Back to the ‘root’ of Incident Response
Boston Park Plaza Hotel | June 22-27, 2014
A New Security Mechanism Controlling the CPU and OS
〜Back to “root” of computer structure〜

Koichi Miyashita, F.TRON
Mariko Miya, Cyber Defense Institute, Inc.
Who am I?

- Cyber Defense Institute, Inc
  - Security Services
    - Penetration Tests
    - Digital Forensics
    - Malware Analysis
    - Incident Response
    - Research and Analysis
  - Cyber Threat Intelligence
  - (Ethical) Hacking Seminars
What's Actually Going On

Attacker(s)

Individual / Organization that the “Target Organization” trusts

Organization who runs (owns) a generally trusted website that the “Target Organization” may browse

Watering Hole Attack

Targeted Email Attacks

Targeted Organization

Other Organization(s)
What's Actually Going On

- Methodology
  - Inside Job
  - Spoofed/Hijacked accounts of SNS /Email
  - Wordlists (called “password lists” in Japan)
  - Zero-day vulnerability

Targeted Email Attacks

Individual / Organization that the “Target Organization” trusts
What's Actually Going On

- **Methodology**
  - Penetrate update server (modified update modules)
  - Penetrate web server (Iframe injection)
  - Zero-day vulnerability

Attacker(s)

Organization who runs (owns) a generally trusted website that the "Target Organization" may browse

Targeted Organization

Other Organization

Watering Hole Attack
What We Learned

• We’ve reached the limit to “CAPABILITY-BASED SECURITY”
  • If you are unfamiliar with this concept, visit: http://en.wikipedia.org/wiki/Capability-based_security

• Upper layers in OSI model became advanced, but lower layers have remained at the former level.
F.TRON

• Founded in 2008
• From Tokyo, Japan
• Business
  - Computer security software
  - Consulting / Training
  - Intellectual property Management
• Core Product
  INTΦ (INT ZERO)
  : An endpoint security product with a whole new new concept
Demo: Without our technology

- Heap Spray
  ⇒ Application Layer
- Domain Hack
  ⇒ Kernel Layer
Demo: Summary

- OS checking mechanism doesn’t work
- CPU environment parameters can be modified even from user applications.
- Conventional technology can’t cope with these level of attacks

OS can be hacked – so easily!
Conventional Technologies

**Limitations**
- Can’t cope with unknown attacks (Relies on pattern matching, white lists, etc.)
- Can’t protect CPU and OS environments
Introducing “INTΦ” (INT-ZERO)

Concept:

1. Protects the OS from outside
2. Takes full control of execution environment
3. Provides new intelligence to CPU instructions

INTΦ starts working first at boot process... and keeps running until shutdown... providing complete protection mechanism.
Conventional Technologies

Application Mail
Browser (Scripts)

OS
SYSCALL (SYSENTER)

Environmental Parameters
GDT
IDT
LDT
TSS
etc.

NT Kernel (Kernel API)

Application
Office Product
Mail
Browser (Script)
etc.
DLL (API)

Application Layer Monitoring
The aggregated into 400 Kernel APIs from 350,000 APIs.
Analyze 400 Kernel APIs and finally according to established a method enabled us to provide a thorough checking mechanism at application layer.

Instruction Monitor (1)
Target: OS and Application
- Prohibit writing on OS environmental parameters by outsiders
- Prohibit masquerading to access OS
- Shut off File I/O and communications based on Kernel API status
- Shut off instructions based on request originators

Instruction Monitor (2)
Target: CPU
- Prohibit writing on CPU environmental parameters (Registers) by outsiders
- Prohibit executing CPU instructions by OS masquerades
- Prohibit controlling and modifying Ring Controller

Judgment control for each CPU instructions

CPU
Register
Memory Read
Memory Write
CPU Cache
Execution (Instruction at OS side)
APIC

Device
BIOS
HDD
MBR
VT-X
Timer
NIC

Communication

26th annual FIRST conference

BOSTON
Instruction Monitor (1)  Target: OS and Applications

- Prohibits Illegal Accesses
  - Prohibit writing on OS environment parameters by outsiders
  - Prohibit masquerading to access OS
  - Shut off File I/O and communications based on Kernel API status
  - Shut off instructions based on request originators
Demo: With INTΦ (INT-ZERO)
INTΦ Log – “Heap Spray”

- **How it works**
  The SWF script make new Allocated Memory, then spray shell-codes to those area.

- **How INTΦ stops it**
  Int φ check which contains the Shell-codes in the memory allocation that was repeated in the same thread.
Instruction Monitor (2)  Target: CPU

■ Prohibits Illegal Accesses

▪ Prohibit writing on CPU environmental parameters (Registers) by outsiders

▪ Prohibit executing CPU instructions by OS masquerades

▪ Prohibit controlling and modifying Ring Controller
Demo: With INTΦ (INT-ZERO)
## INTΦ Log – “Domain Hack”

| Prohibit WRMSR | 0000000000000174 | \SystemRoot\System32\Drivers\******.sys |
| Prohibit RDMSR | 00000000C0000082 | \SystemRoot\System32\Drivers\******.sys |
| Prohibit WRMSR | 0000000000000176 | \SystemRoot\System32\Drivers\******.sys |

### How it works
DNS resolution calls “Sendto”. You can overwrite buffer parameter that is passed on to Kernel API.

### How INTΦ stops it
INTΦ prohibits overwriting MSR which is used to pass parameter to Kernel API.
Conclusion

Back to the root, starting over again from internal mechanism of computer...

INTΦ gives paradigm shift to computer security by:

1. Protecting the OS from outside
2. Taking full control of execution environment
3. Providing new intelligence to CPU instructions