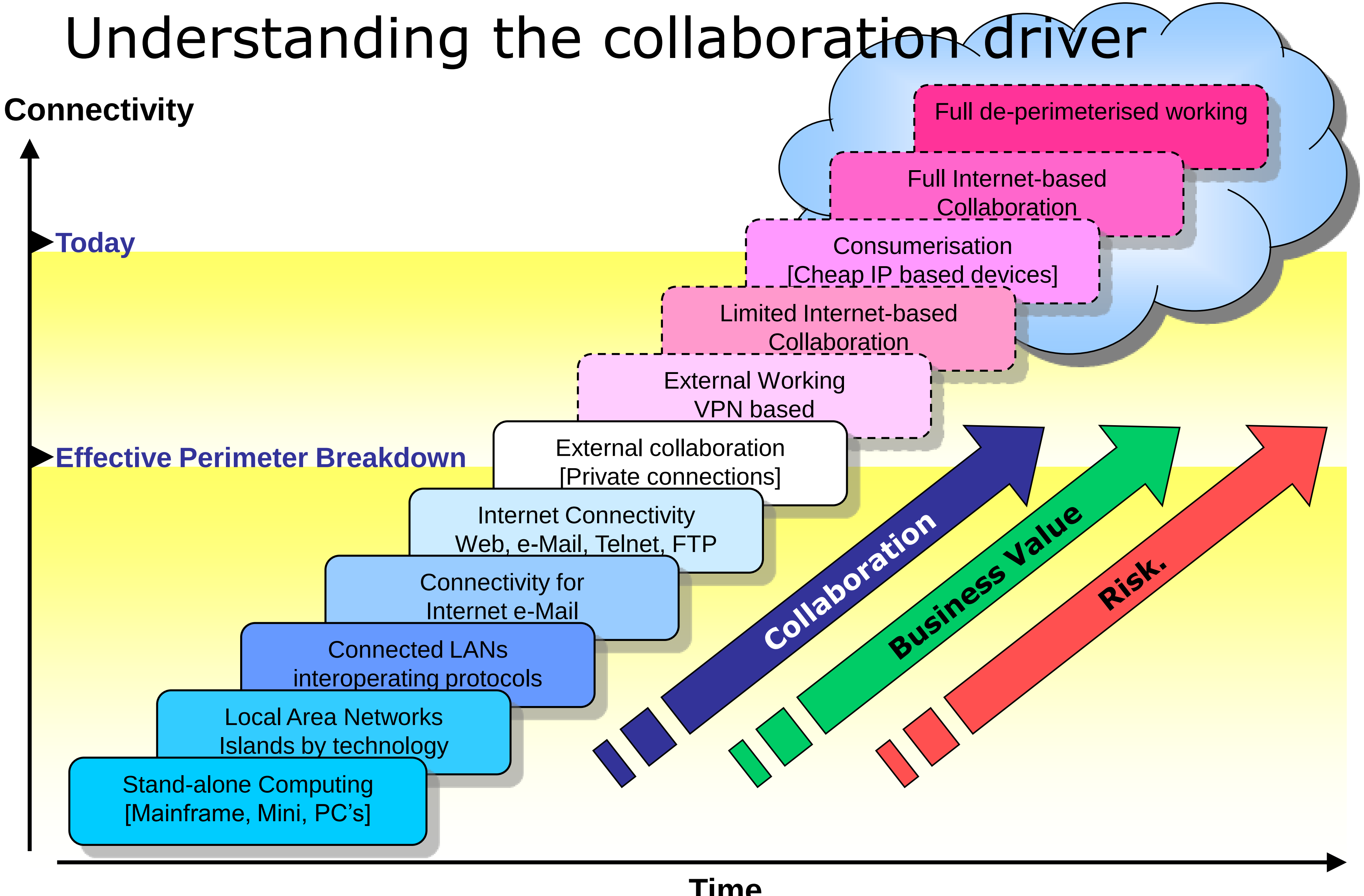
Using identity to empower your organisation

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

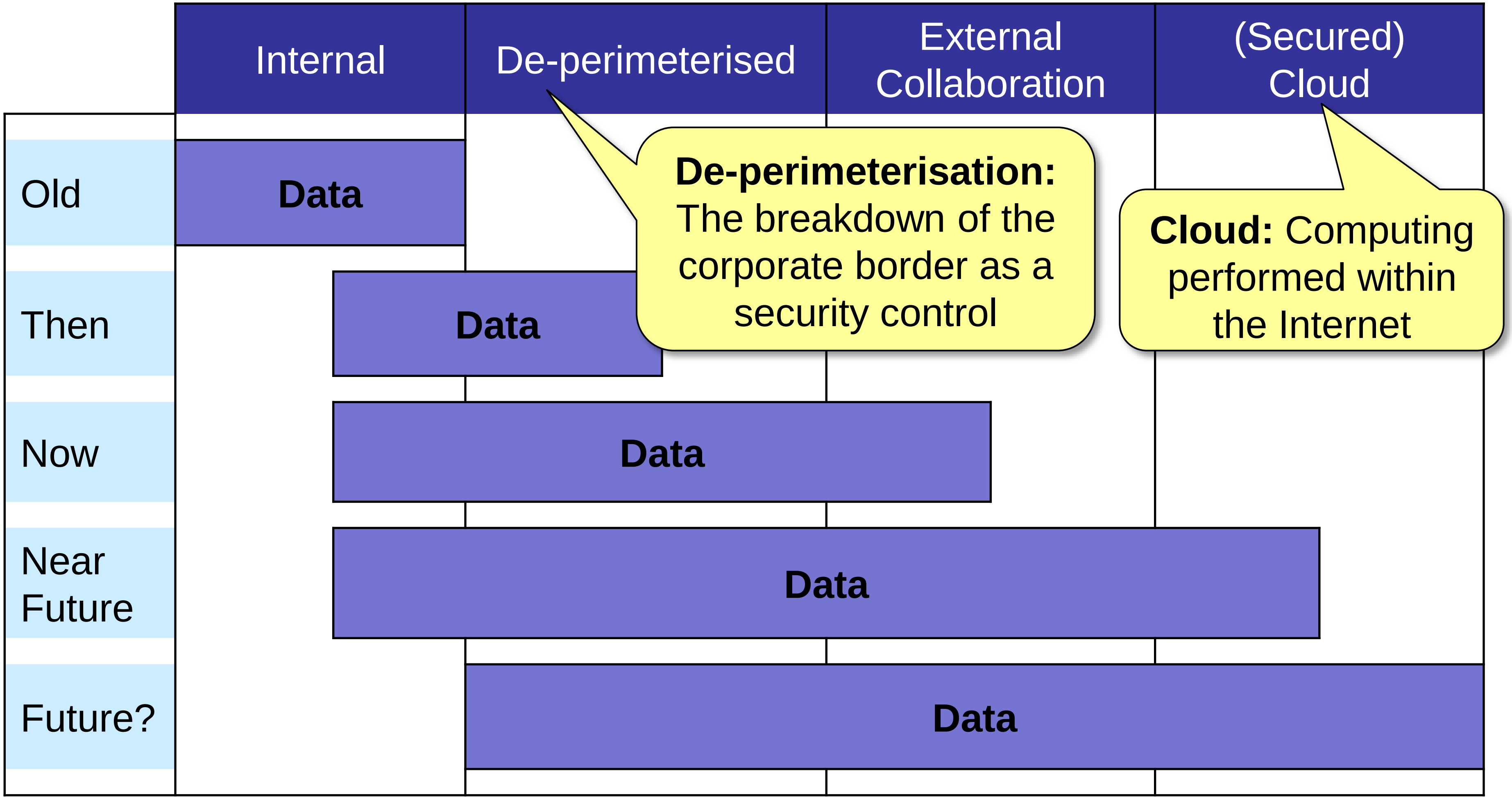
Understanding the collaboration driver



Connectivity
Today
Effective Perimeter Breakdown
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]
Collaboration
Business Value
Risk.
Time

JERICHO FORUM

Understanding the externalisation of data



Internal

De-perimeterised

External Collaboration

(Secured) Cloud

Old

Data

Then

Data

Now

Data

Near Future

Data

Future?

Data

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

Cloud: Computing performed within the Internet

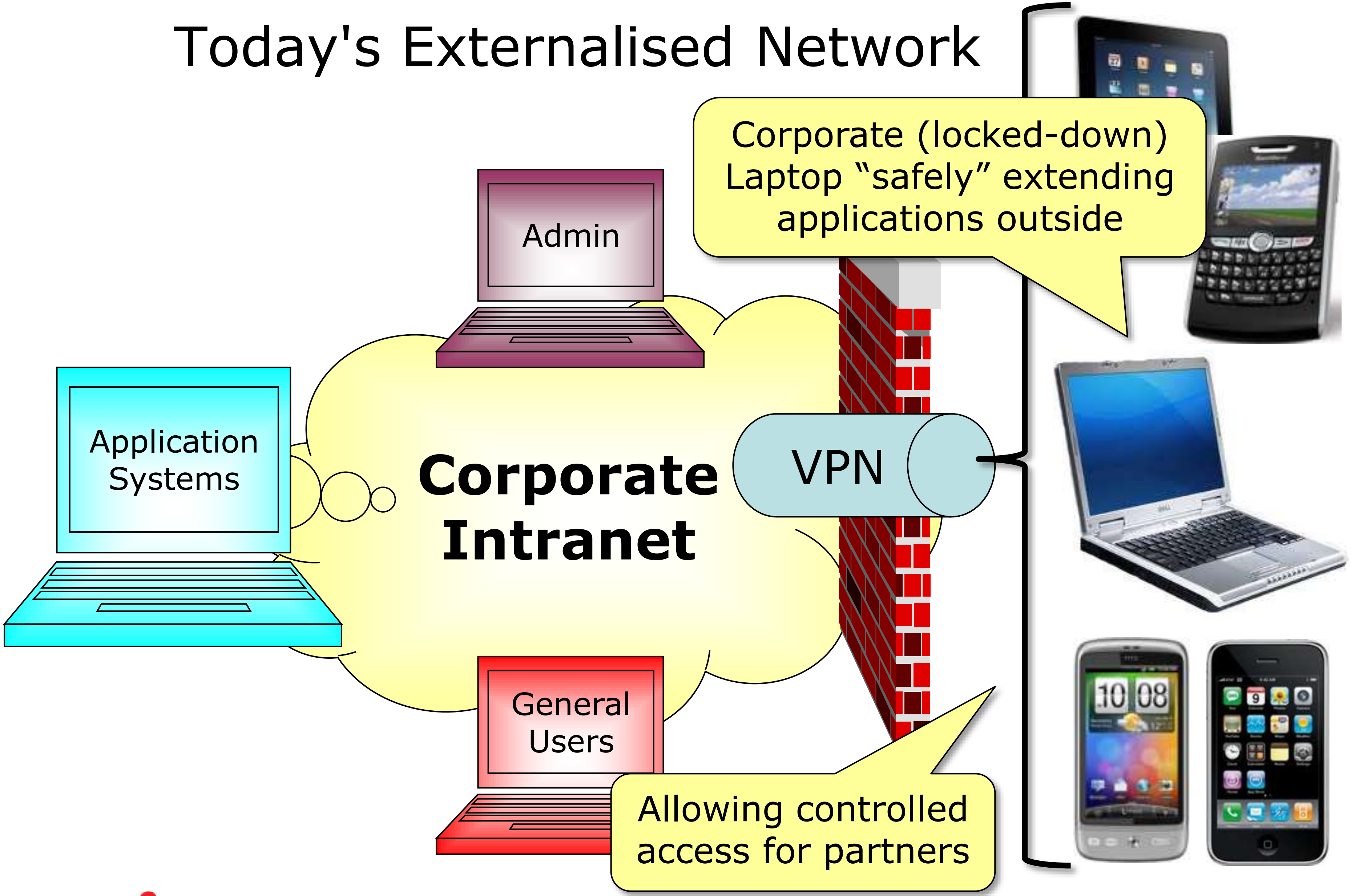
The security of the network becomes increasingly irrelevant, and the security and integrity of the data becomes everything.

The mantra of any good security engineer is: “Security is a 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

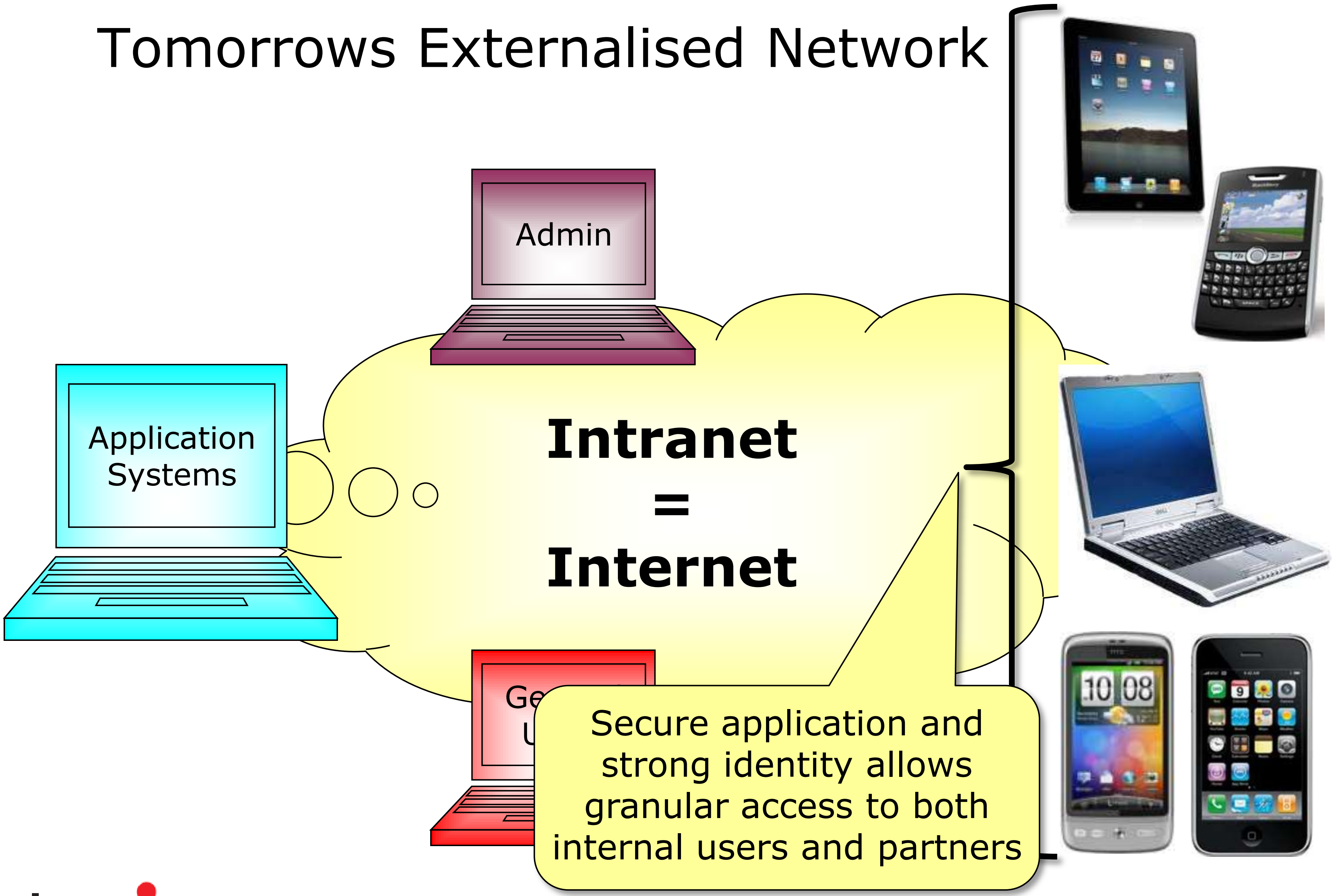
Today's Externalised Network



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

Allowing controlled access for partners

Tomorrows Externalised Network



Intranet = Internet

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

2

Identity is not just about people

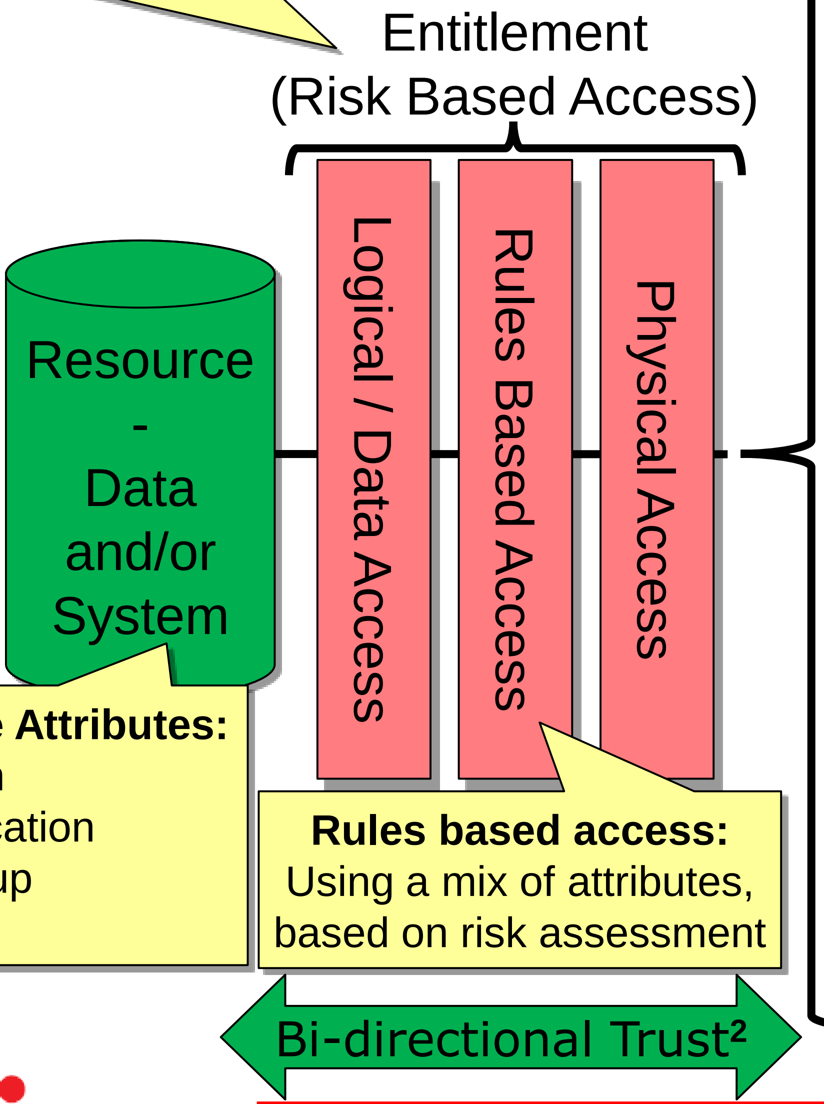
- Identity needs to encompass all objects that need to identify themselves
- This includes;
  - People
  - Devices
  - Code
  - Organisations
  - Agents.

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

Bi-directional Trust[2]

Resource Attributes:

- Location
- Classification
- AD Group
- etc.

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

Martini model[1]: Any IP, any device, any time, anywhere

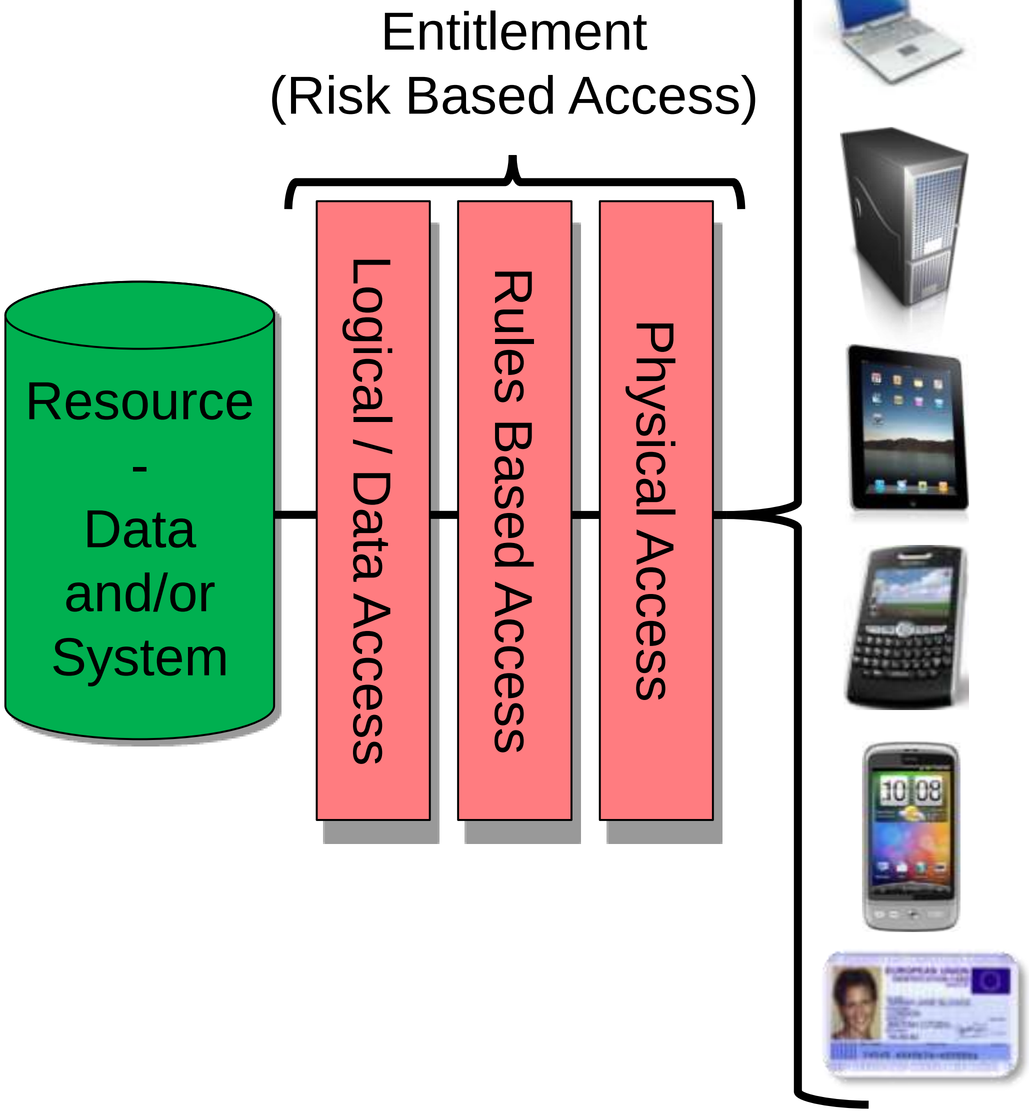
Id / Attributes Asserted

- 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

JERICHO FORUM

[1] Multiple Access Real Time IP Network Implementation

[2] Jericho Forum Commandments #6 & #7



Entitlement
(Risk Based Access)

Resource
-
Data
and/or
System

Logical / Data Access

Rules Based Access

Physical Access

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

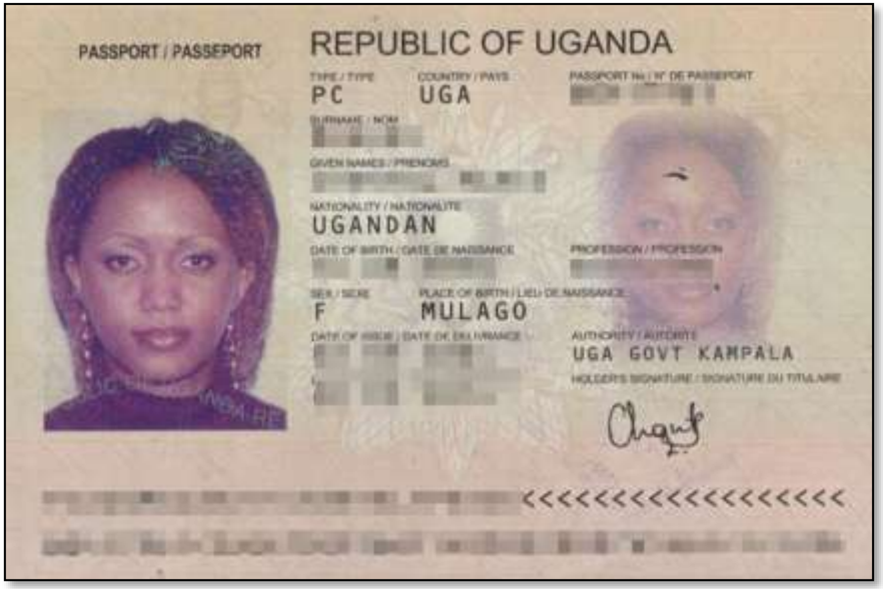
Security Professional

White Water Kayak Instructor

The need for a one-way trust

Multiple Facets

Refugee



PASSPORT / PASSEPORT

REPUBLIC OF UGANDA

TYPE / TYPE PC

COUNTRY / PAYS UGA

PASSPORT No / N° DE PASSEPORT [redacted]

SURNAME / NOM [redacted]

GIVEN NAMES / PRENOMS [redacted]

NATIONALITY / NATIONALITE UGANDAN

DATE OF BIRTH / DATE DE NAISSANCE [redacted]

PROFESSION / PROFESSION [redacted]

SEX / SEXE F

PLACE OF BIRTH / LIEU DE NAISSANCE MULAGO

DATE OF ISSUE / DATE DE DELIVRANCE [redacted]

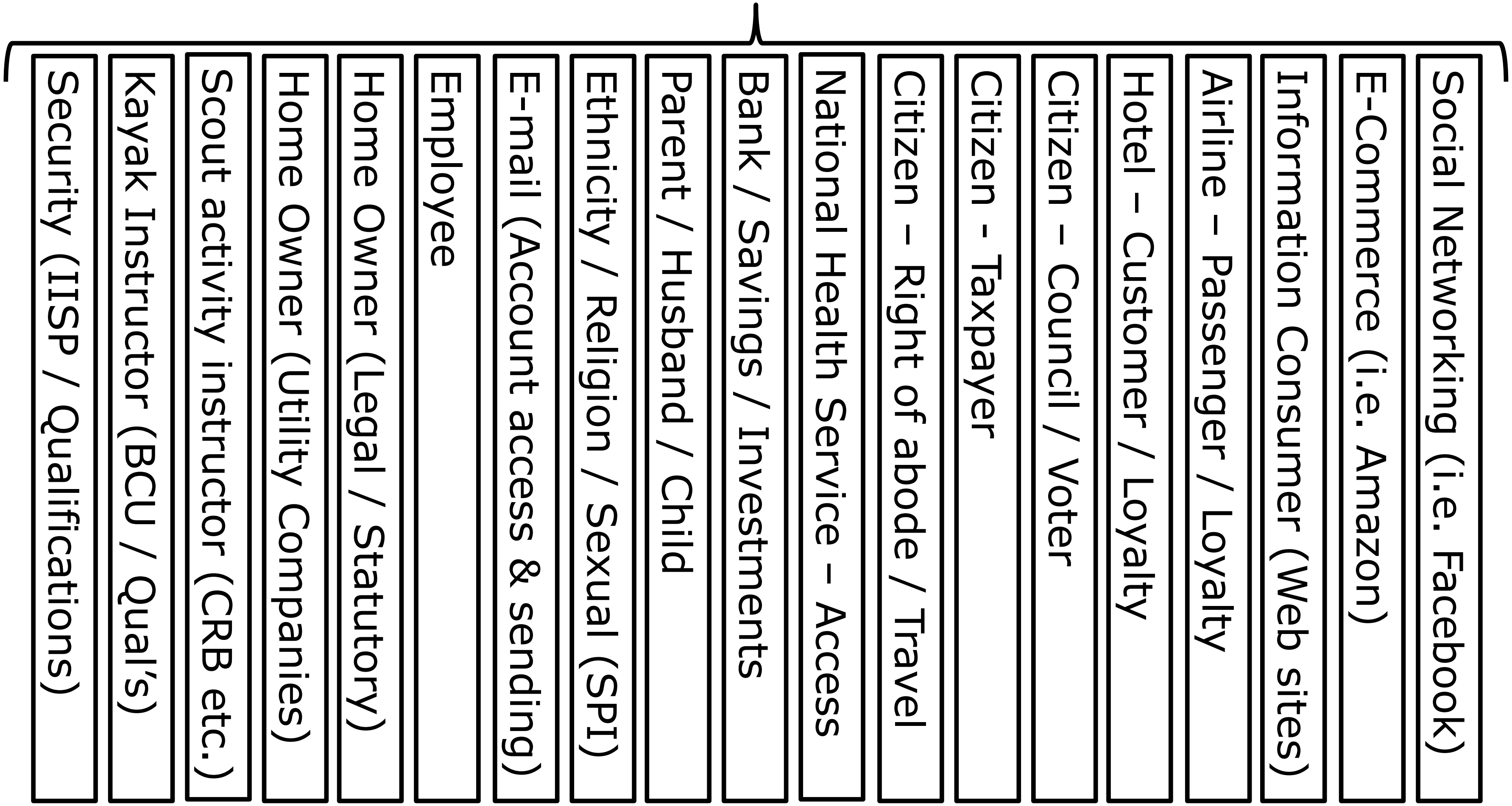
AUTHORITY / AUTORITE UGA GOVT KAMPALA

HOLDER'S SIGNATURE / SIGNATURE DU TITULAIRE

[redacted]<<<<<<<<<<<<<<<<<<

[redacted]

Core Identity
Paul Simmonds



Security (IISP / Qualifications)

Kayak Instructor (BCU / Qual's)

Scout activity instructor (CRB etc.)

Home Owner (Utility Companies)

Home Owner (Legal / Statutory)

Employee

E-mail (Account access & sending)

Ethnicity / Religion / Sexual (SPI)

Parent / Husband / Child

Bank / Savings / Investments

National Health Service – Access

Citizen – Right of abode / Travel

Citizen - Taxpayer

Citizen – Council / Voter

Hotel – Customer / Loyalty

Airline – Passenger / Loyalty

Information Consumer (Web sites)

E-Commerce (i.e. Amazon)

Social Networking (i.e. Facebook)

Facets (or Personas) of my *Core Identity*

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.

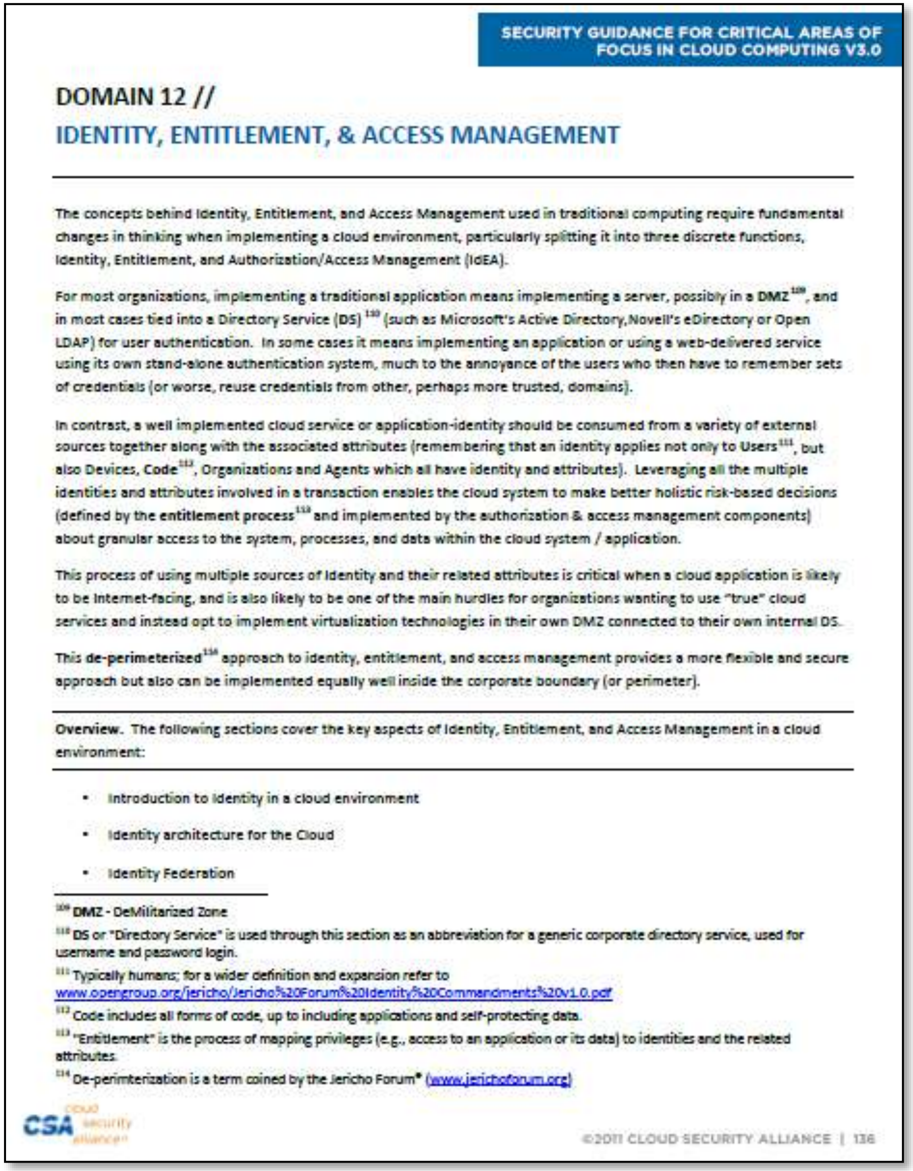
Security is increased by designing for the way humans actually behave

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 application 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 through this section as an abbreviation for a generic corporate directory service, used for username and password login.

[111] Typically humans; for a wider definition and expansion refer to www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf

[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-perimterization is a term coined by the Jericho Forum® (www.jerichoforum.org)

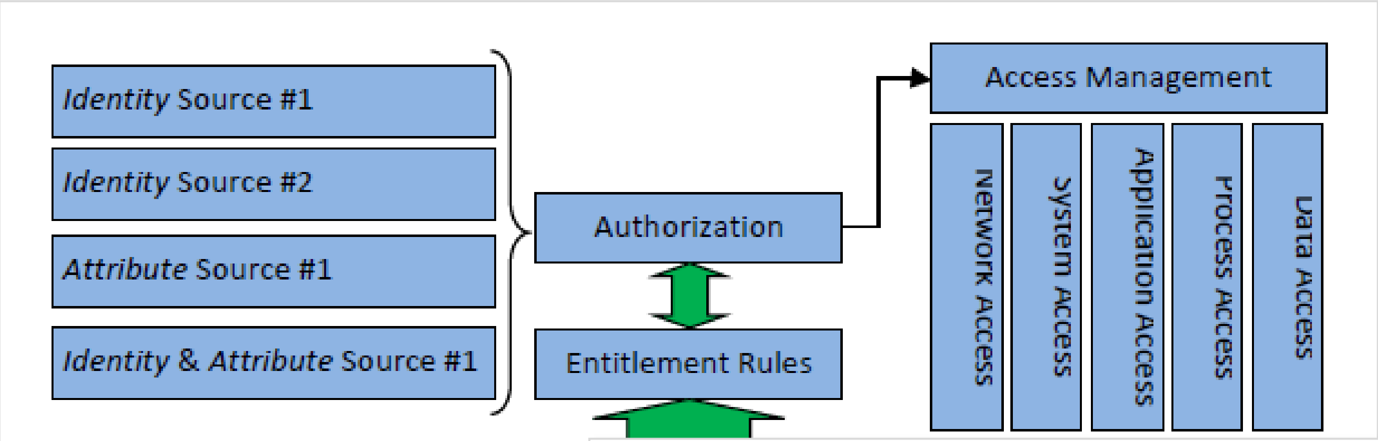
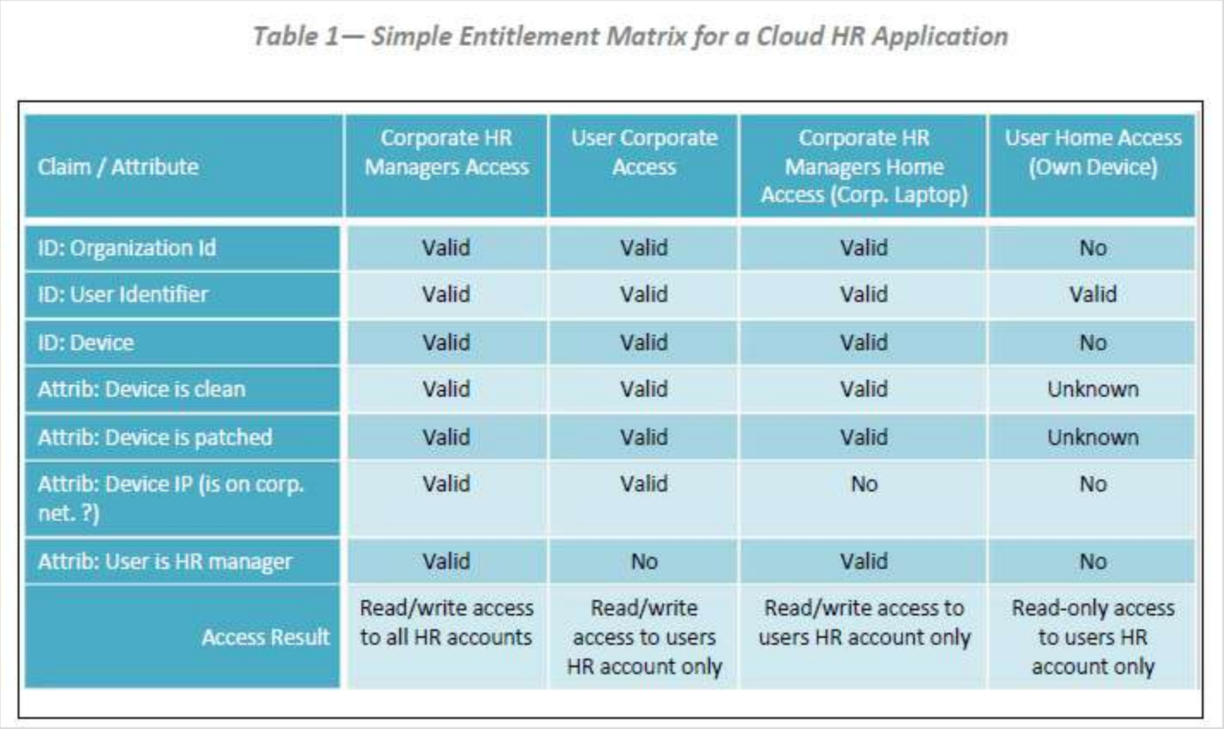


Figure 1: Generic Identity, Er

Table 1— Simple Entitlement Matrix for a Cloud HR Application

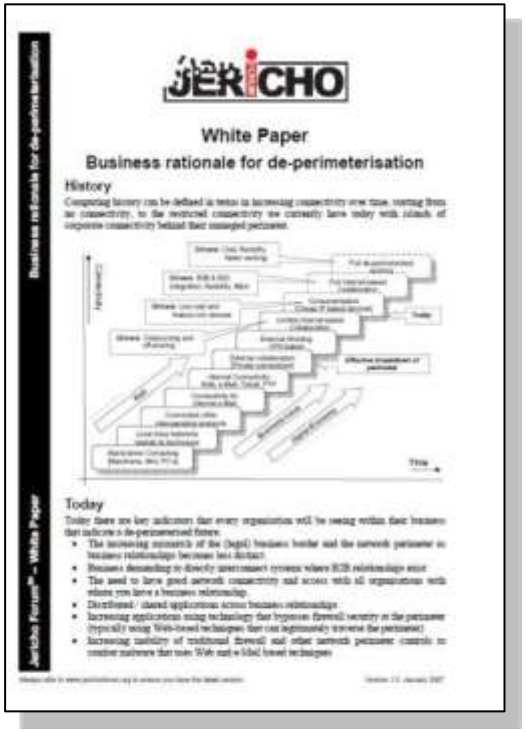


Claim / Attribute	Corporate HR Managers Access	User Corporate Access	Corporate HR Managers Home Access (Corp. Laptop)	User Home Access (Own Device)
ID: Organization Id	Valid	Valid	Valid	No
ID: User Identifier	Valid	Valid	Valid	Valid
ID: Device	Valid	Valid	Valid	No
Attrib: Device is clean	Valid	Valid	Valid	Unknown
Attrib: Device is patched	Valid	Valid	Valid	Unknown
Attrib: Device IP (is on corp. net. ?)	Valid	Valid	No	No
Attrib: User is HR manager	Valid	No	Valid	No
Access Result	Read/write access to all HR accounts	Read/write access to users HR account only	Read/write access to users HR account only	Read-only access to users HR account only

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



Business rationale for de-perimeterisation

White Paper

Business rationale for de-perimeterisation

History

Computing history can be defined in terms in increasing connectivity over time, starting from no connectivity, to the restricted connectivity we currently have today with islands of corporate connectivity behind their managed perimeter.

Today

Today there are key indicators that every organisation will be seeing within their business that indicate a de-perimeterised future.

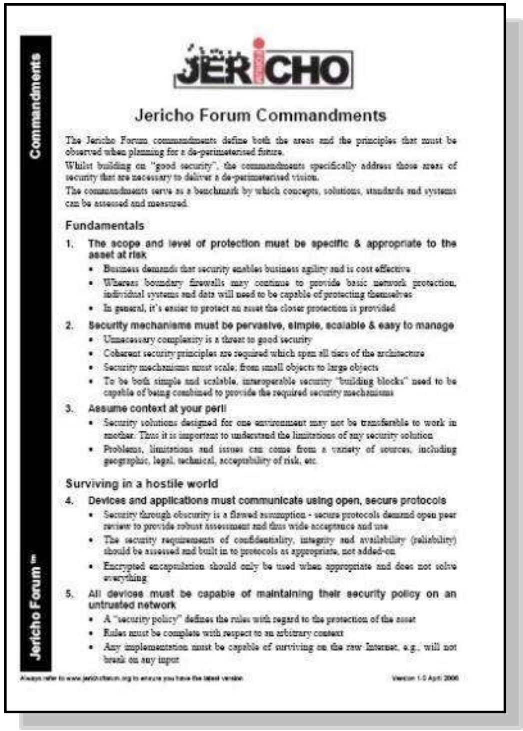
- The increasing mismatch of the (legal) business border and the network perimeter as business relationships becomes less distinct
- Business demanding to directly interconnect systems where B2B relationships exist
- The need to have good network connectivity and access with all organisations with whom you have a business relationship
- Distributed / shared applications across business relationships
- Increasing applications using technology that bypasses firewall security at the perimeter (typically using Web-based techniques that can legitimately traverse the perimeter)
- Increasing inability of traditional firewall and other network perimeter controls to combat malware that uses Web and e-Mail based techniques

Jericho Forum™ – White Paper

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0, January 2007

Business rationale for
de-perimeterisation



Commandments

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision.

The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

1. **The scope and level of protection must be specific & appropriate to the asset at risk**
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it's easier to protect an asset the closer protection is provided
2. **Security mechanisms must be pervasive, simple, scalable & easy to manage**
   - Unnecessary complexity is a threat to good security
   - Coherent security principles are required which span all tiers of the architecture
   - Security mechanisms must scale; from small objects to large objects
   - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms
3. **Assume context at your peril**
   - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
   - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

4. **Devices and applications must communicate using open, secure protocols**
   - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use
   - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
   - Encrypted encapsulation should only be used when appropriate and does not solve everything
5. **All devices must be capable of maintaining their security policy on an untrusted network**
   - A "security policy" defines the rules with regard to the protection of the asset
   - Rules must be complete with respect to an arbitrary context
   - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Jericho Forum™

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

Jericho Forum
Commandments

Identity Commandments

"Identity" Commandments

The Jericho Forum® Identity, Entitlement & Access Management (IdEA) Commandments define the principles that must be observed when planning an identity eco-system.

Whilst building on "good practice", these commandments specifically address those areas that will allow "identity" processes to operate on a global, de-perimeterised scale; this necessitates open and interoperable standards and a commitment to implement such standards by both identity providers and identity consumers[1].

The IdEA commandments serve as a benchmark by which Identity, Entitlement and Access Management concepts, solutions, standards and systems can be assessed and measured. They are supported by a Jericho Forum IdEA Glossary and other related documents. They also build on the higher level Jericho Forum Commandments, in particular Commandments 2, 8, 9 and 10.

Identity and Core Identity

1. All core identities must be protected to ensure their secrecy and integrity
   - Core identifiers[2] must never need to be disclosed and are uniquely and verifiably connected with the related Entity
   - Core identifiers must have a verifiable level of confidence
   - Core identifiers must only be connected to a persona via a one-way linkage (one-way trust)
   - An Entity has Primacy over all the identities and activities of its personae.
   - Entities must never be compelled to reveal a persona, or that two (or more) personae are linked to the same core identity[5]
2. Identifiers must be able to be trusted
   - Identifiers must be appropriately unique and related to the entity's core identifier to enable a definable level of (system) trust of the entity to exist.
   - The identifier for a persona (even if serial pseudo-anonymous[3]) can be used to develop reputational trust of that persona, for example for credit transactions.
   - The identifier for a persona when linked to other attributes or other personae can develop contextual trust, for example linkage to government issued attributes / identifiers.
3. The authoritative source of identity will be the unique identifier[4] or credentials offered by the persona representing that entity
   - Entities have primacy over all linkages of their personae with their public identifiers.
   - The strength of the identity offered will define the level of trust that can be placed in the related persona, especially when a verified identifier or verifiable credentials are offered.

Multiple Identities (Persona)

4. An Entity can have multiple, separate Persona (Identities) and related unique identifiers[4]
   - A Principal or resource owner may choose when to create a Persona (Identity) and related Unique Identifier, and which attributes are connected to that persona.

[1] Jericho Commandment #4 and #6 apply to ensuring open, secure and interoperable standards
[2] A core identifier may refer to a physical, biological or digital entity
[3] Serial pseudo-anonymity, guarantees the same entity in multiple interactions without being able to identify the actual entity
[4] A 3rd party (e.g. organisation) may choose to create a shadow or internal identifier for an entity for internal purposes
[5] We consider this as something that should be enshrined in privacy law, and/or in UN Declaration of Human Rights

Jericho Forum®

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 – May 2011

Jericho Forum
Identity Commandments

Freely available at www.jerichoforum.org