Using identity to empower your organisation

Paul Simmonds
JERICHO Forum® co-founder & board member
Agenda

- The businesses need for collaboration
- Securing the new collaborative architecture
- The need to separate identity
- What needs identifying
- Utilising identity within these new architectures
- Leveraging an assertion based model
- The need for a strong core identity
- Implication for SA Guidance v3.0
- Conclusions
Understanding the collaboration driver

Connectivity

Effective Perimeter Breakdown

Today

Stand-alone Computing
[Mainframe, Mini, PC’s]

Local Area Networks
Islands by technology

Connected LANs
interoperating protocols

Connectivity for
Internet e-Mail

Internet Connectivity
Web, e-Mail, Telnet, FTP

External collaboration
[Private connections]

External Working
VPN based

Limited Internet-based
Collaboration

Consumerisation
[Cheap IP based devices]

Full Internet-based
Collaboration

Full de-perimeterised working

Collaboration

Business Value

Risk.

Time
The security of the network becomes increasingly irrelevant, and the security and integrity of the data becomes everything.
The mantra of any good security engineer is: “Security is not a product, but a process.”

It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

Bruce Schneier
Today's Externalised Network

Corporate Intranet

Application Systems

Admin

General Users

VPN

Corporate (locked-down) Laptop “safely” extending applications outside

Allowing controlled access for partners
Secure application and strong identity allows granular access to both internal users and partners.
Key principles for Next Generation Identity

1. Identity must be separated from Access Management

   - An Identity solution must provide identity to multiple, disparate, Entitlement and Access Management solutions

   - Access Management must consume identity and entitlement from multiple sources.
Key principles for Next Generation Identity

Identity is not just about people

- Identity needs to encompass all objects that need to identify themselves
- This includes:
  - People
  - Devices
  - Code
  - Organisations
  - Agents.
Key principles for Next Generation Identity

3 Federation of existing IAM system will not scale

- Technically difficult
- n-factorial problem
- Transitive trusts problem
- Assertion (or claims) based solutions will allow scalability and flexibility.
IdEA: Identity, Entitlement, Access
Access granted dependent on assertions and rules & risk, not binary on Username

Entitlement
(Risk Based Access)

Resource
- Data and/or System

Logical / Data Access

Rules Based Access

Physical Access

Id / Attributes Asserted
- User Identity
- User Assertions
- Credential strength / trust
- Location Assertions
  - IP-Address
  - Geo-location
  - GPS / GPRS
- Organisation Identity
- Organisation Assertions
- Device Identity
- Device Assertions
  - Functionality Required
  - Functionality Offered
  - Sandbox
  - Secure container
  - Cleanliness of device
- Code Identity
- Code Assertions

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

Resource Attributes:
- Location
- Classification
- AD Group
- etc.

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

Bi-directional Trust²

1. Multiple Access Real Time IP Network Implementation 2. Jericho Forum Commandments #6 & #7
Attributes (or claims) to make risk based decisions

- “I am a qualified doctor” and
- “I want access to this drug data sheet”

- “I work for XXY organisation” and
- “I’m part of the “ZZZ” Project” and
- “I want to access the project area” and
- “I’m a device that can provide a secure sandbox”

- “I’m a British Citizen” and
- “I want to enter the UK”
Key principles for Next Generation Identity

4

Strong identity is key to trust and collaboration on the Internet

- The lack of Strong Identity is hindering adoption
- People operate with facets (or persona)
- Strong core identity (with a one-way trust) is key to making this work
- People must own their own core identity
- Escalating individual persona to a pseudo-core will fail.
Core Identity
Paul Simmonds

Security Professional

White Water Kayak Instructor
The need for a one-way trust

Multiple Facets

Refugee
<table>
<thead>
<tr>
<th>Facets (or Personas) of my Core Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security (IISP / Qualifications)</td>
</tr>
<tr>
<td>Kayak Instructor (BCU / Qual’s)</td>
</tr>
<tr>
<td>Scout activity instructor (CRB etc.)</td>
</tr>
<tr>
<td>Home Owner (Utility Companies)</td>
</tr>
<tr>
<td>Employee</td>
</tr>
<tr>
<td>E-mail (Account access &amp; sending)</td>
</tr>
<tr>
<td>Ethnicity / Religion / Sexual (SPI)</td>
</tr>
<tr>
<td>Parent / Husband / Child</td>
</tr>
<tr>
<td>Bank / Savings / Investments</td>
</tr>
<tr>
<td>National Health Service – Access</td>
</tr>
<tr>
<td>Citizen – Right of abode / Travel</td>
</tr>
<tr>
<td>Citizen – Taxpayer</td>
</tr>
<tr>
<td>Citizen – Council / Voter</td>
</tr>
<tr>
<td>Hotel – Customer / Loyalty</td>
</tr>
<tr>
<td>Airline – Passenger / Loyalty</td>
</tr>
<tr>
<td>Information Consumer (Web sites)</td>
</tr>
<tr>
<td>E-Commerce (i.e. Amazon)</td>
</tr>
<tr>
<td>Social Networking (i.e. Facebook)</td>
</tr>
</tbody>
</table>
The big lie of computer security is that security improves by imposing complex passwords on users. In real life, people write down anything they can't remember. Security is increased by designing for the way humans actually behave

Jakob Nielsen
Jericho Forum work in the CSA Guidance

- 2.1 – Cloud Cube model

- In Guidance 3.0
  - Move from IAM to IdEA
  - Cloud Cube model - unchanged
  - Entitlement into Application Design
  - Re-written Domain 12
    Identity, Entitlement & Access Mgmt
  - Identity as a Service in (new) Domain 14
DOMAIN 12
IDENTITY, ENTITLEMENT, & ACCESS MANAGEMENT

The concepts behind Identity, Entitlement, and Access Management used in traditional computing require fundamental changes in thinking when implementing a cloud environment, particularly splitting it into three discrete functions, Identity, Entitlement, and Authorization/Access Management (IDEA).

For most organizations, implementing a traditional cloud environment means implementing a server, possibly in a DMZ\(^{109}\), and in most cases tied into a Directory Service (DS)\(^{110}\) (such as Microsoft’s Active Directory, Novell’s eDirectory or Open LDAP) for user authentication. In some cases it means implementing an application or using a web-delivered service using its own stand-alone authentication system, much to the annoyance of the users who then have to remember sets of credentials (or worse, reuse credentials from other, perhaps more trusted, domains).

In contrast, a well-implemented cloud service or application-identity should be consumed from a variety of external sources together along with the associated attributes (remembering that an identity applies not only to Users\(^{111}\), but also Devices, Code\(^{112}\), Organizations and Agents which all have identity and attributes). Leveraging all the multiple identities and attributes involved in a transaction enables the cloud system to make better holistic risk-based decisions (defined by the entitlement process\(^{113}\) and implemented by the authorization & access management components) about granular access to the system, processes, and data within the cloud system/application.

This process of using multiple sources of identity and their related attributes is critical when a cloud application is likely to be Internet-facing, and is also likely to be one of the main hurdles for organizations wanting to use “true” cloud services and instead opt to implement virtualization technologies in their own DMZ connected to their own internal DS.

This de-perimeterized\(^{114}\) approach to identity, entitlement, and access management provides a more flexible and secure approach, but also can be implemented equally well inside the corporate boundary (or perimeter).

Overview. The following sections cover the key aspects of Identity, Entitlement, and Access Management in a cloud environment:

- Introduction to identity in a cloud environment
- Identity architecture for the Cloud
- Identity Federation

---

\(^{109}\) DMZ - Demilitarized Zone
\(^{110}\) DS or “Directory Service” is used throughout this section as an abbreviation for a generic corporate directory service, used for username and password login.
\(^{112}\) Code includes all forms of code, up to including applications and self-protecting data.
\(^{113}\) “Entitlement” is the process of mapping privileges (e.g., access to an application or its data) to identities and the related attributes.
\(^{114}\) De-perimeterization is a term coined by the Jericho Forum\(^{\circledast}\) ([www.jerichoforum.org](http://www.jerichoforum.org)).
Table 1: Simple Entitlement Matrix for a Cloud HR Application

<table>
<thead>
<tr>
<th>Claim / Attribute</th>
<th>Corporate HR Managers Access</th>
<th>User Corporate Access</th>
<th>Corporate HR Managers Home Access</th>
<th>User Home Access (Own Device)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID: Organization Id</td>
<td>Valid</td>
<td>Valid</td>
<td>Valid</td>
<td>No</td>
</tr>
<tr>
<td>ID: User Identifier</td>
<td>Valid</td>
<td>Valid</td>
<td>Valid</td>
<td>Valid</td>
</tr>
<tr>
<td>ID: Device</td>
<td>Valid</td>
<td>Valid</td>
<td>Valid</td>
<td>No</td>
</tr>
<tr>
<td>Attr: Device is clean</td>
<td>Valid</td>
<td>Valid</td>
<td>Valid</td>
<td>Unknown</td>
</tr>
<tr>
<td>Attr: Device is patched</td>
<td>Valid</td>
<td>Valid</td>
<td>Valid</td>
<td>Unknown</td>
</tr>
<tr>
<td>Attr: Device IP (is on corp. net. ?)</td>
<td>Valid</td>
<td>Valid</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Attr: User is HR manager</td>
<td>Valid</td>
<td>No</td>
<td>Valid</td>
<td>No</td>
</tr>
<tr>
<td>Access Result</td>
<td>Read/write access to all HR accounts</td>
<td>Read/write access to users HR account only</td>
<td>Read/write access to users HR account only</td>
<td>Read-only access to users HR account only</td>
</tr>
</tbody>
</table>
Summary & Conclusions

- Your organisation should have a robust identity strategy
- An assertion (or claims) based model should be at the heart of your strategy
- Plan to deliver strong identities for all objects (People, Devices, Code, Organisations, Agents) and not just people
- Plan to consume identities from many sources and for many object types
- Getting identity right will allow faster, more secure, and more flexible collaborative business relationships
Related Reading

**Jericho Forum Commandments**

*The Jericho Forum Commandments define both the means and the principles that must be observed when planning and implementing secure business networks.*

**Identity Commandments**

The Jericho Forum MIA Commandments define the principles that must be observed when planning an identity eco-system. While building on "good practice," the commandments specifically address those areas of security that are associated with the perpetual use of online identities. The commandments serve as a benchmark by which entities, solutions, standards, and processes can be assessed and measured.

**Fundamentals**

1. The scope and level of protection must be specific and appropriate to the asset at risk.
   - Business rationale for de-perimeterisation
   - Jericho Forum Commandments
   - Jericho Forum Identity Commandments

Freely available at www.jerichoforum.org