de-risking the cloud through effective risk management

Paul Simmonds, Jericho Forum co-founder & Board Member
Key Publications

Cloud Cube Model:
Selecting Cloud Formations for Secure Collaboration

Jericho Forum Commandments

 CSA Security Guidelines 2.1

Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

Prepared by the Cloud Security Alliance
December 2009

Jericho Forum Commandments

The Jericho Forum commandments define both the means and the principles that must be observed when planning for a dependable service. While building on "good security," the commandments specifically address those areas of security that are necessary to deliver a dependable service. The commandments serve as a benchmark by which concepts, solutions, standards and systems can be measured and compared.

Fundamentals

1. The scope and level of protection must be specific and appropriate to the needs at risk
   a. Business goals determine security levels and costs of failure.
   b. Where security is a concern, customers must participate in the determination of protection, technical controls and the costs associated with them, and be informed of the levels of protection in place.
   c. In general, it's easier to prevent an attack than to recover from one.

2. Security mechanisms must be comprehensive, simple, scalable, and easy to manage
   a. Ensuring simplicity is a direct line to good security.
   b. Comprehensive security principles are required for all areas of the architecture.
   c. Security mechanisms must be flexible enough to accommodate changes at all levels.
   d. The combination of simple and effective, independent security "building blocks" used to be appropriate of being combined to provide the required security mechanisms.

3. Assume control of your part
   a. Security solutions designed for one environment may not be transferrable to work in another. Data is stored in a manner that makes it accessible to many sources within or outside the environment.
   b. Policies, mechanisms and issues may come from a variety of sources, including geographic, legal, network, and environmental.

Surviving in a hostile world

4. Devices and applications must be connected via open, secure protocols
   a. Secure through simplicity is a flawed assumption: secure protocols demand openness and thus enable interconnection.
   b. The security requirements of confidentiality, integrity and availability (calulating) should be understood and built into protocols and applications.
   c. Interoperability standards should be used where appropriate and not set aside.

5. All threats must be capable of maintaining their security policy on an open network
   a. A "security policy" defines the rules with respect to the protection of the data.
   b. Rules must be compiled with respect to each domain of control.
   c. Any implementation must be capable of maintaining its role (i.e., "on the open network," all not limited by any layer.

Cloud Cube
From Connectivity to Collaboration

- Full de-perimeterised working
- Full Internet-based Collaboration
- Consumerisation [Cheap IP based devices]
- Limited Internet-based Collaboration
- External Working [VPN based]
- External collaboration [Private connections]
- Internet Connectivity [Web, e-Mail, Telnet, FTP]
- Connectivity for Internet e-Mail
- Connected LANs [interoperating protocols]
- Local Area Networks [Islands by technology]
- Stand-alone Computing [Mainframe, Mini, PC’s]

Connectivity

Effective Perimeter Breakdown

Today

Business Value

Risk

Time
Understanding the externalisation of data

<table>
<thead>
<tr>
<th></th>
<th>Internal</th>
<th>De-perimeterised</th>
<th>External Collaboration</th>
<th>(Secured) Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Then</td>
<td>Data</td>
<td></td>
<td></td>
<td>Cloud: Computing performed within the Internet</td>
</tr>
<tr>
<td>Now</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Near Future</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Future?</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**De-perimeterisation:** The breakdown of the corporate border as a security control

**Cloud:** Computing performed within the Internet

The security of the network becomes increasingly irrelevant, and the security and integrity of the data becomes everything.
“The perimeter going away? That's baloney ....... The perimeter cannot go away and does not get less important in the future.”

John Pescatore, Gartner, 2005

Digital Natives

• New expectations from both employer and employee
• Characteristics for generation Y/M:
  – Individualists
  – Sceptic on authorities
  – Grown up with IT/Internet
  – IT is a social tool
• Collaboration is the norm
• Expectation of ”always-on”
• Just find it on the Web.
• More consumer software
Why Cloud?

- Logical conclusion of the business direction
- Cheap
- Fast to market
- Little capital investment (true cloud)
  - Start-ups
  - African virtual mobile operators
- Great for “off-load computing”
Jericho Forum Cloud Cube Model

**Dimension Four:**

- Insourced / Outsourced

- Location
  - Internal
  - External

- Architecture
  - De-perimeterised
  - Perimeterised

- Ownership - technology/services/code

“The Cloud”
Cloud Cube – Proprietary Axis - Risks

- Vendor Lock-in
- Reliance on vendor APIs
- Difficulty in collaborating?
- Proprietary standards?
- Proprietary software?
- Process-as-a-Service Solutions
- SaaS Solutions
Cloud Cube – De-perimeterised Axis - Risks

- Lack of open & secure standards
- Reliance on vendor APIs
- Issues extending Identity into cloud
- Lack of shared identity standards

Ownership - technology/services/code

De-perimeterised Architecture
Clouds & the Cloud Cube model

- The ‘commandments’ still valid for the cloud

- Hybrid Computing will be the norm
  (a mix of traditional and various cloud computing)
  - Private Clouds are Perimeterised
  - Collaborative Clouds are best de-perimeterised

- Select one of the eight types with care!
The Cloud Identity Crisis

- The Cloud won't take off fully without appropriate Identity Management and Access Management
- Private Clouds will be able to take advantage of the old Perimeterised Identity and Entitlement & Access Management models
- Collaborative Clouds will need a significant shift from Enterprise Centric security to User Centric Security
- Clouds also will benefit greatly from the shift from;
  - Access by Lists (Role-based Access Control), to;
  - Access by Assertions [Claims] (Rules-based Access Control)
Future Research

- RSA 2010 Awards
  *Excellence in the Field of Mathematics*

- Dr. David Chaum developed a cryptography research group at the Center for Mathematics and Computer Science (CWI) in Amsterdam. During that time Dr. Chaum founded DigiCash, which pioneered electronic cash innovation. Dr. Chaum’s contributions to cryptography include the invention of two anonymity networks – mix networks, the basis for virtually all modern anonymity networks and DC-Nets, including the invention of partial key techniques and the invention of cryptographic voting.
Risk Based Access

- Current access methods
  - Do not support business needs / granularity
  - Do not support “real” cloud working
  - Do not support the move the securing the data

- Trust but verify
  - Basic trust models for devices & users do exist
  
  *But;*
  
  - How do you verify environments you do not own?
  - How do you verify that environments you do not own are cleaned up after use?
Granular Access:
Access granted dependent on attributes and rules, not binary on Username

Device Attributes:
- User Credentials
  - Classification of User
  - AD Group
  - Credential strength
- Location
  - IP-Address
  - Geo-location
  - GPS / GPRS
- Device Information
  - Corporate Credentials
  - Corp. Managed Device
  - Functionality Required
  - Functionality Offered
  - Sandbox
  - Secure container
  - Cleanliness of device

Data Attributes:
- Location?
- Classification
- AD Group
- etc.

Rules based access:
Using a mix of attributed, based on risk assessment

Risk Based Access

Martini model¹: Any IP, any device, any time, anywhere
Conclusions

- De-perimeterisation still a relevant topic with plenty to be highlighted and addressed
- Commandments are both relevant and still relevant as we move to cloud issues
- There is a shift from Enterprise Centric to User Centric IAM
- Shift needed from RBAC & ACL’s to Claims based access