

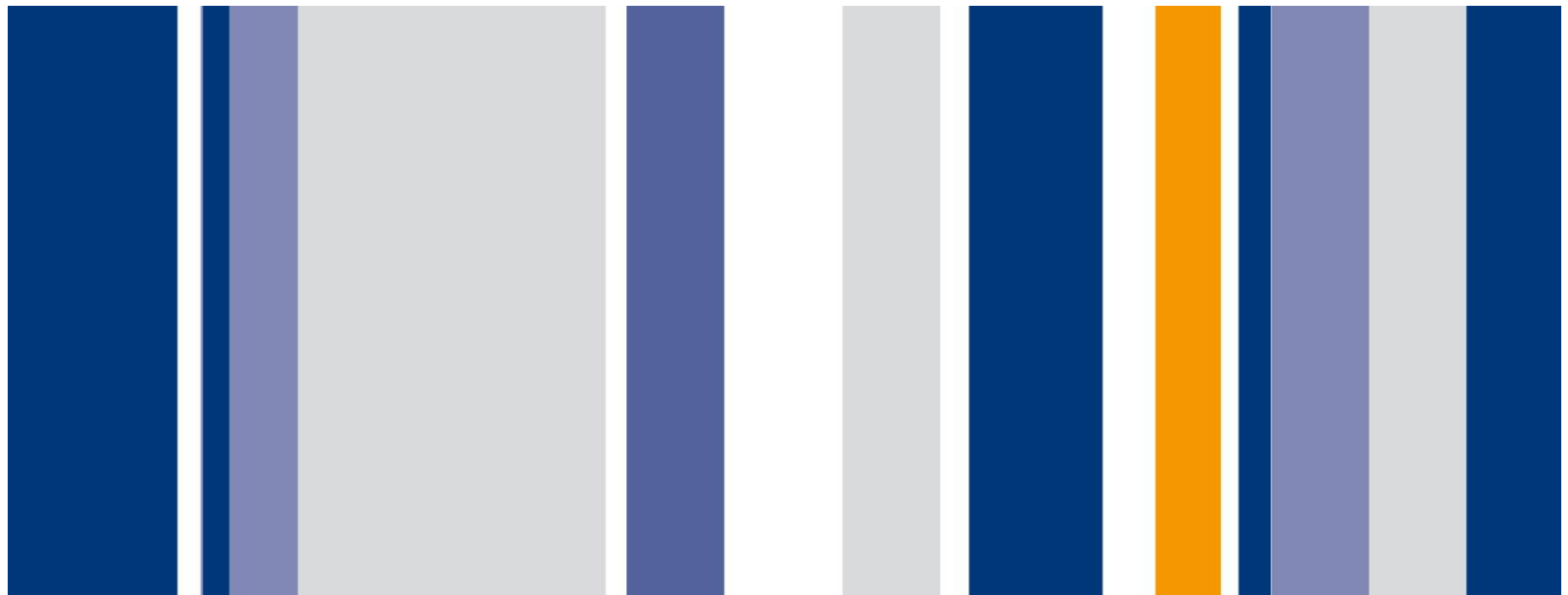
---

# Forecasting Cloud Vulnerabilities

Making Sense of Risk – January 2012

**Ian Shaw, Managing Director**

---



- Refresher on Cloud Computing
- Top Threats to Cloud Computing
- Conclusions and Forecast

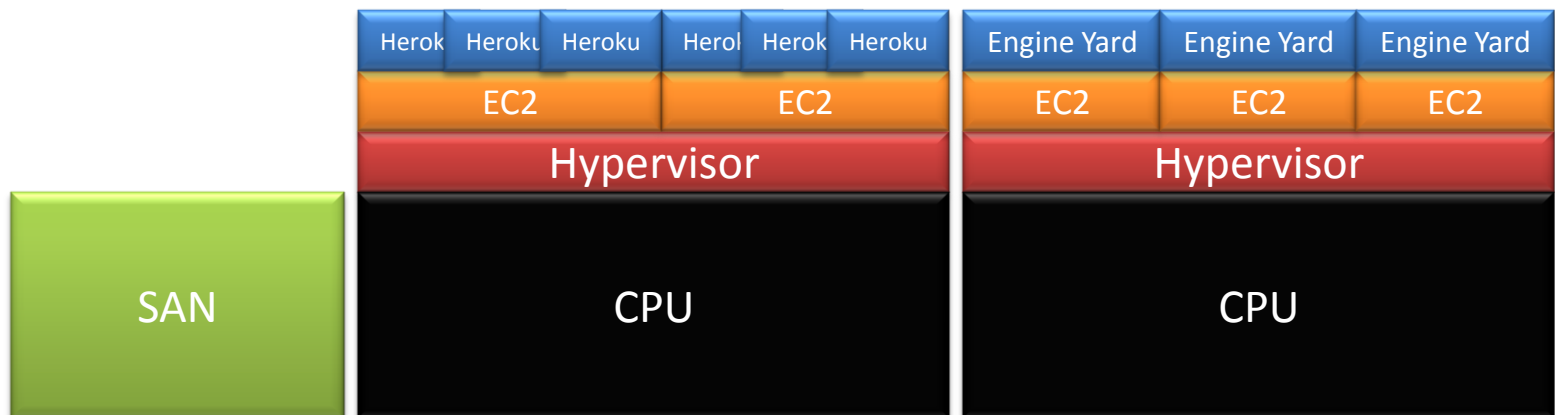
# What is Cloud Computing?

---

- Platform as a Service (PaaS)
  - .net, RoRails, Oracle
- Software as a Service (SaaS)
  - Think Google Apps, Salesforce etc.
- Infrastructure as a Service (IaaS)
  - Amazon EC2, Rackspace Cloud Servers
- Cloud Washing
- Ignoring Grid, Utility, etc.

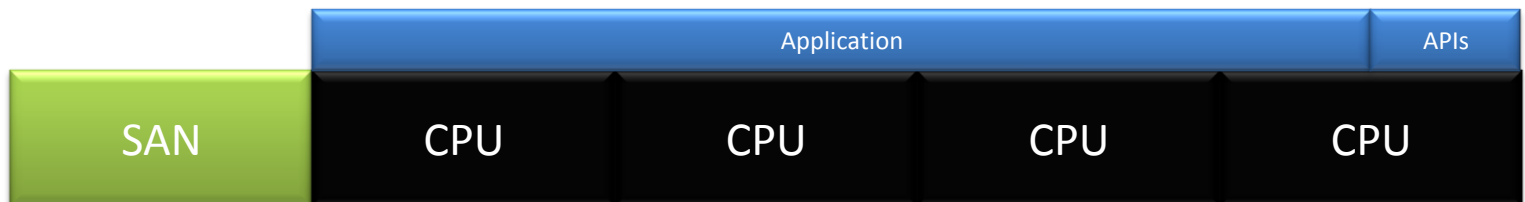
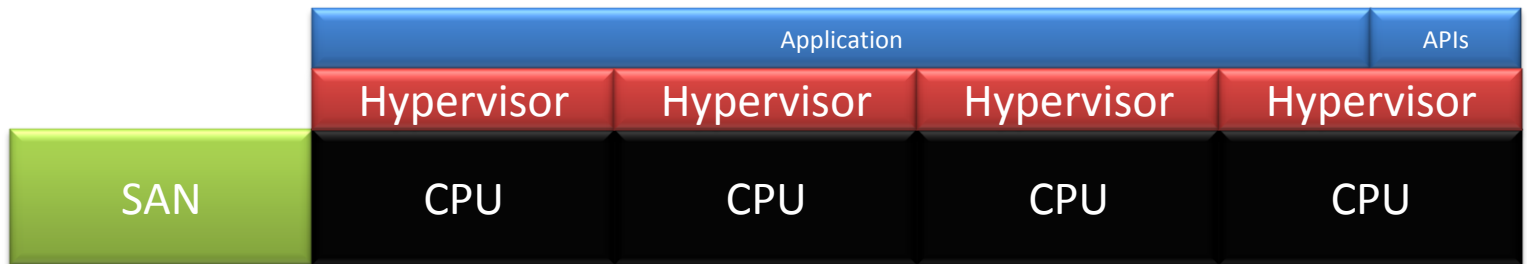
# Platform as a Service (PaaS)

## Example: Heroku / Engine Yard



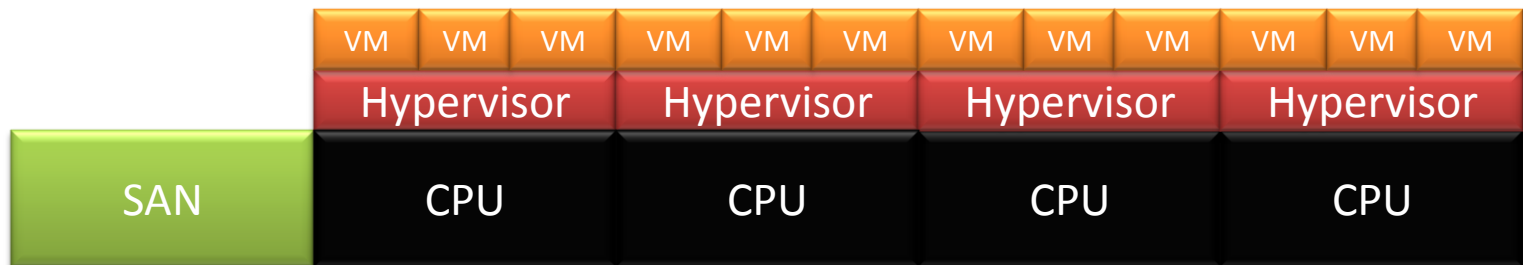
# Software as a Service (SaaS)

Examples: Office365, Salesforce, Google Apps



# Infrastructure as a Service (IaaS)

- Amazon EC2 / Rackspace Cloud Servers
  - VMWare
  - Xen
  - Microsoft Hyper-V



## CSA – Top Threats (Mar2010)

---

1	Abuse and Nefarious Use	Approach	
2	Insecure Interfaces and APIs	Approach	Research Example
3	Malicious Insiders	Approach	
4	Shared Technology Issues	Approach	Research Example
5	Data Loss or Leakage	Approach	
6	Account or Service Hijacking	Approach	
7	Unknown Risk Profile	Approach	

Top Threats to Cloud Computing V1.0, prepared by the Cloud Security Alliance (March 2010)

- Hosting of Botnets
- Hosting of Trojan Horses
- Distribution of Malware (Drive by Attacks)
- CSA: Primarily Applies to PaaS and IaaS environments

(Secure) Business as Usual

## Insecure Interfaces and APIs

- Instantiate, start, stop and pause machines
- Create / modify machine images
- Manage storage devices
- Manage networking
- Manage security access

## Security of Management Interfaces

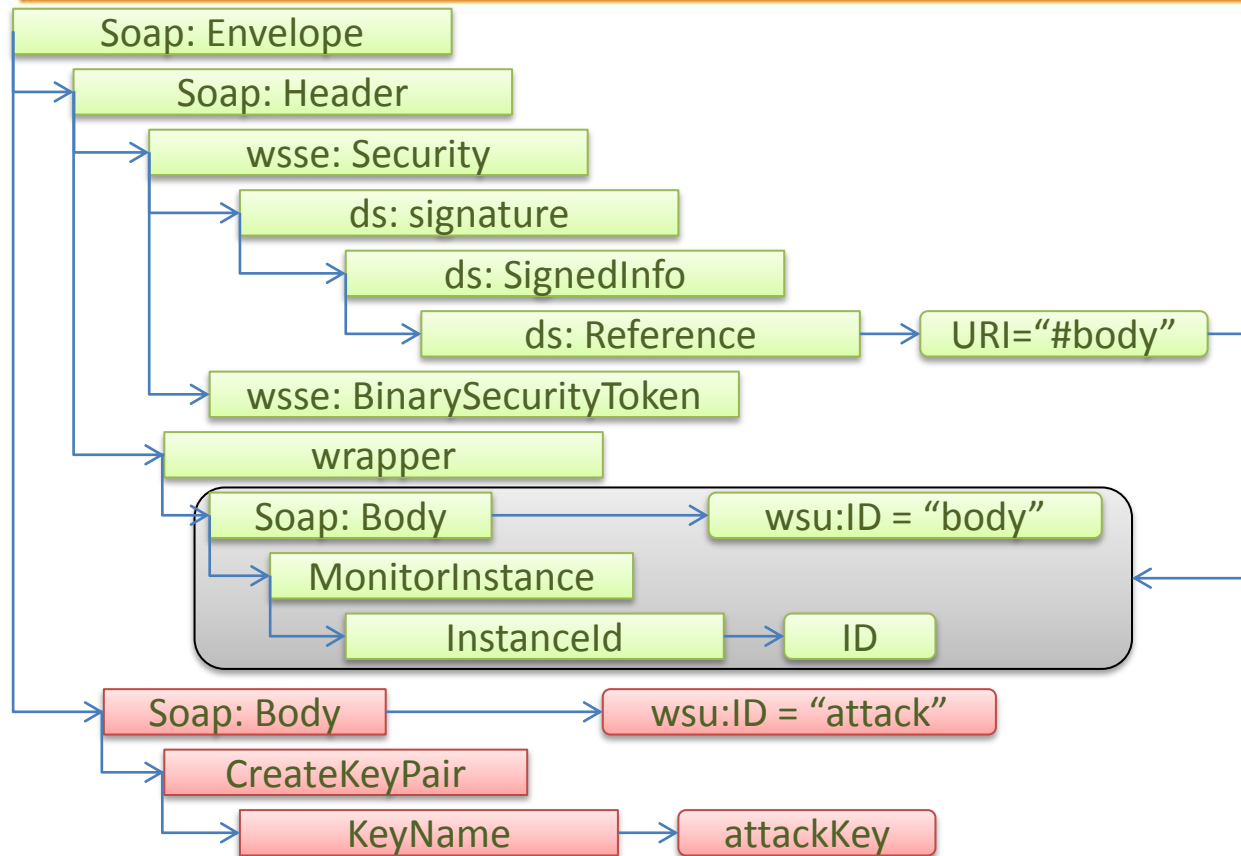
- Broken authentication
- Broken authorisation
- Message authenticity Issues
- Injection attacks
- XSS Vulnerabilities


- Excellent research out of Ruhr University Bochum – “All Your Clouds are Belong to us”
- Explores Amazon EC2 Management Interfaces both Web and Web Services
- Found XSS vulnerabilities in Management Interfaces – weakened by Amazon’s Authentication Model
- Successful signature wrapping attacks through vulnerabilities in the way SOAP parsers were used

- Elastic Compute Cloud (EC2) and Simple Storage Service (S3)
- SOAP- and REST-based Web Services
- Web Service provides same functionality as AWS Management Console
- WS-Security is deployed for integrity and authenticity of messages
- Vulnerabilities in Amazon EC2 SOAP Interface

- XML Signature Wrapping Attacks
- Takes advantage of the use of Tree (object reference) and Streaming XML parsers
- Malicious SOAP messages included two body elements. Only one of which was validly signed
- By including two `<wsu:Timestamp>` elements the researchers circumvented the ‘fresness’ test

# XML Signature Wrapping Attack



- Management interfaces are an attractive target and increase attack surface
- Two-Factor Auth (EC2 Opt-in) 
- Manage Users
- Rotate Keys and Passwords
- Encrypt Communications

## Malicious Insiders

- Cloud provider employees
- Third-party support providers
- Employee access
- Not other cloud customers (that's malicious access)

It's outsourcing, so are they:

- Security certified e.g. ISO27001
- Vetting employees
- Contractually committed

Your employees

(think logging and monitoring)

## Shared Technology Issues

- Escaping (to) the Hypervisor
- Difficulty achieving (secure) segregation
- Implied trust relationships (same hardware)

- Administrative VM Vulnerabilities
  - Compromise config / mgmt console
- Local / Remote Administration Relationships
  - Used to attack Mgmt Console / Admin VM



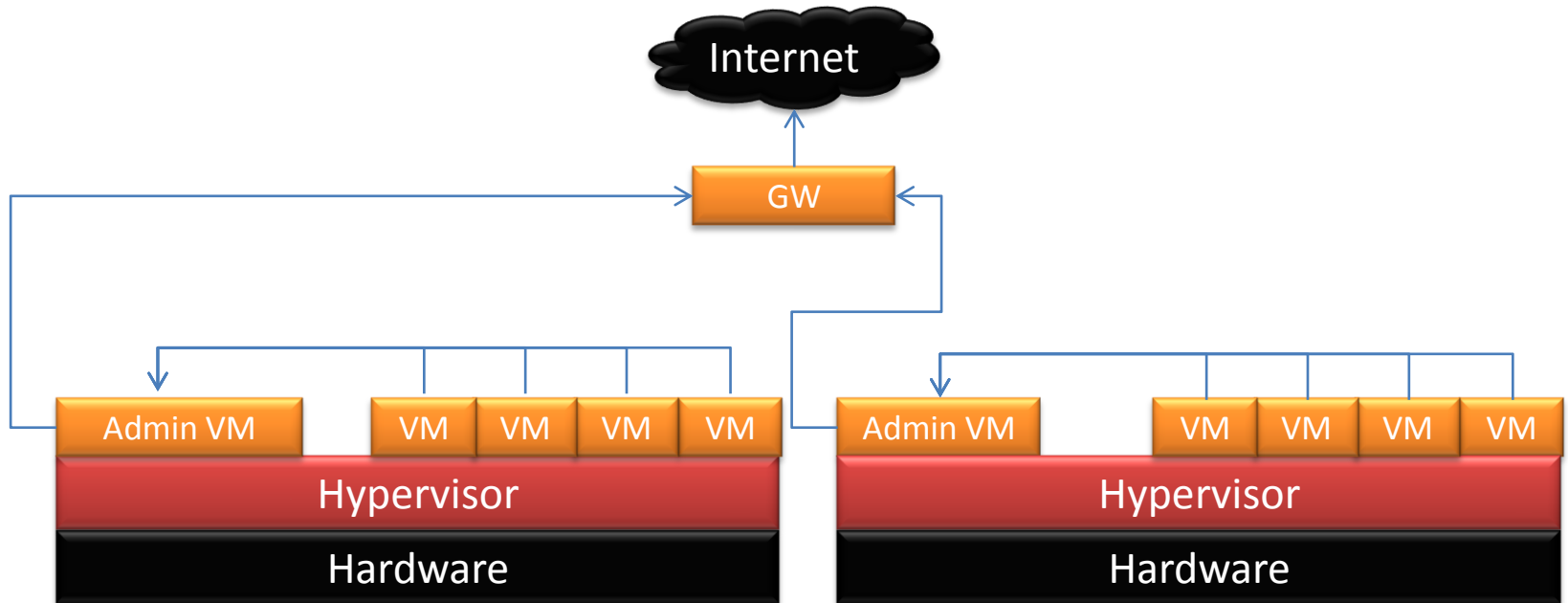
- Defence in depth approach
- Monitor for malicious activities in relation to the Hypervisor
- Ensure patching policy extends to Hypervisor environments

## Data Loss or Leakage

- Use of Encryption
- Persistent Storage
- Backups
- API Access Control
- Data in transit (including moving VM's)
- Key management

- Hey, You, Get Off of My Cloud – research from Ristenpart, Tromer, Schcham and Savage (MIT)
- Identify VM's residing on same hardware (EC2/Xen)
- Identify disk usage by other VM's
- Potentially for more fine grained attacks (looking at CPU usage)

# Xen Architecture



- Defence in depth
  - Design for security requirements
- Encrypt data in transit
- Implement and regularly review key management
- Look to ensure contractual controls for destruction of media, backup and log data

## Account or Service Hijacking

- Two-factor authentication (it's remote access)
- Manage account access (and audit)
- Deploy monitoring

- You are unlikely to be able to audit many of the cloud provider's claims
- It is new, there are likely to be new (classes of) vulnerabilities

## Unknown Risk Profile

- It's necessary to trust your cloud provider
- Ask for the scope in relation to statements of compliance
- Competition is improving security
- If you have leverage, use it
- Operate defensively

---

## Top Threats:

1. Lack of knowledge
2. Reliance on security of the cloud providers implementation
  - Management console / API
  - Hypervisor
  - Networking
3. Inability to effectively manage an incident

---

## References

- All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces - Heiderich, Somorovsky, Jensen, Schwenk, Gruschka, Iacono. 2011.  
(<http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/AmazonSignatureWrapping.pdf>)
- Guidelines on Security and Privacy in Public Cloud Computing – NIST  
([http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144\\_cloud-computing.pdf](http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf))
- Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds – Ristenpart, Tromer, Shacham, Savage  
(<http://www.cs.tau.ac.il/~tromer/papers/cloudsec.pdf>)
- Use of Virtualisation Products for Data Separation: Managing the Security Risks – CESG (Aug 2010)
- Top Threats to Cloud Computing V1.0 – Cloud Security Alliance (Mar 2010)
- Security Procedures – VMware vSphere 4.0 – CESG Augst 2011
- Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 – Cloud Security Alliance 2011