATARIA | JK3319@COLUMBIA.EDU

BLACKHAT BRIEFINGS USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

Prior Work

FX, 2003
LYNN, 2005
UPPAL, 2007
DAVIS, 2007
MUNIZ, 2008
FX, 2009
MUNIZ AND ORTEGA, 2011

Not comprehensive, but is a good start
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION

Cisco IOS is a high value target
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION

Cisco IOS is a high value target

Cisco IOS is “undefended”
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION

Cisco IOS is a high value target
Cisco IOS is “undefended”
Cisco IOS is “unmonitored”
Killing the Myth of Cisco IOS Diversity

Motivation

Cisco IOS is a high value target
Cisco IOS is “undefended”
Cisco IOS is “unmonitored”
Cisco IOS can be exploited, just like everything else
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION

BUT THERE THE PROBLEM OF SOFTWARE DIVERSITY
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION

But there the problem of software diversity

Approximately 300,000 unique IOS images
No reliable binary invariant

BlackHat Briefings USA 8.3.2011
KILLING THE MYTH OF CISCO IOS DIVERSITY

MOTIVATION

But there the problem of software diversity

Approximately 300,000 unique IOS images
No reliable binary invariant

The (last) major obstacle in large-scale IOS exploitation
KILLING THE MYTH OF CISCO IOS DIVERSITY

RELIABLE SHELLCODE

• IOS DIVERSITY MEANS BINARY DIVERSITY
Killing the Myth of Cisco IOS Diversity

Reliable Shellcode

- IOS Diversity means Binary Diversity, not functional diversity
KILLING THE MYTH OF CISCO IOS DIVERSITY

RELIABLE SHELLCODE

• IOS Diversity means Binary Diversity, not functional diversity

• In fact, IOS is rich in Functional invariants

• For example:

  ![Image of a router command prompt showing a functional monoculture](image.png)

  Functional monoculture in every box!
KILLING THE MYTH OF CISCO IOS DIVERSITY

RELIABLE SHELLCODE

• General strategy to overcome IOS diversity
  • Use functional invariants to resolve binary targets
  • For example: (see FX, 2009)
Killing the Myth of Cisco IOS Diversity

Reliable Shellcode

- General strategy to overcome IOS diversity
  - Use functional invariants to resolve binary targets
  - For example: (see FX, 2009)
Killing the Myth of Cisco IOS Diversity

Reliable Shellcode

• General strategy to overcome IOS diversity
  
  • Use functional invariants to resolve binary targets
  
  • For example: (see FX, 2009)

B: xref

A: str

.text

.data
Killing the Myth of Cisco IOS Diversity

Reliable Shellcode

• General strategy to overcome IOS diversity

  • Use functional invariants to resolve binary targets

  • For example: (see FX, 2009)
Killing the Myth of Cisco IOS Diversity

Disassembling Shellcode #1

• There is a catch (called the watchdog timer)

---

Compute too long, and you will get caught!

Shellcode is heavily resource constrained.

Must resolve binary target using fast, (sub)linear algorithms.
KILLING THE MYTH OF CISCO IOS DIVERSITY

INTERRUPT-HIJACK SHELLCODE

• LET’S KILL 3 BIRDS WITH ONE STONE
KILLING THE MYTH OF CISCO IOS DIVERSITY

INTERRUPT-HIJACK SHELLCODE

- Let’s kill 3 birds with one stone
- Faster
  - ENABLE-BYPASS SHELLCODE: 2n algorithm
  - INTERRUPT-HIJACK SHELLCODE: twice as fast
Killing the Myth of Cisco IOS Diversity

Interrupt-Hijack Shellcode

- Let’s kill 3 birds with one stone
  - Faster
  - Stealthier

- Enable-bypass, vty rebind, etc requires persistent TCP connection
- Interrupt-Hijack uses the payload of process-switched packets as a covert command and control channel
- C&C is bidirectional thanks to IOMEM scrubber
Killing the Myth of Cisco IOS Diversity

Interrupt-Hijack Shellcode

• Let’s kill 3 birds with one stone
  • Faster
  • Stealthier
  • More Control

• No need to be constrained by IOS shell
• Rootkit runs @ supervisor mode. We can even write to eeprom (See last slide)
KILLING THE MYTH OF CISCO IOS DIVERSITY

INTERRUPT-HIJACK SHELLCODE

• 1st STAGE:
Killing the Myth of Cisco IOS Diversity

Interrupt-Hijack Shellcode

- 1st stage: Unpack 2nd stage
Killing the Myth of Cisco IOS Diversity

Interrupt-Hijack Shellcode

• 1st stage: Unpack 2nd stage, hijack all int-handlers
Killing the Myth of Cisco IOS Diversity

Interrupt-Hijack Shellcode

- 1st stage: Unpack 2nd stage, hijack all int-handlers, compute hash on addresses of "ERET" instructions (why?)

checksum: 0x3e27f3de
INTERRUPT-HIJACK SHELLCODE

- 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 ULTERIOR MOTIVE

- USE ERET LOCATIONS IN THE IMAGE TO FINGERPRINT IOS VERSION

INTERRUPT-HIJACK SHELLCODE FREES US FROM THE TYRANNIES OF THE WATCHDOG TIMER.

PERPETUAL, STEALTHY EXECUTION!
KILLING THE MYTH OF CISCO IOS DIVERSITY

INT-HIJACK SHELLCODE: FINGERPRINT EXFILTRATION

- ICMP IS CONVENIENT, BUT ANY “PROCESS-SWITCHED” PACKET WILL SUFFICE
- C&C INSIDE PAYLOAD OF “NORMAL” TRAFFIC
- COMPLEX THIRD-STAGE PAYLOADS CAN BE ASSEMBLED IN A “PROTOCOL-SPREAD-SPECTRUM” MANNER
- PING, DNS, PDUs, TCP, ALL THE SAME AS LONG AS IT IS PROCESS-SWITCHED
Killing the Myth of Cisco IOS Diversity

Int-Hijack Shellcode: Fingerprint Exfiltration

- ICMP is convenient, but any “process-switched” packet will suffice
- C&C inside payload of “normal” traffic
- Complex third-stage payloads can be assembled in a “protocol-spread-spectrum” manner
- PING, DNS, PDUs, TCP, all the same as long as it is process-switched
Killing the Myth of Cisco IOS Diversity

Int-Hijack Shellcode: Fingerprint Exfiltration

- ICMP is convenient, but any "process-switched" packet will suffice.
- C&C inside payload of "normal" traffic.
- Complex third-stage payloads can be assembled in a "protocol-spread-spectrum" manner.
- PING, DNS, PDUs, TCP, all the same as long as it is process-switched.

BlackHat Briefings USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

**INT-HIJACK SHELLCODE: FINGERPRINT EXFILTRATION**

- ICMP is convenient, but any “process-switched” packet will suffice
- C&C inside payload of “normal” traffic
- Complex third-stage payloads can be assembled in a “protocol-spread-spectrum” manner
- PING, DNS, PDUs, TCP, all the same as long as it is process-switched
Killing the Myth of Cisco IOS Diversity

Int-Hijack Shellcode: Fingerprint Exfiltration

- ICMP is convenient, but any “process-switched” packet will suffice.
- C&C inside payload of “normal” traffic.
- Complex third-stage payloads can be assembled in a “protocol-spread-spectrum” manner.
- Ping, DNS, PDUs, TCP, all the same as long as it is process-switched.

Runtime fingerprint gives us positive ID on the victim router’s hardware, platform and IOS version!

BlackHat Briefings USA 8.3.2011
KILLING THE MYTH OF CISCO IOS DIVERSITY

RELIABLE SHELLCODE

• General strategy to overcome IOS diversity
  • Use functional invariants to resolve binary targets
  • IOS Diversity is (very) finite
    • How do you defeat address space randomization?
Killing the Myth of Cisco IOS Diversity

Reliable Shellcode

• General strategy to overcome IOS diversity
  • Use functional invariants to resolve binary targets
  • IOS Diversity is (very) finite
    • How do you defeat ASR if there are ONLY 300,000 possible permutations?
KILLING THE MYTH OF CISCO IOS DIVERSITY

RELIABLE SHELLCODE

• General strategy to overcome IOS diversity
  • Use functional invariants to resolve binary targets
  • IOS Diversity is (very) finite
    • How do you defeat ASR if there are ONLY 300,000 possible permutations?
    • Build a lookup table!
Killing the Myth of Cisco IOS Diversity

Generalized reliable exploitation of IOS (in 4 simple steps)

1.a: exploit vulnerability, load and run 1st stage eret-hijack rootkit (~400 bytes, pic, will run anywhere)
KILLING THE MYTH OF CISCO IOS DIVERSITY

GENERALIZED RELIABLE EXPLOITATION OF IOS (IN 4 SIMPLE STEPS)

1.a: EXPLOIT VULNERABILITY, LOAD AND RUN 1ST STAGE ERET-HIJACK ROOTKIT (~400 BYTES, PIC, WILL RUN ANYWHERE)

1.b: 1ST STAGE CODE LOCATES/HIJACKS ALL ERET INSTRUCTIONS, EXFILTRATE HASH (FINGERPRINT) OF ERET-ADDRESSES BACK TO ATTACKER (VIA ICMP, ETC)
KILLING THE MYTH OF CISCO IOS DIVERSITY

GENERALIZED RELIABLE EXPLOITATION OF IOS (IN 4 SIMPLE STEPS)

1.a: EXPLOIT VULNERABILITY, LOAD AND RUN 1ST STAGE ERET-HIJACK ROOTKIT (~400 BYTES, PIC, WILL RUN ANYWHERE)

1.b: 1ST STAGE CODE LOCATES/HIJACKS ALL ERET INSTRUCTIONS, EXFILTRATE HASH (FINGERPRINT) OF ERET-ADDRS BACK TO ATTACKER (VIA ICMP, ETC)

2.a: ATTACKER CONSULTS OFFLINE IOS FINGERPRINT DATABASE, MAKES POSITIVE ID (HARDWARE PLATFORM, IOS VERSION)

BlackHat Briefings USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

Generalized reliable exploitation of IOS (in 4 simple steps)

1.a: EXPLOIT VULNERABILITY, LOAD AND RUN 1ST STAGE ERET-HIJACK ROOTKIT (~400 BYTES, PIC, WILL RUN ANYWHERE)

1.b: 2ST STAGE CODE LOCATES/HIJACKS ALL ERET INSTRUCTIONS, EXFILTRATE HASH (FINGERPRINT) OF ERET-ADDRS BACK TO ATTACKER (VIA ICMP, ETC)

2.a: ATTACKER CONSULTS OFFLINE IOS FINGERPRINT DATABASE, MAKES POSITIVE ID (HARDWARE PLATFORM, IOS VERSION)

2.b: CONSTRUCT VERSION DEPENDENT 3RD STAGE PAYLOAD, UPLOAD USING 2ND STAGE C&C (AGAIN, USING ICMP, ETC)... WIN!

BlackHat Briefings USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

3rd Stage Payloads!

- More demos
- Third-stage payloads to:
  - Disable IOS integrity verification command “show sum”
  - Disable password authentication
  - Remote Bricking of router motherboard
Killing the Myth of Cisco IOS Diversity

SACRIFICE TO THE DEMO GODS

Remotely bricking router using 3rd-stage payload over ICMP!

BlackHat Briefings USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

What’s Next (Offensive)?

• More comprehensive fingerprint database
  • ~3,000 images in the fingerprint DB. Roughly 1% coverage.
KILLING THE MYTH OF CISCO IOS DIVERSITY

WHAT’S NEXT (OFFENSIVE)?

• MORE COMPREHENSIVE FINGERPRINT DATABASE
  • ~3,000 images in the fingerprint DB. Roughly 1% coverage.

• EEPROM RESIDENT MALWARE
  • Current rootkit will not survive IOS update
  • Better to live in EEPROM
    • Line cards
    • Network modules
    • Motherboard EEPROM
Killing the Myth of Cisco IOS Diversity

What’s Next (Offensive)?

• More comprehensive fingerprint database
  • ~3,000 images in the fingerprint DB. Roughly 1% coverage.

• EEPROM resident malware
  • Current Rootkit will not survive IOS update
  • Better to live in EEPROM
  • Line cards
  • Network modules
  • Motherboard EEPROM

• Lawful Intercept Hijacking, routing shenanigans, be creative!

BlackHat Briefings USA 8.3.2011
KILLING THE MYTH OF CISCO IOS DIVERSITY

WHAT’S NEXT (DEFENSIVE)?

- SOFTWARE SYMBIOTES
  - GENERIC HOST-BASED DEFENSE FOR EMBEDDED DEVICES.
  - “DEFENDING LEGACY EMBEDDED SYSTEMS WITH SOFTWARE SYMBIOTES”
  - TO APPEAR IN RAID 2011. LOOK OUT!
KILLING THE MYTH OF CISCO IOS DIVERSITY

WHAT’S NEXT (DEFENSIVE)?

• Cisco IOS Rootkit Detectors
  • Runs on Real Cisco Iron
  • Deployed in real networks
  • Will catch real IOS malware

BLACKHAT BRIEFINGS USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

What’s Next (Defensive)?

• Cisco IOS Rootkit Detectors
  • Runs on Real Cisco Iron
  • Deployed in Real Networks
  • Will catch Real IOS Malware

• A friendly shootout to test our defenses? -)

• Please contact us!
KILLING THE MYTH OF CISCO IOS DIVERSITY

ANSWERS!

• FEEL FREE TO CONTACT US
  • {ANG|SAL}@CS.COLUMBIA.EDU

• PLEASE CHECKOUT OUR PUBLICATIONS AND ONGOING RESEARCH
  • HTTP://IDS.COLUMBIA.EDU

• This work was partially supported by:
  • DARPA Contract, CRASH Program, SPARCHS, FA8750-10-2-0253
  • Air Force Research labs under agreement number FA8750-09-1-0075
KILLING THE MYTH OF CISCO IOS DIVERSITY

BACKUP SLIDES
KILLING THE MYTH OF CISCO IOS DIVERSITY

DISASSEMBLING SHELLCODE #1

• Originally presented by Felix Linder

Somewhere in every IOS image...

FLAG = passwordisright()

IF (FLAG!=0){
   rootme()
}
ELSE {
   printf("BAD SECRETS -("")
}

BlackHat Briefings USA 8.3.2011
Killing the Myth of Cisco IOS Diversity

Disassembling Shellcode #1

- Originally presented by Felix Linder

Somewhere in every IOS image...

```
Flag = 1
If (flag! = 0){
    rootme()
}
Else {
    printf("BAD SECRETS -("
}
```
KILLING THE MYTH OF CISCO IOS DIVERSITY

COMPARISON OF POTENTIAL FINGERPRINT FEATURES

- Fairly random, can be used to fingerprint IOS
- A single feature fingerprint
- One firmware, one address
- Potential for collision higher than the next option

Distribution of “Bad Secrets” string x-ref in IOS (32-bit memory space)
KILLING THE MYTH OF CISCO IOS DIVERSITY

COMPARISON OF POTENTIAL FINGERPRINT FEATURES

• Concentrated in a predictable range in IOS memory

• Yet diverse enough to uniquely identify unknown firmware version

• Also needed in 2nd stage rootkit, kill 2 birds with one stone

• In our opinion, a pretty good target, but there are many others.

• Multi-vector feature. Each image contains approximately 6-30 ERET instructions.

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

BLACKHAT BRIEFINGS USA 8.3.2011
KILLING THE MYTH OF CISCO IOS DIVERSITY

THE BASIC IDEA

• Reduce (binary) diverse target to a (functional) monoculture

• Take advantage of offline processing

  • Use a two-phase attack
  • Build a database of device fingerprints

  • Macro-ize 3rd stage payloads, generate device specific payloads on the fly
KILLING THE MYTH OF CISCO IOS DIVERSITY

FOR EXAMPLE

DOTPLOT OF TWO MINOR REVISIONS OF 12.4 IOS IMAGES FOR THE SAME HARDWARE

IOS 12.4-23b vs 12.4-12
CISCO 7200 / NPE-200