TBD

Challenges for Digital Forensics and Incident Response on Virtualization and Cloud Computing Platforms

terremark

Introduction

Christopher Day, Chief Security Architect, Terremark

- Responsible for Terremark’s global information security services
- Very active incidence response team
- Terremark owns and operates a number of IaaS cloud computing platforms
- Robert Rounsavall is a member of my team and this talk is a follow-on to his

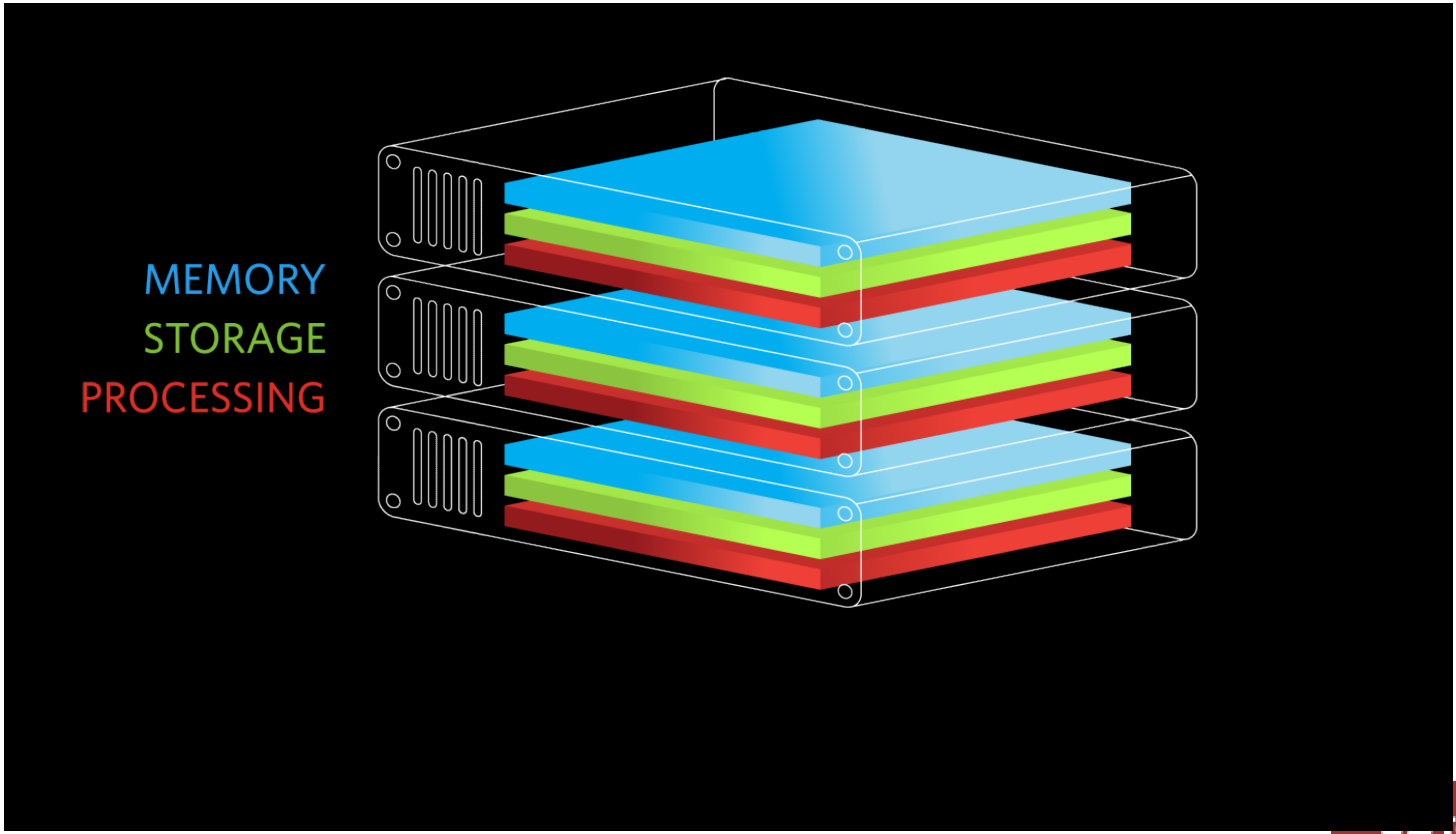
- This talk is an operator’s view

Agenda

- Introduction to Virtualization and Cloud Computing Technology
- Forensic and IR Challenges
- Hard-Won Lessons Learned and Recommendations

Introduction to Virtualization Technology

- Virtualization fundamentally decouples an operating system or virtual machine from the underlying hardware
- We go from this:

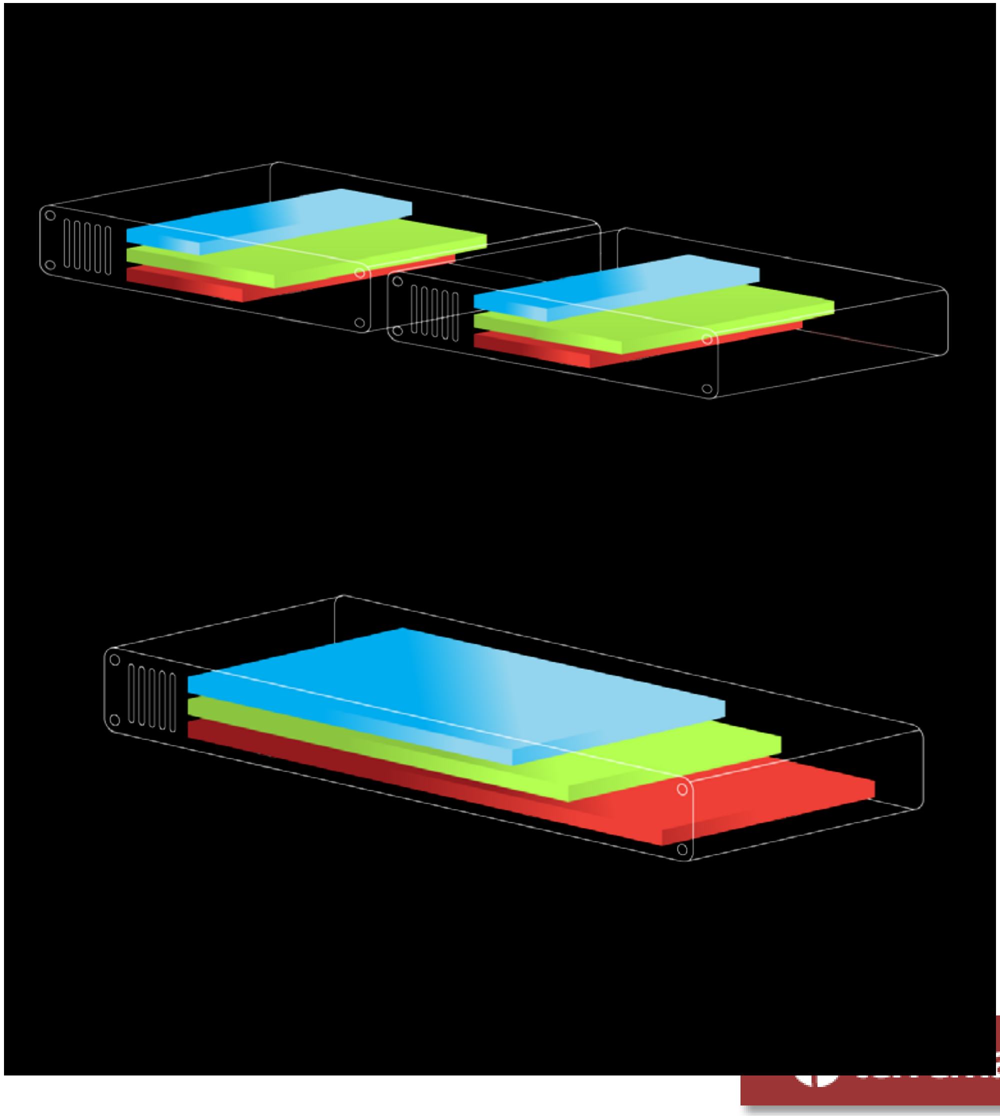


Introduction to Virtualization Technology

- To this:

Virtualized Machines/Operating Systems Running On

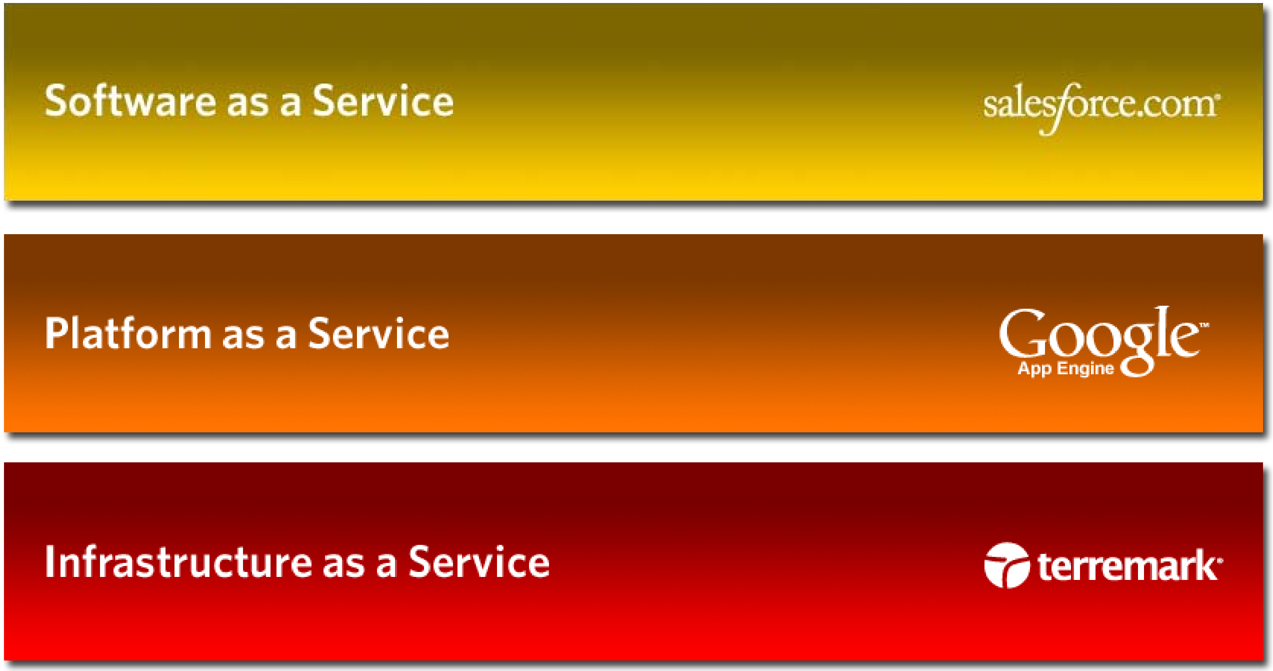
Physical Hardware Running A Hypervisor



Introduction to Cloud Computing

- Agreement on NIST’s 5 characteristics of Cloud computing:
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service
- Even this definition is still being refined

Introduction to Cloud Computing



Software as a Service

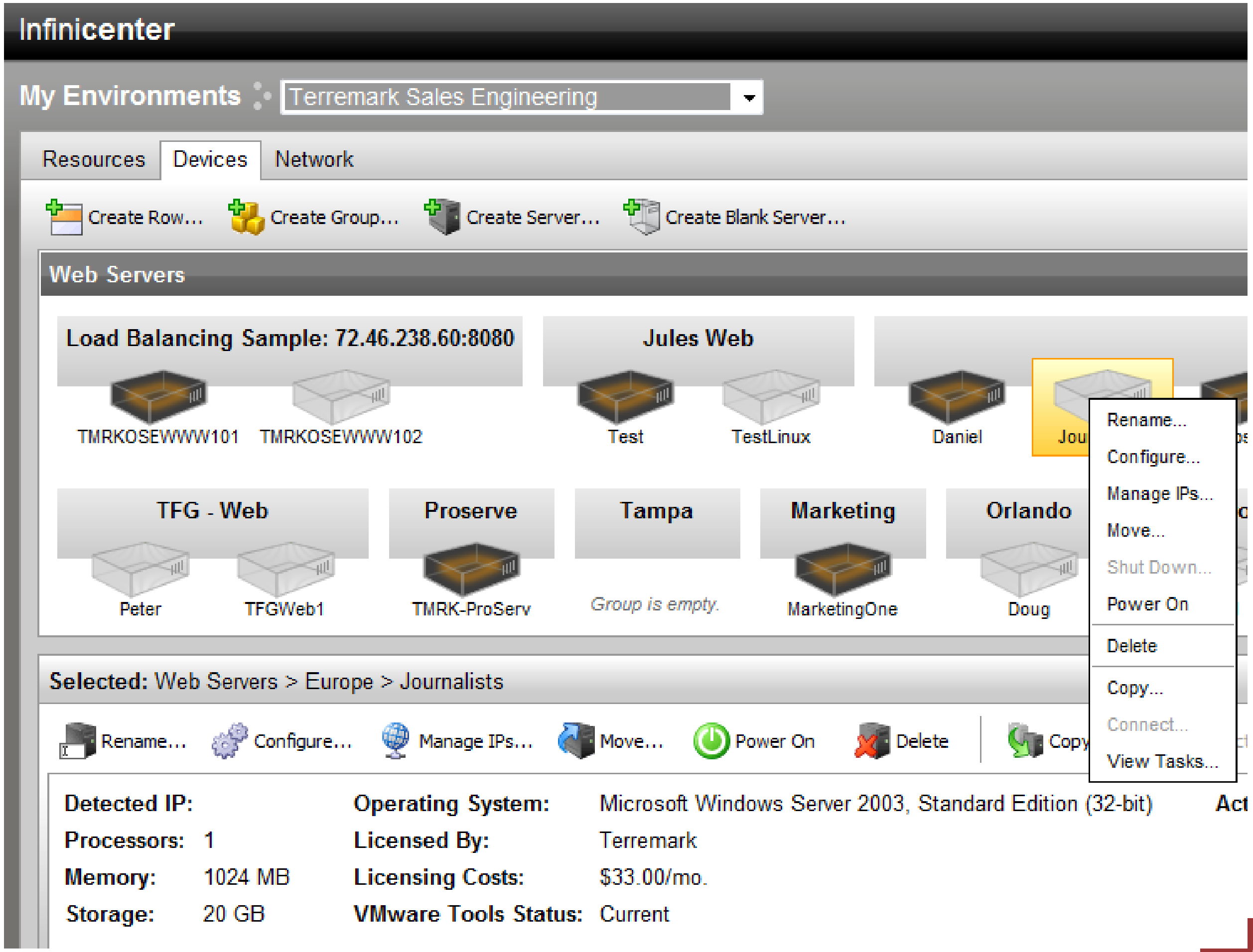
Platform as a Service

Infrastructure as a Service

- Enterprise’s may also have private Cloud infrastructures
- Higher layers are built on and include lower layers
- Clouds used to be all (SaaS) or nothing
- Today’s marketplace has more fine-grained distinctions

Introduction to Cloud Computing

- While Cloud Computing often serves as a simplifying abstraction of computing resources:



Selected: Web Servers > Europe > Journalists

Detected IP:		**Operating System:**	Microsoft Windows Server 2003, Standard Edition (32-bit)	**Act**
Processors:	1	**Licensed By:**	Terremark	
Memory:	1024 MB	**Licensing Costs:**	$33.00/mo.	
Storage:	20 GB	**VMware Tools Status:**	Current	

terremark

Introduction to Cloud Computing

- It actually hides a complicated and messy reality for the digital forensic investigator or incident responder:

Forensic and IR Challenges of Cloud/Virtualization Environments

Cloud environments present some unique challenges at a number of stages of the incident response process:

- Acquisition
- Analysis

Forensic and IR Challenges of Cloud/Virtualization Environments

For the most part, the challenges are those of scale:

- Quantities (Storage, Network, RAM, Nodes)
- Temporal
- Geographical
- Visibility (or lack thereof)

In other words, there are a lot of things you can't see well happening very quickly in many different places

Acquisition Challenges

Ephemeral Nature of VMs

- One of the defining characteristics of Cloud computing is the ability to support rapid provisioning and decommissioning of virtual machines
- This characteristics coupled with the potential mobility of VMs can create challenges for digital forensics and incident response
- Some of these challenges include:
  - Where are the actual files that comprise the VM located?
  - Forensically sound acquisition due to current limitations of tools and skill sets
  - What happens if a bad actor decommissions a VM? Does it disappear immediately from the storage systems?

Acquisition Challenges

VMs Moving Across Security or Jurisdictional Boundaries

- Many Cloud computing designs allow for VMs to be moved to different locations within the architecture.
- Depending on the specifics of this architecture and the control regime, a VM could end up in a jurisdictional or geographical location that puts it beyond legal access of the investigators
- Even when the location does not preclude access by the investigator, geographic location or distance may make acquisition much harder or even impossible

Acquisition Challenges

Others

- Virtual machine sprawl (inventory)
  - How many VMs are running /secure?
  - What about suspended machines/snapshots (persistence) ?
- Data/logging commingling (multi-tenancy)
- Physical hardware dependencies
  - Forensics licensing dongles/USB support/etc
- Platform/virtualization technology dependencies (files?/locks)
- Acquired data migration/verification

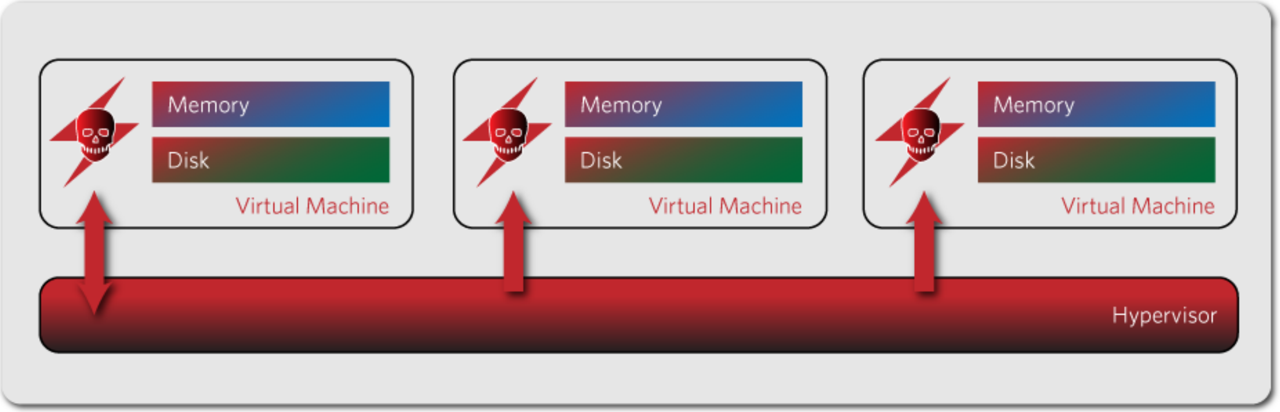
Analysis Challenges

- Volume of data
  - Determining scope of investigation
  - Storage devices, VM inventory, meta-files, snapshots, etc
  - We have had to analyze VMs utilizing 14 TB of disk, 16 GB RAM
  - Cisco UCS greatly amplifies this scale problem
- Visibility
  - Opaque infrastructure/communication channels
  - Intra-machine traffic/host physical memory/etc
- Commercial/public forensics analysis tools for virtualization/cloud systems nascent (if they exist at all)
- Proprietary data formats (minimal tool support)
  - Disk (VMFS -> OSVMFS, MOA), memory, delta-files, etc
- Increasing layers of abstraction → increasing complexity
  - Physical memory → vmem, vmsn, vswp, nvram

Analysis Challenges

Hypervisor Attacks

- An vulnerability that is exploitable from a guest virtual machine (VM) potentially puts every other VM on that hypervisor at risk
- Such a vulnerability may allow for data leakage or access across VM boundaries, arbitrary code execution on another VM, or in the worst case, arbitrary code execution or control at the hypervisor level (Immunity's CloudBurst is an example)
- Only observables in memory (exploitation/comm conduit)
- Visibility: You may not even know you have been hit!



Incident Response Opportunities

- All is not lost!
- Virtualization and Cloud computing environments offer a number of opportunities to greatly enhance incident response if leveraged properly

Incident Response Opportunities

- Forensic preparedness
  - Incident response team and infrastructure (pre-deployed)
  - Temporal proximity (nearly instant backup of an environment)
- Abstract hardware incompatibility issues
- Atomic data acquisitions/samples (snapshots)
  - Current runtime state of the suspected guest
  - Subsequent changes are isolated from the data (delta files)
- Minimize obtrusiveness (service/machine impact)
- Minimize trust placed in the suspected guest system
- Facilitate distributed/parallelized incident response efforts
- Isolated incident response environment

Terremark Cloud IR/Forensics Strategy

- Terremark has been working with various local/state/federal agencies developing forensic acquisition processes.
- ***Intrusion suppression*** philosophy: minimize impact of compromise while rapidly denying adversary further use of their attack vector
- Segmenting the Cloud
  - Cloud (virtual private, federal, commercial, vCloud express)
- Multifactor authentication
- Incident Response Virtual Environments
- Trinity of IR/Digital forensics
  - Volatile memory samples, targeted disk acquisition, full packet capture
- Sampling the runtime state of the Cloud!

terremark

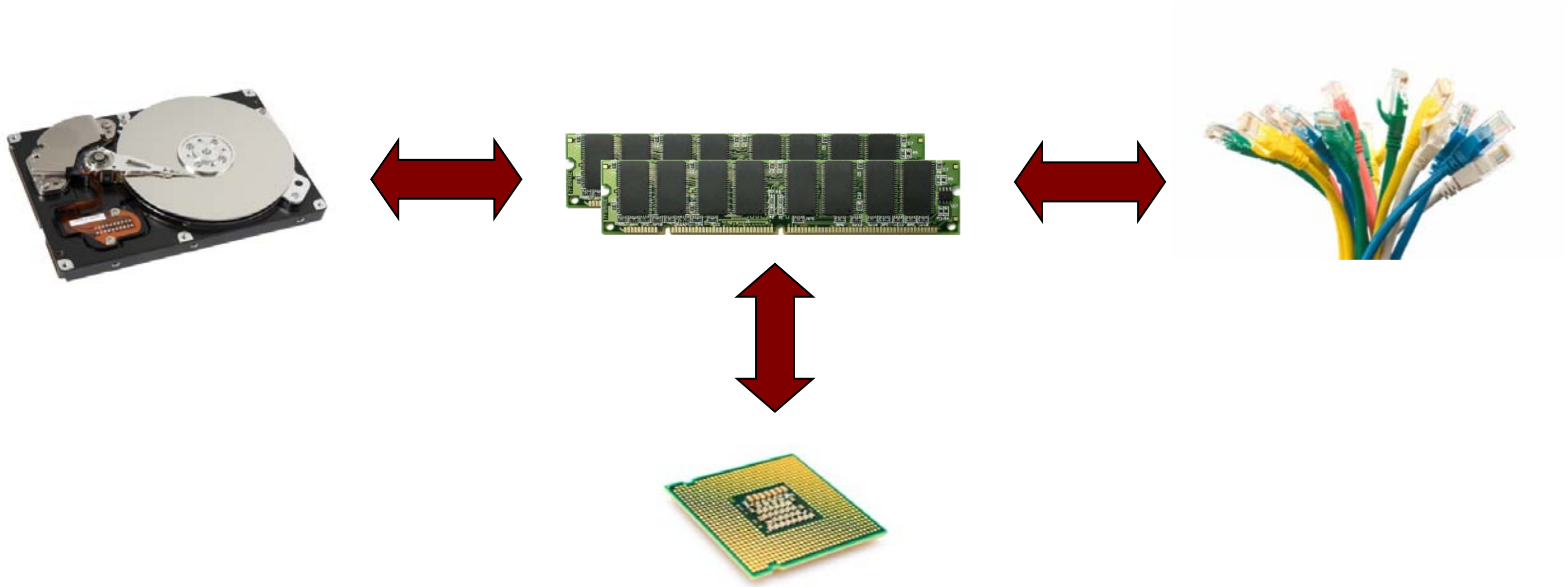
How to Deal with Scale Problems

Use the properties of the Cloud to your advantage:

- Pre-built analysis images we can rapidly deploy as needed
- Massive amount of available storage
- Move capability around as needed to adapt to incident
- Pre-instrument (network forensics, flow, IR nodes)
- Leverage Service Provider IR team (your provider has one, right?)

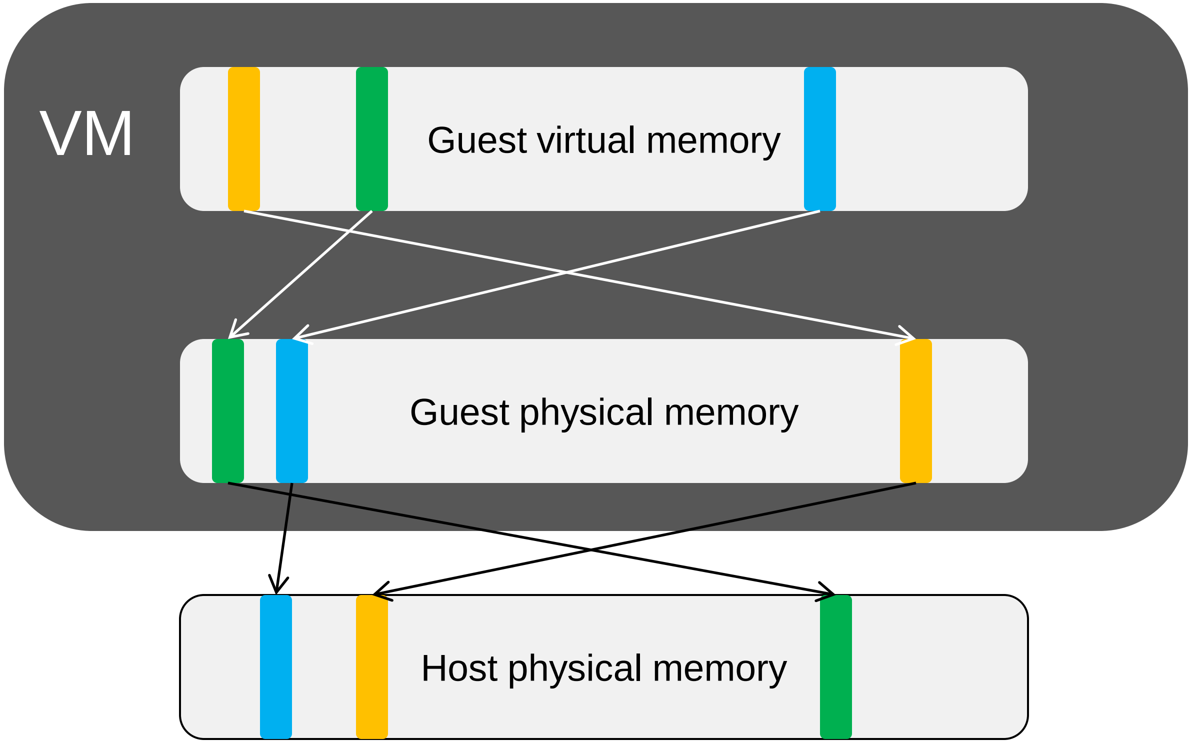
How to Deal with Scale Problems

Memory and Network Analysis Drive Targeted Disk Acquisition (suspicious binaries, Registry, local logs, etc.)



VMware ESX Memory Management

- Three virtual memory layers within ESX
  - host physical, guest physical, guest virtual
- Memory reclamation
  - Transparent page sharing, ballooning, and host swapping



Lessons Learned

Know the Platform(s)

- It is important to understand the forensically impacting subtleties of the various virtualization technologies that underlie many of the cloud computing platforms in use today .
- Even then, some of the technology is proprietary and you may need support from the service provider. This could be “interesting” if they are the target of an investigation.

Lessons Learned

Know the Platform(s)

- In some scenarios, law enforcement may be forced to seize all of a multi-tenant environment if the target's specific VMs can't be isolated and acquired forensically.
- To this end, Terremark has been working with various Federal agencies to help ensure that we jointly have developed processes for performing forensic acquisition on our VMWare-based Cloud computing platform.

Lessons Learned

Know the Platform(s)

- Acquisitions are currently performed by leveraging VMware’s snapshot capabilities which allow us to capture forensically relevant information in an atomic fashion without suspending, shutting down, or otherwise disrupting the state of the suspected system
- The other advantages with this approach are that we do not need to run foreign software on the guest, that would modify the state of the system and potentially overwrite important artifacts, and this approach also reduces the susceptibility to malware or rootkit subversion.

Lessons Learned

Know the Platform(s)

- The VMware snapshot will preserve the state (disk, memory, etc) at a particular point in time. Any further changes to the state of the system after the snapshot are subsequently isolated from the data preserved within the snapshot.
- The memory files are in a proprietary format must be converted to be analyzed with available tools
- There are differences between ESX and ESXi with regards to file locking

Lessons Learned

Process, Techniques, and Technology in Place for IR

- Create a step-by-step process for performing the necessary forensic acquisitions on your target virtualization/Cloud platform (memory, disk, network)
- Perform an actual acquisition test to ensure this process is complete and realistic
- Ensure that the location of the constituent files for a given VM can be quickly and easily located (which hypervisor node, which storage array, and so on) by the Cloud management system

Lessons Learned

Process, Techniques, and Technology in Place for IR

- Understand the limitations imposed by the Cloud environment on acquisition (USB support, bandwidth concerns for image acquisition, and so on)
- Understand what happens to a VM when it is decommissioned. How long do you have to perform acquisition on a decommissioned VM? Is it possible to delay the wiping of the VM files to ensure there is no retention requirement?

Conclusions

- Virtualization and Cloud computing platforms are becoming increasingly ubiquitous and represent a fairly significant shift in how computing is being performed.
- Digital forensic investigators and incident responders will need to have the necessary tools and processes in place to successfully acquire and process evidence from these platforms
- Investigators must be aware of the capabilities of these platforms as well as some of the unique features that will impact forensic acquisition
- There is much research that needs to be done in this space as well as a future tools to be developed to facilitate acquisition and analysis of digital evidence on these platforms