

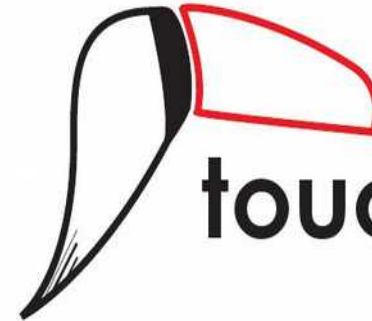
Breaking virtualization by any means



Jonathan Brossard
CEO – Toucan System

111010 - 141010 (11TH - 14TH OCTOBER)
HITBSECCONF
2010
MALAYSIA

jonathan@
toucan-system.com



toucansystem

IT serenity

Who am I ?

Security Research Engineer. Focus on low level bugs, RCE, code/binary auditing.

CEO of Toucan System (French Startup).

Previous research :

<http://www.slideshare.net/endrazine>

Getting in touch :

<http://twitter.com/endrazine>

Agenda

 **Virtualization : big picture**

 **Attack surface analysis**

 **Shared Guest OS Isolation**

 **Attacking the host**

 **Privileges escalation**

Virtualization : big picture

Market shares

Definitions

Usage

Virtualization : market shares

Source : Forrester Research 2009

78% of companies have production servers virtualized.

20% only have virtualized servers.

Virtualization : market shares

Source : Forrester Research 2009

VMWare is present in **98%** of the companies.

Microsoft virtualization products are used by **17%**.

Citrix/Xen is used by **10%**.

In a nutshell...

- As widespread as Apache or Bind
- Proprietary software, very few builds
(= reliable exploitation)
- You don't need a « remote » exploit :
you buy a shell at the same hosting
provider.

Definitions

Virtualization : Definitions

Virtualization

Virtualization is the name given to the simulation with higher level components, of lower level components.

NOTE: Virtualization of applications (as opposed to full Oses) is out of topic.

Virtualization : Definitions

Virtual Machine

A virtual machine (VM) is : "an efficient, isolated duplicate of a real machine".

-- Gerald J. Popek and Robert P. Goldberg (1974). "Formal Requirements for Virtualizable Third Generation Architectures", Communications of the ACM.

Usage

- Cost reduction (shared hosting)
- Scalability (cloud computing)
- Run broken (old) applications

Attack surface analysis

Previous research

Privilege escalation on a guest

CVE-2009-2267 « Mishandled exception on page fault in VMware » Tavis Ormandy and Julien Tinnes

Privilege escalation on the host

VMware Tools HGFS Local Privilege Escalation Vulnerability

(<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=712>)

Attacking other guests

Vmare workstation guest isolation weaknesses (clipboard transfer)

[http://www.securiteam.com/
securitynews/5GP021FKKO.html](http://www.securiteam.com/securitynews/5GP021FKKO.html)

DoS (Host + Guests)

CVE-2007-4591 CVE-2007-4593 (bad
ioctls crashing the Host+Guests)

Escape to host

Rafal Wojtczuk (Invisible things, BHUS 2008)

IDEFENSE VMware Workstation Shared Folders Directory Traversal Vulnerability (CVE-2007-1744)

Time for action

Shared Guest OS Isolation

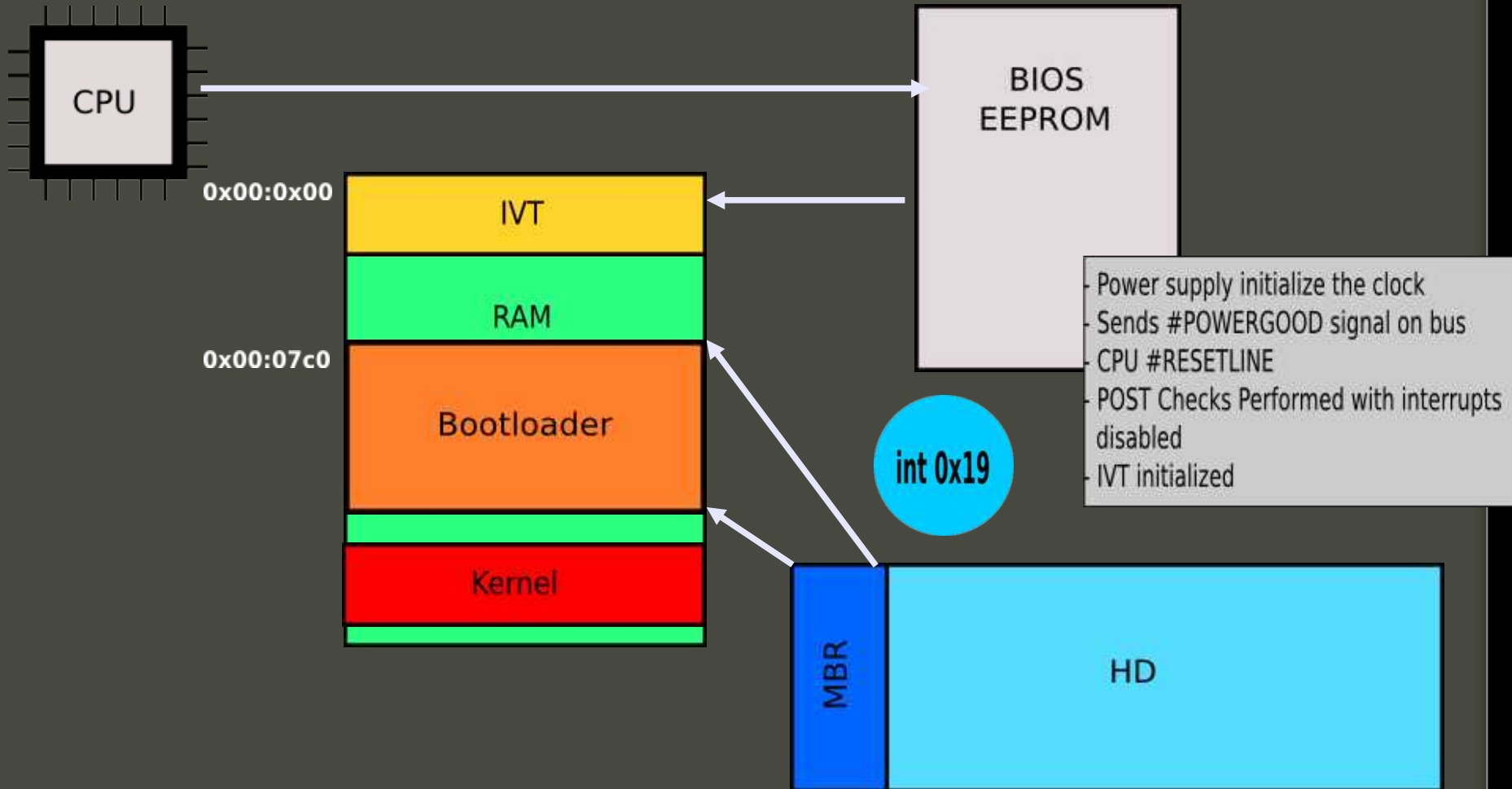
Rebooting an alternate operating system

- Overwrite the MBR directly with autonomous offensive code
- Instrument the MBR

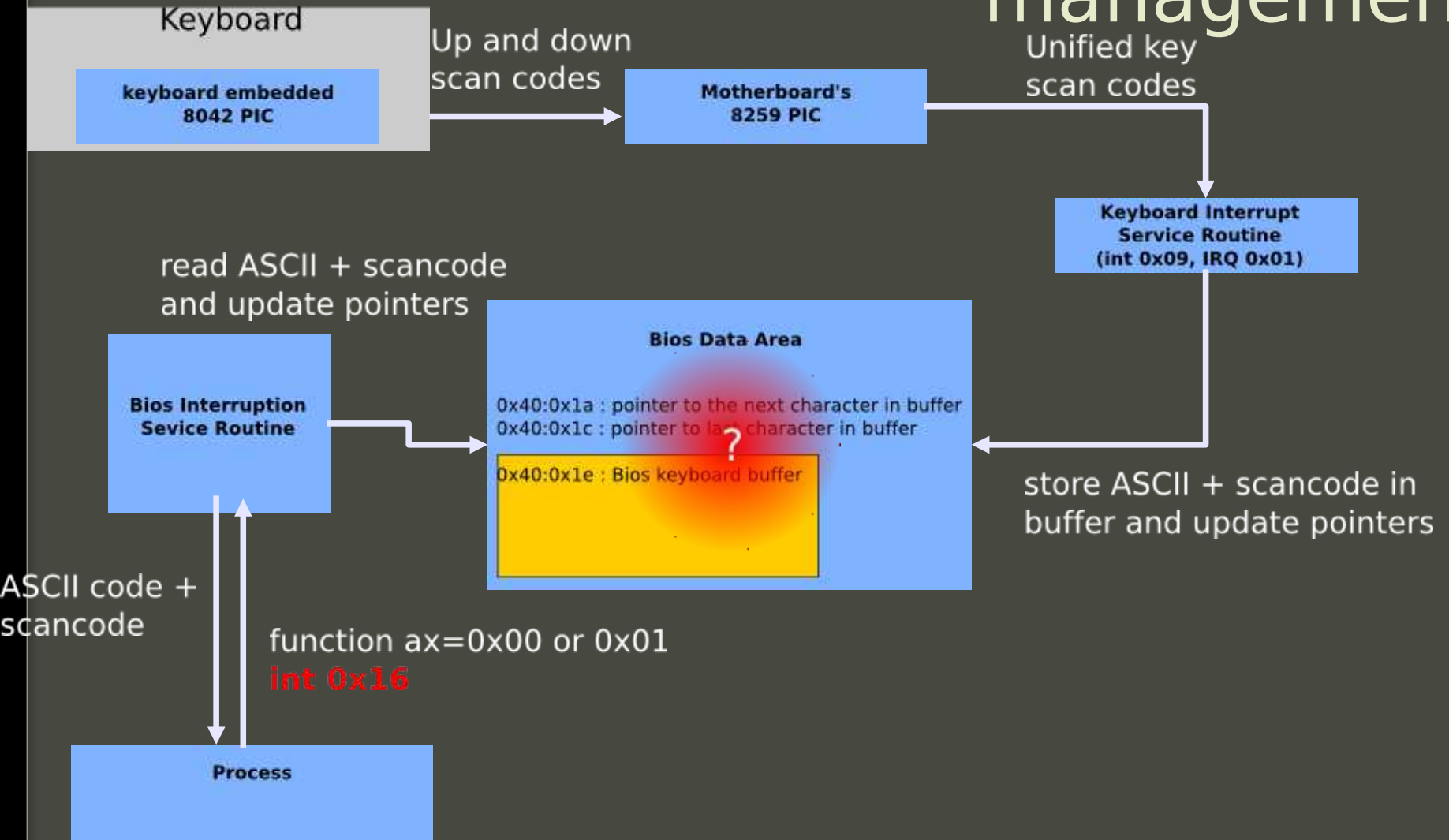
Optionally:

- Break boot passwords
- Attack disk encryption
- (Bootkiting, backdooring...)

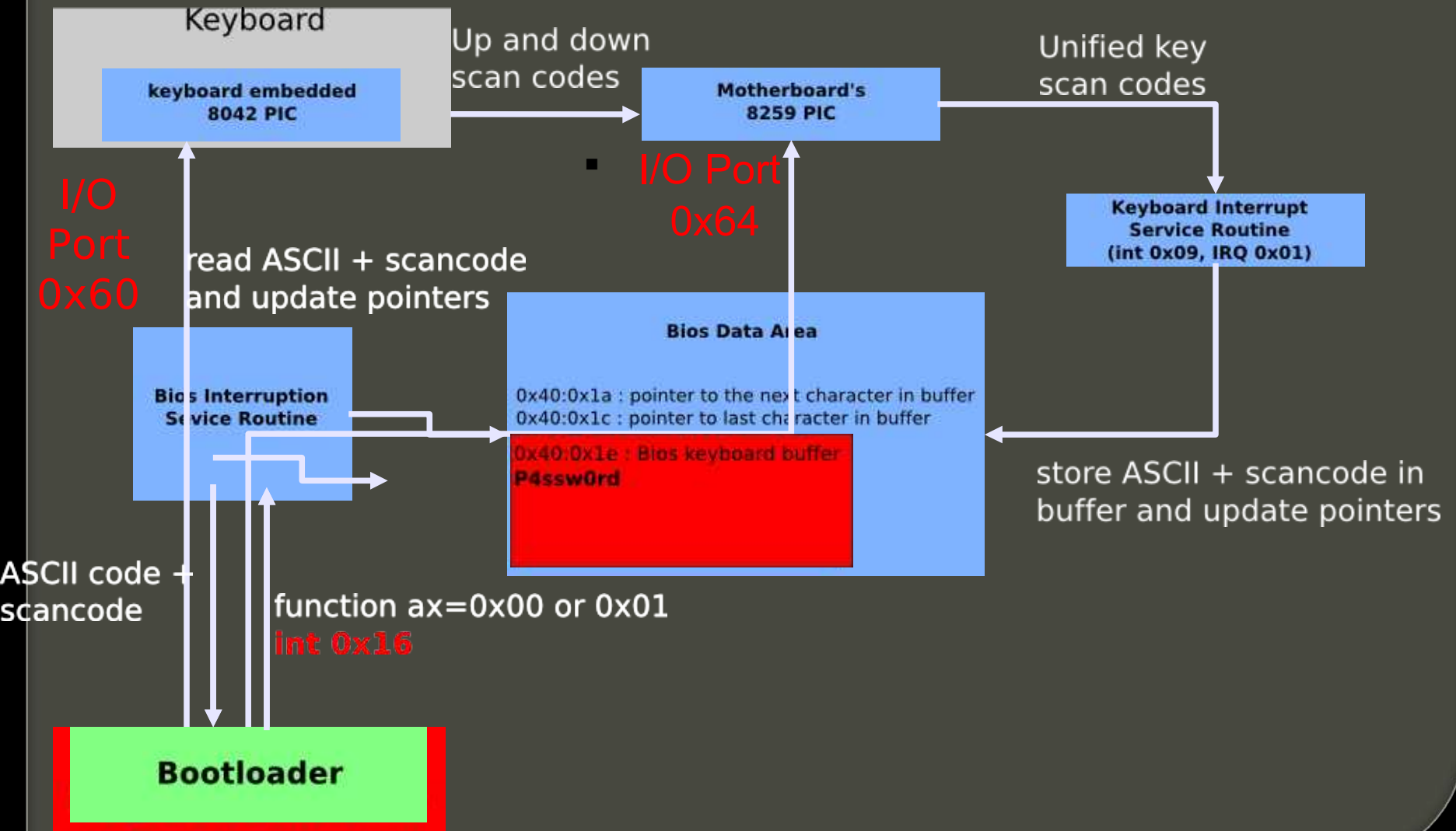
Boot sequence overview




BIOS internals for keyboard management



Bruteforcing Passwords





Attacking the hypervisor or
host OS

Attacking the hypervisor or host OS

- VM 86 fuzzing
- ioports fuzzing
- pci fuzzing

Switching to virtual 8086 mode

- Switch to VM 86 using :

```
#define __NR_vm86old    113  
#define __NR_vm86      166
```

- Use old school 16b interrupts to fuzz the hardware
- Note : It's (kernel) emulated. Good news ! We can use it with x64 too :)

example:

```
Mov ah, 0x42 ; read sector from drive
Mov ch, 0x01 ; Track
Mov cl, 0x02 ; Sector
Mov dh, 0x03 ; Head
Mov dl, 0x80 ; Drive (here first HD)
Mov bx, offset buff ; es:bx is destination

Int 0x13 ; hard disk operation
```

Vm86 fuzzing under x64

The screenshot shows the Windows Event Viewer application. The left-hand pane displays a tree view of event logs, with 'Summary page events' selected. The main pane shows a summary of one event, followed by a table of event details. The event is an error (level 'Error') from the source 'Hyper-V-VMMS' on 26/06/2010 at 22:30:00, with event ID 14070 and no task category. The event details pane is open, showing the message: 'Virtual machine 'Ubuntu-fuzzing' (ID=C079C835-0249-49DE-8A5D-1FBFA50D7D57) has quit unexpectedly.' Below the message, a list of properties is displayed, including Log Name, Source, Event ID, Level, User, OpCode, and More Information.

Level	Date and Time	Source	Event ID	Task Category
Error	26/06/2010 22:30:00	Hyper-V-VMMS	14070	None

Event 14070, Hyper-V-VMMS

Virtual machine 'Ubuntu-fuzzing' (ID=C079C835-0249-49DE-8A5D-1FBFA50D7D57) has quit unexpectedly.

Log Name: Microsoft-Windows-Hyper-V-VMMS/Admin
Source: Hyper-V-VMMS Logged: 26/06/2010 22:30:00
Event ID: 14070 Task Category: None
Level: Error Keywords:
User: SYSTEM Computer: WIN-M5M10P60MNO
OpCode: Info
More Information: [Event Log Online Help](#)

Switching to virtual 8086 mode

Limitation : Hardware unknown at BIOS
Post time can't be fuzzed this way.

=> We need complementary techniques to be exhaustive.

Other techniques

- PCI fuzzing (fuzzing hot plug devices)
- IOPorts fuzzing : interact with any hardware.

loports fuzzing:

loports:

outb, outw, outl, outsb, outsw, outsl,
inb, inw, inl, insb, insw, insl, outb_p,
outw_p, outl_p, inb_p, inw_p, inl_p

Problems: sequence, multiple ports ...

PCI Fuzzing

- In 16b mode : use int 0x1a
- In 32 or 64b mode : fork from pciutils :)



Escalating privileges on
the host

Privilege escalation

- attacking (suid) hypervisors
- attacking kernel modules with ioctls

Thank you for coming

Questions ?

