What is Identity Management (IDM)?

- the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities [The Burton Group*]
  - sometimes called "Identity and Access Management"
  - missing from this definition: "removal of identities" and "enforcement of policies"
- secure management of the identity life cycle and the exchange of identity information (e.g., identifiers, attributes and assertions) based on applicable policy of entities such as:
  - users/groups
  - organizations/federations/enterprise/service providers
  - devices/network elements/systems
  - objects (application process, content, data)

* a research firm specializing in IT infrastructure for the enterprise

Identity: definitions (1)

- attributes: distinct & measurable properties belonging to a particular entity
- identity: dynamic collection of all of the entity’s attributes (1 entity: 1 identity)
- partial identities: specific subset of relevant attributes
- identifier: attribute or set of attributes of an entity which uniquely identifies the entity in a given context
- credential: piece of information attached to an entity and attesting to the integrity of certain stated facts

If these definitions reflect a specific vision on identity and identity management.
Identity: definitions (2)

- **entity authentication or identification**: using claimed or observed attributes of an entity to distinguish the entity in a given context from other entities it interacts with.
  - **Note**: In computer security, often identification is providing one’s username and authentication is proving who an entity is.
- **authorization**: the permission of an authenticated entity to perform a defined action.
- **registration**: process in which a partial identity is assigned to an entity and the entity is granted a means by which it can be authenticated in the future.

If these definitions reflect a specific vision on identity and identity management.

Identity management

- Physical world
- Consumer space
- Business environment
- e-Government
- Services and objects

Identity management has many dimensions

- technical
- international
- organizational
- political
- social
- economical

... so it’s not sufficient to add an “identity layer” to the Internet.

Entity authentication is based on one or more of the following elements:

- **what someone knows**
  - password, PIN
- **what someone has**
  - magstripe card, smart card
- **what someone is** (biometrics)
  - fingerprint, retina, hand shape, ...
- **how someone does something**
  - manual signature, typing pattern
- **where someone is**
  - dialback, location based services (GSM, secure GPS)

Step 1: centralize (identity 1.0)

- **integrate** entity authentication
  - but move authorization decision to application and services
- **embrace** multiple authoritative sources
  - authoritative for attributes, not people
- **account names should be ephemeral**
  - Users should be free to select and change
  - Applications should record account ID, not name
- **dynamic rules, not static roles**
Integrated identity management (inside one organization)

How to grow? Step 2: federate (identity 1.5)

- **federated identity**: credential of an entity that links an entity’s partial identity in one *context or trust domain* to an entity’s partial identity in another *context or trust domain*

  - **Note**: can also be used inside an organization for convenience

Single sign on: login only once

Single Sign-On (SSO) (1/4)

1. Access RP1
2. Redirect to IdP
3. Authenticate
4. Create SSO token for subject
5. Get claims for RP1 and issue security token

Single Sign-On (SSO) (2/4)

6. Redirect back to RP1 w/ security token
7. Access RP2
8. Redirect to IdP
9. Don’t reauth subject because SSO token exists
10. Get claims for RP2 and issue security token

Single Sign-On (SSO) (3/4)
7. Access RP2

8. Don’t reauth subject because SSO token exists

9. Get claims for RP2 and issue security token

10. Redirect back to SP2 w/ security token

---

Single Sign-on (SSO) (4/4)

- User
- IdP
- RP2

9. Don’t reauth subject because SSO token exists

10. Get claims for RP2 and issue security token

11. Redirect back to SP2 w/ security token

---

Single Sign-On Variants

- initiate contact with IDP or with RP
- access token can be pushed by user to RP or can be pulled by RP from IDP
- token: symmetric versus public key
  - symmetric token: IDP and RP have to share a secret key (example: Kerberos)
  - asymmetric token (digital signature): IDP and RP have to trust a common CA (example: SAML)

---

Single Sign-on with symmetric keys: Kerberos

- Alice/Bob shares a long term secret with KDC: $K_{AT}$/$K_{BT}$
- $K_{AT}$/$K_{BT}$ are synchronized clocks
- ticket${\text{B}} = E_{K_BT}(k ||A || L)$
- $L$: life time of a ticket – limits validity of a key

1. $A||B||n_A$
2. $E_{K_BT}(k||n_A||L||B)$
3. $E_{K_AT}(k||A||L)$
4. $E_{K_BT}(t_A)$
5. $E_{K_AT}(t_A)$

---

SAML (Security Assertion Markup Language) (2001)

- OASIS Security Services Technical Committee (SSTC)
- XML-based standard for exchanging authentication and authorization data
  - SAML assertions that describe security tokens representing users
  - SAML bindings: map to standard communication protocol
  - SAML profiles for a single sign-on protocol
  - generic but rather complex
  - IDP-friendly (e.g., preconfigure large IDP in RPs)
  - offers various pseudonyms
- SAML 1.0 (Nov. ’02)
- SAML 2.0 (March ’05) – incompatible with 1.0/1.1
  - input from Liberty Alliance ID-FF 1.2 but not compatible
  - Profiles: Web browser SSO, WSS-Security, Liberty ID-FF and ID-WSF, XAXML v2.0

---

Single Sign-On

- convenient
- more secure than multiple passwords
- can leverage a single but more secure authentication mechanism
- risk of breach of authentication mechanism is substantially larger
- is there a single sign-off?
- redirection by RP may facilitate phishing
- IDP is single point of failure
- If RP is contacted first, how does it know which IDP to contact? (the discovery problem)
- privacy risks
  - data sharing: e.g., Facebook or LinkedIn access Gmail email addresses
  - central control of who accesses which services at which time
The great thing about standards is… there are so many to choose from!

Microsoft .NET Passport (1999)
- Problems:
  - online services had to pay a subscription fee
  - single point-of-failure
  - do we trust Microsoft to take part in all of our online transactions?
  - no context-based identity
- 2007: MSN (Windows Live ID)
  - CardSpace
  - OpenID

Shibboleth (2000)
- Internet2 Middleware Initiative: developing interoperable identity and access management infrastructures for research and higher education
- architecture and open-source implementation for federated identity-based authentication and authorization infrastructure based on SAML (web-based)
- v1.3: Aug’05
- v2.0: March ’08 (SAML 2.0)
- focus on research and higher education (> 4 million users)
- basis of InCommon federation

The Liberty Alliance (2001)
- 150 organizations: Sun, Sprint, Sony, Verisign, eBay...
- Single sign-on system based on a “circle of trust”
- Federated identity
  - Aggregating personal information across multiple systems
  - Authenticating a user across multiple systems
  - Exchanging claims via SAML
- Focus on corporate environments, not individual Internet users (> 1 billion Liberty-enabled identities and devices)

The Liberty Alliance (2001)
- 2002
  - Liberty "Phandle it"
  - Liberty ID-FF 1.1, 1.2
- 2003
  - SAML, 1.1
  - Shibboleth 1.1, 1.2
  - Liberty ID-FF 1.3
- 2004
  - SAML 2.0
  - Shibboleth 2.0
- 2005
  - Liberty Federation
  - Identity Federation
- 2007
  - Identity Governance Framework
- 2008
  - Identity Assurance Framework

- Identity Federation specification for web services and web applications developed by BEA Systems, BMC Software, CA, Inc., IBM, Layer 7 Technologies, Microsoft, Novell, Ping Identity, and VeriSign
  - mechanisms for brokering of identity, attribute discovery and retrieval, authentication and authorization claims between federation partners, and protecting the privacy of these claims across organizational boundaries
  - mechanisms are defined as extensions to the Security Token Service (STS) model
  - mapping mechanisms and the WS-Trust token issuance messages, onto HTTP (for use in browsers)
- tokens can be: X.509 certificates, Kerberos tickets, UserID/Password credentials, SAML-Assertion, Custom defined
- Aligned with WS-Security
- V1.1 Dec. ’06
Outline

- What is identity management?
- Entity authentication
- ID management 1.0
- ID management 1.5
- Principles of identity and ID management 2.0
- eID
- Conclusions

Identity: principles [Kim Cameron, Microsoft, ’05] also called “laws”

1. user control and consent
2. minimal disclosure of information for a constrained use
3. disclosure limited to justifiable parties
4. directed identities: omni-directional and uni-directional
5. open – operators and technologies
6. human integration
7. consistent experience across contexts

- insightful and though provoking
- dependent on IT context and technology – rather principles than “laws”
- could also be called: the 7 mistakes made by Passport

Identity meta-system

Identity selectors (1/2)

Microsoft CardSpace (formerly known as InfoCard) [2006]
http://cardspace.netfx3.com

- .NET component (integrated with O/S)
- identities are represented as cards
- token produced on demand by IDP based on card selected by the user (constraints imposed by RP)
- support for any digital identity system: managed and unmanaged cards
- solves problem of IDP discovery
- based on the following technologies:
  - WS-* (Security, Trust, Federation,...)
  - SAML 2.0 Enhanced* Client Proxy Profile
  - SSL EV (extended validation)

* enhanced: helps with discovery

Identity selectors (2/2)

Eclipse project Higgins: open source browser add-on (plug-in API)
- Identity agent
- Identity services
- Personal data store

Main issues: “identity 2.0”

- Need consistent view for user: identity selector
  - essential: mental model and ease of use
- Move from enterprise centric to user-centric (user in control)
  - no unique definition
  - assuring attributes by proving claims
  - claims: “…an assertion of the truth of something, typically one which is disputed or in doubt”.
  - key questions:
    - are users capable of managing their identities?
    - are users qualified to manage their identities? (e.g. not in e-gov)
- Increased privacy
  - Can mean many things…
URL-Based Identity Management: OpenID (2005)

- User enters identity URL at the relying party
- Relying party redirects browser to identity URL
- User logs in at identity URL
- Identity URL verifies relying party by checking access control list
- Identity URL sends security token back to browser
- Browser redirects security token to relying party (user confirms)
- Relying party verifies security token directly with identity URL

- V 1.0 2005 - V 2.0 2007
- Openness is privacy challenge:
  - no agreement needed between RPs and IDPs
  - RPs can correlate information
  - IDP knows which RPs are visited

URL-Based Identity Management: OpenID (2005)

- V2.0
  - supports pseudonymous login
  - XRI Extensible Resource Identifier (URI or IRI)
    - personalized XRI i-name (bart.prenneel) can be resolved into multiple URIs: blog, SkypeID, Yahoo! ID
  - similar to DNS for IP address
  - XRID (eXtensible Resource Description): simple generic format for describing and discovering resources
  - Yadis: communications protocol for discovery of services such as OpenID, OAuth, and XDI connected to a Yadis ID

Focus on consumers: Dec. 09: > 1 billion OpenIDs on the Internet, 9 million sites have integrated OpenID consumer support

Providers include AOL, BBC, Google, IBM, Microsoft, MySpace, Orange, PayPal, VeriSign, LiveJournal, Yandex, Ustream, Yahoo!

Pros and Cons of URL-Based Identity

- simple, lightweight and scalable
- RP friendly
- user can self-assert attributes and host its own provider
- uses existing web & browser technologies
  - easy to adopt: no new software needed
  - accessible from anywhere
  - inconvenient typing of URLs (no IDP discovery by RP)
  - open to phishing attacks (because of redirection)
  - black and white trust model
  - user interface not always consistent
  - no SSL required
  - can self-asserted claims be trusted?

OpenID vs. SAML

- OpenID advantages
  - more open source stacks, i.e. free
  - IDPs can support new RPs without requiring them to register
  - RPs can support new IDPs without registering with them, but may still need a list of ones it trust (or a list from a trusted authority)
  - lighter and more scalable but less focus on security
- SAML advantages
  - higher industry confidence in security details of protocols and existing implementations
  - much larger number of existing E-mail domains have a SAML IDP
  - IDP discovery can be hard

Conclusions

Both can be user-centric and enable direct interactions between IDPs and RPs

- SaaS vendors will focus on SAML
- Consumer RP sites will use whatever big IDPs deploy (which happens to be OpenID)
- Longer term the vendors and open source implementations will support both

OpenAuth (2006): access delegation

- Started by Twitter developer, support from Google, Yahoo!, MySpace
- open protocol: allow users to share their private resources stored on site A with site B without having to hand username/password
- users hand out tokens to access their data hosted by a service provider
- each token grants access for specific resources at a specific site for a defined duration
- users can share verifiable assertions about themselves without having to release any personally identifiable information.
- Orthogonal to federated identity management
- OAuth Core 1.0 Revision A (Jan’09)
  - Underspecified: standardization effort in IETF working group since 2008
- Quality of open source implementations not yet optimal
- Further developments:
  - OpenID is developing an OAuth extension
  - WRAP: hide OAuth crypto to developer

Conclusion

- Identity management is closely intertwined with our social and economic interactions
- Identity management technology is evolving quickly, yet the concepts in our society change only slowly
  - Concept of identity will probably evolve
- Ease of use and increased profiling has higher importance than data minimization
- Data minimization may be hopeless anyway because of information that leaks at lower layers
- Staying anonymous becomes harder and harder
- Security for society will grow but privacy of individual will erode
- Impact on our society not understood