Security in the age of Virtualization

Why most of the important things haven't changed(*)

Tim Chipman

May 2011

HASK Presentation

(*But the stuff you don't know about, which has changed, might nail you)

Disclaimer

- No original / new / primary work here - this presentation is a summary of work done by others.
- Credit is given where credit is due

Who is this guy anyway?

- Independant I.T. Consultant
- Business of one; operating since 2008
- ~15 years experience
- Based in Halifax, Nova Scotia
- http://FortechITSolutions.ca
- Tim.Chipman@FortechITSolutions.ca

Topics

- Security - context
- Virtualization - concepts and key issues
- "New" Areas of Risk
- Consequences of Failure
- Known exploits / approaches of attack
- Review of 3 examples
- Managing Risk
- Questions, Comments ?

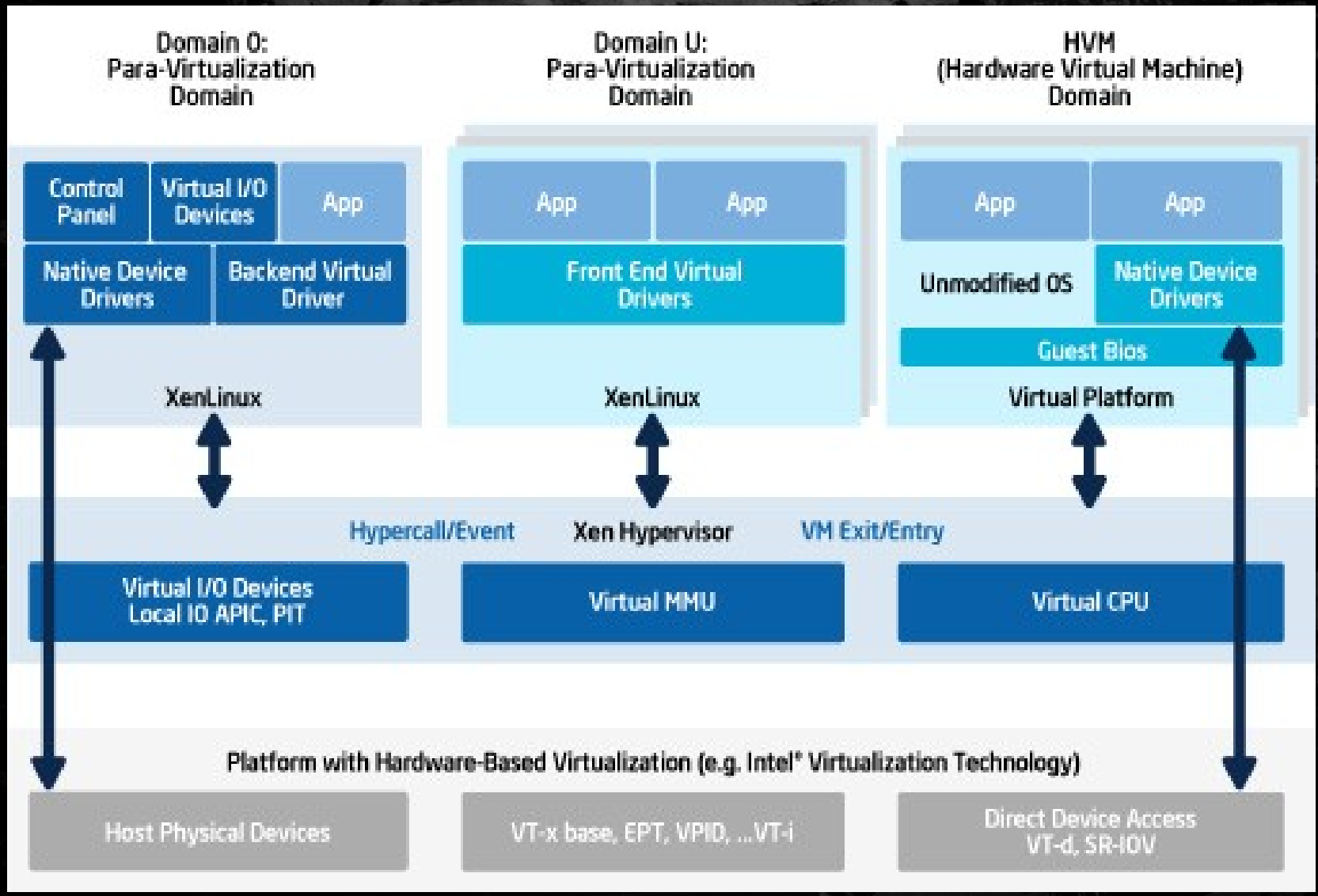
Security - Context

- Managing and understanding Risks
  - balance business needs of (users, operations, services) against the risks / exposures these create

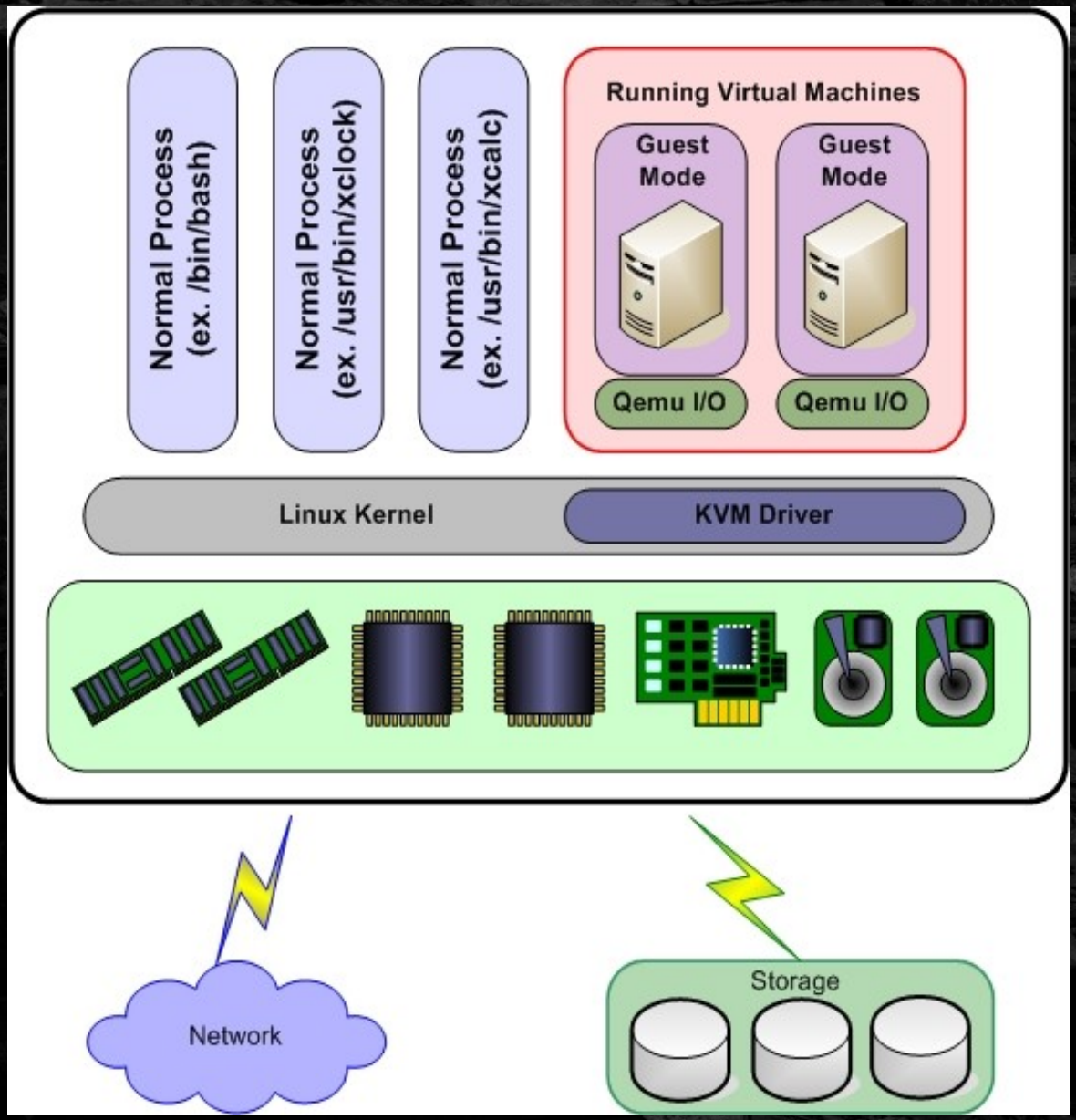
Virtualization - key concepts

- Abstraction of hardware from OS / App stack
- Permits more efficient utilization of hardware resources
- Simplifies many aspects of server management:
  - template based deployment
  - snapshots, rollback
  - development & testing
  - live migration, DR, HA

Typical Xen Stack

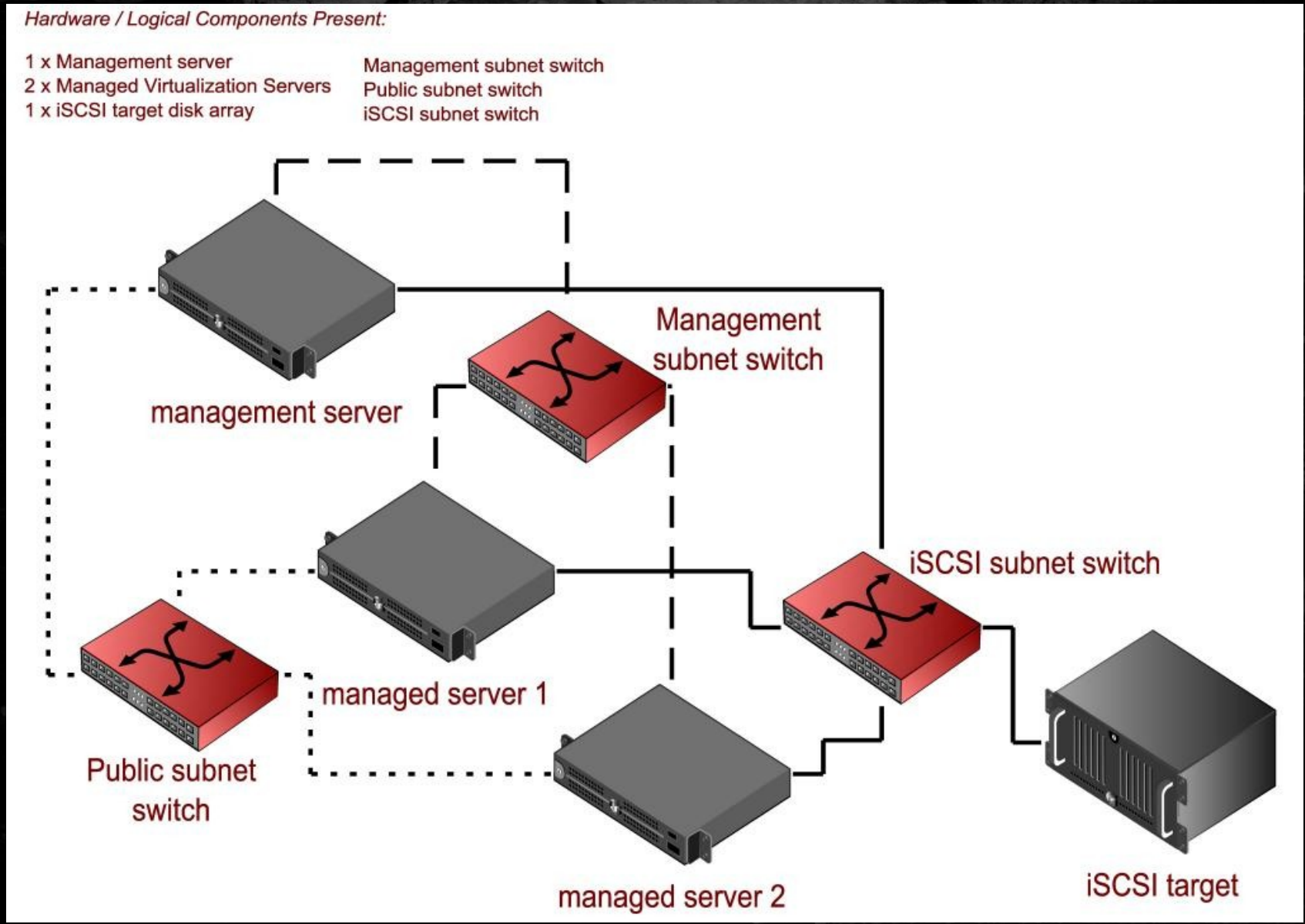


Typical KVM Stack



My hypervisor is more secure than your hypervisor!

Typical Deployment



"New" areas of risk

- Hypervisors are complex pieces of code
- lots of opportunity for bugs
- more 'attack surfaces'

"New" areas of risk

- Drivers / interface between Guest and Host
  - virtualized framebuffer (Console screen)
  - (para)virtual network drivers
  - (para)virtual IO device drivers (SCSI, SAS, Serial, USB)
  - Device passthrough (Scsi, Fibre HBA, etc)
- Trusted management network
- Trusted management server
- Live migration -> Guest memory transfer to another (trusted) VM host via(trusted) network

Consequences of failure

Print Retweet Facebook Alert

Webhost hack wipes out data for 100,000 sites

Vaserv suspects zero-day virtualization vuln

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Small Biz, 8th June 2009 20:02 GMT

A large internet service provider said data for as many as 100,000 websites was destroyed by attackers who targeted a zero-day vulnerability in a widely-used virtualization application.

Technicians at UK-based Vaserv.com were still scrambling to recover data on Monday evening UK time, more than 24 hours after unknown hackers were able to gain root access to the company's system, Rus Foster, the company's director told *The Register*. He said the attackers were able to penetrate his servers by exploiting a critical vulnerability in HyperVM, a virtualization application made by a company called LXLabs.

Known Exploits

Known Exploits-Some Examples

"Old News but Good Examples"

1. Xen Framebuffer exploit (PVFB) (2008)
2. VMWare Desktop:Shared Folder exploit (2008)
3. Xen / VMWare Live Migration exploit (2008)

In Progress:

1. Blue Pill: Nested hypervisor(2008)
- Attacking Intel Bios (2009)
- SMM memory attack via Intel CPU cache Poisoning (2009)
- SW attacks on Intel VT/D (2011)

Known Exploits

- **Xen Framebuffer exploit (PVFB)**
- Rafal Wojtczuk, Invisible Things Labs
- October 2008
- Exploit of 32-bit Paravirtualized Xen Guest
- takes advantage of frame buffer code
- full root access to Dom0

Known Exploits

- VMWare Workstation 6.02 or earlier - **Shared Folder Exploit**
- GuestVM can pass parameters to Host & gain access to filesystem (create, delete files)
- Issue: Improper validation of paths
- Default config: Shared folders turned off; only at risk if turned on
- Fix: Update or patch
- Bug ID: 1004034

Known Exploits

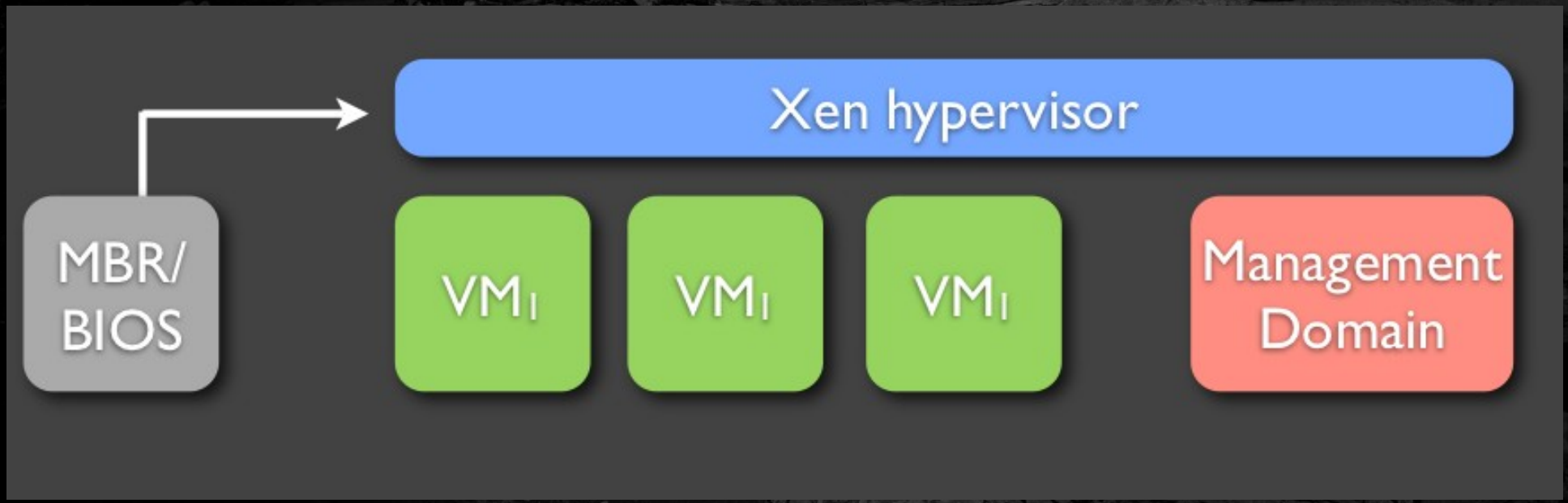
- **Live Migration exploit**
- Oberheide, Cooke, Jahanian (2008)
- XenServer 3.1.0 and VMWare ESX 3.0.1
- exploits 'trusted' management network to modify SSHD process in memory of a migrating VM
- exploit uses classic man-in-the-middle attack; requires access on a 'neighbour' VM
- outcome: grants root SSH access

Known Exploits

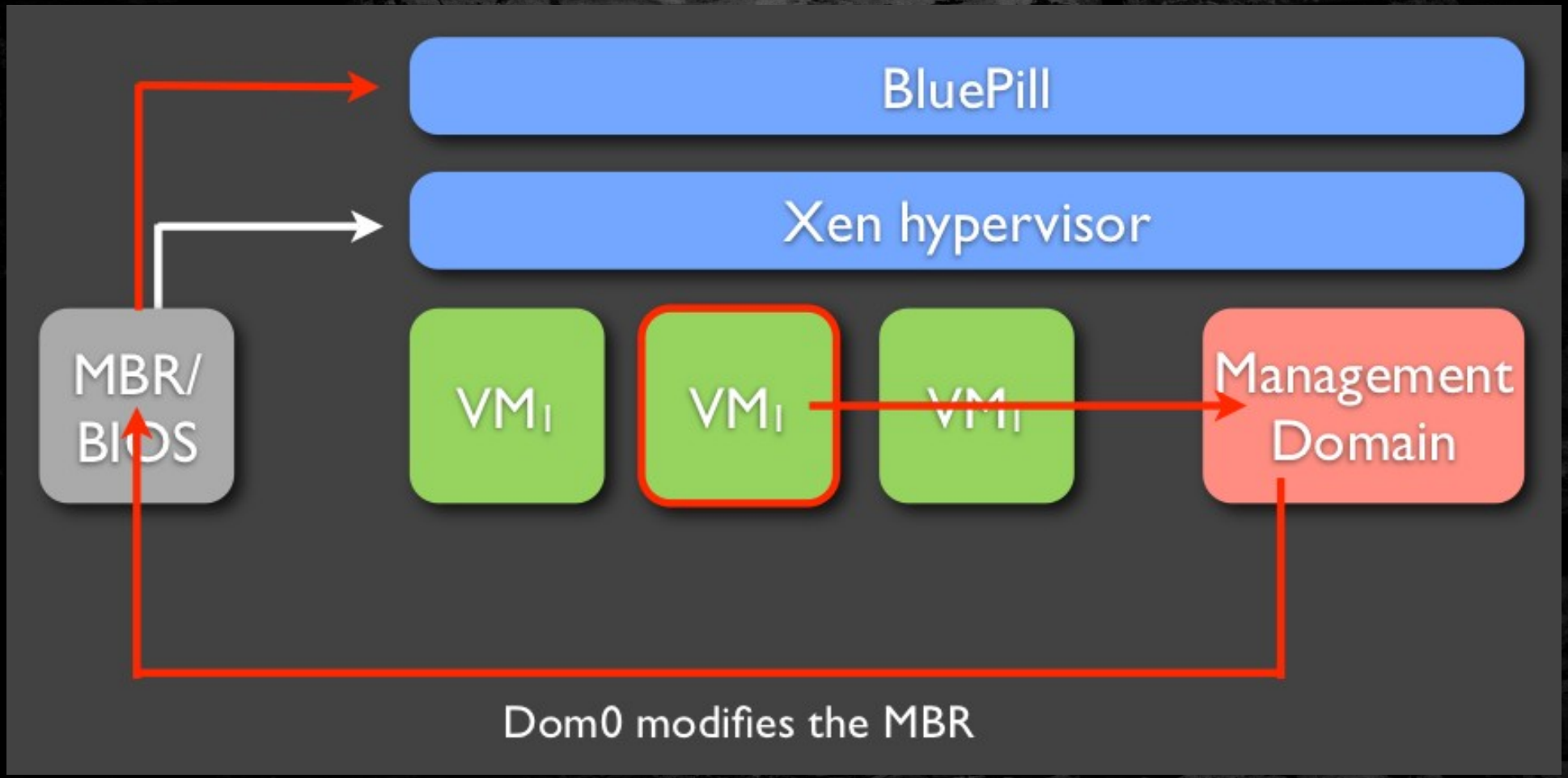
Known Exploits

- "The Blue Pill"
- "Matrix inside the Matrix" - or ...
- Hypervisor inside a hypervisor
- Live transfer, no way to detect
- (am I screwed?) never retruns "true"

Known Exploits



Known Exploits



Known Exploits

- Other examples: Intel BIOS; Intel CPU Cache exploit; Intel VT/D:
- Invisible Things Labs:
- http://www.invisiblethingslab.com/itl/Resources.html

Managing Risk

- Security remains an issue for Virtualized Environments
- Virtualization introduces new attack surfaces
- Mitigation ?
  - Design & Deploy - best practices
    - secure management network
  - Patch, patch, patch!
  - Don't forget:
    - VM Isolation != Hardware isolation

Questions, Comments ?

- Thanks for your attention

Fortech IT Solutions
http://FortechITSolutions.ca

Slides will be available at the URL,
http://Sandbox.FortechITSolutions.ca