Identity Systems

Jim Fenton
“Defining identity is like nailing Jell-O® to the wall.”

– Source Uncertain
Terminology

- **Subject**
  - The person (usually) whose identity is involved
  - Sometimes called the User

- **Relying Party**
  - The entity the Subject is interacting with
  - Sometimes called the Service Provider

- **Attribute**
  - A piece of information about the Subject
  - Sometimes called a Claim
A Basic Identity System

Identity Provider

Government

Authentication Request

Commerce

Social Media
A Basic Identity System

Identity Provider

User Authentication

Government

User Credentials

Commerce

Social Media
A Basic Identity System

Identity Provider

Government

Commerce

Social Media

Authorize Info Release

Attribute Request/Response
Elements of Identity Management

Authentication
Establish who the Subject is

Credential Management
Prove to Relying Parties who the Subject is

Attribute Management
Provide information about the Subject
User Trust

- User trust in their Identity Provider is fundamental
  - Not all users trust any one entity
  - Most likely to trust entities they do business with and strong, trusted brands
  - Different trusted entities in different cultures

- An ecosystem of identity providers is required
  - Users need to choose their own identity provider
  - Need to consider ability to migrate to a different provider if required
Authentication
Authentication Methods

- Methods useful for user authentication are situation-specific
  - Type of endpoint being used
  - Required authentication strength (transaction value, etc.)
- **Problem**: Many existing identity systems are bound tightly to specific authentication methods
Authentication Strength

- Authentication strength should depend on transaction value
  - iTunes purchase (99 cents) vs. vehicle purchase
- NIST Special Pub 800-63 defines 4 levels:
  - Level 1: Minimal challenge/response
  - Level 2: Single-factor identity proofing
  - Level 3: Multi-factor identity proofing
  - Level 4: Hardened multi-factor
- Relying party specifies the required strength to the identity management system
Authentication Endpoint Diversity

- The Web is pervasive, but not *everything* is a browser

- Examples
  - Vending Machines
  - Set-top boxes
  - Doors (physical security)

- Modular approaches to authentication needed to consider a wide range of use cases
Security Opportunities

- Users that authenticate frequently at a given service are more likely to detect anomalies
  - More likely to be suspicious about, for example, lack of a certificate
  - Browsers can be configured to specially flag “chosen” identity providers

- Identity providers can detect anomalous user behavior
  - Similar to detection of fraudulent credit card transactions
  - Business/policy framework should encourage this
Credential Management
Credential Management: Functions

- Act as a “key cabinet” for the user
  Each relying party has its own credentials

- Support Directed Identity
  Prevent undesired release of correlation handles
  Identifiers to Relying Parties are opaque by default

- Enforce secure use of credentials
  Require use of secure channel (e.g., SSL)
Directed Identity

- It should not necessarily be possible for different Relying Parties to correlate identifiers
  - Insurance company vs. supermarket account
  - Pseudonymous identifiers for tip hotlines
- Users may still choose to link relying parties’ identifiers
- Attributes may also provide correlation handles
- Credential manager can be subpoenaed if appropriate
Security and Availability Issues

- **Security**
  - The credential store is a very high-value target
  - Credentials can be distributed to diffuse attack
  - High-level physical security is also required

- **Availability**
  - Failure of an Identity Manager may have severe impact on its Subjects
  - Solvable problem, but needs to be addressed
Attribute Management
Distributed Attributes

- Self-asserted attributes have limited utility
- **Authoritative** sources for different attributes come from different places
  - FICO scores from a credit bureau
  - Driving record from state Motor Vehicle Department
  - Proof of employment from employer
- Identity system has a role in locating trustable sources of attributes
- Attributes delivered as signed assertions
Attribute Distribution: Example

Identity Provider

- Healthcare Provider
- Authorization Request
- Birthdate Request
- Wine Merchant

Motor Vehicle Department
Attribute Distribution: Example

Identity Provider

Healthcare Provider

Motor Vehicle Department

Wine Merchant

Release Authorization

Trust Negotiation
Attribute Distribution: Example

Identity Provider

Birthdate Request

Motor Vehicle Department

Healthcare Provider

Wine Merchant
Attribute Distribution: Example

Identity Provider

Motor Vehicle Department

Healthcare Provider

4 July 1976 – DMV

Wine Merchant
Attribute Trust

- Federation: Prearranged trust relationships
  Personnel Security Clearances among Federal agencies
  Business partners

- Accreditation: Indirect federation
  Financial institutions, schools
  Scales much better than direct federation
Identity Provider Trust

- Identity Provider has a fiduciary responsibility
- To the Subject:
  - Must use credentials only for the proper Subject
- To Relying Parties:
  - Must associate attribute requests and responses reliably
- Identity Provider may coincidentally function as an Attribute Provider
  - Functions should be considered separate to maintain privacy
Summary
Observations

- Scaling is critical
  - Technical (protocol) aspects of scaling are a solved problem
  - Scaling of trust relationships is the real limitation

- Chosen technologies need to consider a very wide range of use cases

- An ecosystem of identity and attribute providers is needed
  - Need business models for these functions
  - Public policy should encourage constructive behavior and help these entities manage liability exposure
Questions