Cloud Computing Security

Fuzzy Computers Lead to Fuzzy Protections

Alex Stamos, Partner

February 19th, 2009

iSEC PARTNERS

Our Discussion Today

- What is Cloud Computing?
- Cloud Computing Models
  - Cloud Services (Google Apps)
  - Custom Cloud Applications (Salesforce)
  - Virtual Machines (Amazon EC2)
- Security Impacts
  - Technological
  - Policy and Roles
  - Legal and Compliance
- Some unfounded predictions
- Discussion and Q&A

iSEC PARTNERS

Ground Rules

- I would like your feedback and experiences
  - This talk should grow every time I give it
- This is an explanation of security model changes and not a vuln list
- These companies were chosen because they are leaders and good examples of the different models
  - Not trying to beat up on anybody
  - Issues with the model are more important than specific bugs

What you should take away

- Cloud computing models vary widely, as do their security implications
- Traditional security architectures and processes are insufficient with dealing with cloud-based infrastructures
- Major legal and regulatory issues remain in this field
- Current cloud computing technologies are not mature enough for a proper judgment of risk

Who am I?

- Co-Founder and Partner at iSEC Partners, Inc.
  - Founded in October 2004 from @stake
  - ~35 people, offices in SFO, SEA, NYC
- Application security researcher
  - Mobile applications
  - Cloud infrastructures
- Frequent Speaker and Author
  - BlackHat, CanSecWest, OWASP AppSec, MSFT BlueHat, Web 2.0 Conf, ETech, ISSA, ISACA
  - Hacking Exposed Web 2.0, Mobile Application Security

iSEC PARTNERS

What is Cloud Computing?

Why do people like Cloud Computing?

What is scary about Cloud Computing?

The basic security problem.

What is Cloud Computing?

A) A new buzzword to attract VC

B) Way to monetize the sunk cost of lots of machines in your datacenter

C) A revolutionary new idea in computing

D) A very confusing suite of technologies for security teams

E) All of the above 

iSEC PARTNERS

What is Cloud Computing?

- Nebulous by definition (puns are too easy)

- Generally means:
  - Lots of general purpose hosts
  - Central management
  - Distributed data storage
  - Ability to move applications from system to system
  - Low-touch provisioning system
  - Soft failover/redundancy

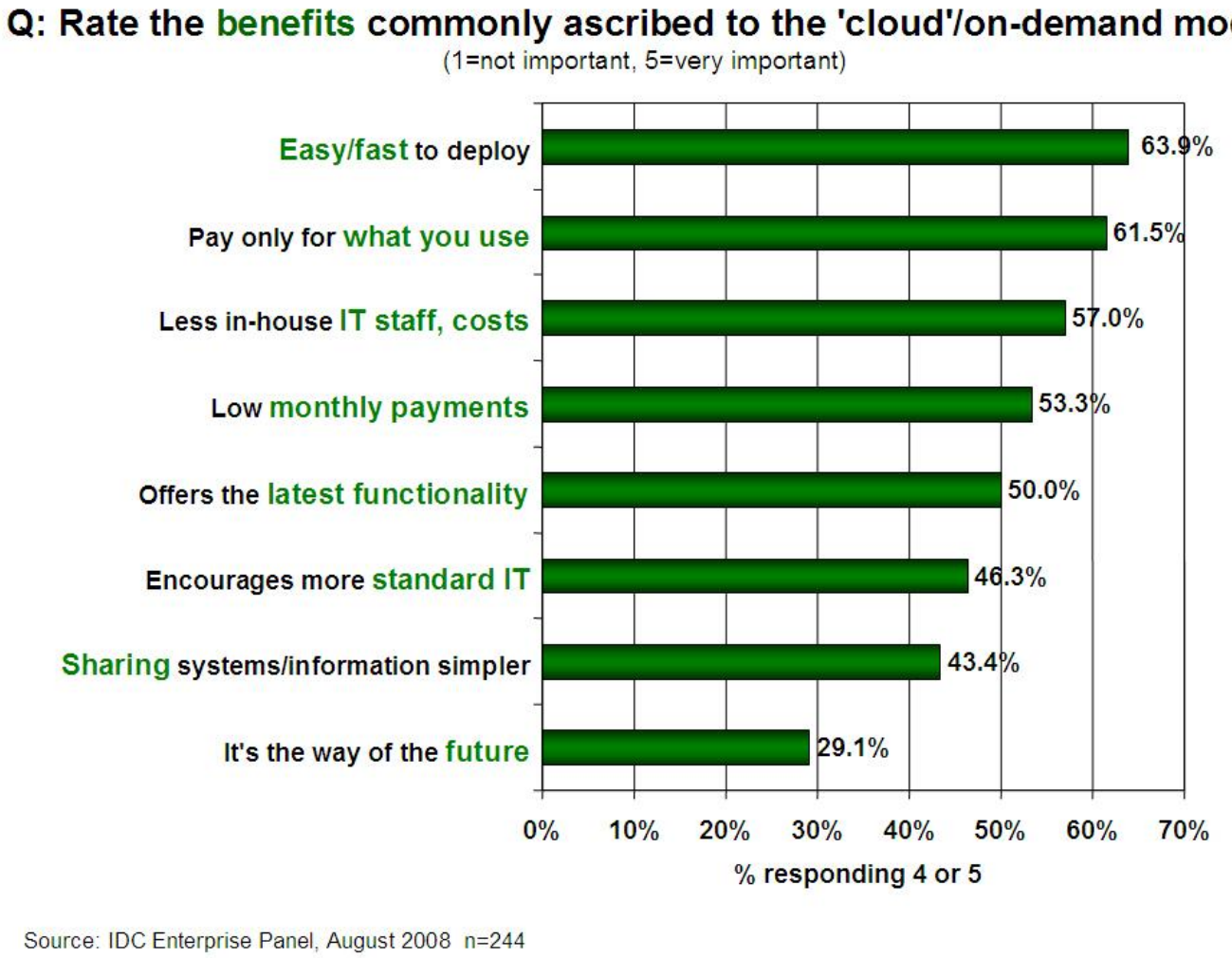
Two Genres of Cloud Computing

- Internal Enterprise IT
  - Lower management costs
  - Quickly re-provision resources to meet needs
  - More efficient use of idle resources
  - I have some experience here. Turns out to be hard.

- Third party hosted
  - Allows you to use somebody else's investment
  - Easy IT bootstrap for a new company or product
  - Very quick provisioning
  - When you are done, no costs

iSEC PARTNERS

Why do people like Cloud Computing?

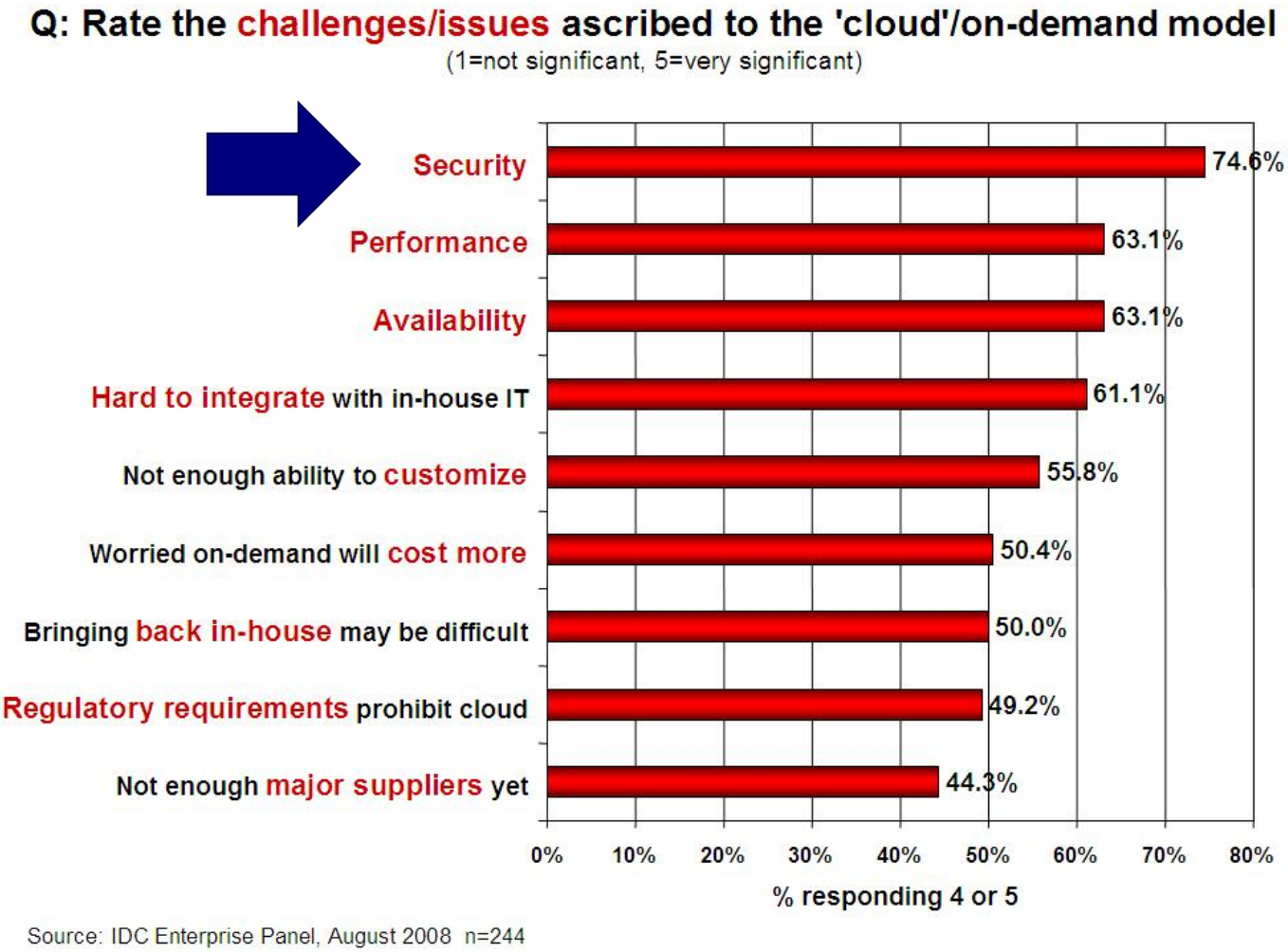


Source: IDC Enterprise Panel, August 2008 n=244

http://blogs.idc.com/ie/?p=210

iSEC PARTNERS

What is scary about Cloud Computing?



http://blogs.idc.com/ie/?p=210

iSEC PARTNERS

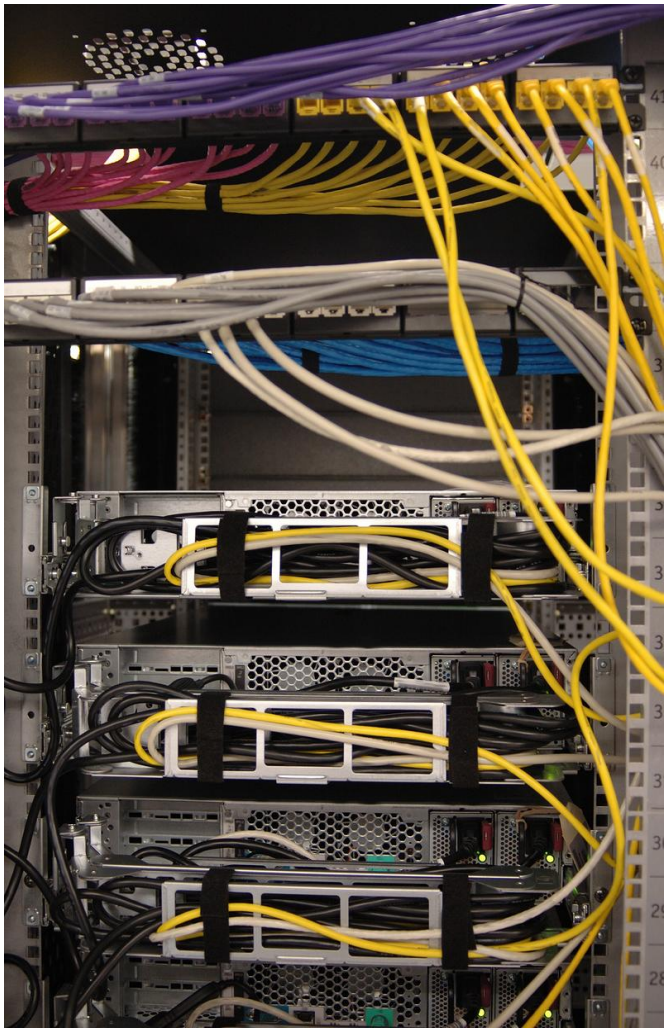
The Basic Security Problem

- The key selling points of cloud computing create security tension
  - Easy deployment/cloning == monoculture
  - Ease of management == single point of security failure
  - Easy movement of resources == lack of segmentation
  - Other people's infrastructure == trusting those people
- Complexity and inefficiency in a datacenter can serve as an unintentional security precaution
  - Hackers are human too
  - Multiple platforms and technologies means changing up your game and having wide skillsets

iSEC PARTNERS

Traditional Computing - Barriers

- What are the attack vectors into these systems?
  - Network port
  - Console port(s)
  - Physical access to storage
- Where is the data?
  - Direct attached storage
  - SAN
  - NAS
- Barriers are obvious
  - Like the metal case!

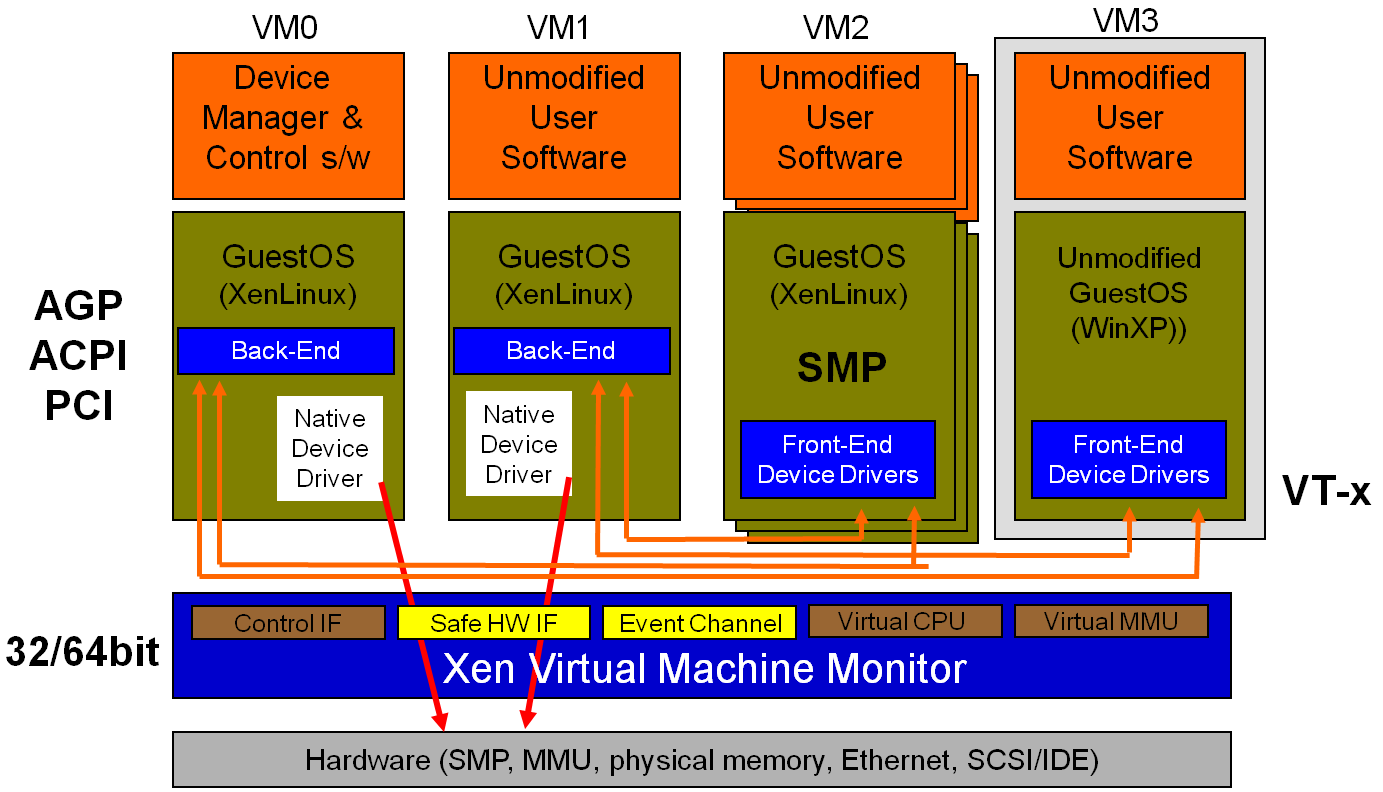


iSEC PARTNERS

Cloud Computing - Barriers

- How about here?

Xen 3.0 Architecture



Xen Summit Status Report
http://www.cl.cam.ac.uk/netos/papers/ian-status.ppt

Cloud Computing Models

- Cloud Services (Google Apps)
- Custom Cloud Applications (Salesforce)
- Virtual Machines (Amazon EC2)

Cloud Computing Models

- The differences between models are ~~cloudy~~ murky
- Honestly, the three listed models are generalizations and differ from how others categorize cloud computing
- We are mostly concerned about the different security models

iSEC PARTNERS

Cloud Services

- For years, we have been hearing how stand alone PCs/servers will become useless

"The network is the computer…"

- The last several years have made it possible to spend your day without storing local data
  - Online office suites
  - Web mail
  - Death of thick client consumer apps

iSEC PARTNERS

Cloud Services

- Google is pushing this hard with Apps for your Domain
- GMail was the start, now you can also have:
  - Calendaring
  - (Kinda) Intranet
  - Private Video Hosting
  - Office suite with collaboration
  - Chat
- Targeting a whole stack of Microsoft products:
  - Office
  - Sharepoint
  - Exchange

iSEC PARTNERS

Cloud Services

- Plenty of players in this space
  - Productivity Suites

  - Online Collaboration

iSEC PARTNERS

Cloud Services - Security

- Really SaaS, but using that Cloud word sounds better
- Most of the security concerns in this area fall into "control of data"
  - Are you a competitor to the provider? Will you be?
  - Who at the company has access?
  - Legal ownership of data
- App and Network security is important, but not your problem in this model
- Accessing your most important secrets over the public web rankles IT departments a bit
  - VPN, tokens, perimeters? What are those?

iSEC PARTNERS

Custom Cloud Applications

- SaaS is great for well defined products, but if you want to host your own application…

- A number of vendors will host your application in a pre-defined app server environment

iSEC PARTNERS

Salesforce Hosting

- Salesforce has been a leader in SaaS
  - Full Disclosure: also a client of ours
- Figured out and exploited the frustration with Enterprise software packages early on
  - $500K for CRM? How many servers does it need?
- A major competitive advantage of big CRM systems was interoperability
  - Needed a way to allow 3rd parties to extend their platform

iSEC PARTNERS

Salesforce Hosting

- Several different integration methods
  - AppExchange
  - Standard web services, SOAP
- You can also host your app on their servers
  - Two basic technologies
    - APEX: Strongly-typed programming language, Java-esque
    - VisualForce: GUI layout framework
  - Also provide data storage with Force.com DB
- Idea was based around CRM integration, but not required anymore

iSEC PARTNERS

Hosted Application Security

- All of the standard data security concerns apply
  - Who owns it, forensics, etc…
- New concerns:
  - Front-end attacks against same-origin
  - Attacks against the Application VM
  - Vulnerabilities in the web app server

Hosted Application Security

- Interpreted Languages vary greatly in VM security
  - Java and .NET: Built to withstand nasty bytecode
  - Python, Ruby and PERL: Not so much
- My colleague Justin Ferguson demonstrated a new Python issue that caused a AppEngine vuln
  - This is a large an mostly unexplored area of research
- Attacks against the VM might get you…
  - Access to other user's data
  - Access to host machine
  - Access to other running processes

iSEC PARTNERS

Hosted Application Security

- Still, there are potential security benefits to this model
  - Don't have to worry about patching and network security
    - Trust but verify
  - App Server engine could provide security benefits

- Salesforce has aggressively tried to add magic web security protections
  - CSRF, XSS, Injection Attacks, Access Controls

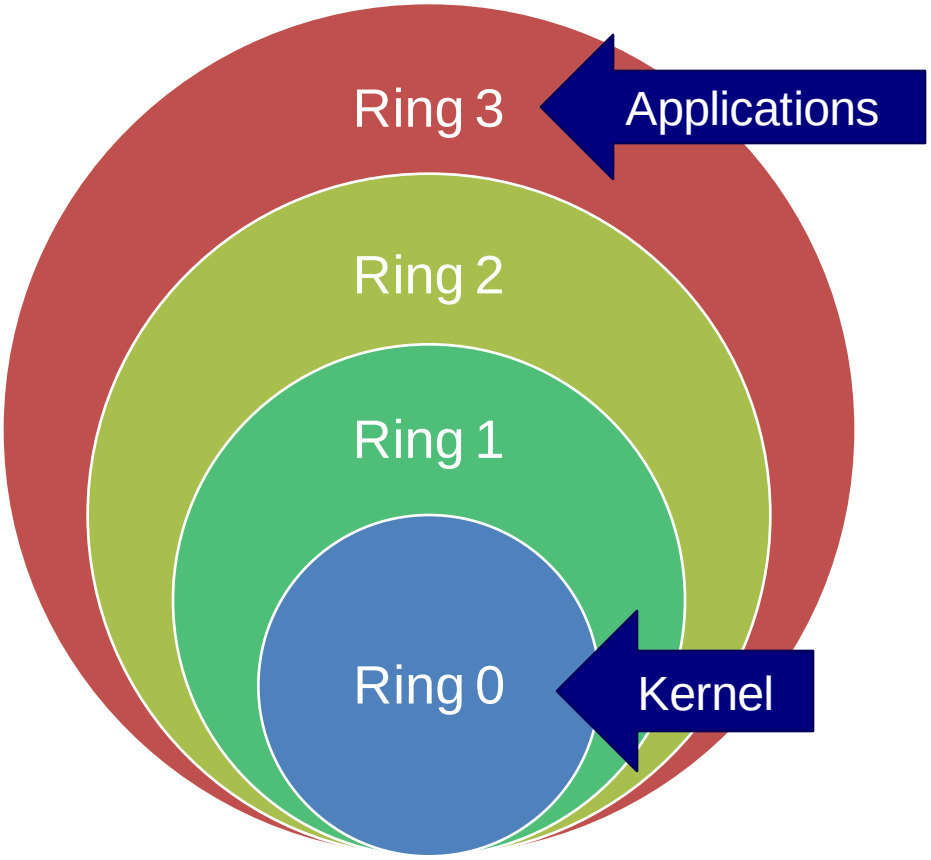
iSEC PARTNERS

Virtual System Hosting

- A natural evolution from internal IT virtualization
- Several different types of services fall into this category
  - Virtual machine hosting
  - "Cloud enable" data storage
  - Automatically provisioned physical servers
- Virtual hosts are mostly based off of existing VM technologies

Virtual Machine Security

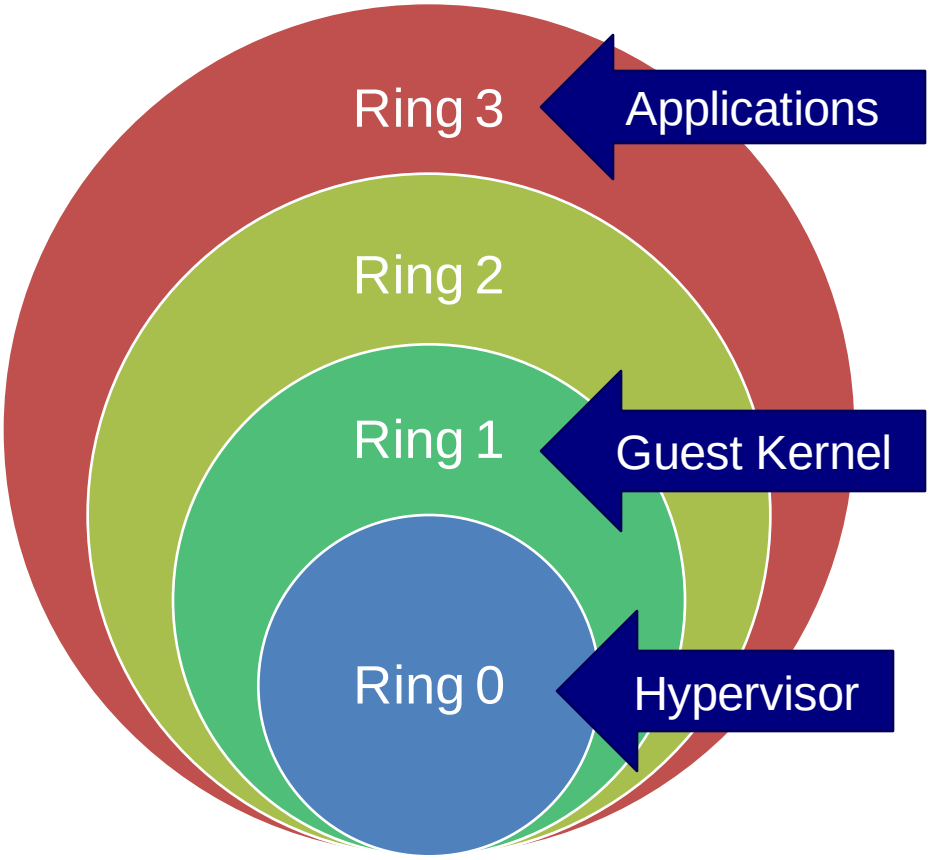
- Let's talk about the x86 privilege model



iSEC PARTNERS

Virtual Machine Security

- How does Xen do it?



iSEC PARTNERS

Virtual Machine Security

- How can VM hosts be attacked?
  - Missed privileged instruction
    - Re-write error
    - Bad masking with VT-x
  - Vulnerabilities in device drivers
    - Software implementation of devices can contain flaws
    - Becoming more interesting with paravirtualized hardware
  - Host-client bridging mechanisms
    - VMWare Tools
    - AMI Tools
    - Xen hypervisor calls
- Lots of interesting research in this area

iSEC PARTNERS

Amazon Cloud Services

- The bookstore is dominating the cloud
  - Broadest array of offerings
  - Most mature developer environment

- Amazon Elastic Compute Cloud (EC2)
  - Virtual server instance hosting
  - SOAP interface for management
  - XEN based
    - Linux paravirtualized
    - Windows 2003 now offered (VT-x?)

iSEC PARTNERS

Amazon Cloud Services

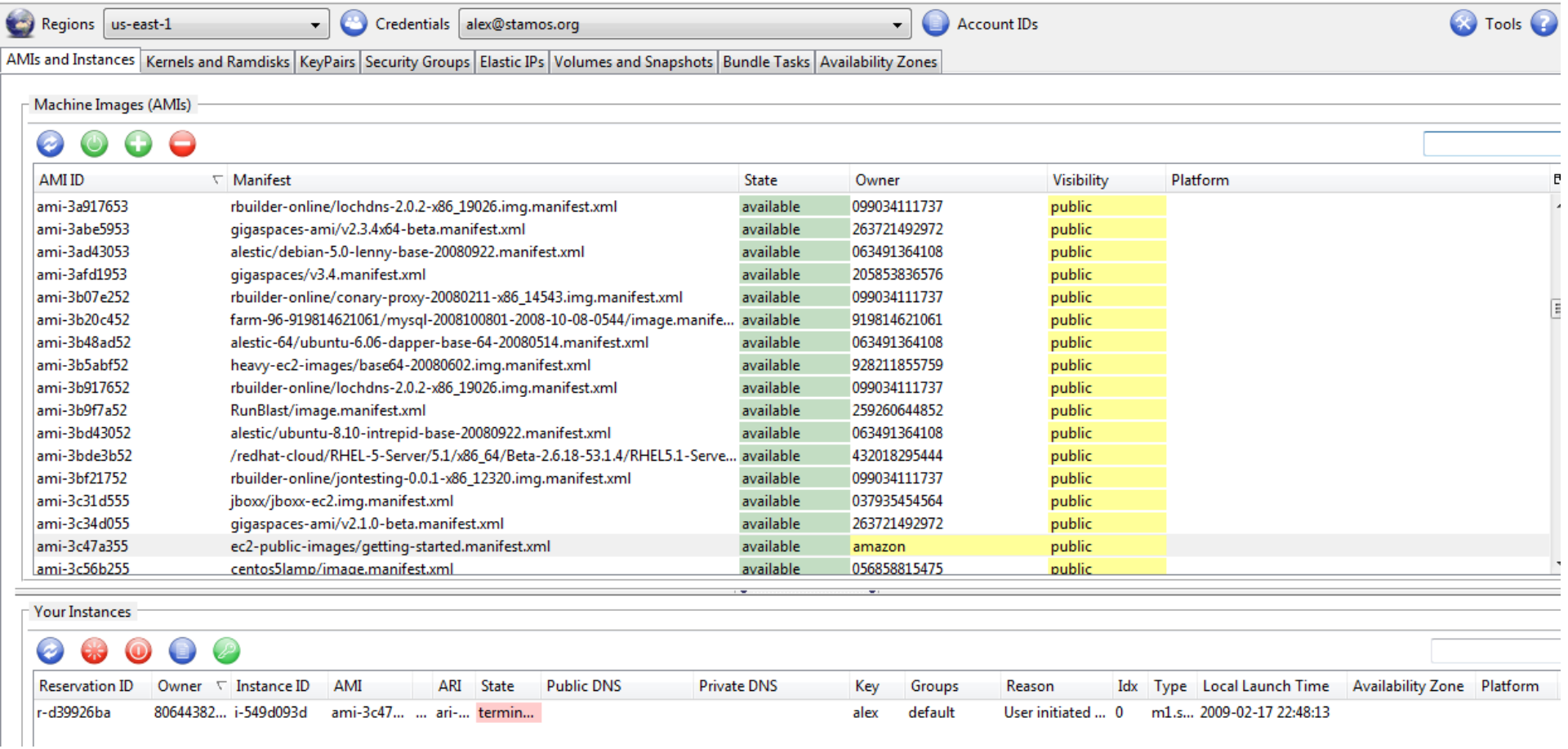
- Amazon Elastic Block Store (EBS)
  - Block devices attached to EC2 instances
  - Support snapshots, cloning
  - Magic replication, optionally across continents
- Amazon Simple Storage Service (S3)
  - File based storage service
  - Where EC2 instances live
  - HTTP/HTTPS access, custom protocol
  - Can be made public
  - Simple access control support

iSEC PARTNERS

Amazon Cloud Service

- Amazon Simple DB (SDB)
  - Simple, non-relational database
  - Structured query API, not SQL
  - Coarse-grained access controls
  - All the magic cloud redundancy

Amazon EC2 Interface



iSEC PARTNERS

Amazon Specific Concerns

- Same password buys books and manages your infrastructure. A bit disturbing.
- Network segmentation is not easy, unlikely to be used much
- Much less fine-grained access controls than enterprise VM platforms
- HTTPS optional for many things
- XEN hypervisor is a big target
- Lots of pre-made AMI images from untrusted folks
  - Like downloading your OS from warez.ru

General Cloud Hosting Concerns

- Cloud computing makes it easier to provision systems, not much easier to manage
  - Hardening
  - Patching
  - AuthN and AuthZ
- Can create a monoculture
  - 500 VMs with the exact service settings and patch level can make a target rich environment
  - Need to watch for private key-like issues with non-Amazon VMs

Amazon EC2 Bugs

- Two interesting flaws since launch, perhaps indicative:
  - SSH Key cloning
  - Authentication scheme break

- Just as with virtualization, security response is immature
  - OSes not designed to be cloned securely
  - Disconnect from hardware can cause issues
    - Where do you get your /dev/random?
  - No standard protocols for interfacing with cloud controls

iSEC PARTNERS

Security Impacts

Technological

Policy and Roles

Legal and Compliance

Technological Impacts

- Cloud computing introduces a new relationship to the security model, between application and host
  - In traditional enterprise architectures, most machines are dedicated to a single application
  - Equivalent of what VM infrastructure has introduced
  - Security barrier at hypervisor or language VM

- Client->Host Attacks
  - Emerging threat for hosted solutions
  - Research from hypervisor security is applicable

Technological Impacts

- Host->Client Attacks
  - Host always wins, for now…
- Might be possible to harden your applications using DRM-like technologies
  - Encrypted databases
  - Obfuscated code
  - Many levels of in-process memory encryption
- VMWare has been doing some research on application security on compromised Hosts
  - *Towards Application Security on Untrusted Operating Systems* by Dan Ports and Tal Garfinkel , HOTSEC '08

iSEC PARTNERS

Policy and Roles

- Policy and process is turned on its head with a cloud computing environment
  - What is your new standard architecture?
  - What is the host hardening process when you can clone a machine 100 times with a button push?

- Incident response is quite different
  - In many ways, easier to do forensics on VMs
  - Gathering off-machine data will be very difficult
  - Need forensically sound processes worked out with the providers

iSEC PARTNERS

Policy and Roles

- Roles
  - Half of traditional security roles are at the cloud provider
    - Network, host, physical security is outsourced
    - This is good if their people are better!
  - Providers are going to need to get better at integrating with client security teams
    - Who ya gonna call?
    - Incident responders need to practice on the cloud
- So don't worry, your security job isn't going away

iSEC PARTNERS

Legal and Compliance

- Legal issues abound
  - Uptime SLA
  - Security SLA
  - Insurance
  - Ownership of data
  - Data retention policies
  - Legal interference, subpoenas, NSLs

- Read the user agreements for these services, if you dare…

iSEC PARTNERS

Legal and Compliance

- How do you delete data in the cloud?
  - SSNs, CCs, HIPPA
  - Lots of companies end up with radioactive bits
- We have had several clients with this issue
  - Traditional forensics investigation
  - Automated data deletion and free-space wiping
- Cloud storage is intentionally murky about physical location
  - Deletion on distributed file systems is always lazy, garbage collection is unpredictable
  - No way a smart expert can swear "this data is gone"

iSEC PARTNERS

Legal and Compliance

- How many of these bullets can you even answer in the cloud?

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

iSEC PARTNERS

Legal and Compliance

- Auditing your cloud infrastructure is complicated
  - How do you pen-test a hosted solution?
    - Get permission from provider. Unlikely.
    - Test VM in your own network.
    - Test app-level only and hope that's legal.
  - Difficult to get your auditor access to provider security staff

- Compliance regimes need a "cloud provider" certification
  - For example: "Amazon EC2 was awarded the PCI DSS Cloud Gold Checkmark of power…"
  - Split network/host audit from client OS and applications

iSEC PARTNERS

Predictions

- Cloud computing is an irresistible management-level IT meme and will overwhelm us in the next 5 years
- Security standards will have to adapt to build secure cloud infrastructures
- Traditional ideas of segmentation are out the window
- Enterprise software will start to protect against untrusted-host attacks
- We will see another embarrassing cloud computing flaw in the next year
- Watch Windows Azure. Microsoft already has a lot of these basic technologies in the bag

iSEC PARTNERS

Conclusion

- Cloud computing brings many great changes to traditional IT architectures
- Those changes are diametric to some security precautions
- Current cloud computing systems have unreliable security assurances
- Security professionals need to prepare to support internal and external clients

Thank you for coming

Q & A

alex@isecpartners.com

iSEC PARTNERS