SAND2010-6808C

Cloud Computing Security

October 7, 2010

Dongwan Shin
Bill Claycomb
Vince Urias

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Agenda

- **Introduction to Cloud Computing Security**
- Cloud Computing Implementation Considerations
- Role Based Access Control and Demo
- Cloud Computing Forensics
- The Future of Cloud Computing Security

Cloud Deployment Models

- Public
- Private
  - May be managed and hosted on-site or off-site
  - May be part of a public cloud, a *virtual private cloud*
- Community
  - Shared by several organizations
- Hybrid
  - Composition of two or more clouds
  - Data and application portability exists between clouds

Cloud Services Models

- **Software as a Service (SaaS)**
  - **Service provider delivers everything**
    - **Applications provided by the cloud**
  - **Google Apps**
- Platform as a Service (PaaS)
  - Customer deploys applications on to a platform provided by the cloud
  - Google App Engine
- Infrastructure as a Service (IaaS)
  - Only fundamental resources are provided
  - Customer responsible for deployment and management
  - Amazon EC2

Software as a Service (SaaS)

Returning user? Sign in here | La

Reliable, secure online applications wherever you work

Google Apps reduces IT costs and empowers today's employees. Gmail, Google Docs, Google Sites, and more - $50 per user per year. Try it free for 30 days.

Gmail for business 25GB storage, less spam, and a 99.9% uptime SLA, and enhanced email security.

Google Calendar Agenda management, scheduling, shared online calendars and mobile calendar sync.

Google Docs Documents, spreadsheets, and presentations. Work online without attachments.

Google Groups User-created groups providing mailing lists, easy content sharing, searchable archives.

Google Sites Secure, coding-free web pages for intranets and team managed sites.

Google Video Private, secure, hosted video sharing.

Switch to Google Apps

Learn how switching from Microsoft Exchange or Lotus Notes helps you save money and reduce IT hassles.

Estimate your cost savings.

Cloud Services Models

- Software as a Service (SaaS)
  - Service provider delivers everything
    - Applications provided by the cloud
  - Google Apps
- **Platform as a Service (PaaS)**
  - **Customer deploys applications on to a platform provided by the cloud**
  - **Google App Engine**
- Infrastructure as a Service (IaaS)
  - Only fundamental resources are provided
  - Customer responsible for deployment and management
  - Amazon EC2

Platform as a Service (PaaS)

Google code Search

e.g. "templates" or "datastore"

Google App Engine Home Docs FAQ

Run your web apps on Google's infrastructure.

Easy to build, easy to maintain, easy to scale.

Java™ Language Support

App Engine recently unveiled its second language: Java. This release includes our Java runtime, integration with Google Web Toolkit, and a Google Plugin for Eclipse, giving you an end-to-end Java solution for AJAX web applications. The Java runtime is now available for anyone to use, so please give it a try and send us your feedback.

- Get the full scoop in our blog post.
- Click over to YouTube to watch our Campfire One announcements.
- See our docs for other new features like cron support, database import, and access to firewalled data.

Get an overview of App Engine's new Java runtime and see a demo of a sample app from creation to deployment.
Watch Now

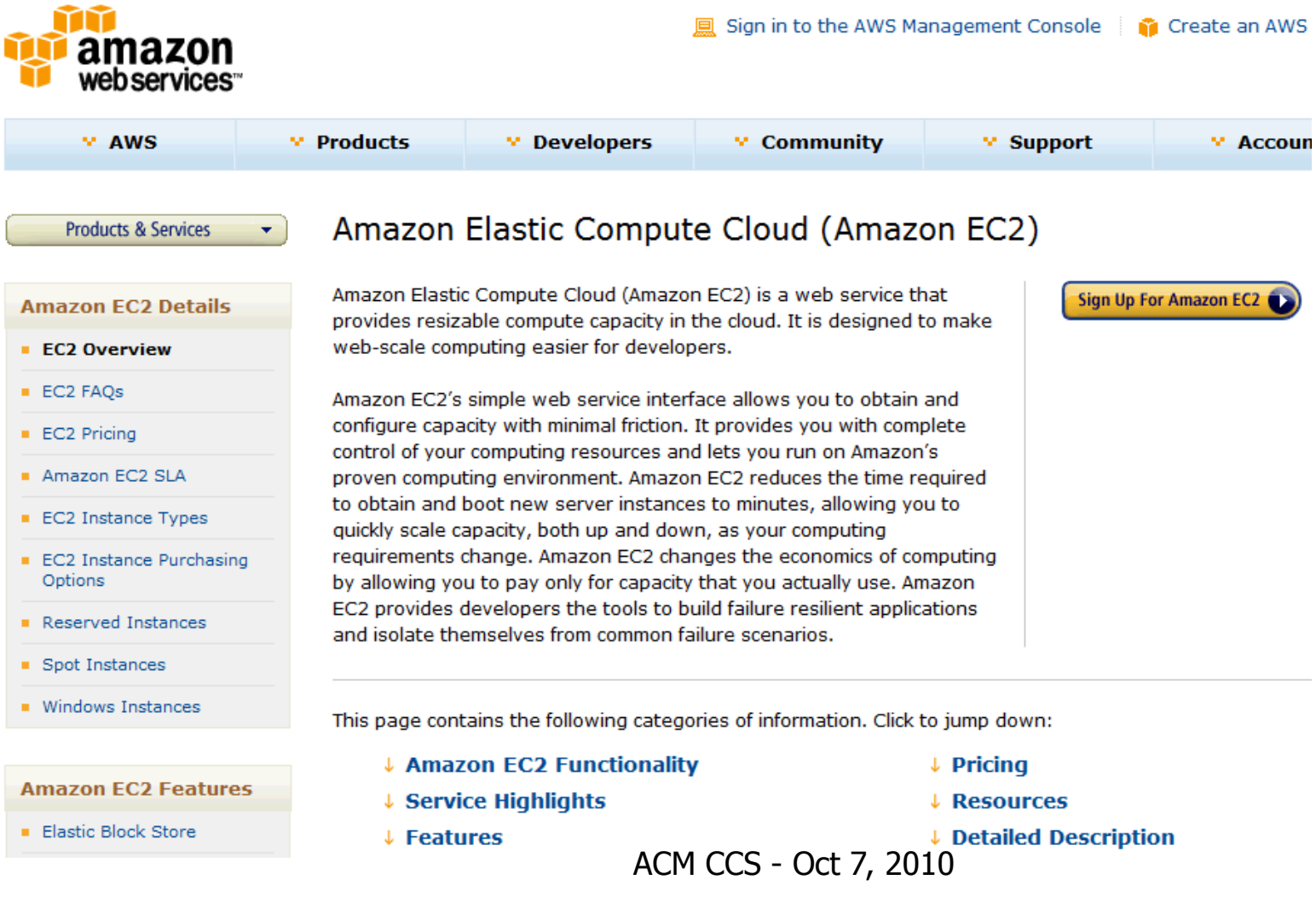
Grow Beyond The Free Quotas

App Engine developers can now purchase additional computing resources beyond the free quota limits. Scale your application to millions of users and pay only for what you use. App Engine will always be free to get started so you can try it out with no risk.

Cloud Services Models

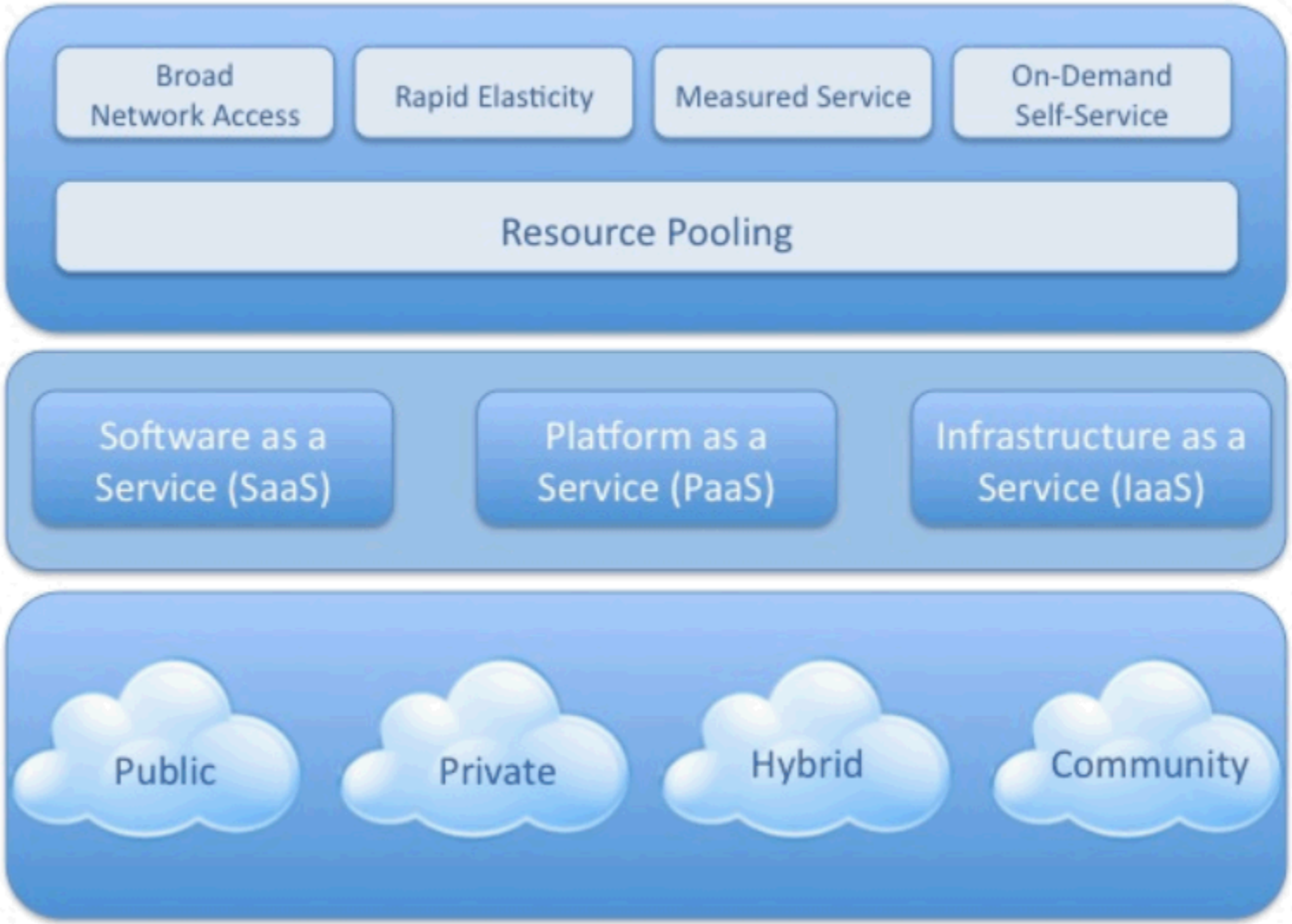
- Software as a Service (SaaS)
  - Service provider delivers everything
    - Applications provided by the cloud
  - Google Apps
- Platform as a Service (PaaS)
  - Customer deploys applications on to a platform provided by the cloud
  - Google App Engine
- **Infrastructure as a Service (IaaS)**
  - **Only fundamental resources are provided**
  - **Customer responsible for deployment and management**
  - **Amazon EC2**

Infrastructure as a Service (IaaS)

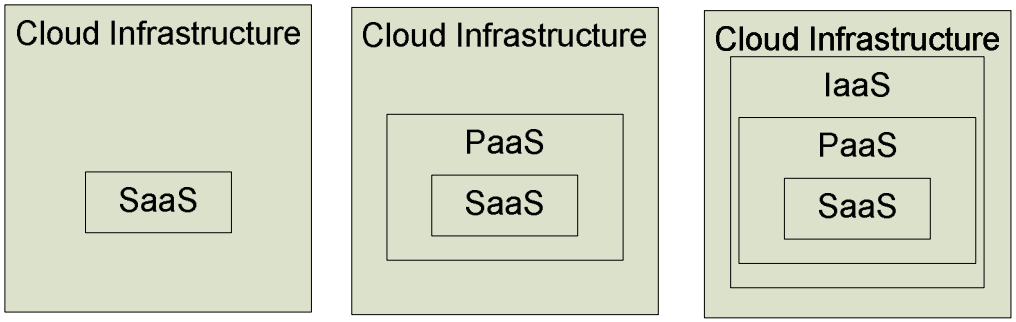


Visual Model Of NIST Working Definition Of Cloud Computing

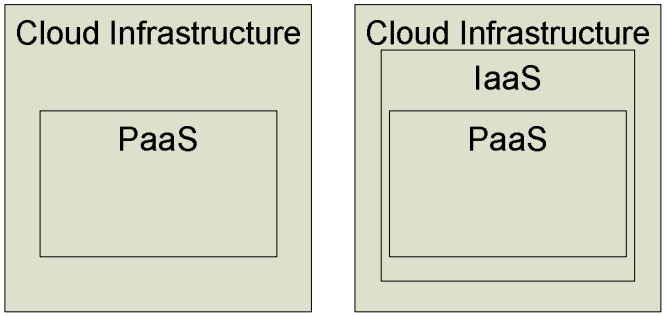
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



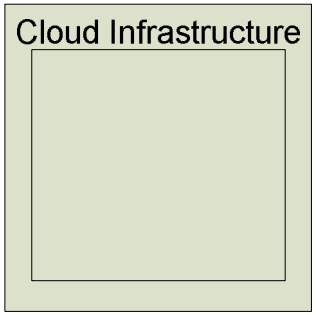
Service Model Architectures



Software as a Service (SaaS) Architectures



Platform as a Service (PaaS) Architectures



Infrastructure as a Service (IaaS) Architectures

Cloud Security Threats*

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service, and Traffic Hijacking
7. Unknown Risk Profile

* As Identified by the Cloud Security Alliance, 2010

Abuse and Nefarious Use

- Password and key cracking
- DDOS
- Launching dynamic attack points
- Hosting malicious data
- Botnet command and control
- Building rainbow tables
- CAPTCHA solving

- Exploits exist already

Prevention

Insecure Interfaces and APIs

- Could expose more functionality than intended
- Policy could be circumvented
- Credentials may need to be passed – is the interface secure?

Prevention

Malicious Insiders

- Particularly poignant for cloud computing
- Little risk of detection
- System administrator qualifications and vetting process for cloud services provider may be different that that of the data owner

Prevention

Shared Technology Issues

- Underlying architecture (CPU cache, GPU, etc.) not intended to offer strong isolation properties
- Virtualization hypervisor used to mediate access between guest OS and physical resources

- Exploits exist (Blue Pill, Red Pill)

Prevention

Data Loss or Leakage

- Data is outside the owner's control
- Data can be deleted or decoupled (lost)
- Encryption keys can be lost
- Unauthorized parties may gain access

- Caused by
  - Insufficient authentication, authorization, and access controls
  - Persistence and remanance
  - Poor disposal procedures
  - Poor data center reliability

Prevention

Account or Service Hijacking

- Exploits phishing attacks, fraud, or software vulnerabilities
- Credential reuse

Prevention

Unknown Risk Profile

- How well is the cloud being maintained?
  - Many companies are unwilling to release details
- Is the infrastructure up to date
  - Patches
  - Firmware
- Does the combination of different service providers create previously unseen vulnerabilities?

Prevention

Agenda

- Introduction to Cloud Computing Security
- **Cloud Computing Implementation Considerations**
- Role Based Access Control and Demo
- Cloud Computing Forensics
- The Future of Cloud Computing Security

Implementation Considerations

- **Demo**

Agenda

- Introduction to Cloud Computing Security
- Cloud Computing Implementation Considerations
- **Role Based Access Control and Demo**
- Cloud Computing Forensics
- The Future of Cloud Computing Security

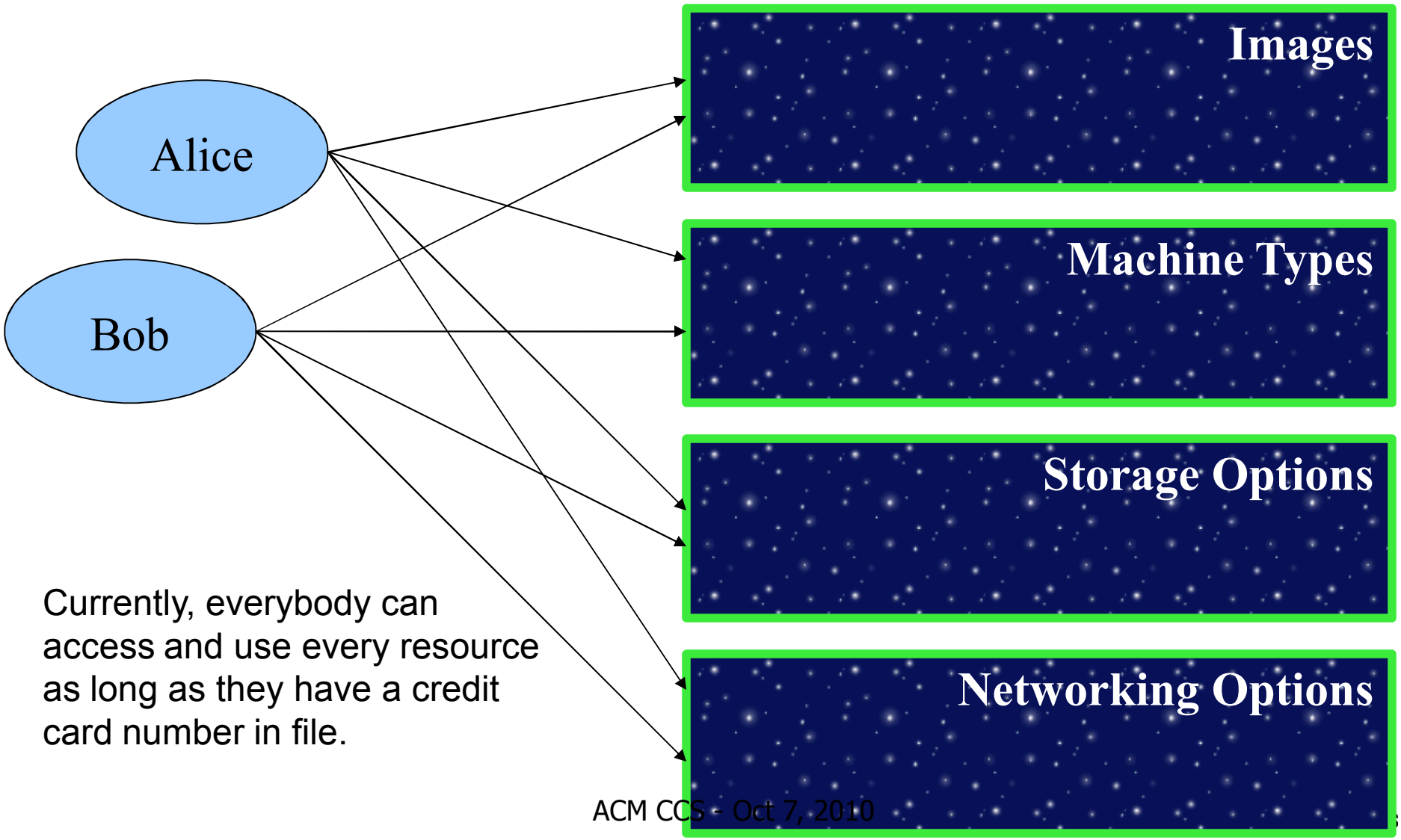
Motivation

- Access control in current IaaSes
  - User-resource direct mapping model
  - Utility (pay-as-you-go) computing
  - Very primitive access control support
  - Some of them only provide ACLs for images
- No organization-level security/governance policy support
- Inflexible pricing model for business

Motivating Example

- Assume that **SunnyTech.edu**, a fictitious university, decides to transition its university-wide information technology (IT) as well as department-wide service and research IT to the cloud services provided by **GoCloud.com**. The cloud services under consideration include not only software services such as email and HR applications, but also infrastructure services such as virtual machines with operating systems (OSes) having pre-configured application images installed. In addition, **SunnyTech.edu** decides to control access to, and thus limit the usage of, the virtualized resources based on the roles of the members of the university. Lastly, the university wants to keep access logs based on its audit policy as well as to implement other policies related to governance.

GoCloud.com



Currently, everybody can access and use every resource as long as they have a credit card number in file.

Motivating Example

- How to support an advanced access control such as role-based access control?
- How to implement organizational security and governance policies?
- How to support different pricing for individual users vs. businesses?

Our Objective

- We propose a domain-based framework for provisioning and managing users and resources in IaaS
  - Introduce the notion of domain to the user-resource direct mapping
  - Can address the three problems
- Provide a proof-of-concept implementation using Eucalyptus

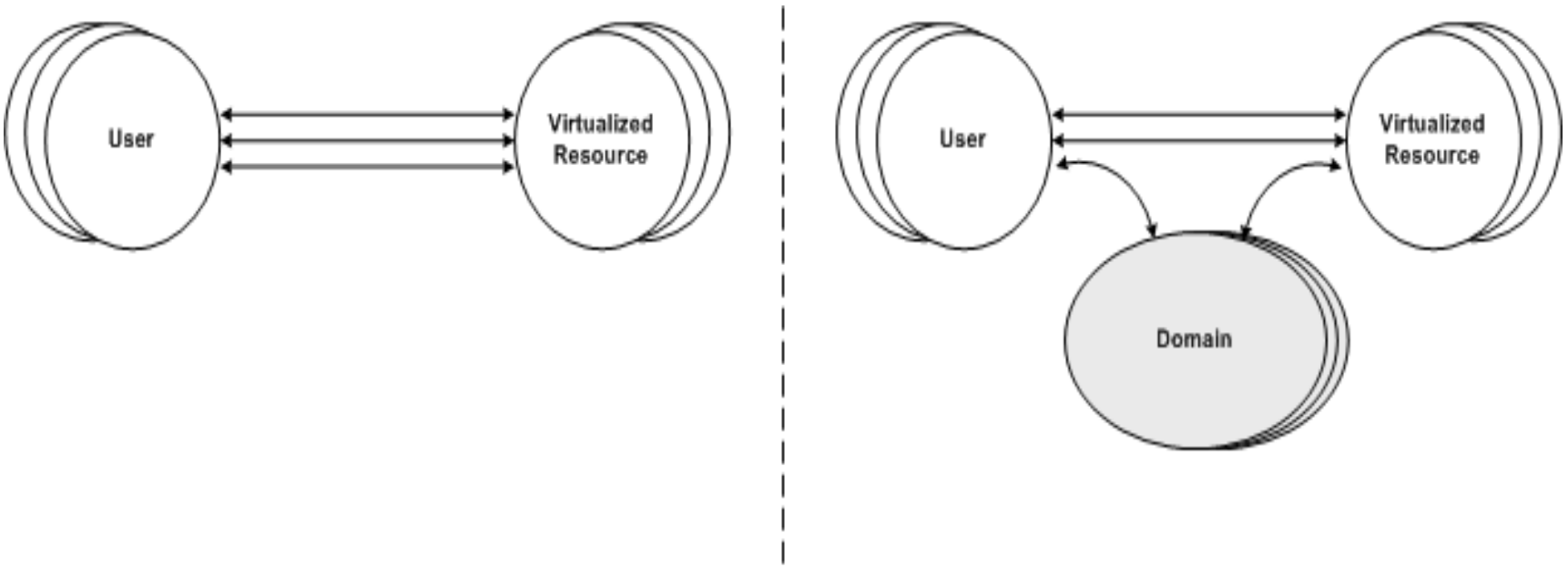
Background – Role Support in Clouds

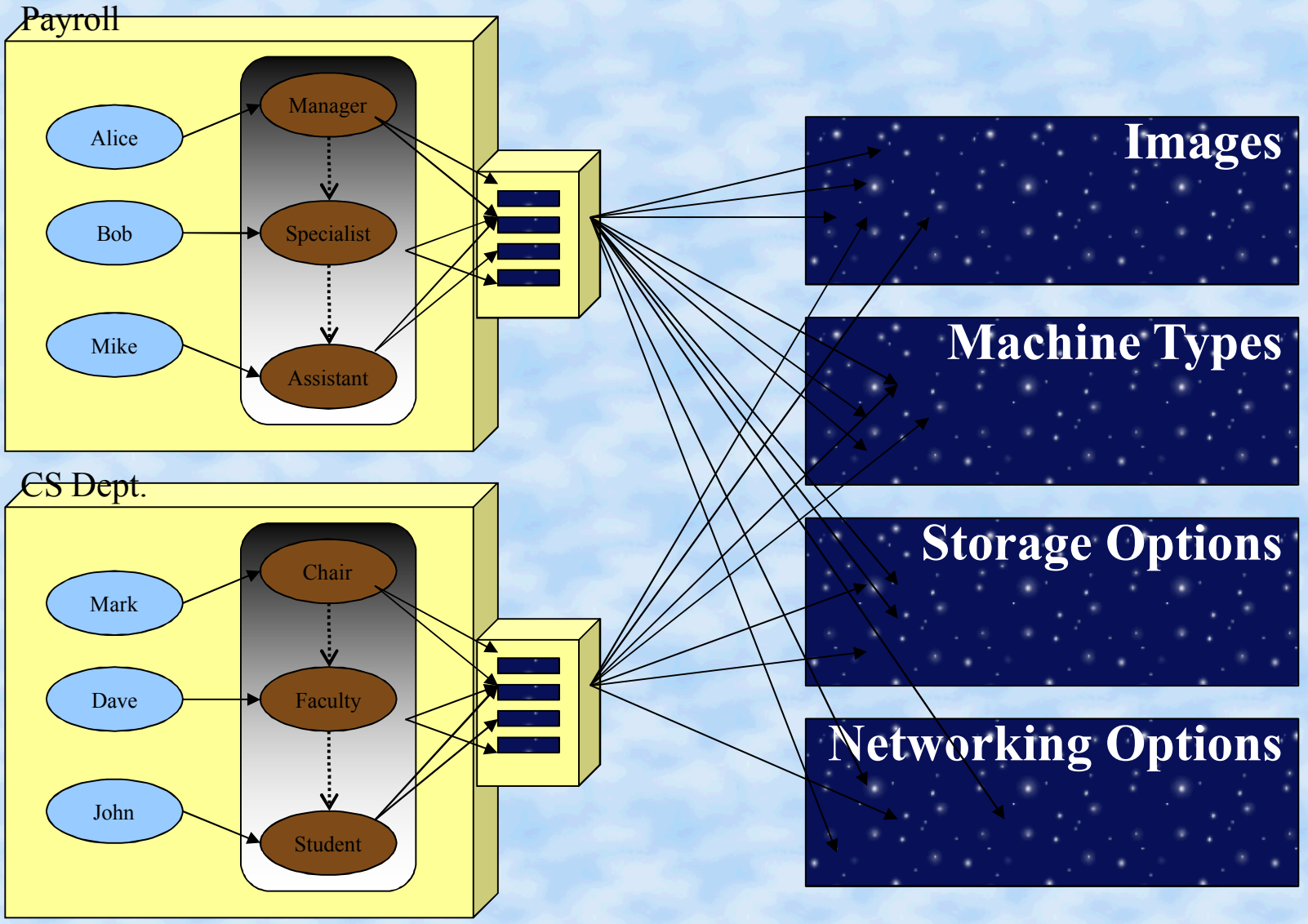
- Most of existing IaaSes do not support the notion of grouping
  - Amazon EC2
  - Nasa's Nebula
  - Windows Azure

Our Approach

- We want to add an access control mechanism so that the all-or-nothing approach will not be supported any more
- We want to group users and permissions so that all users belonging to the same group have exactly the same permissions
- Furthermore, we want to organize groups into a hierarchy
- Furthermore, we want to have separate administration domains

Our Approach




Payroll
Alice
Bob
Mike
Manager
Specialist
Assistant
CS Dept.
Mark
Dave
John
Chair
Faculty
Student
Images
Machine Types
Storage Options
Networking Options

Design

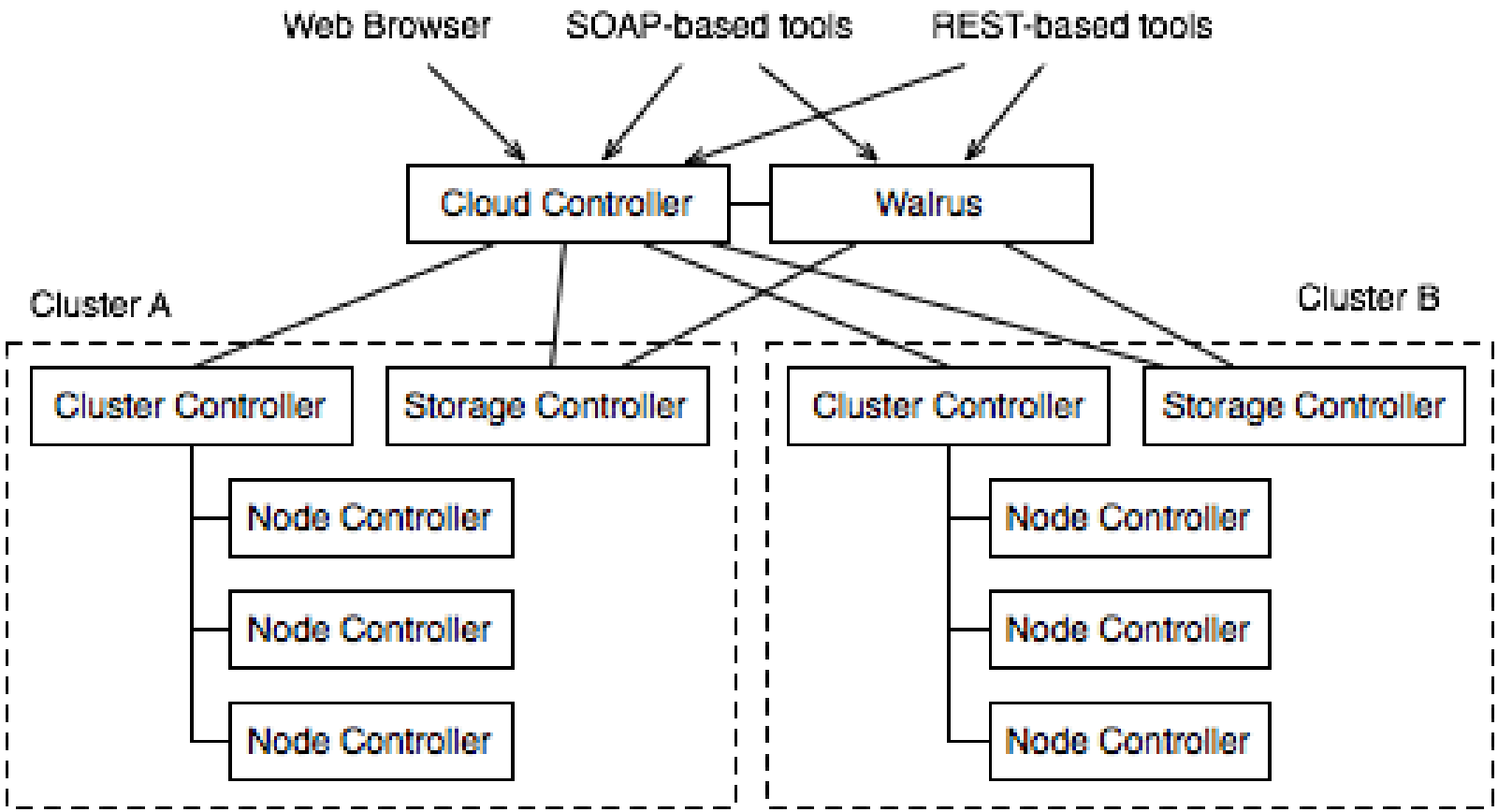
Cloud vs. Domain Administrators

- Domains create more indirection
  - Less messy mapping
- Cloud administrator:
  - Creates a domain
  - Assigns permissions to the domain
  - Creates a domain administrator
  - Manages the cloud
- Domain administrator:
  - Creates roles and builds a hierarchy
  - Creates users and assigns them to roles
  - Manages the domain

Implementation

- Open source project Eucalyptus v1.6.2
  - Designed to be exact clone of Amazon EC2
- Uses other open source Linux tools
  - Xen/KVM hypervisors
  - DHCP/Iptables/VLAN for network management
  - AoE for storage devices

Eucalyptus Architecture

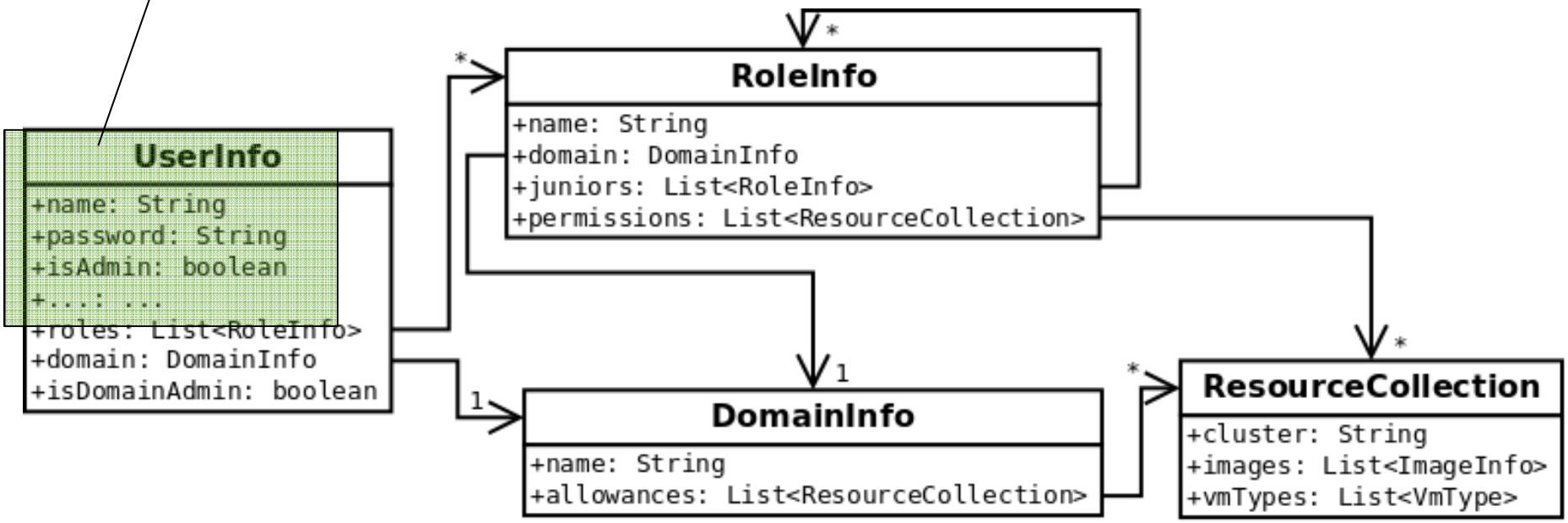


Implementation

- Our additions are only in the Cloud Controller
- Created objects that represent roles, domains, and permissions
- Modified the web administration interface for domain, role, and user management
- Added a reference monitor that makes the access control decisions

Implementing Objects

Original UserInfo object and attributes

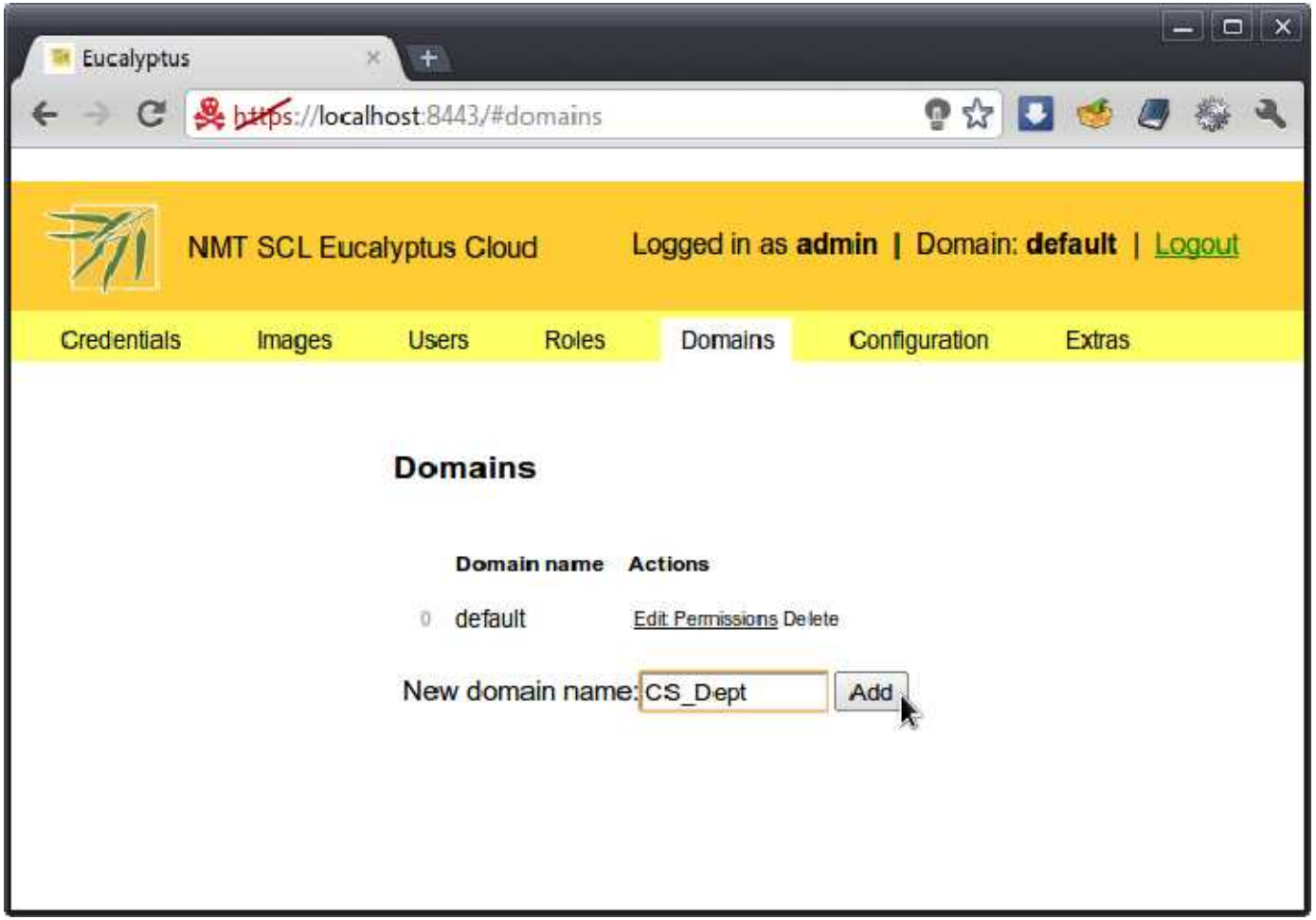


Representing Permissions

- **A ResourceCollection object represents all the images and virtual machine types that the domain/role is allowed to use in the specified cluster:**

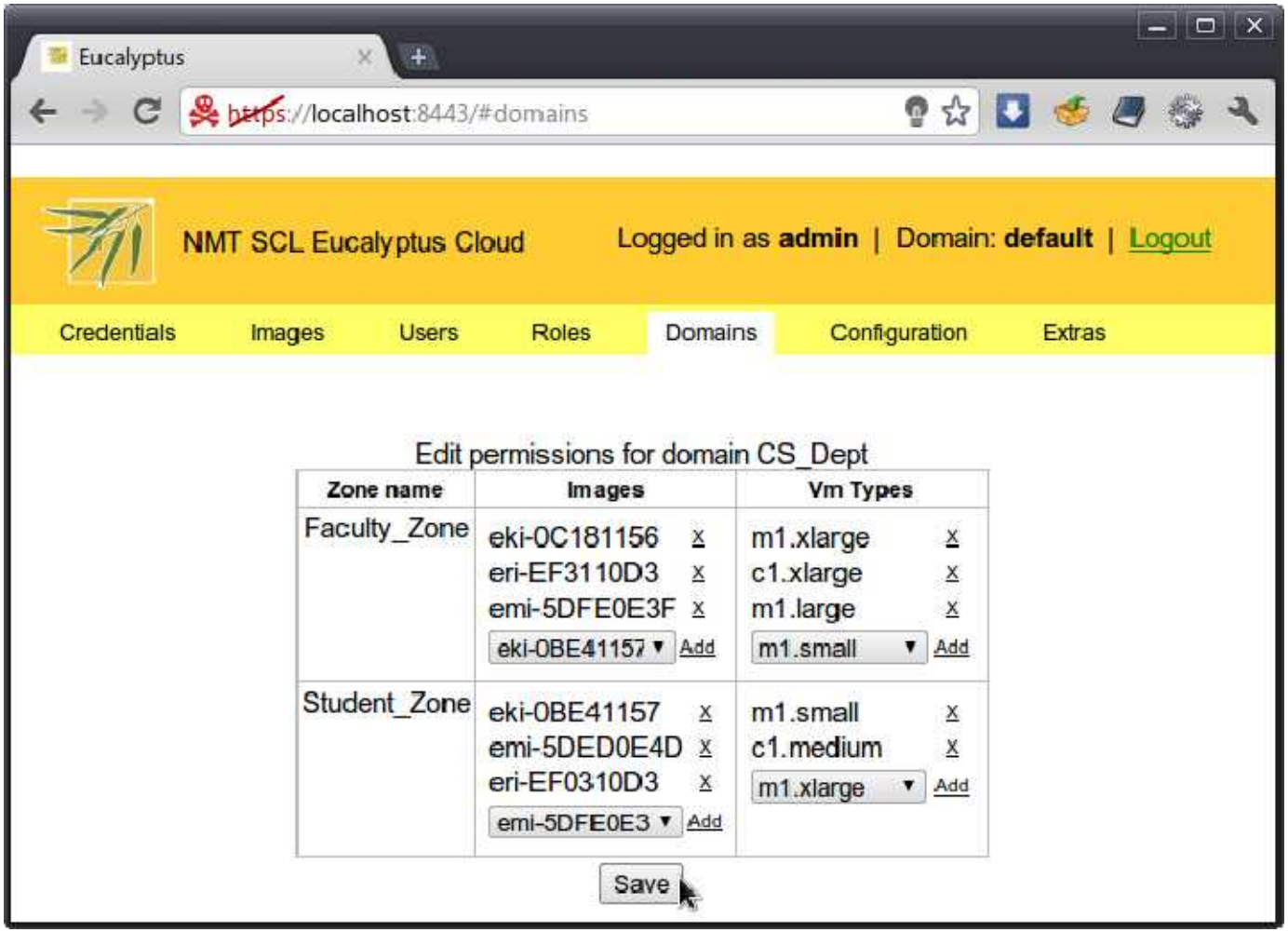
```
RC = {
cluster=”ZoneA”,
images=[“emi-AAAAAA”,”eri-BBBBBB”],
vmTypes=[“m1.small”, “m1.medium”]
}
```

Creating a New Domain

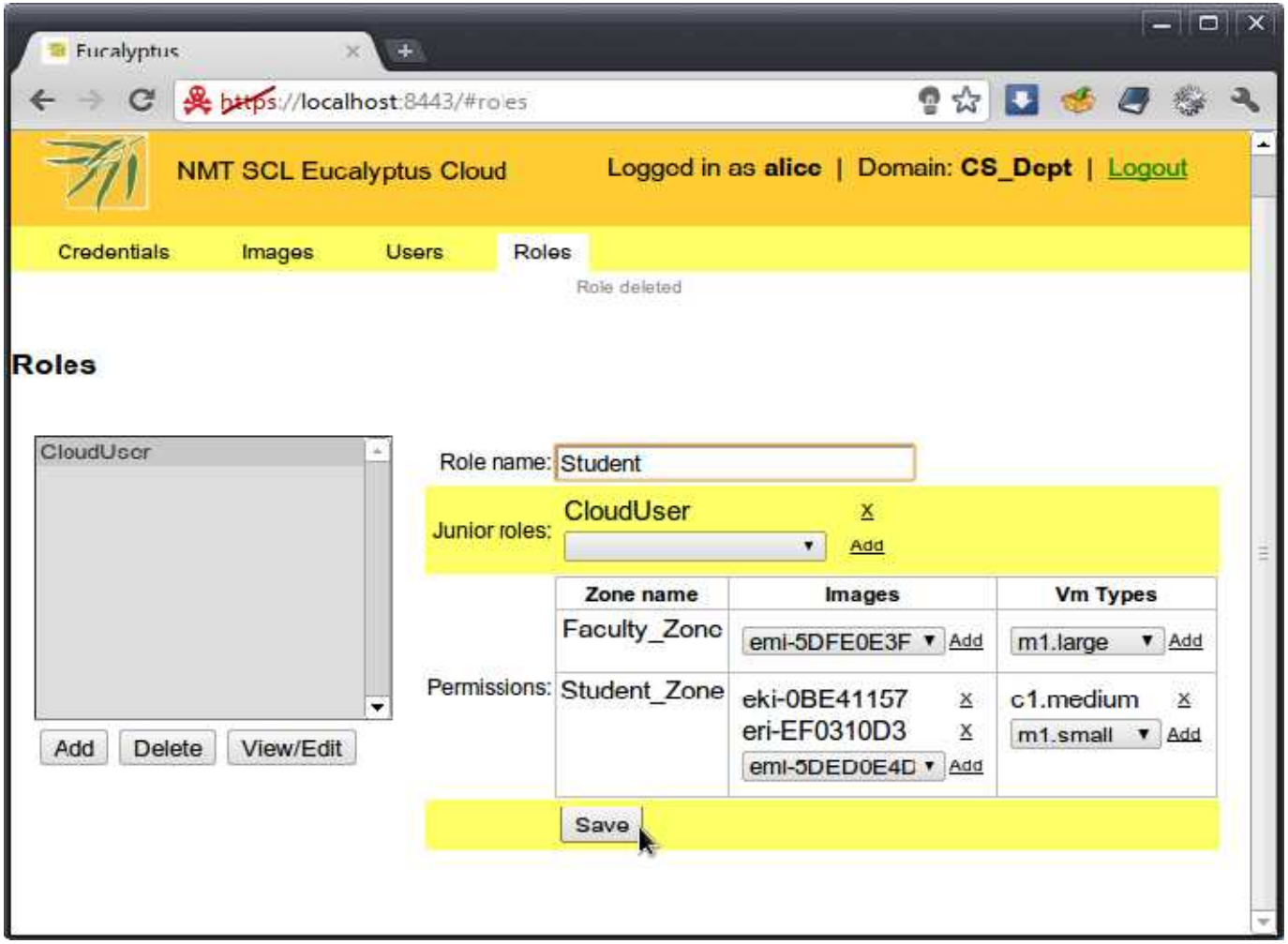


Sandia National Laboratories

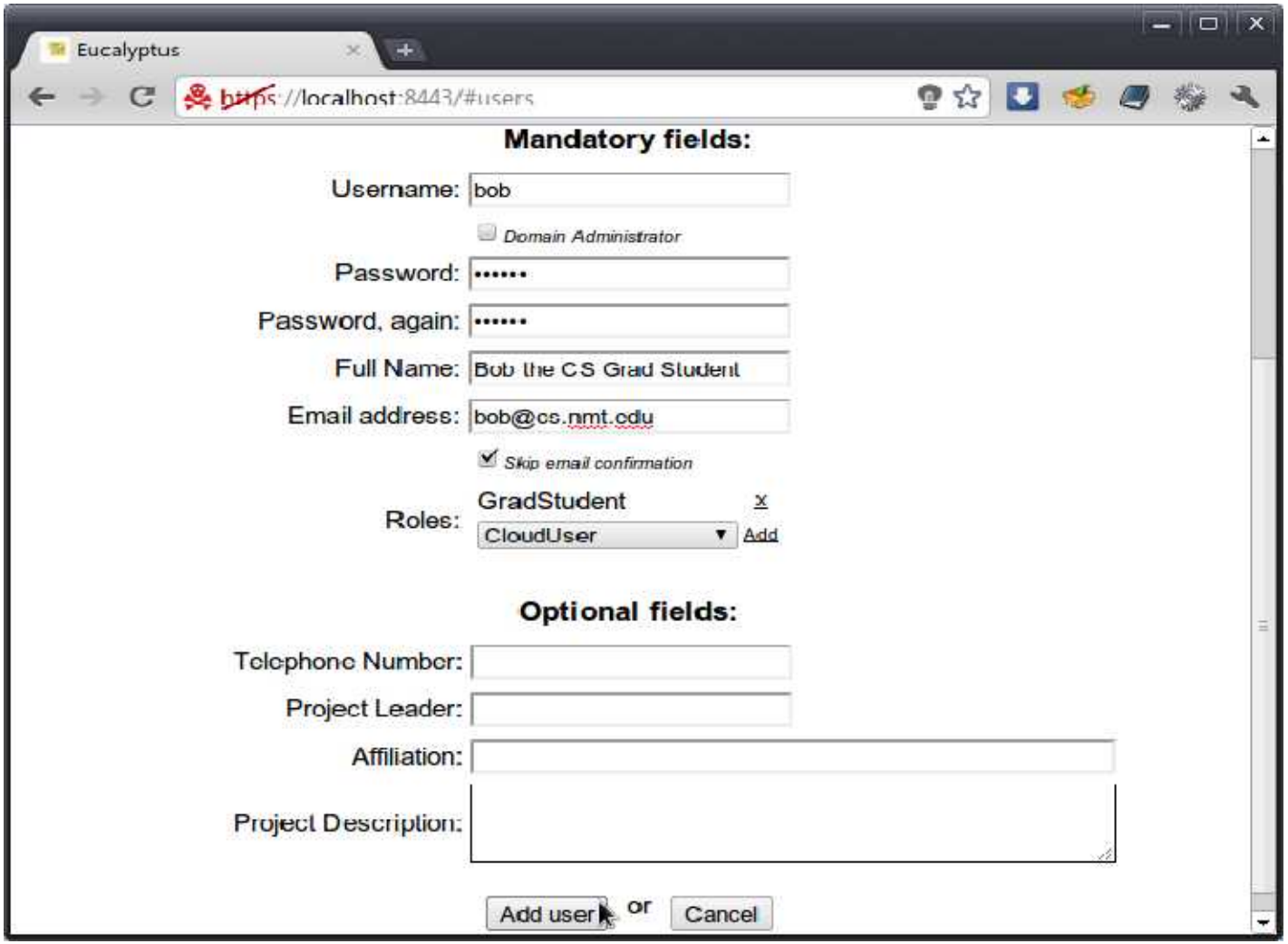
Domain Permission Management



Domain Role/Hierarchy Management



Domain User Management



Demo

Agenda

- Introduction to Cloud Computing Security
- Cloud Computing Implementation Considerations
- Role Based Access Control and Demo
- **Cloud Computing Forensics**
- The Future of Cloud Computing Security

Road Map

- Objectives
- Case studies
- Conclusions

Sandia National Laboratories

Objectives

- Identify the challenges of cloud computing to digital forensics
- Evaluate and test the cloud computing environment using **traditional forensics methodology**
- Evaluate the forensic process as it pertains law enforcement
- Propose solutions to the issue of cloud computing and digital forensics

Digital Forensics

- **"Tools and techniques to recover, preserve, and examine digital evidence on or transmitted by digital devices"**

Sandia National Laboratories

General Observations

In the initial discussions several interesting problems were presented:

- Legal issues
- Virtual hardware
- Data distribution
- Ephemeral nature of computing
- Data permanence

Case Studies

- **Addressed questions asked during a digital forensics investigation**

- **Tested several sub-disciplines of digital forensics**
- **Disk Forensics**
- **Memory Forensics**
- **Network Forensic**

- **Focused on the practicality of doing forensic in the cloud**

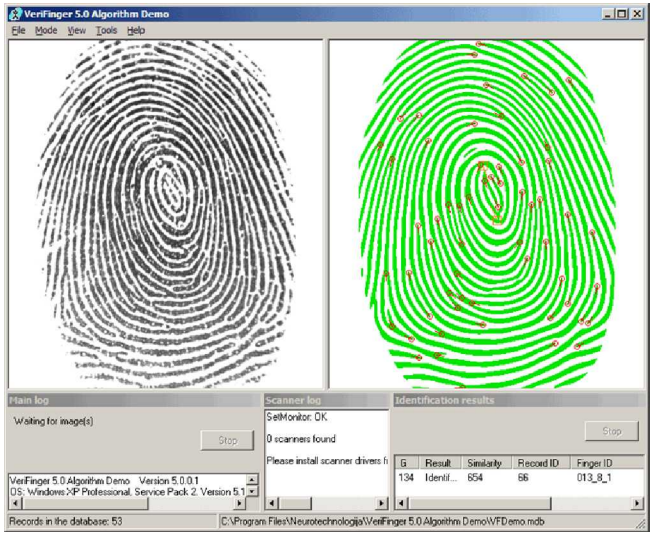
Sandia National Laboratories

Tools

Forensics Tools

- Helix/ Knoppix
- Access Data FTK
- Sleuth Kit
- Sysinternals
- LiveView
- DT Search
- vmfs specific

Digital Forensics : Identification



Sandia National Laboratories

Experiment 1: Identification

- Goal:
  - Identify vSphere specific artifacts
  - Understanding the key components of the vSphere architecture
- Actions:
  - Navigated the ESX datastore
  - Searched for files created by vmfs
  - Searched for log files
- Results:
  - Identified important files
    - Example .flat.vmdk – data from the virtual hard drive

Experiment 1: Identification (cont.)

- .flat.vmdk - data from the virtual hard drive
- .vmdk - configuration file from the virtual hard drive
- .vswp - unknown purpose
- .vmx - complete configuration file for the virtual machine (i.e. MAC,machine name, uuid)
- .log - documented changes to the virtual machine and logins
- .nvram - bios information for the virtual machine (changes often)

Experiment 1: Identification (cont.)

- .nvram - bios information for the virtual machine (changes often)
- .vmxf - template for a virtual machine (user created template)
- .vmsn - configuration snapshot file (times the number of snapshots)
- .delta.vmdk - changes from one snapshot to another or any modifications to the disk
- .vmsd - snapshot manager
- .000N.vmdk - configuration file for the delta
- .vmdk.vmss - suspended virtual machine information

Experiment 2: Characterization of vSphere's 'Moving Parts'

- **Goal:**
  - Understand each vSphere component and where the forensic/artifacts are located
- **Action:**
  - Installed various elements of vSphere
  - Configured various setting associated with the vSphere elements
- **Results:**
  - Familiarization of the vSphere private cloud components

Sandia National Laboratories

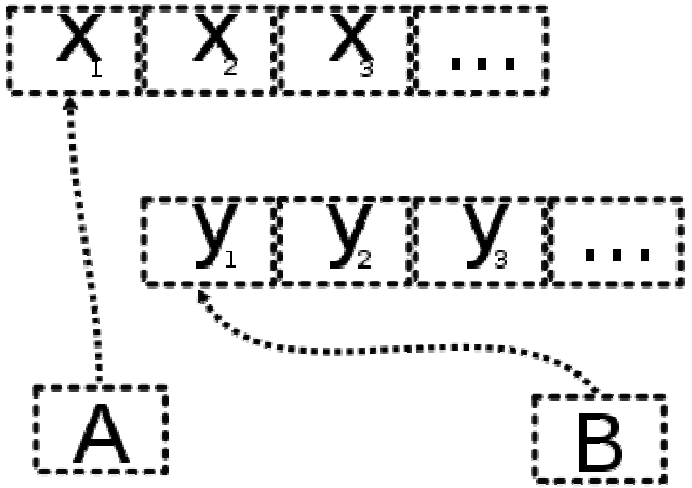
Experiment 2: Characterization of vSphere's 'Moving Parts' (cont.)

vSphere private cloud components

- Datacenter
- Cluster
- Host
- Virtual Machine (VM)
- Datastore
- NFS
- Local (vmfs)
- iSCSI
- SAN/NAS
- ESX version 4.0
- ESXi version 4.0
- ESXi version 3.5

Sandia National Laboratories

Digital Forensics : acquisitions



Experiment 3: Acquisitions

- **Goal:**
  - Determine what methods are used to do acquisition
  - Determine if the cloud environment hinders or improves the acquisitions process
- **–Actions:**
  - Use vCenter interface
  - Use a NFS based datastore
  - Acquire through the ESX management service console
  - Using VMware Converter
- **–Results:**
  - Results in copying vm off from /vm/storage/instance
  - Anomalies
  - Determined what techniques work
  - Determined locked files

Experiment 4: Traditional Tools

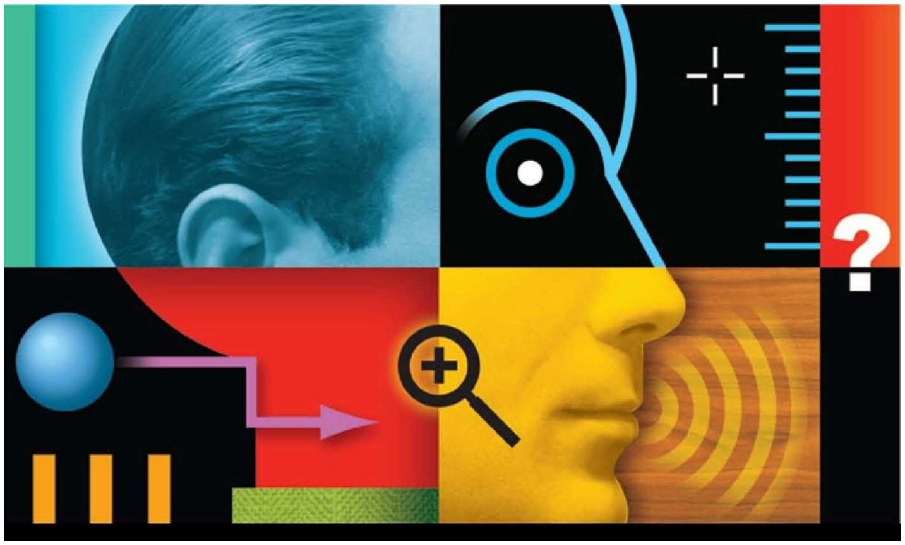
- Goal:
  - Identify the challenges and short comings of cloud forensics
  - Identify what forensic actions in the cloud Identify what tools are better suited for doing forensics in the cloud
- Actions:
  - Loaded forensic tools onto the virtual machines (tainted drive)
  - Conducted a digital forensics investigation
  - Virtual disk mount technique
- Results:
  - Tools worked, and were supported
  - Limited to what the host sees
  - Did not see data from other experiments

Experiment 5: NFS on the Cloud

- **Goal:**
  - Determine what effects using NFS as an external datastore and see if additional information can be extracted
- **Actions:**
  - Created an NFS datastore
  - Created vms on datastore
  - Investigated datastore
- **Results:**
  - Determined with an NFS share a non-VMFS volume will be created
  - Using an network file system (NFS) datastore full control is given to the virtual machine's
  - This technique eliminated the need to "hot" pull a disk from a host in order to retrieve and analyze locked files

Acquisition Results

- Cloud computing hindering traditional acquisition process
- NFS persevered the integrality of the file system during acquisition
- vmfs locking prohibits acquisition on non-NFS solution
- Traditional tools only worked in a limited capacity



Digital Forensics : Analysis

Experiment 6: Artifacts on the Hypervisor

- Goals:
  - Determine if installing forensic tools on hypervisor will enable increased analysis capabilities
  - Determine if unallocated space can be mined for information
- Actions:
  - Used ESX 4.0, installed numerous tools packages from source not an option in ESXi
  - Installed Sleuthkit
- Results:
  - Installed Sleuthkit on the ESX 4.0
  - Sleuthkit failed
  - Realized limitations of vmfs volume
  - Need alternative methods
  - Realized the benefits of using ESX over ESXi for forensics

Experiment 7: Inode Analysis

- **Goals:**
  - **Determine if traditional inode analysis can be applied to vmfs on an NFS**
- **Actions:**
  - **Create VMs on a NFS datastore**
  - **Used Sleuthkit and found all directed blocks associated with vm**
  - **Carved out smaller files**
  - **Deleted files from the ESX host**
  - **Attempted to reconstruct files**
- **Results:**
  - **Determined that upon deletion vSphere does not zero-out deleted files**
  - **Using NFS vswp can be extract independently**
  - **Used icat to catalog the .vswp file and reconstruct it**
  - **Need to create custom applications for filesystem carvers**

Experiment 8: Explored vmfs Volumes

- **Goals:**
  - Determine what can be extracted from the volume
  - Explore tools which support vmfs
- **Actions:**
  - Loaded ‘hot’ ESX datastore, attached to write-blocker and mounted on a Linux machine
  - Used both vmfstools and debugvmfs to explore the volume
  - Mount and read the vfms
  - Explore file attributes (i.e. files locks)
- **Results:**
  - Developed method to mount vmfs datastore (non-disruptive) manner
  - Analyze and preserved the data

Sandia National Laboratories

Experiment 9: Network Tests

- **Goals:**
  - **Determine what artifacts exist on the network**
  - **Test SSL end-to-end encryption, self-signed CA**
  - **Determine if network forensic is viable**
- **Actions:**
  - **Sniffed the traffic**
  - **Created a virtual network tap (via tcpdump at host)**
  - **Used Solar Winds virtual appliance**
  - **Characterize network traffic**
- **Results:**
  - **Determined that the traffic being sent back and forth between host and client is only the management information**
  - **SOH, SOAP commands to vms ch feature utilize differing ports**
  - **Suspect that vSphere is using VNC connection to manage hosts**

Experiment 10: Private Networks

- Goals:
  - Determine what artifacts would exist from a virtual, non-routable network on the physical wire
  - Create insulated network
- Actions:
  - Sniffed the traffic
  - Characterize traffic
- Results:
  - Determined that it is possible to create non-routable networks
  - vDistributed Switch complicates traffic analysis

Experiment 11: vSwap analysis

- Goal:
  - Identified vSwap as a potential source of memory
  - Leveraged existing memory tools to analyze vSwap
  - Determine what is stored in the file, when it was cached, and what relevant information can be gained
- Actions:
  - Attempted to acquire vSwap file
  - Attempted to populate vSwap file
  - Wrote c applications to over commit memory
  - Wrote randomizing memory access to force swap
  - Ran on several vms at once
  - Overcommitted total ESX memory by 8X
  - Attempted to characterize use case of vSwap population
- Results
  - vSwap remained unchanged
  - Using NFS, enabled detection of vSwap

Experiment 12: vmss file analysis

- Goal:
  - Analysis of the vm suspended file
  - Determine if any useful memory can be carved out
- Actions:
  - Suspend a VM through the vCenter web based management tool
  - Extract the .vmss file
  - Ran strings looking for known data
- Result:
  - This analysis was successful and yielded lots of information about the virtual machine's memory
  - Technique is limited

Analysis Results

- Realized the benefits of using ESX over ESXi for forensics
- Sleuthkit failed
- Determined that upon deletion vSphere does not zero-out deleted files
- Developed method to mount vmfs datastore (non-disruptive) manner
- Limited support for USB dongles
- Snapshots can prevent artifacts from being found
- Higher reliance on network traffic
- Network evidence is more pertinent
- Memory forensics will change

Conclusions

- Cloud computing is a disruptive technology for digital forensics

- Traditional tools are not useful in the cloud Inode analysis
- vmfs is currently unsupported by the digital forensics community
- Paradigm shift
  - Memory, acquisitions, …
- Increase reliance on incident response

Conclusions

- “Gorilla warfare”
- Cloud computing poses a challenge due to provision polices
- The digital forensics industry will be impacted
- Predecessors of cloud technologies have not considered the impact of incident response/digital forensics

Agenda

- Introduction to Cloud Computing Security
- Cloud Computing Implementation Considerations
- Role Based Access Control and Demo
- Cloud Computing Forensics
- **The Future of Cloud Computing Security**

Future Directions

Questions

http://www.sandia.gov

http://scl.cs.nmt.edu

doshin@nmt.edu

wrclayc@sandia.gov

veuria@sandia.gov