The Laws of Identity

http://www.identityblog.com
Kim Cameron
Architect of Identity and Access
Microsoft Corporation

Problem Statement

- The Internet was built without a way to know who and what you are connecting to
  - Everyone offering an internet service has had to come up with a workaround
  - Patchwork of identity one-offs
  - We have inadvertently taught people to be phished and pharmed
  - No fair blaming the user – no framework, no cues, no control
- We are “Missing the identity layer”
- Digital identity currently exists in a **world without synergy** because of identity silos

Criminalization of the Internet

- Greater use and greater value attract professionalized international criminal fringe
  - Understand ad hoc nature of identity patchwork
  - Phishing and Pharming (Phraud) at 1000% CAGR
  - Combine with “stash attacks” reported as “identity loses”…
- Unwinding of acceptance where we should be seeing progress.
  - Opportunity of moving beyond “public-ation”
  - Need to intervene so web services can get out of the starting gate
- ***The ad hoc nature of internet identity cannot withstand the growing assault of professionalized attackers***
  - **We can predict a deepening public crisis**

From Patchwork to Identity Fabric

- The evolution to an identity fabric is hard
  - Partial successes in specific domains – SSL; Kerberos
  - But little agreement on what identity layer is or how it should be run
    - Digital identity related to contexts
    - Many contexts - each jealously guarded
  - Enterprises, governments, verticals prefer one-offs to loss of control
  - Individual is also a player – the key player – and has a veto
    - Role of convenience, coolness, privacy, safety
    - **Nuanced and cogent privacy advocates** in a world of pathetic "identity loss"
- No simplistic solution is realistic
  - Cross cultural and international problems are the final straw

An Identity Metasystem

- Diverse needs of players mean integrating multiple constituent technologies
- Not the first time we've seen this in computing
  - Think back to things as basic as abstract display services made possible through device drivers
  - Or the emergence of sockets and TCP/IP
    - Unified Ethernet, Token Ring, Frame Relay, X.25 and even the uninvented wireless protocols
- We need a "unifying identity metasystem"
  - Protect applications from complexities of systems
  - Allow digital identity to be loosely coupled
- Avoid need to agree on dominant technologies **a priori** – they will emerge from the ecosystem

The role of “The Laws”…

- We must be able to **structure our understanding** of digital identity
  - We need a way to avoid returning to the **Empty Page** every time we talk about digital identity
  - We need to inform peoples’ thinking by teasing apart the factors and dynamics explaining the successes and failures of identity systems since the 1970s
  - We need to develop hypotheses – resulting from observation – that are testable and can be disproved
  - Our goals must be pragmatic, bounding our inquiry, with the aim of defining the characteristics of an unifying identity metasystem
  - The Laws of Identity offer a “good way” to express this thought
  - Beyond mere conversation, the Blogosphere offers us **a crucible**. The concept has been to employ this crucible to *harden and deepen the laws.*

Words to allow dialogue

- Digital Identity: A set of claims made by one digital subject about itself or another digital subject
- Digital Subject: A person or thing represented in the digital realm which is being described or dealt with
  - Devices, computers, resources, policies, relationships
- Claim: An assertion of the truth of something, typically one which is disputed or in doubt
  - An identifier
  - Knowledge of a secret
  - Personally identifying information
  - Membership in a given group (e.g. people under 16)
  - Even a capability
- These definitions embrace Kerberos, X.509, SAML, and newly emerging technologies

1. User Control and Consent

- *Digital identity systems must only reveal information identifying a user with the user's consent*
  - Appeal by means of convenience and simplicity
  - Endure by earning the user's trust
    - Requires a holistic commitment
    - Put the user in control of what identities are used and what information is released
    - Protect against deception (destination and misuse)
    - Inform user of auditing implications
    - Retain paradigm of consent across all contexts

2. Minimal Disclosure for Limited Use

- *The solution that discloses the least identifying information and best limits its use is the most stable long term solution*
  - Consider Information breaches to be inevitable
  - To mitigate risk, acquire and store information on a “need to know” and “need to retain” basis
  - Less information implies less value implies less attraction implies less risk
  - “Least identifying information” includes:
    - Reduction of cross-context information (universal identifiers)
    - Use of claim transformation to reduce individuation (example of over an age threshold as compared to specific birth date
  - Limiting information hoarding for unspecified futures
  - Relation of this law to information catastrophes

3. Justifiable Parties

- *Digital identity systems must limit disclosure of identifying information to parties having a necessary and justifiable place in a given identity relationship*
  - The user must be aware of the party with whom information is being shared
  - Justification requirements apply both to the subject and to the relying party
    - Example of Microsoft's experience with Passport
  - In what contexts will use of government identities succeed and fail?
  - Same issues face "intermediaries" (but don't preclude them)
  - Parties to a disclosure must provide a statement about information use
  - Criminal investigation does not make the state a party to disclosure in the normal sense

4. Directed Identity

- *A unifying identity metasystem must support both "omni-directional" identifiers for public entities and "unidirectional" identifiers for private entities*
  - Digital identity is always asserted with respect to some other identity or *set of identities*
  - Public entities require well-known "beacons"
    - Examples: web sites or public devices
  - Private entities (people) require the option to *not be a beacon*
    - Unidirectional identifiers used in combination with a single beacon: no correlation handles
  - Example of Bluetooth and RFID – growing pushback
  - Wireless was also misdesigned in light of this law

5. Pluralism of Operators and Technologies

- *A unifying identity metasystem must channel and enable the inter-working of multiple identity technologies run by multiple identity providers*
  - Characteristics that make a system ideal in one context disqualify it in another
  - Example of government versus employer versus individual as consumer and human being
  - Craving for “segregation” of contexts
  - Important new technologies currently emerging – must not glue in a single technology or require “fork-lift” upgrade
  - Convergence can occur, but only when there is a platform (identity ecology) for that to happen in

6. Human Integration

- *A unifying identity metasystem must define the human user as a component integrated through protected and unambiguous human-machine communications*
  - We've done a good job of securing the first 5,000 miles but allowed penetration of the last 2 feet
  - The channel between the display and the brain is under attack
  - Need to move from thinking about a protocol to thinking about a ceremony
  - Example of Channel 9 on United Airlines
  - How to achieve highest levels of reliability in communication between user and rest of system

7. Consistent Experience Across Contexts

- *A unifying identity metasystem must provide a simple consistent experience while enabling separation of contexts through multiple operators and technologies*
  - Need to “thingify” identities – make them “things” on the desktop so users can see them, inspect details, add and delete
  - What type of digital identity is acceptable in any context?
    - Properties of potential candidates specified by the relying party
    - Matching thingified identities presented to user, allow her to select one and understand information associated with it.
  - Single relying party may accept more than one type of identity
  - User can select best identity for the context
    - Example of 401(k) portal in a large enterprise
- See this as the synergetic expression of all the laws

Contributors to the discussion

- *Arun Nanda, Andre Durand, Bill Barnes, Carl Ellison, Caspar Bowden, Craig Burton, Dan Blum, Dave Kearn, Dave Winer, Dick Hardt, Doc Searls, Drummond Reed, Ellen McDermott, Eric Norlin, Ester Dyson, Fen Labalme, Identity Woman Kaliya, JC Cannon. James Kobielus, James Governor…*
- *Jamie Lewis, John Shewchuk, Luke Razzell, Marc Canter, Mark Wahl, Martin Taylor, Mike Jones, Phil Becker, Radovan Janocek, Ravi Pandya, Robert Scoble, Scott C. Lemon, Simon Davies, Stefan Brandt, Stuart Kwan and William Heath*
- *And others…*

Conclusion

- Those of us working on and with identity systems need to obey the laws of identity
- Ignoring them results in unintended consequences.
  - Similar to what would happen if civil engineers ignored the laws of gravity
- By following the Laws of Identity we can build an identity metasystem that can be very widely accepted and enduring