Identity the New Perimeter

Adrian Seccombe
Surrey University
25th March 2010
Key questions this session will answer

- Which are the key attributes of Cloud Types
- What are some of the key cloud choice drivers?
- Identify primary transformational **SHIFTS** required to enable a secure but collaborative clouds?
- Why does Identity and Access Management have to **SHIFT**?
To Cloud or Not to Cloud?

Traditional

“or”

Cloud
Let’s get real!

We are all “Hybrid” already!
Unfortunately...

- Our Business Partners are pressing ahead into the clouds, often unaware that they are!
- We are NOT architecting our way into the Clouds
- Seems like we’ve been here before...
  ... remember the early PCs?
- This is where the Jericho Forum Self Assessment Scheme will be able to help you...
Some Definitions

- **NIST** and the **Jericho Forum** have it wrapped!

  "**NNN as a Service**"

- **Essential Characteristics:**
  - *On-demand self-service.*
  - *Broad network access.*
  - *Resource pooling.*
  - *Rapid elasticity.*
  - *Measured Service.*

- **"Deployment Models"**
  - Public
  - Private
  - Community
  - Hybrid

- **"Cloud Cube"**

http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf
"NNNNNN as a Service"
Maturity of the Cloud Layers

Cloud Maturity Scale

- 1st: Infrastructure
- 2nd: Platform
- 3rd: Software
- 4th: Process
- Last!: Outcome / Value

Orchestration:

- Immature

Abstract occurs here!
The Cloud Cube revisited

Proprietary

Deperimeterised

Open

Perimeterised

External

Internal
The Cloud Cube revisited

- External
- Internal
- Proprietary
- Open
- Private
- New Perimeters
- Traditional Perimeters
Choose the Clouds with care!

• Private Clouds are Silos
  (Sometimes you need Silos)
• Proprietary Clouds Can Lock You In
• Internal Clouds are a Stop Gap
• Clouds with the Old Perimeters do not enable external collaboration
The key shifts

The Identity Shifts

Identity the new Perimeter
Privilege Management in Ten Words

Identification

Who are you?

- Identification: The presentation of an identifier so that the system can recognize and distinguish the presenter from other principals

Authentication

Prove it!

- Authentication: The exchange of information in order to verify the claimed identity of a principal

Authorization

You can access this stuff...

- Authorization: The granting of rights, including access, to a principal, by the proper authority

Principal: An entity (people, devices, applications, etc.) whose identity can be authenticated

Reference: Open Group XDSF (X/Open Distributed Security Framework), ISO 10181-3
Did you spot the gap?

Inside the Old Perimeter
• Identify: Who are you?
• Authorise: You are you
• Authorise: Have this!

Outside the Old Perimeter
• Principal declares Identity
• Identity Authenticated
• Resource Requested
• Resource Identified
• Resource declares Rules
• Rules verified
• User claims capabilities / attributes
• Claims verified
• Access Control Decision

Identity Shift #1 Resource Centric
“Identity” Lifecycle of a Resource

• Create Resource Identity
• Verify Resource Identity
• Set the Access Rules (eg Must be Over 18)
• Enable Rule Authentication
• Entitlement Check (Are you Over 18?)
• Verify Claim
• Evaluate
• Allow Access to Resource

Resource: Service, System, Code, Information
ISO Authorization Model

Diagram Courtesy Steve Whitlock

Asymmetrical

Principal
- Identity, Access Request
- Additional Attributes

Access Control Enforcement Function
- Access
- Decision
- Access Support Information

Resource
- Environmental, Resource, & Principal Attributes; Identifiers
- Policy Admin
- Rules
- Resource Labels

Relatively Dynamic
- Audit Logs

Relatively Static

Note
The Resource attributes are separate from the Resources. While the principals have attributes and a place to verify them.
Evolving Jericho Authorization Model

Principal
- Identity, Attributes
- Access Request
- Attribute Updates

Access Control
- Enforcement Function

Resource
- Identity, Attributes
- Access Request
- Attribute Updates

Access Control
- Enforcement Function

Note
The differences are subtle but key, Symmetrical Identity, Entitlement and Access Management
Evolving Jericho Authorization Model

Principal

Access Control Enforcement Function

Resource

Identity, Attributes Access Request
Attribute Updates

Access

Rules

Decision Cache

Request, Identity, Rules, Attributes
Decision Support Information
Verified Rules Verified Attributes

Access Control Decision Function

Environmental, Resource, & Principal Attributes; Identifiers

Audit Logs

Policy Admin

Note
The differences are subtle but key, Symmetrical Identity Entitlement and Access Management
Identity Shift #2

- Federated
  - Professionals
  - Customers
  - Organisations

- Traditional (Access Control List)
  - Enterprise
  - Partners
  - Suppliers
  - Collaborators
“Identity” Lifecycle of a Principal

• Create Identity
• Verify Identity
• Stake Claims (Set Identity Capabilities / Attributes)
• Verify Claims
• Use / Present Identity
• Authenticate Identity
• Request Resource
• State required Capability or Attribute (Claims)
• Authenticate Claims
Identity is the key to the Clouds

Old Frame
• Enterprise Centric
• Access Control List
• Directory Server
• Authentication Svcs

New Frame
• Principal Centric
• Resource Centric
• Rules Based Access
• Authentication Routing

An ACTION for you, to enable your SHIFT:
Get your architects defining and / or divining the Access Rules that apply to YOUR resources.
Hint: Keep them Simple!
And finally

• It's really all about the new perimeter.....

• ....the Identity Perimeter

• What are we Human’s or Ostriches?

• We have been complacent for too long!
• We need to bolster our defences at the same time as redesigning them.
• How best can we do that?
“I see no Clouds”