COLUMBIA UNIVERSITY

IN THE CITY OF NEW YORK

KASPERSKY lab

Adventures In Embedded Exploitation

When Routers Hack Printers!

Ang Cui, Columbia University

"IT Security for the Next Generation"
International Round, Delft University of Technology
11-13 May, 2012
The Netherlands

Kaspersky® Academy
IT Security
for the Next Generation
International Student Conference

Adventures In Embedded Exploitation

Hi there!

W h o a m I

W h a t d o I

D O

Adventures In Embedded Exploitation

Hi there!

Kaspersky® Academy
IT Security
for the Next Generation
International Student Conference

W h o a m I

W h a t d o I D O

4th Year Ph.D. Candidate
Intrusion Detection Systems Lab
Columbia University

KASPERSKY lab

Adventures In Embedded Exploitation

Hi there!

Kaspersky® Academy
IT Security for the Next Generation
International Student Conference

W h o a m I

W h a t d o I D O

4th Year Ph.D. Candidate
Intrusion Detection Systems Lab
Columbia University

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]

Adventures In Embedded Exploitation

Hi there!

Kaspersky® Academy
IT Security
for the Next Generation
International Student Conference

W h o a m I

W h a t d o I D O

4th Year Ph.D. Candidate
Intrusion Detection Systems Lab
Columbia University

Recent:

- Killing the Myth of (Cisco) IOS Diversity. [BlackHat USA]
- Print Me If You Dare: Firmware Modification Attacks and the Rise of Printer Malware. [28c3]

Adventures In Embedded Exploitation

Hi there!

Two adventures in embedded exploitation

Adventures In Embedded Exploitation

Hi there!

Two adventures in embedded exploitation

Cisco Routers

Adventures In Embedded Exploitation

Hi there!

Two adventures in embedded exploitation

Cisco Routers

HP Printers

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

- 300,000 IOS Images

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

- 300,000 IOS Images
- Binary diversity makes reliable shellcode difficult

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

- 300,000 IOS Images
- Binary diversity makes reliable shellcode difficult
- Solved using Interrupt Hijack Shellcode

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

- 300,000 IOS Images
- Binary diversity makes reliable shellcode difficult
- Solved using Interrupt Hijack Shellcode

  ~400 bytes

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

- 300,000 IOS Images
- Binary diversity makes reliable shellcode difficult
- Solved using Interrupt Hijack Shellcode

  ~400 bytes

  IOS Version Agnostic

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Killing the Myth of (Cisco) IOS Diversity

- 300,000 IOS Images
- Binary diversity makes reliable shellcode difficult
- Solved using Interrupt Hijack Shellcode

  ~400 bytes

  IOS Version Agnostic

  And it works like this…

Your typical IOS firmware memory layout

At exploitation time: do not know exact memory layout of target

Interrupt Hijack Shellcode

Stage 1: Unpack Stage 2

Adventures In Embedded Exploitation

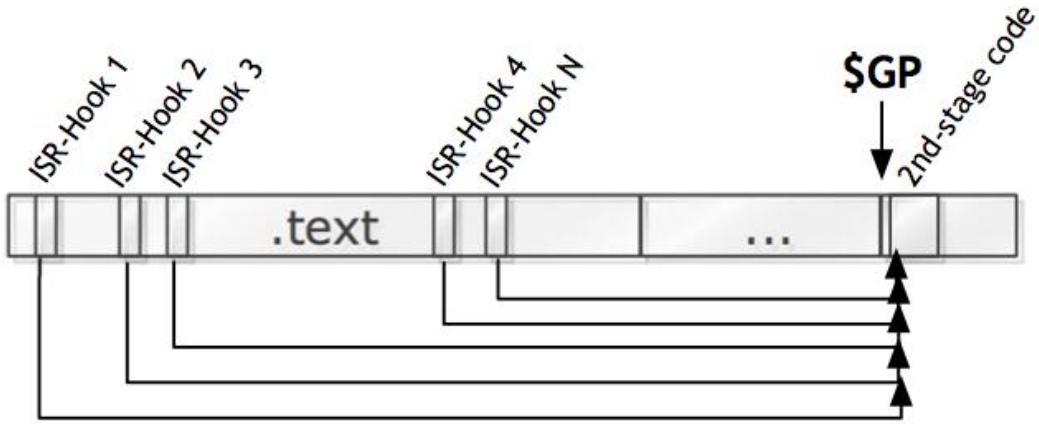
Version Agnostic Cisco IOS Malware

Interrupt Hijack Shellcode

Stage 2: Hijack all Interrupt Handlers

```
.text:805614BC    sw      $at, 0x623733D4
.text:805614C0    ld      $k0, 0xD0($sp)
.text:805614C4    ld      $at, 8($sp)
.text:805614C8    ld      $t4, 0x60($sp)
.text:805614CC    ld      $sp, 0xE8($sp)
.text:805614D0    sync
.text:805614D4    eret
```

```
MEMORY:605614BC  # ---------------------------------------------------------
MEMORY:605614BC sw      $at, dword_623733D4
MEMORY:605614C0 ld      $k0, 0xD0($sp)
MEMORY:605614C4 ld      $at, 8($sp)
MEMORY:605614C8 ld      $t4, 0x60($sp)
MEMORY:605614CC ld      $sp, 0xE8($sp)
MEMORY:605614D0 sync
MEMORY:605614D4 jr      $gp
MEMORY:605614D8 nop
MEMORY:605614D8  # ---------------------------------------------------------
```



Interrupt Hijack Shellcode

Stage 2: Hijack all Interrupt Handlers

Hijack Interrupt handlers because:

- Perpetual control of CPU
- Escapes watchdog timer
- Addr of ERET instructions very useful

Adventures In Embedded Exploitation

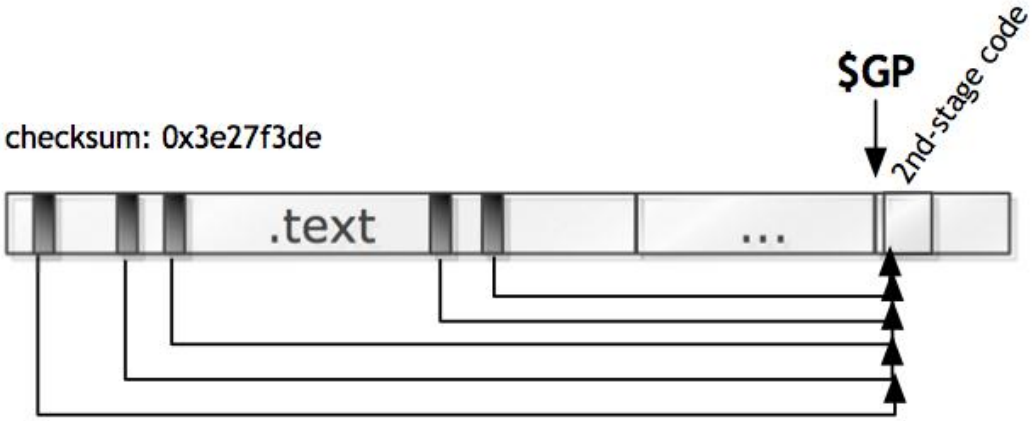
Version Agnostic Cisco IOS Malware

Stage 2 shellcode calculates fingerprint

```
.text:805614BC
.text:805614C0
.text:805614C4
.text:805614C8
.text:805614CC
.text:805614D0
.text:805614D4
```

```
sw      $at, 0x623733D4
ld      $k0, 0xD0($sp)
ld      $at, 8($sp)
ld      $t4, 0x60($sp)
ld      $sp, 0xE8($sp)
sync
eret
```

```
MEMORY:605614BC  # ---------------------------------------------------------
MEMORY:605614BC sw      $at, dword_623733D4
MEMORY:605614C0 ld      $k0, 0xD0($sp)
MEMORY:605614C4 ld      $at, 8($sp)
MEMORY:605614C8 ld      $t4, 0x60($sp)
MEMORY:605614CC ld      $sp, 0xE8($sp)
MEMORY:605614D0 sync
MEMORY:605614D4 jr      $gp
MEMORY:605614D8 nop
MEMORY:605614D8  # ---------------------------------------------------------
```



Adventures In Embedded Exploitation

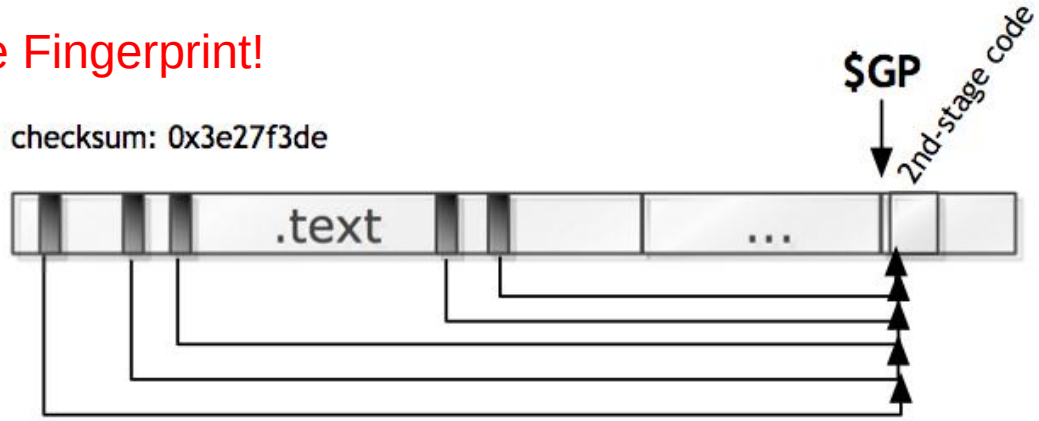
Version Agnostic Cisco IOS Malware

Stage 2 shellcode calculates fingerprint

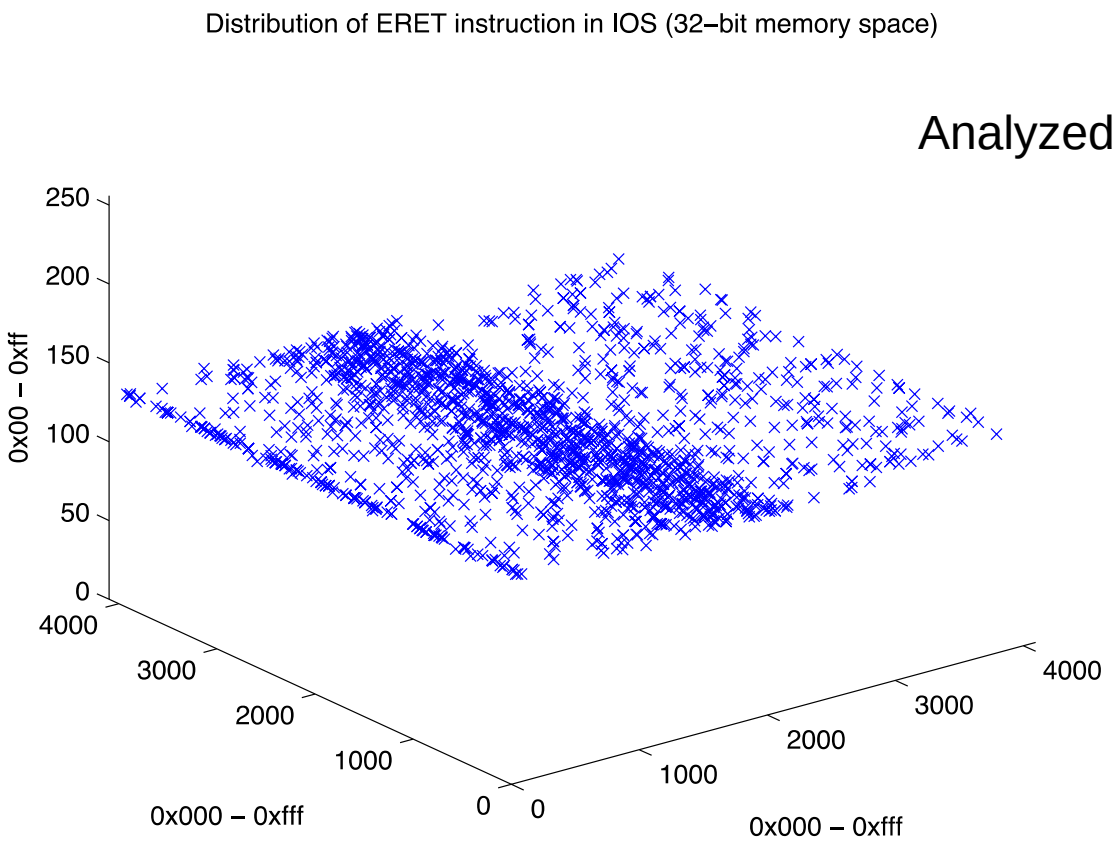
```
.text:805614BC  sw      $at, 0x623733D4
.text:805614C0  ld      $k0, 0xD0($sp)
.text:805614C4  ld      $at, 8($sp)
.text:805614C8  ld      $t4, 0x60($sp)
.text:805614CC  ld      $sp, 0xE8($sp)
.text:805614D0  sync
.text:805614D4  eret
```

```
MEMORY:605614BC  # ---------------------------------------------------------
MEMORY:605614BC sw      $at, dword_623733D4
MEMORY:605614C0 ld      $k0, 0xD0($sp)
MEMORY:605614C4 ld      $at, 8($sp)
MEMORY:605614C8 ld      $t4, 0x60($sp)
MEMORY:605614CC ld      $sp, 0xE8($sp)
MEMORY:605614D0 sync
MEMORY:605614D4 jr      $gp
MEMORY:605614D8 nop
MEMORY:605614D8  # ---------------------------------------------------------
```

Unique Fingerprint!



Stage 2 shellcode calculates fingerprint



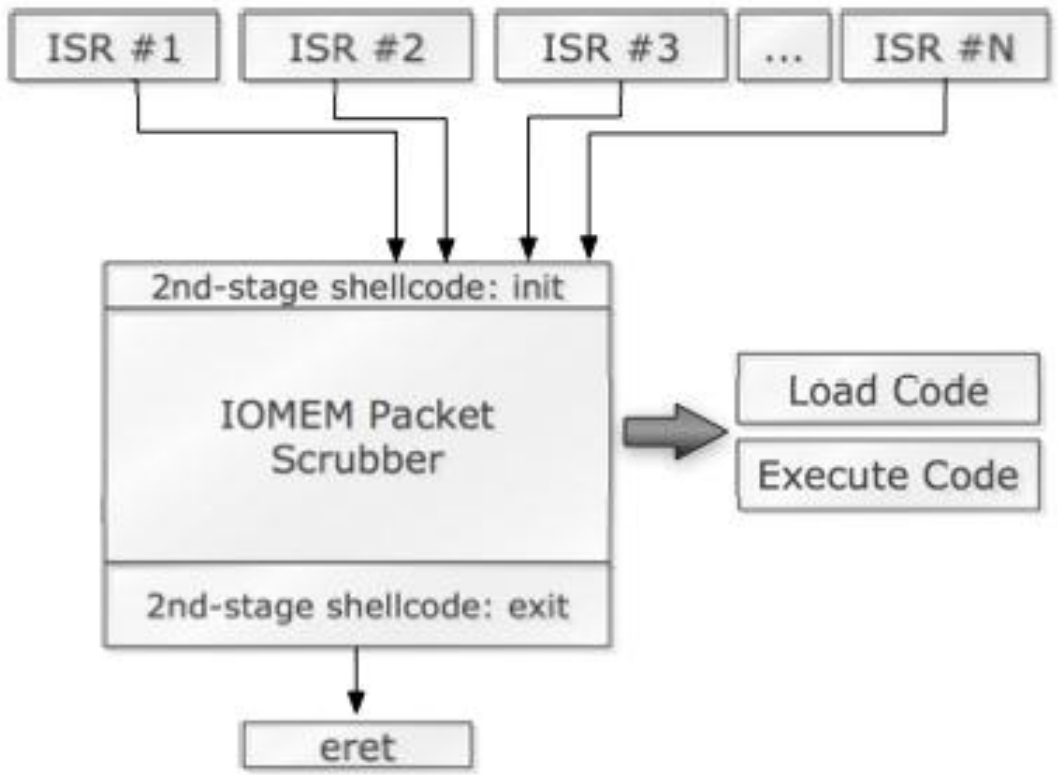
Analyzed Large IOS Firmware Set

ERET-Hash: Good Enough
for IOS Fingerprinting

Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Unpacked shellcode, ready for action



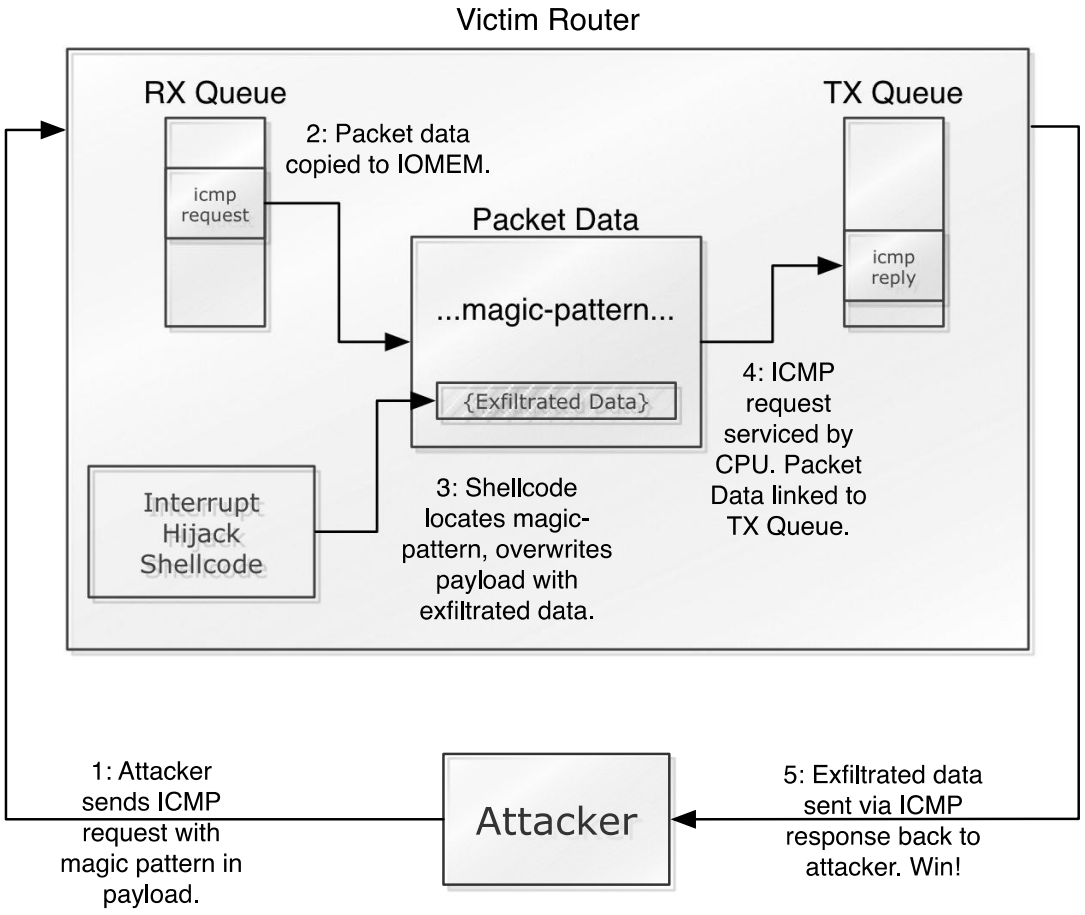
Command and Control Over Processor switched Packets.

Any packet punted to CPU can be used

We use ICMP in the demo

Can you think of another packet type?

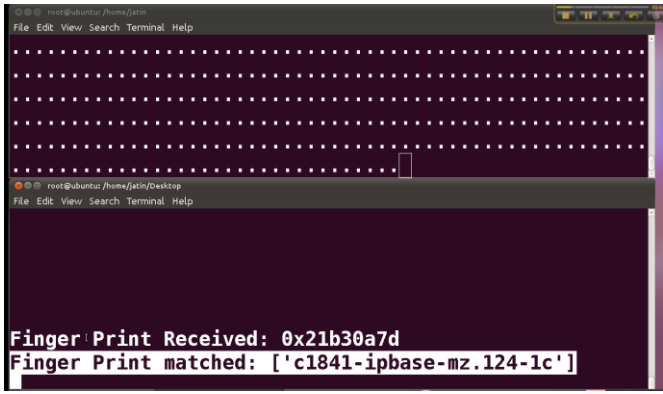
Fingerprint Exfiltration via ICMP



Adventures In Embedded Exploitation

Version Agnostic Cisco IOS Malware

Demo Videos are online:
http://www.hacktory.cs.columbia.edu



- Fingerprinting Cisco 1841
- Authentication Bypass
- Arbitrary Memory modification
- EEPROM Overwrite

Full Paper:

Killing the Myth of Cisco IOS Diversity: Towards Reliable Large-Scale Exploitation of Cisco IOS.

[USENIX WOOT 11]

Let's Talk

Adventures In Embedded Exploitation

HP LaserJet Printer Exploitation

HP-RFU Vulnerability

- Arbitrary Firmware Modification via PJL

Adventures In Embedded Exploitation

HP LaserJet Printer Exploitation

HP-RFU Vulnerability

- Arbitrary Firmware Modification via PJL
- Firmware update in a resume!

Adventures In Embedded Exploitation

HP LaserJet Printer Exploitation

HP-RFU Vulnerability

- Arbitrary Firmware Modification via PJL
- Firmware update in a resume!

- Print2Pwn

Adventures In Embedded Exploitation

HP LaserJet Printer Exploitation

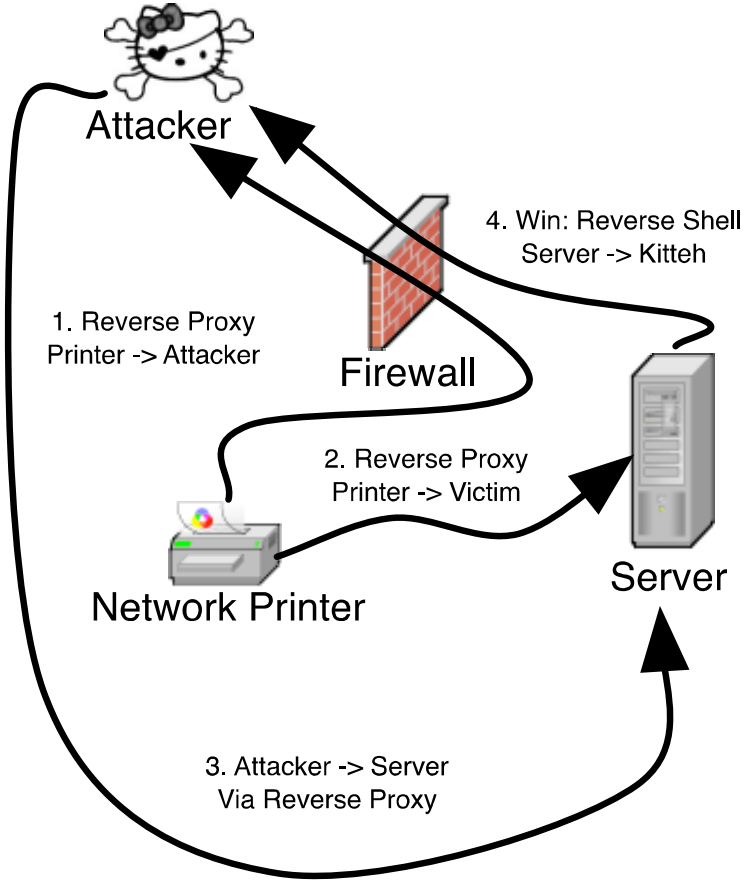
HP LaserJet Enterprise 500 color M551
HP LaserJet Enterprise 600 M601
HP LaserJet Enterprise 600 M602
HP LaserJet Enterprise 600 M603
HP Color LaserJet CM1312 Multifunction
HP LaserJet Pro CM1415 Color Multifunction
HP Color LaserJet CP1510
HP LaserJet M1522 Multifunction Printer
HP LaserJet Pro CP1525 Color Printer
HP LaserJet Pro M1536 Multifunction Printer
HP Color LaserJet CP2025
HP LaserJet P2035
HP LaserJet P2055
HP Color LaserJet CM2320 Multifunction
HP LaserJet M2727 Multifunction Printer
HP Color LaserJet 3000
HP LaserJet P3005
HP LaserJet Enterprise P3015
HP Color LaserJet CP6015
HP LaserJet P4014
HP LaserJet P4015
HP LaserJet 4240
HP LaserJet 4250
HP LaserJet 4345 Multifunction Printer
HP LaserJet 4350
HP LaserJet P4515
HP Color LaserJet Enterprise CP4520
HP Color LaserJet Enterprise CP4525
HP Color LaserJet Enterprise CM4540
HP LaserJet Enterprise M4555 Multifunction
HP Color LaserJet 4700
HP Color LaserJet 4730 Multifunction Printer
HP Color LaserJet CM4730 Multifunction
HP LaserJet M5025 Multifunction Printer
HP LaserJet M5035
HP LaserJet 5200n
HP Color LaserJet Professional CP5225
HP Color LaserJet CM6030
HP LaserJet M9040 Multifunction Printer
HP LaserJet 9050
HP LaserJet M9050 Multifunction Printer
HP 9200c Digital Sender
HP 9250c Digital Sender
HP Color LaserJet 9500
HP Color LaserJet CM3530
HP Color LaserJet 3800
HP Color LaserJet CP4005
HP Color LaserJet CM6040
HP CM8060 Color Multifunction Printer
HP LaserJet 9040
HP LaserJet M3027 Multifunction Printer
HP LaserJet M3035
HP Color LaserJet CP3505
HP Color LaserJet CP3525
HP Color LaserJet CP5525
HP Color LaserJet 5550

CVE: CVE-2011-4161

SSRT: 100692 rev.5

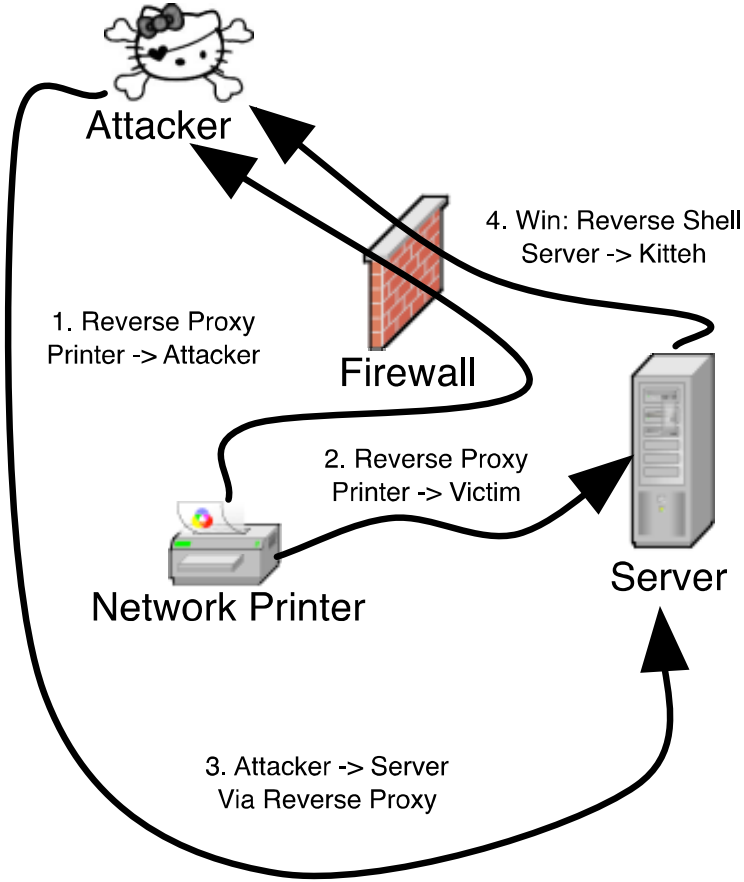
Adventures In Embedded Exploitation

HP LaserJet Printer Exploitation



Adventures In Embedded Exploitation

HP LaserJet Printer Exploitation



Watch the demo: Ang Cui 28c3 YouTube

Poly-species

Malware Propagation

Adventures In Embedded Exploitation

Poly-Species Malware Propagation

Remember this?

Adventures In Embedded Exploitation

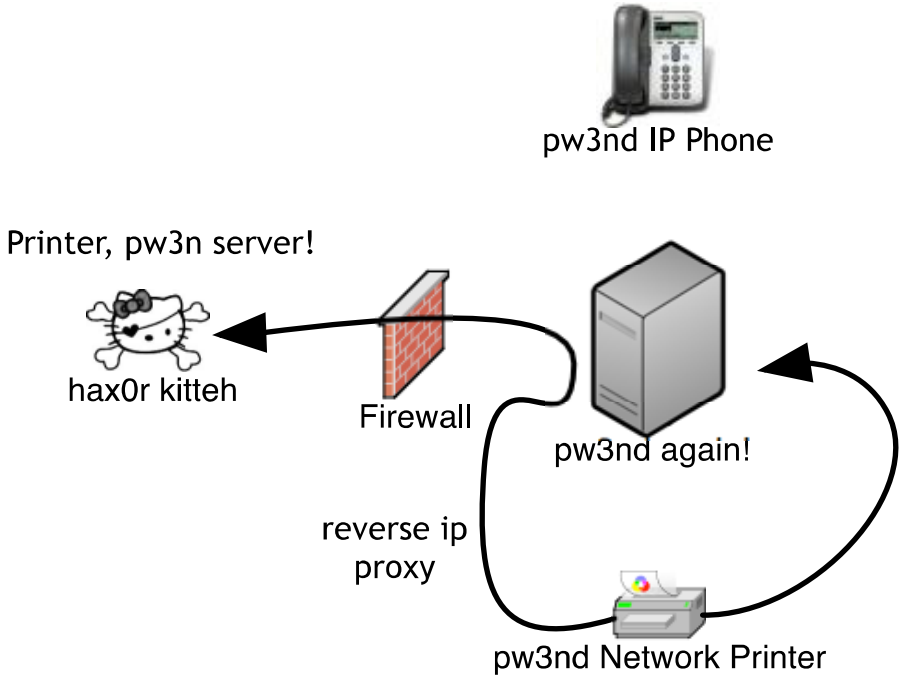
Poly-Species Malware Propagation

Where is Kaspersky for Phone?

Cisco 7912G

Poly-Species Malware Propagation Is Coming

Are you ready?



Adventures In Embedded Exploitation

Hello Delft University!


```
mysql> SELECT ip,dnsname  FROM `ip_info` WHERE `asname` LIKE '%tudelft%';
+-----------------+--------------------------+
| ip              | dnsname                  |
+-----------------+--------------------------+
| 130.161.167.149 | aerodj3.lr.tudelft.nl    |
| 130.161.209.43  | duti6wst.twi.tudelft.nl  |
| 130.161.43.125  | duteelpspr.et.tudelft.nl |
+-----------------+--------------------------+
3 rows in set (0.11 sec)

mysql>
```

I am here in spirit =)

```
h1m0m3-2:~ angcui$ telnet 130.161.167.149
Trying 130.161.167.149...
Connected to aerodj3.lr.tudelft.nl.
Escape character is '^]'.
HP JetDirect
Password is not set

Please type "menu" for the MENU system,
or "?" for help, or "/" for current settings.
> oh gorsh! -)
```

Adventures In Embedded Exploitation

Hello Delft University!

Kaspersky® Academy
IT Security
for the Next Generation
International Student Conference

```
mysql> select organization, count(organization) as occurance from ip_info
    -> where dnsname like '%.nl%' group by organization
    -> order by occurance DESC;
+-------------------------------------------------+-----------+
| organization                                    | occurance |
+-------------------------------------------------+-----------+
| University Twente                               |       193 |
| Rijks Universiteit Groningen                    |        69 |
| Technische Universiteit Eindhoven               |        66 |
| XS4ALL Internet BV                              |        25 |
| Chello                                          |        16 |
| PLANET TECHNOLOGIES                             |        12 |
| Hogeschool van Amsterdam                        |        12 |
| Universiteit Utrecht                            |         9 |
| Demon NL                                        |         5 |
| Solcon Internetdiensten B.V.                    |         5 |
| UCI - Radboud University Nijmegen               |         5 |
| Essent Kabelcom B.V. B.V.                       |         5 |
| Universiteit van Amsterdam                      |         4 |
| Delft University of Technology Network (Main netwo |         3 |
| Euronet Internet BV                             |         3 |
```


KASPERSKY lab

Adventures In Embedded Exploitation

Hello Delft University!

Potentially vulnerable printers	90,847
Printers with identifiable firmware datecode	74,770
Number of patched printers	808
Overall patch rate	1.08%

Table 1: Observed population of printers vulnerable to the HP-RFU attack on IPv4.

Adventures In Embedded Exploitation

Hello Delft University!

Potentially vulnerable printers	90,847
Printers with identifiable firmware datecode	74,770
Number of patched printers	808
Overall patch rate	1.08%

Table 1: Observed population of printers vulnerable to the HP-RFU attack on IPv4.

We also identified the following populations of vulnerable printers within several notable organizations:

- United States Department of Defense: *201 printers*
- Hewlett-Packard: *6 printers*

Adventures In Embedded Exploitation

Hello Delft University!

Vulnerable Embedded Devices are Everywhere

	Count	Avg Age (years)	Oldest Firmware
N. America	47,840	4.46	1992-12-16
Europe	14,196	4.16	1993-08-20
Asia	10,353	3.77	1998-09-02
Oceania	1,081	4.79	1998-09-02
S. America	673	3.43	1999-01-27
Africa	60	4.56	2001-04-26

Table 3: Geographical distribution of vulnerable printers.

	Count	Avg Age (years)	Oldest Firmware
Education	48,626	4.13	1993-08-20
ISP	4,650	3.70	1994-10-12
Enterprise	2,842	4.02	1992-12-16
Military	201	4.63	1999-10-30
Government	126	4.33	1996-12-20

Table 4: Organizational distribution of vulnerable printers.

Adventures In Embedded Exploitation

Hello Delft University!

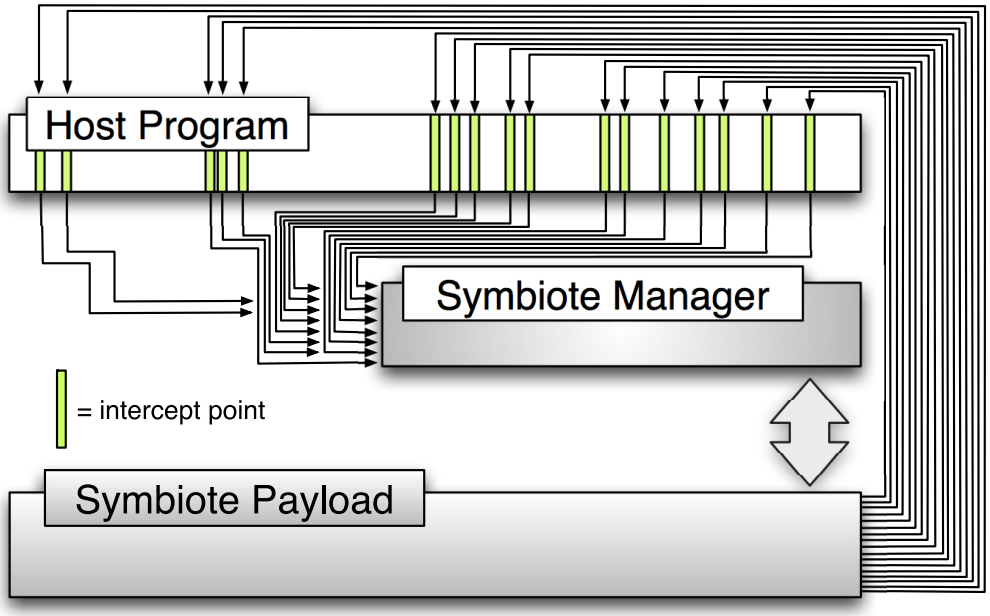
Symbiotic Embedded machines

- Dynamic Attestation

- Time-multiplexed embedded host-based defense

- No hardware dependence
- No OS dependence
- More useful than static attestation
- More powerful than guards

- More resilient to attack than all previous software-only solutions



Drop in a Defensive Symbiote Payload

Thank You

Ang Cui, Columbia University

“IT Security for the Next Generation”

International Round, Delft University of Technology

11-13 May, 2012

The Netherlands

KASPERSKY lab

COLUMBIA UNIVERSITY

IN THE CITY OF NEW YORK