Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing

By

Josiah Dykstra and Alan Sherman

Presented At

The Digital Forensic Research Conference

DFRWS 2012 USA Washington, DC (Aug 6th - 8th)

Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing

Exploring and Evaluating Tools, Trust, and Techniques

Josiah Dykstra and Alan T. Sherman

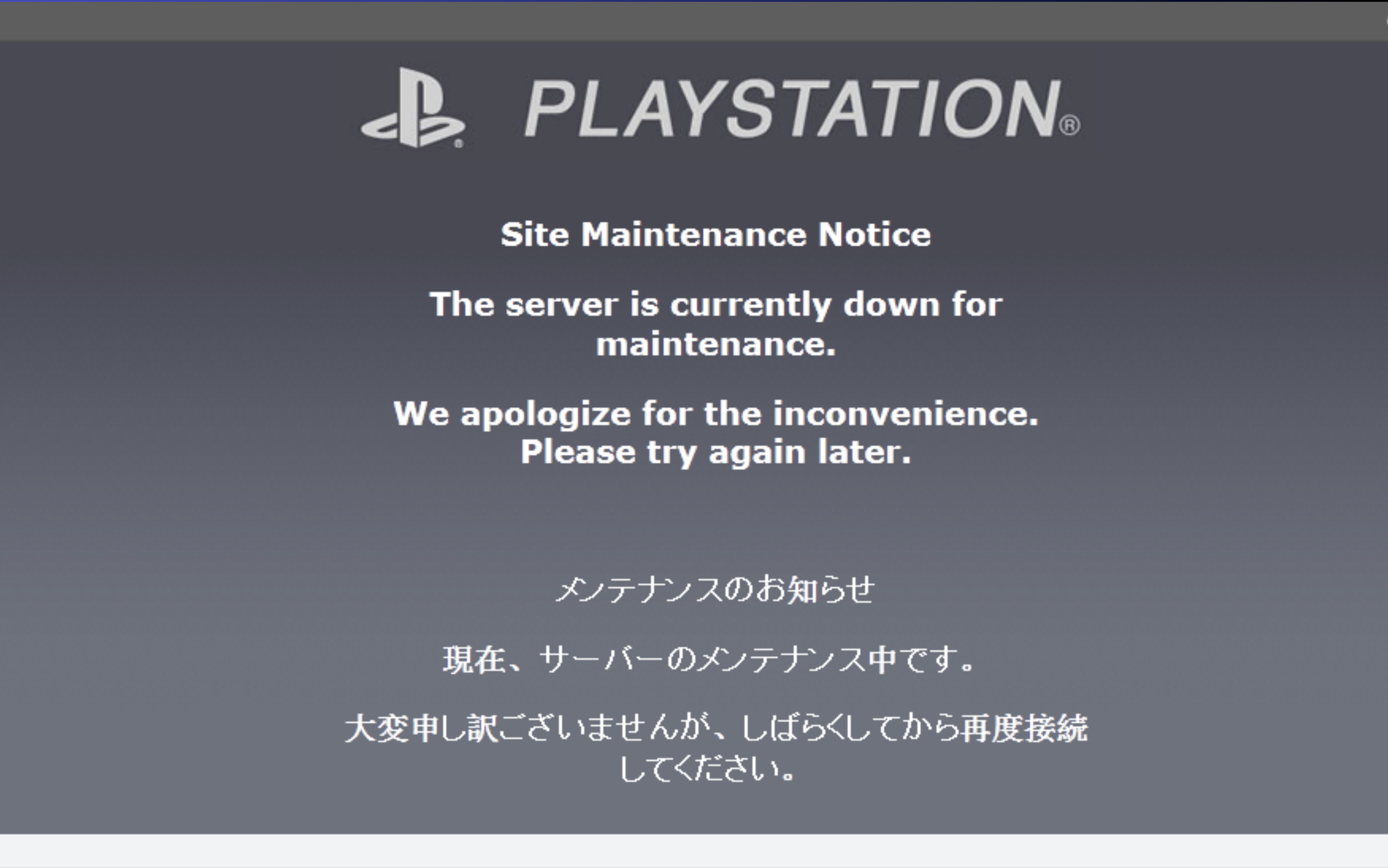
August 7, 2012

The views expressed in this presentation are mine alone. Reference to any specific products, process, or service do not necessarily constitute or imply endorsement, recommendation, or favoring by the United States Government or the Department of Defense.

Outline

Today	What's the problem?
Trust	Can you believe the data?
Tests	Experiments in forensic acquisition
Trouble	Results and alternatives
Tomorrow	Future work

Today: What's the problem?



Site Maintenance Notice

The server is currently down for maintenance.

We apologize for the inconvenience. Please try again later.

メンテナンスのお知らせ

現在、サーバーのメンテナンス中です。

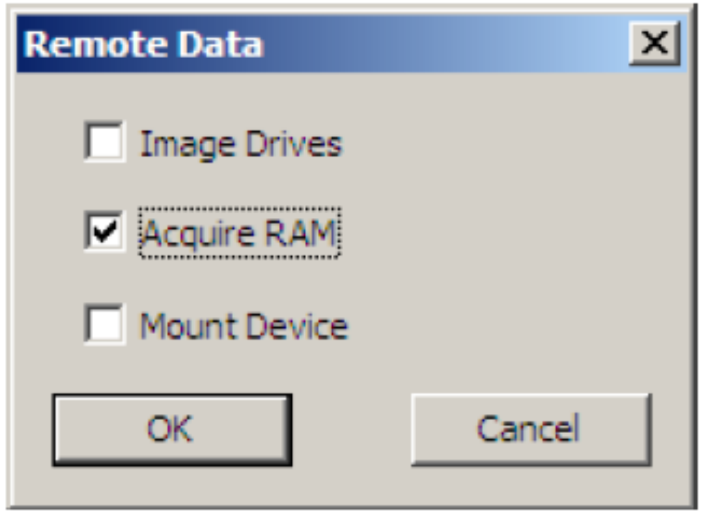
大変申し訳ございませんが、しばらくしてから再度接続してください。

Investigating Crimes in the Cloud

Acquiring Remote Data

STATE OF CALIFORNIA - COUNTY OF LOS ANGELES

RETURN TO SEARCH WARRANT

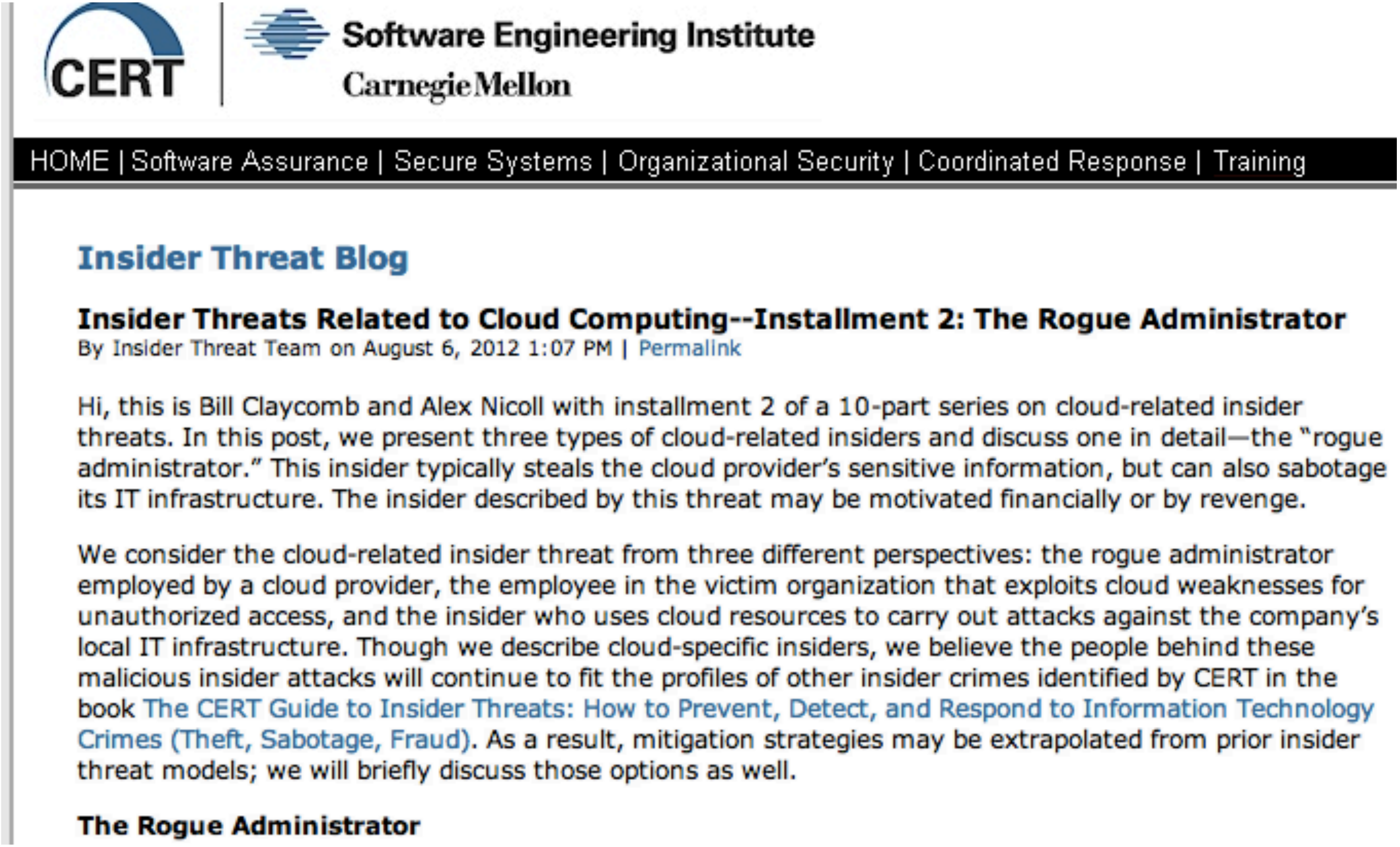


Remote Data

☐ Image Drives

☑ Acquire RAM

☐ Mount Device


CERT
Software Engineering Institute
Carnegie Mellon
HOME | Software Assurance | Secure Systems | Organizational Security | Coordinated Response | Training

Insider Threat Blog

Insider Threats Related to Cloud Computing--Installment 2: The Rogue Administrator

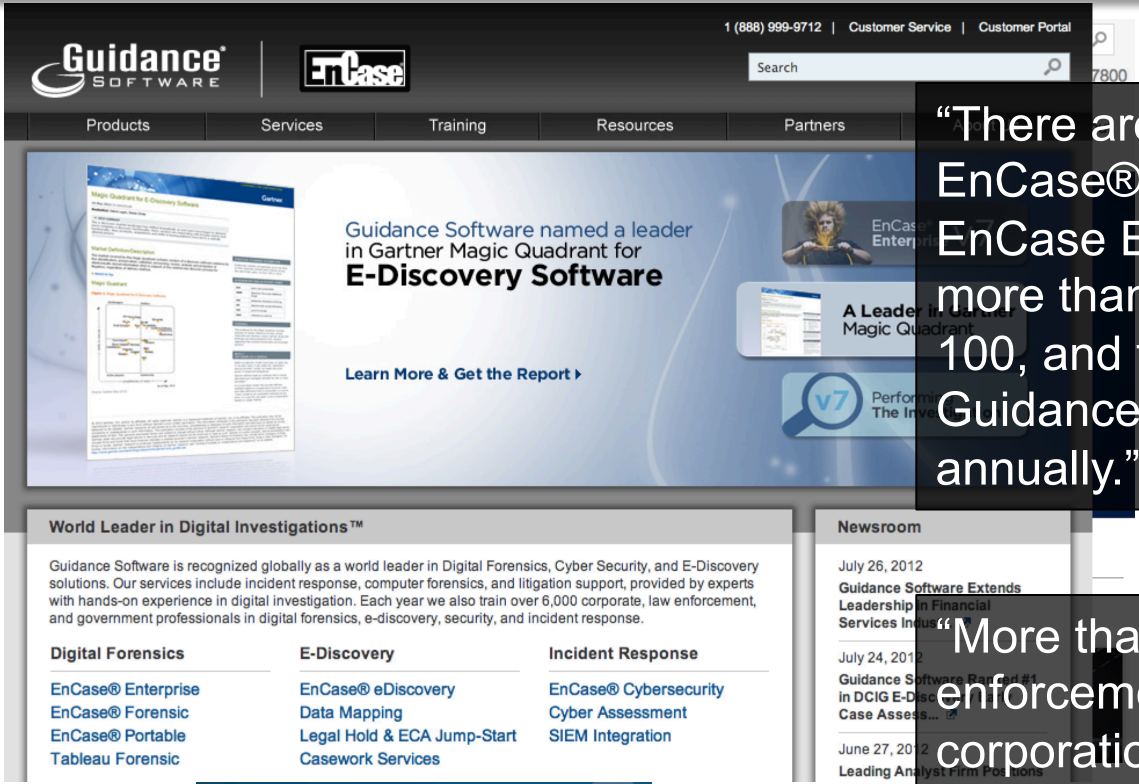
By Insider Threat Team on August 6, 2012 1:07 PM | Permalink

Hi, this is Bill Claycomb and Alex Nicoll with installment 2 of a 10-part series on cloud-related insider threats. In this post, we present three types of cloud-related insiders and discuss one in detail—the "rogue administrator." This insider typically steals the cloud provider's sensitive information, but can also sabotage its IT infrastructure. The insider described by this threat may be motivated financially or by revenge.

We consider the cloud-related insider threat from three different perspectives: the rogue administrator employed by a cloud provider, the employee in the victim organization that exploits cloud weaknesses for unauthorized access, and the insider who uses cloud resources to carry out attacks against the company's local IT infrastructure. Though we describe cloud-specific insiders, we believe the people behind these malicious insider attacks will continue to fit the profiles of other insider crimes identified by CERT in the book The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). As a result, mitigation strategies may be extrapolated from prior insider threat models; we will briefly discuss those options as well.

The Rogue Administrator

What would they use?



1 (888) 999-9712 | Customer Service | Customer Portal

Search

Products | Services | Training | Resources | Partners

Guidance Software named a leader in Gartner Magic Quadrant for **E-Discovery Software**

Learn More & Get the Report ›

EnCase Enterpris

A Leader in Gartner Magic Quadrant

Perform
The Inve

World Leader in Digital Investigations™

Guidance Software is recognized globally as a world leader in Digital Forensics, Cyber Security, and E-Discovery solutions. Our services include incident response, computer forensics, and litigation support, provided by experts with hands-on experience in digital investigation. Each year we also train over 6,000 corporate, law enforcement, and government professionals in digital forensics, e-discovery, security, and incident response.

Digital Forensics
- EnCase® Enterprise
- EnCase® Forensic
- EnCase® Portable
- Tableau Forensic

E-Discovery
- EnCase® eDiscovery
- Data Mapping
- Legal Hold & ECA Jump-Start
- Casework Services

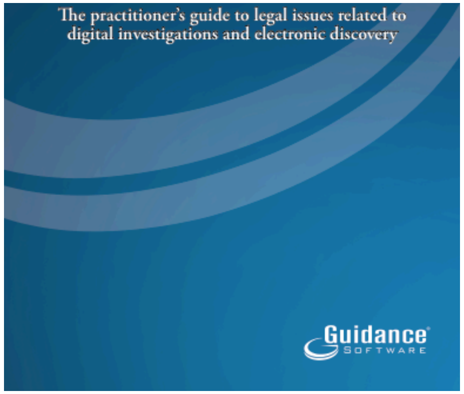
Incident Response
- EnCase® Cybersecurity
- Cyber Assessment
- SIEM Integration

Newsroom

July 26, 2012
Guidance Software Extends Leadership in Financial Services Indus

July 24, 2012
Guidance Software Ranked #1 in DCIG E-Disc
Case Assess...

June 27, 2012
Leading Analyst Firm Positions



The practitioner's guide to legal issues related to digital investigations and electronic discovery

Guidance Software

"There are more than 40,000 licenses of EnCase® technology worldwide, the EnCase Enterprise platform is used by more than sixty percent of the Fortune 100, and thousands attend renowned Guidance Software training programs annually." – guidancesoftware.com

"More than 100,000 users in law enforcement, government agencies, corporations and law firms around the world rely on AccessData software solutions and its premier digital investigations and hosted review services" – accessdata.com

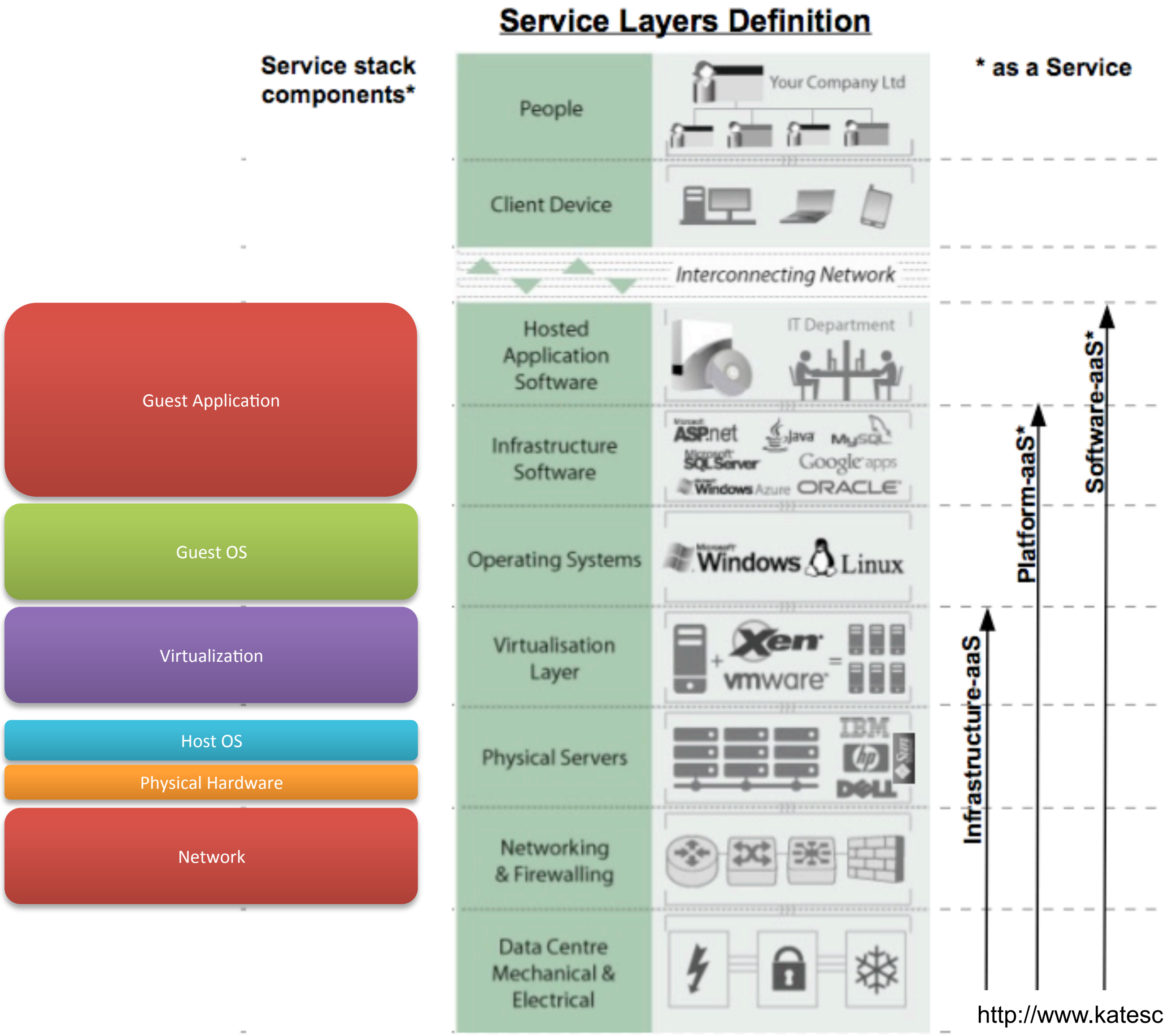
Today: What’s the problem?

“Incident response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training…”

Challenging Security Requirements for US Government Cloud Computing Adoption (Draft), Version 1.6, 2012

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Trust



Guest Application

Guest OS

Virtualization

Host OS

Physical Hardware

Network

http://www.katescomment.com/iaas-paas-saas-definition/

***Notes**:*
Brand names for illustrative / example purposes only, and examples are not exhaustive.

Cumulative Trust

Layer	Cloud Layer	Acquisition Method	Cloud Trust required
6	Guest Application	Depends on data	OS, HV, Host, Hardware, Network
5	Guest OS	Remote forensic software	OS, HV, Host, Hardware, Network
4	Virtualization	Introspection	HV, Host, Hardware, Network
3	Host OS	Access virtual disk	Host, Hardware, Network
2	Physical Hardware	Access physical disks	Hardware, Network
1	Network	Packet capture	Network

Tests

Experiment 1 (Guest OS)

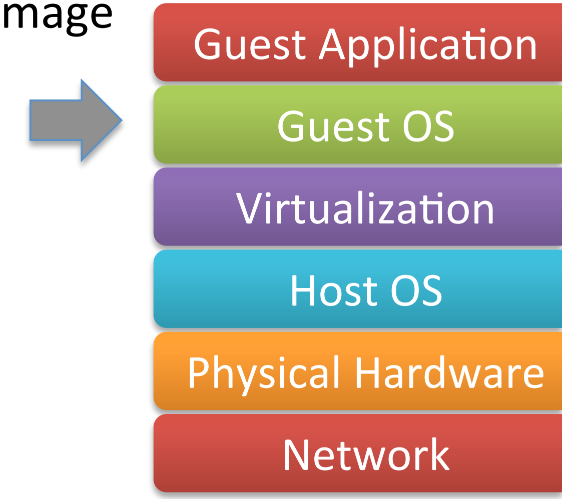
- Launch and “hack” a virtual machine in EC2
- Use EnCase and FTK agents to acquire disk images remotely
- Use Fastdump, FTK Imager, Memoryze to acquire memory images remotely
- Analyze data to determine success

Experiment 2 (Virtualization)

- Launch and “hack” a virtual machine on a private Eucalyptus cloud
- Use LibVMI to inject an EnCase agent to acquire disk image
- Analyze data to determine success

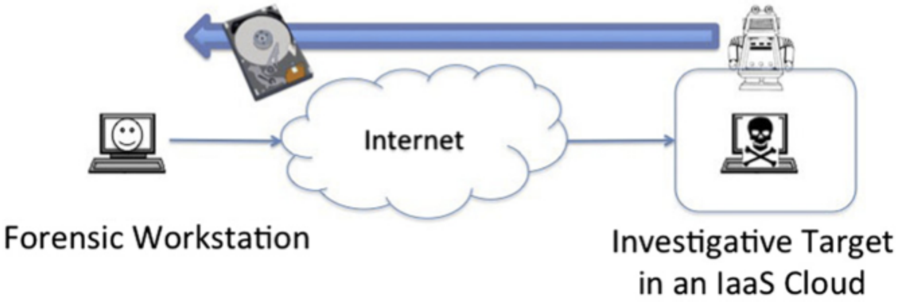
Experiment 3 (Host OS)

- Launch and “hack” a virtual machine in EC2
- Use AWS Export to obtain a disk image
- Analyze data to determine success



Success

- Microsoft Windows 2008 R1 SP2 Datacenter Edition, 32bit, m1.small, 30GB HDD, 2GB RAM



- Full drive/memory images (lacking checksum)
- Correct timeline
- Little evidence of the cloud (drivers, etc.)
- *Could the data have been manipulated?*

Results

Experiment	Tool	Evidence Collected	Time (Hrs)	Trust Required
1	EnCase	Success	12	OS, HV, Host, Hardware, Network
1	FTK	Success	12	OS, HV, Host, Hardware, Network
1	FTK Imager (disk)	Success	12	OS, HV, Host, Hardware, Network
1	Fastdump	Success	2	OS, HV, Host, Hardware, Network
1	Memoryze	Success	2	OS, HV, Host, Hardware, Network
1	FTK Imager (memory)	Success	2	OS, HV, Host, Hardware, Network
1	Volume block copy (dd)	Success	14	OS*, HV, Host, Hardware, Network
2	Agent Injection	Success	1	HV, Host, Hardware, Network
3	AWS Export	Success	120	AWS Technician, Technician's Host, Hardware & Software, AWS Hardware, AWS Network

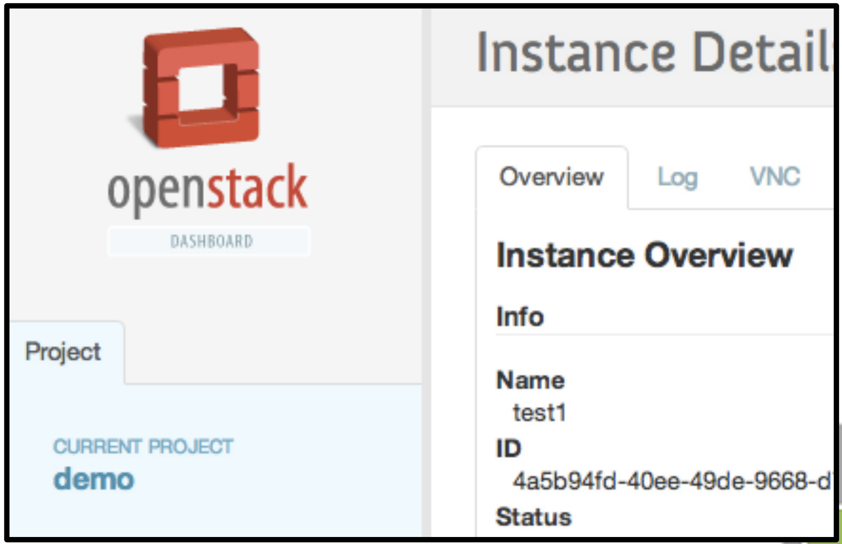
Trouble

- Vulnerability of forensic workstation online
- Security of remote agent
- Cost – time and $$$
- Require changes to cloud environment
- Unanswered legal questions
- *Is this "better" than today?*

Alternatives

- Root Trust in the Host/VM with TPMs
- Collection from Management Plane
- Forensics Support as a Service
- Contract and Legal Solutions

Management Plane



CURRENT PROJECT
demo

Instance Detail

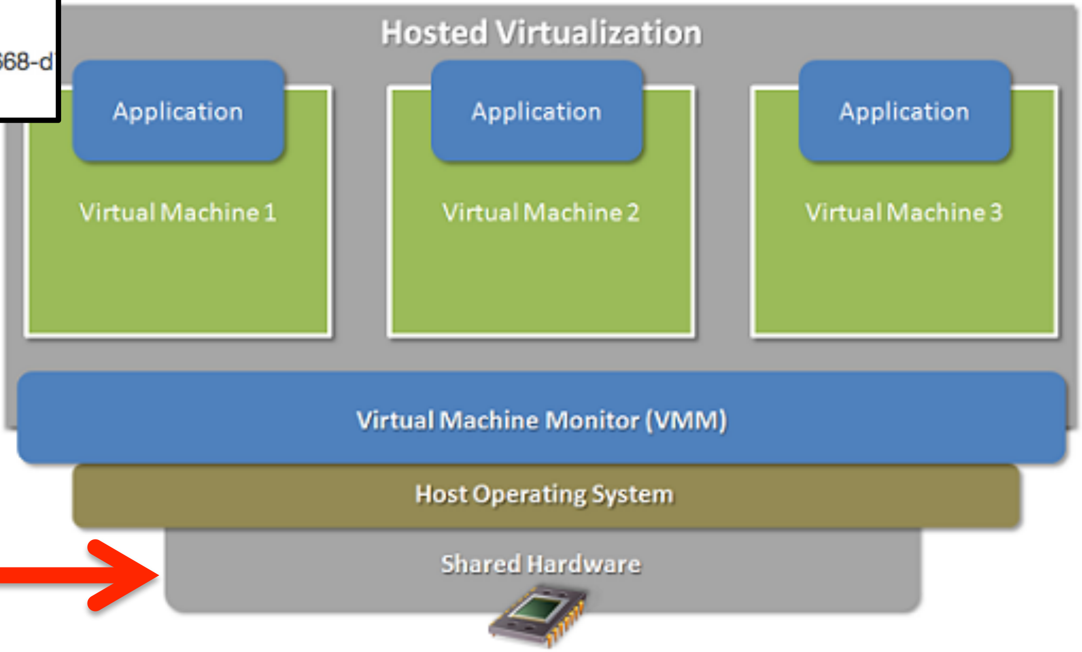
Instance Overview

Info

Name
test1

ID
4a5b94fd-40ee-49de-9668-d

Status



Tomorrow: Future work

- Corroborate from multiple layers
- “Live” Forensics with Snapshots
- Parallel analysis of PaaS and SaaS
- Consumer-driven forensic capabilities
- Legal analysis

Questions

dykstra@umbc.edu
sherman@umbc.edu