Inadequacies of Current Risk Controls for the Cloud

Name: Michael Goldsmith

Michael Auty, Sadie Creese and Paul Hopkins

Venue: CPSRT@CloudCom2010, Indianapolis

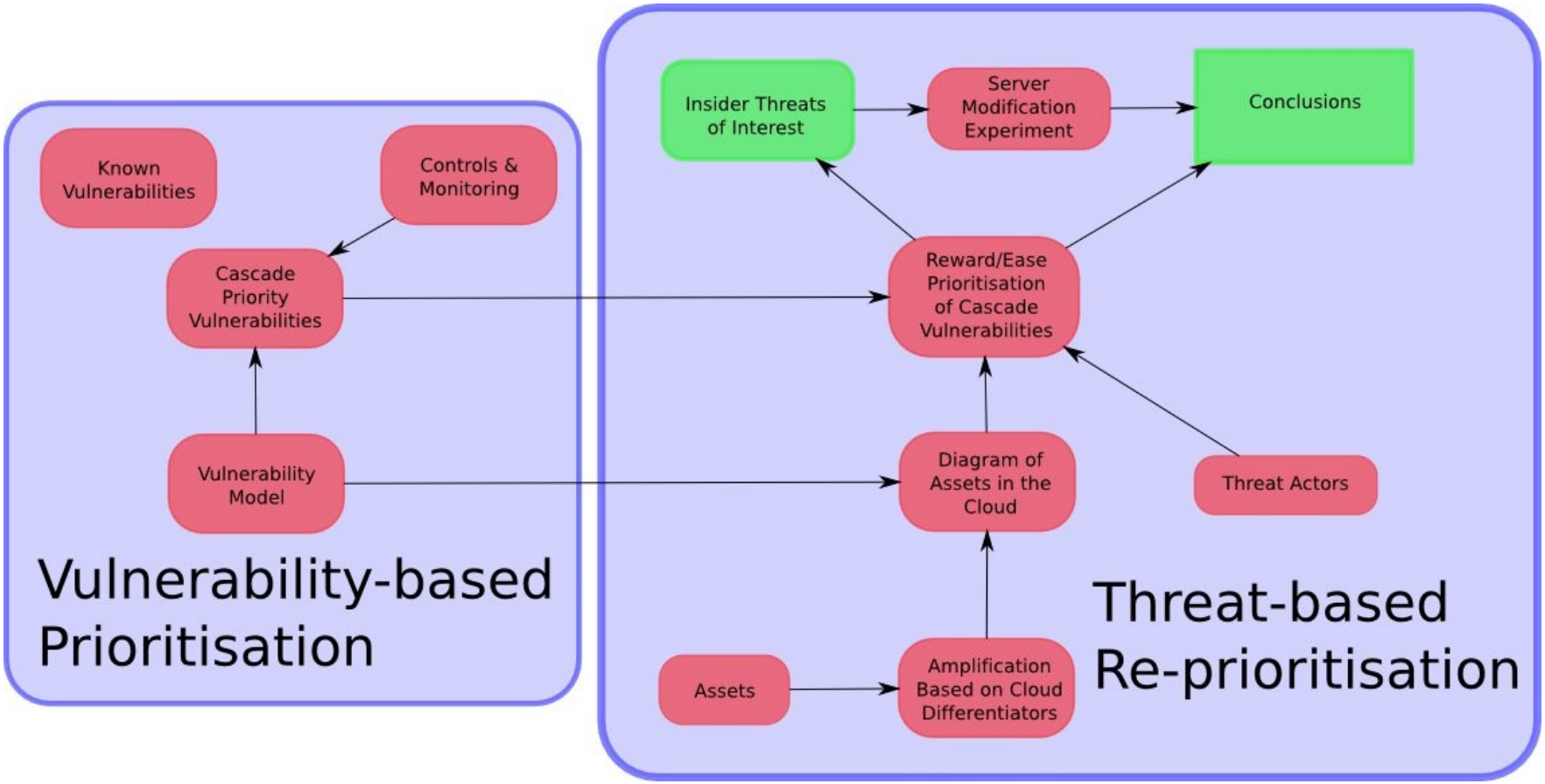
Date: 2 December 2010

Research supported by LOCKHEED MARTIN *We never forget who we're working for™*

THE UNIVERSITY OF WARWICK

WMG DIGITAL

Methodology to Identify High-Priority Vulnerabilities



Pre-Conclusion

Current Risk Controls Inadequate for Mature Public Cloud Ecology

Inadequacy of Current Security Controls

- Physical Controls
- Application Development and Maintenance
- Vulnerability Management
- Monitoring
- Identification and Authentication
- Access Control
- Encryption
- Continuity and Incident Management
- People
- Security Control Testing
- Accredited Components
- Obsolescence / Secure Disposal / Data Remanence
- Asset Management

Complete w.r.t. ISO27001/2

Physical Controls

- **Physical access and protection necessary for restricting access to software and hardware (assuring integrity of data, apps, services etc)**
  - For security testing and investigatory / audit functions
  - Best practice guidelines for outsourcing call for physical audits and certifications
- **In the Cloud this is problematic**
  - Data and applications stored on potentially untrusted and multi-tenanted machines – making the control potentially more important
  - Relationships may be short-lived and the ability rapidly and practically to verify physical controls of multiple cloud service providers becomes difficult to achieve
    - Relationships may even be only indirect and even unconscious, mediated by branded service provider

Application Development and Maintenance

- **Clouds currently offering proprietary development environments and variable service abstraction levels**
  - Limits portability of applications between clouds
- **Evidence that APIs are being standardised to achieve interoperability, but not the security controls**
  - Means that security aspects will require bespoke rationale which is costly
- **Unclear how integrity of codebase and intellectual property will be protected in the cloud**
  - Not a specific cloud challenge, but the physical location of code in a multiple-user 3rd party environment could make this more problematic
- **Current standard controls protecting code development and test environments involve strong access control, account management and logging may be difficult to achieve and remain portable**

Vulnerability Management

- **A single-patch or configuration change in a service or API could disable cloud deployed code**
  - Could result in unstable environments during patch cycles unless using shrink-wrapped application stack cloud service (although these can still be vulnerable)
    - but hesitation leaves them open to vulnerability exploitation
- **Patch management cycle not in the control of the cloud consumer**
  - And lack of control over patch cycles leaves the cloud consumer unable to close vulnerability gap on their own terms

Monitoring

- **Required for audit and compliance, but also to detect threat / attack.**
- **Unclear where and how logging and monitoring should take place**
  - VM, Hypervisor, hardware box, virtual sub-system (cloud user with multiple machines), cloud, between clouds (as machines move between providers)
  - How to cope with dynamism / tuning conflicts
  - Could it limit portability (takes time to tune)?
- **Who can / should access the log data and under what controls?**
  - And if cloud users can access log files are there privacy issues?
- **Can monitors be protected when physical separation of appliances may not be possible?**
- **Should a cloud be monitoring activities of users to detect malicious users?**

Identification and Authentication

- **Mobility requires interoperability of identification mechanisms, which will require ...**
  - An open question!
  - Focus on proprietary development environments may hamper progress

Access Control

- **Content delivery networks do not provide strong access control and authentication mechanisms**
  - But cloud service providers are off-loading large data files into these environments
- **Access controls can be created for cloud based services but are either entirely or partially under the administrative control of the cloud**
  - Even where cloud user has demanded administrative control of the service remotely the cloud provider will necessarily retain some controls over the hardware and consequently the software
- **Lack of interoperability of access control mechanisms across cloud environments may hamper portability**

Encryption

- **If doing anything other than storing data then it must reside in plain text at some point, making the lack of physical and administrative control over environment more problematic**
  - Cloud model may offer scope for enhanced use of data fragmentation, threshold cryptography, etc; but no sign of such technologies being adopted
  - Possibility of restricting unencrypted access to only tier-one supplier?
- **Full homomorphic encryption not practical yet, despite recent advances**
    - and PROCEED initiative, etc
  - Certainly not for petabytes of data!

Continuity and Incident Management

- **How to achieve continuity when depending upon a cloud supply chain will require maintaining state across multiple suppliers and through contract flow-down?**
  - Accountability of cloud service provider difficult for continuity as vanilla terms currently offered with limited opportunity for negotiation
  - Negotiation might achieve current best practice, but them limit portability within cloud ecosystem unless common terms can be agreed across a range or pre-determined providers
  - Difficult to check proper flow-down to ensure liability, antagonised when seeking high dynamism and portability
  - Ability to conduct investigations hampered by lack of access to physical location of assets, and entirely dependent upon cloud service provider cooperation
    - plus cross-jurisdictional issues!

People

- **Security Team**
  - Function will change to focus on subcontracts with cloud suppliers, organisational cloud policy and monitoring consumption of cloud against policy
- **Business Function**
  - Many current best-practice controls prevent workers from releasing data and interacting with third-party services now in control of cloud service provider
  - Usage of the cloud may make risk less tangible as it becomes common practice to move data outside the organisational boundaries (desensitising people)
  - Awareness and training material may need to change to take stock of new control architectures

Security Control Testing

- **Best practice involves assessing whole security of a solution (including system and wider environment), and imitating an attacker to measure potential for penetration**
  - No current professional practice for penetration testing a cloud service
  - Will cloud providers have concerns about the wider cloud infrastructure being impacted by the volume of testing required?
  - Will other tenants be concerned about such testing? What about privacy? What about potential performance or data losses?

Accredited Components

- **Unclear how this control can be applied in a cloud environment outside of Hypervisor elements (selected VM builds)**
  - Perhaps accredited storage modules?
  - Possible exploitation of Trusted Platform Module?
    - problem with both is with penetration of the provider market

Data Remanence / Asset Management

- **May be issues with data remaining in previously allocated memory, previously owned disk space**
  - But solutions possible and common with other uses of virtualisation
    - preliminary experiments suggest no actual problem
- **May be issues with decommissioning of hardware**
  - Hard to see how to implement effective controls when decommissioning is in the hands of each cloud service provider
    - but if transient problem reliably solved, extends to long-term release of resources
  - Will require asset management techniques capable of tracking uniquely configured virtual machines and data stores across a cloud infrastructure, which could be quickly replicated / replaced / tampered with as they are provisioned and de-provisioned

Thank you!

Questions?