# Gaps and Overlaps in Identity Management Solutions

OASIS Pre-conference Workshop, EIC 2009

**Dale Olds**

Novell Distinguished Engineer

dolds@novell.com

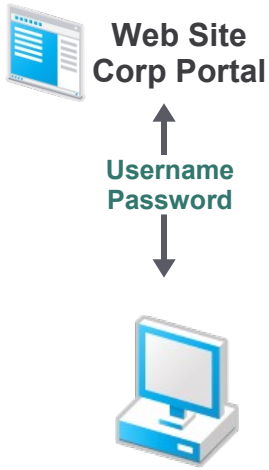
Novell®

# Overview

- Problems with identity management today
  - It's a mess, why can't it be easy enough for Grandma?
  - Online relationships need more intuitive usability, context, courtesy, and respect – as well as security.
- Significant improvements and trends
  - Cross domain identity systems and the identity provider model
  - More authorization less identification
  - Token transformation/combination rather than connect/retrieve
- Overlaps and gaps
  - Are overlaps bad?
  - Some examples of overlaps and gaps
  - What can be done about them

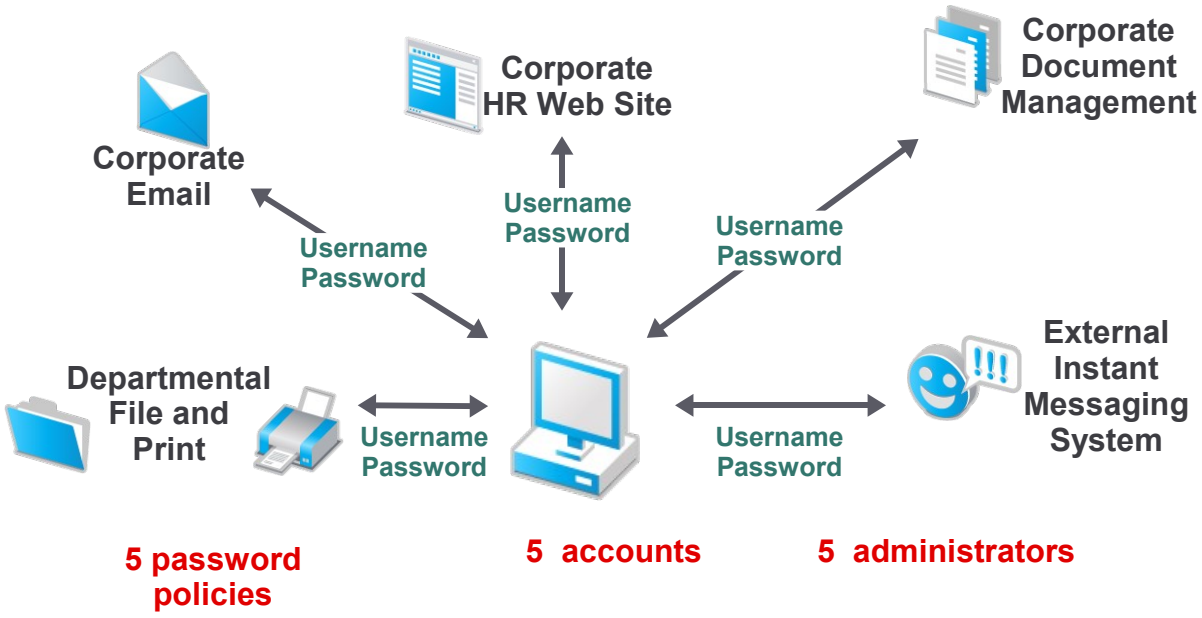
# Problems of Identity Management in the Real World

# Simple Beginnings

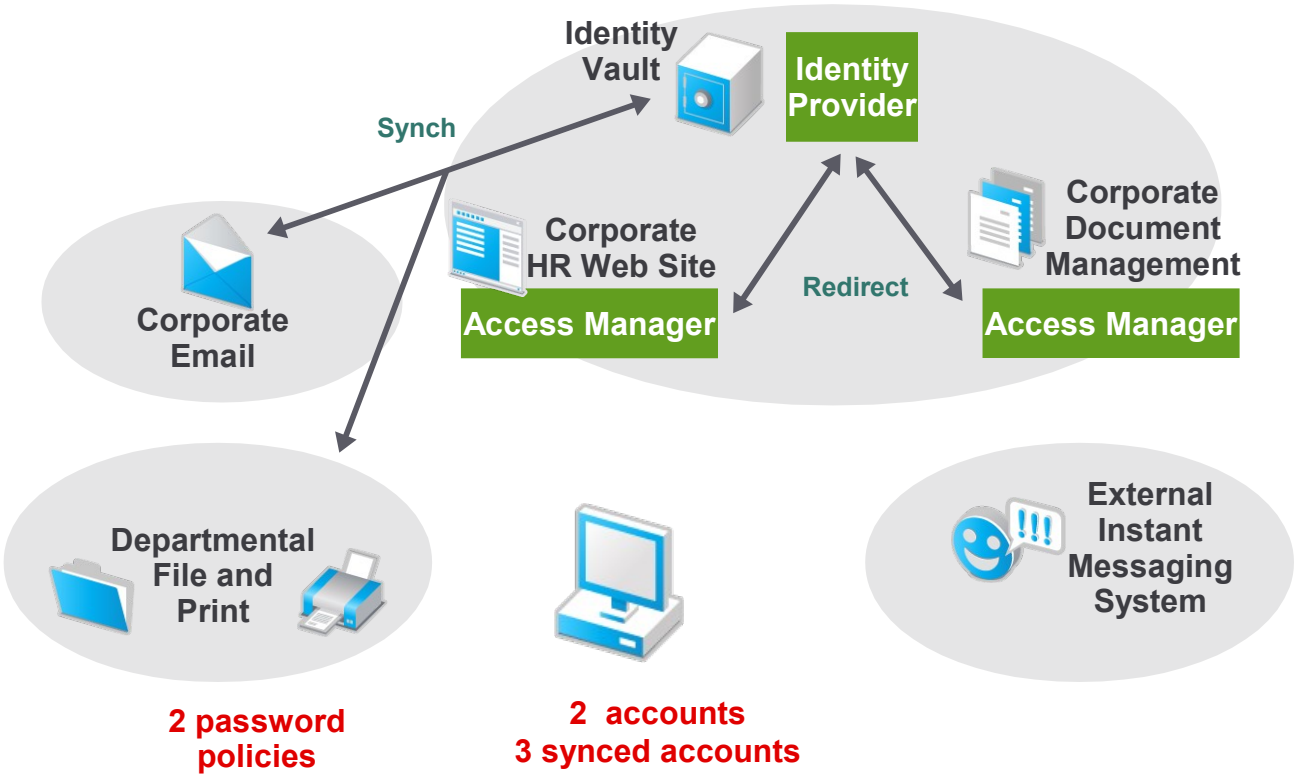



It seemed like such a good idea at the time...

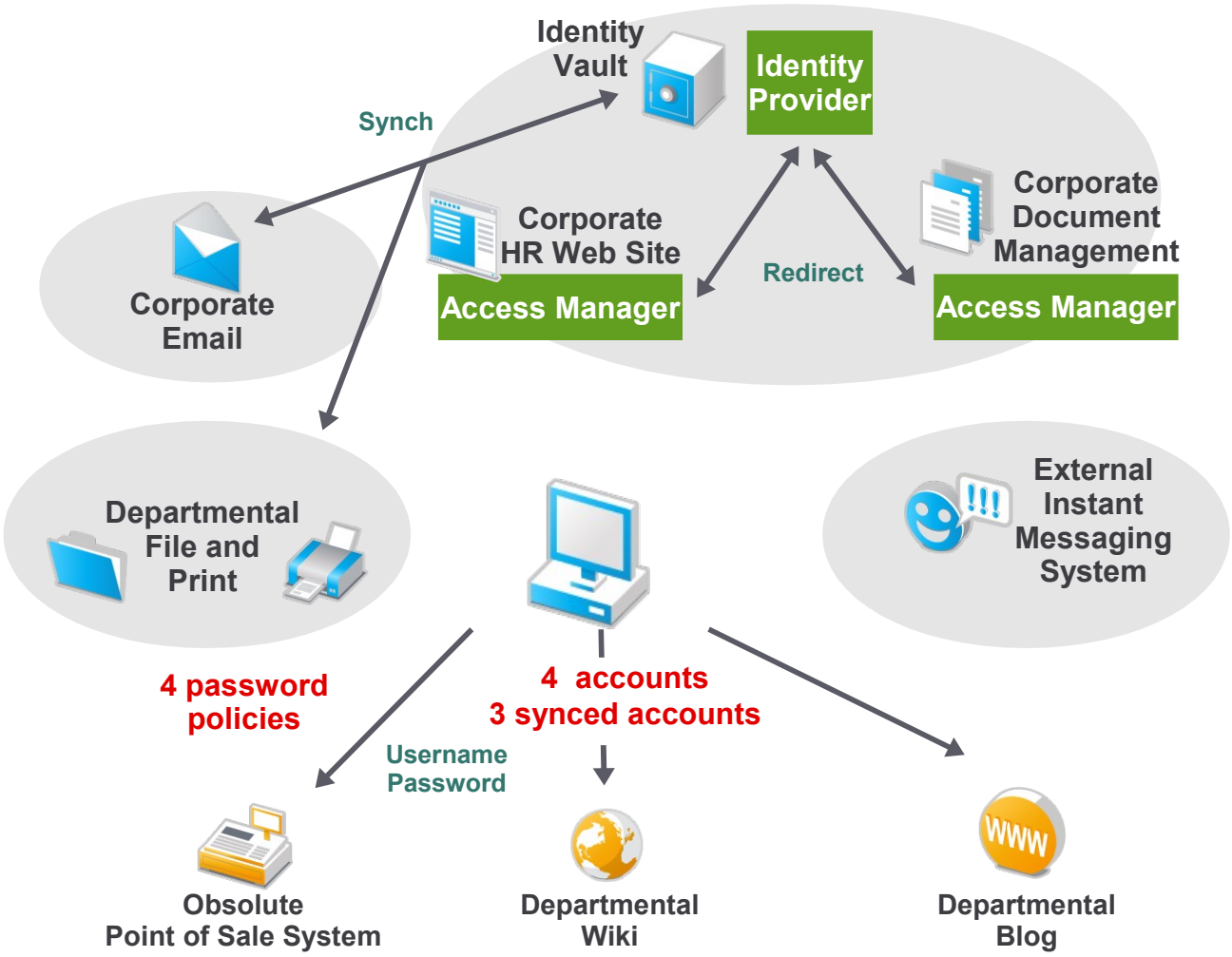
# Multiplication of Network Services



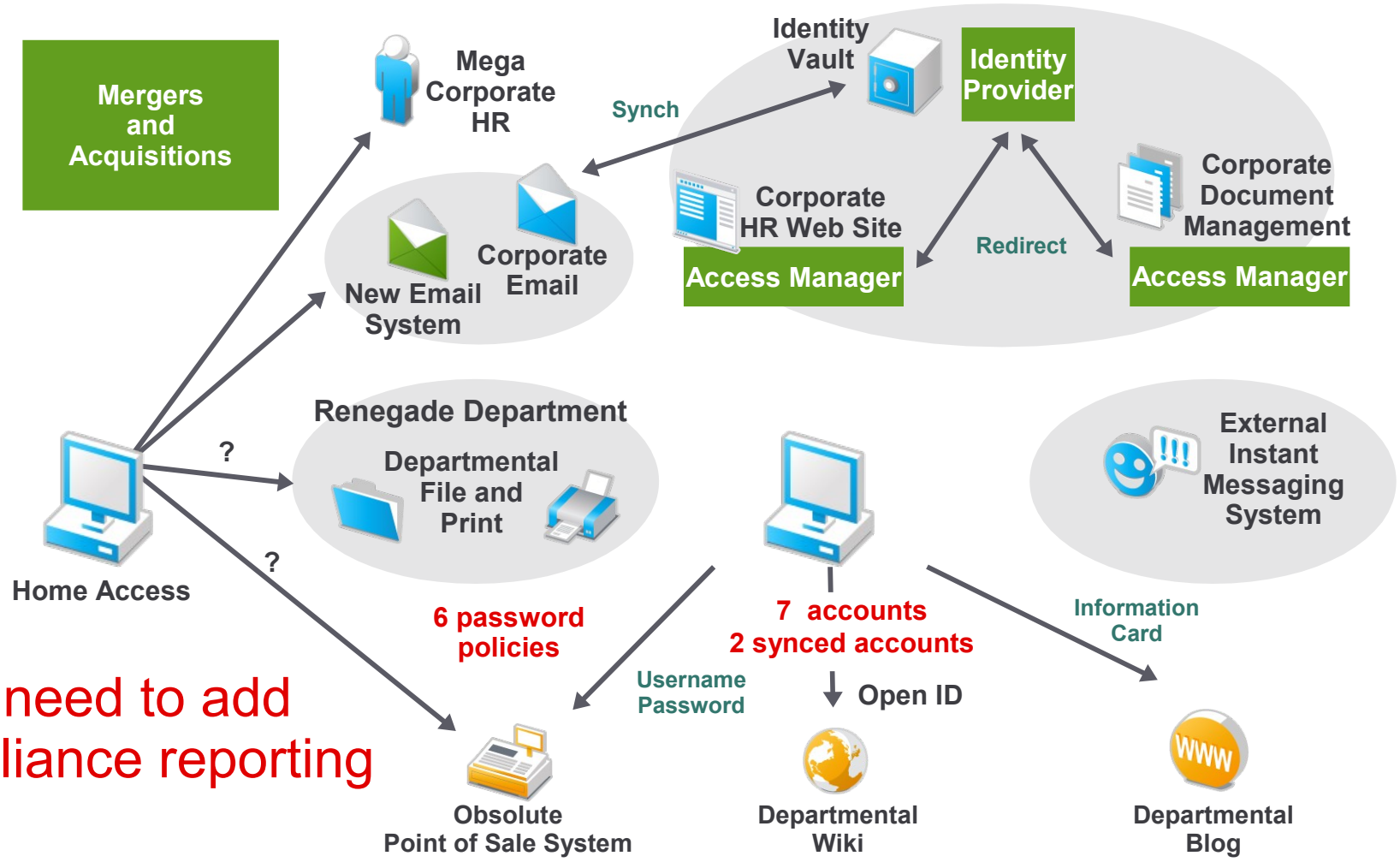
# Boundaries and Identity Management



# Obsolete and Evolving Services

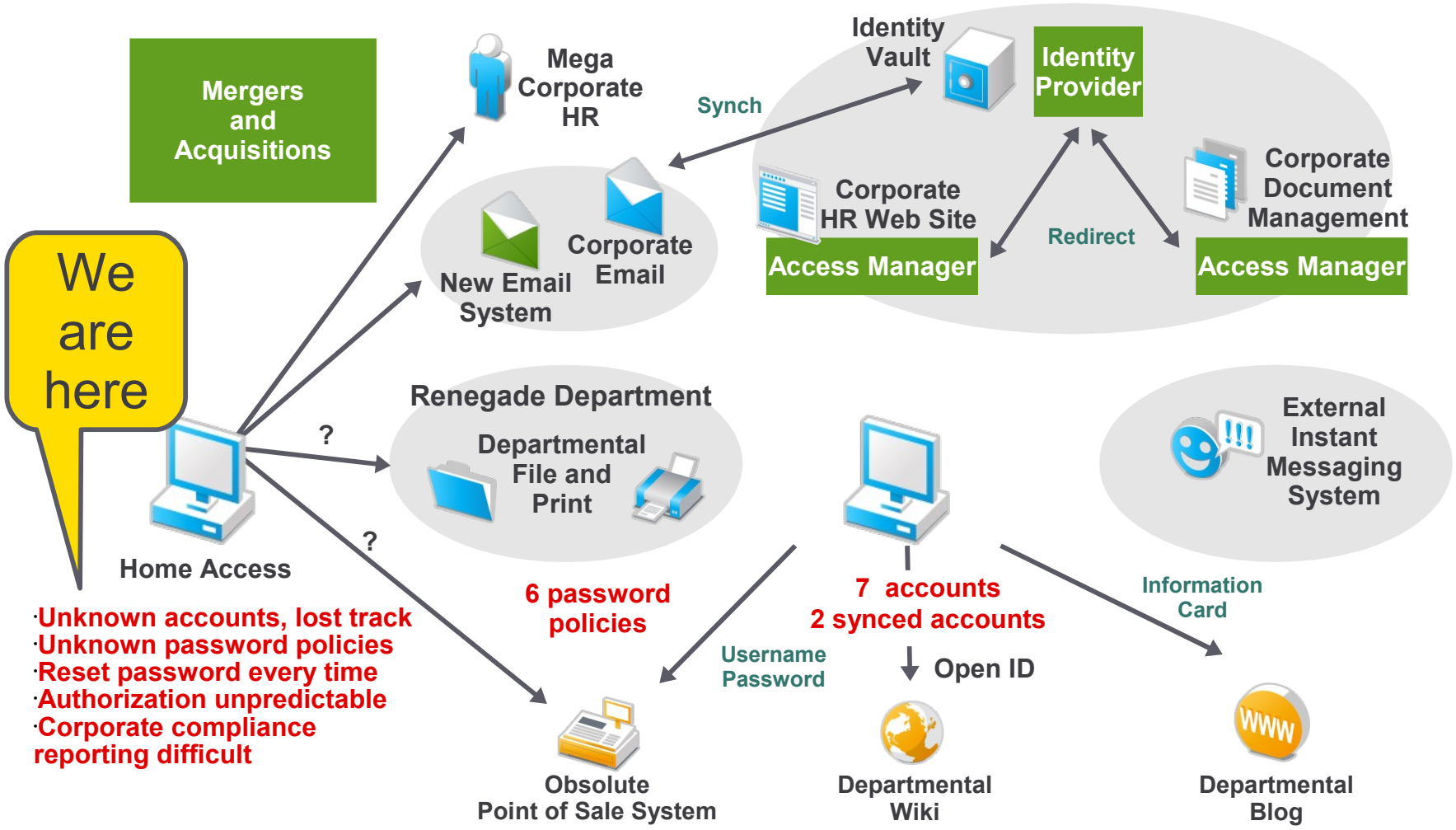


# Changing Boundaries, Dissolving Perimeters




Also, need to add compliance reporting

# It's Not So Simple Anymore



# The Problem with Identity Systems

"Internet identity systems won't be widely used until they are simple enough for grandma, and she will only remember one username and password."

*Statement from panel discussion at EIC 2008*

*(as best as I can remember it)*

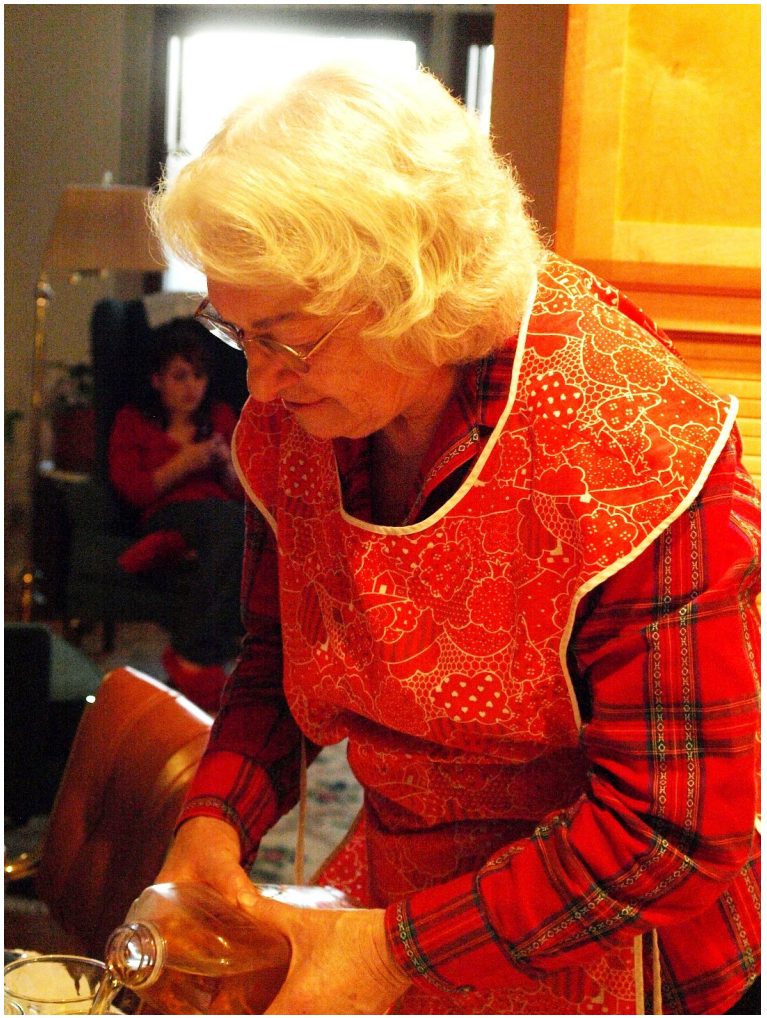
**I could not disagree more.**

# Granny Needs a Richer Identity System

We don't need to dumb it down for her. She can easily handle complex forms like politeness. She can handle context, courtesy, respect … relationships.

***Politeness is calibrated to the level of the threat to the hearer's face. The threat level in turn depends on the size of the imposition, the social distance from the hearer (the lack of intimacy or solidarity), and the power gap between them.***

*The Stuff of Thought – Language as a Window into Human Nature, by Steven Pinker*



# The Real Problem for Identity Systems

- The problem is not to make is simple enough – as in one username and password – for granny.
- The problem is that it needs to be intuitive, contextual, and nuanced enough for granny to express the subtleties and richness of her relationships.
- These issues exist in employee and customer relationships as much as they do for granny.
- Granny manages it all just fine in real life – better than most technologists.

# Trends to Help Granny and the Rest of Us

# Multi-domain Identity Systems and the Identity Provider Model

- In the picture of the current mess, most problems are related to one user account per online service.
- The Identity Provider model separates (frees) the user account, authentication, and identity information from the online service.
- Federation and user-centric approaches all follow the model, e.g. SAML, WS-Fed, OpenID, Information Cards, OAuth.
- The identity provider model is just as useful within an enterprise (across departmental boundaries) as it is for consumer Internet services (multiple service providers).
- This is good timing since the enterprise walls are coming down.
- Cloud computing services are accelerating the collapse.

# Less Identification More Authorization

- We are moving to less identification by a service.
- Instead access is granted due to token contents rather than authentication.
- Authentication is external to application or service, only to Identity Providers.
  - The anonymous student health clinic story
- The difficulty is that it involves a paradigm shift for programmers  who are used to asking “who is this and what can they do” (authentication then authorization).

# Token Transformation & Combination

- Many identity information transactions involve more than 2 identities.
  - The identity provider(s) who assert the information
  - The user(s) who release the information
  - The service that uses the information
- Token and document transformation/combination rather than connection/credential.
  - Token based (e.g. SAML) rather than connection (LDAP)
- For example, consider the grade school field trip permission system.

# Progress, Overlaps, and Gaps

# Progress in Internet Identity Systems

- Last year this stuff (OpenID, information cards, user-centric, federation) was a hot topic, now...
  - “Don't hear much about it anymore...”
  - “Not much traction...”
  - “So... how's that identity metasystem coming?”
- However, progress has been steady and fast:
  - Before the dawn of time there were Directory Services which begat LDAP. Shortly thereafter the Liberty Alliance begat federation...
  - 2006: Protocol consolidation and open implementation issues resolved (Open Specification Promise, OpenID 2.0 started, and, um, federation kept going).
  - 2007: Dozens of interoperable implementations developed and demonstrated.
  - 2008: Vendor supported products developed and early adopters deploy.
  - 2009: Started with shipping products (insert shameless Novell plug here), government deployments scheduled, even identity conference usage (like EIC).
- What's next? It should be real world deployments.

# Are Overlaps Bad?

- The world runs on a financial services model that is similar to the identity provider model
- Checks similar to OpenID: easy to implement, but spoofable.
- Information cards similar to credit/debit/business cards: useful for many things, but more difficult to implement.
- Electronic transfers between linked accounts are like federation: difficult to set up trust relationship, but essential.
- All are useful for some scenarios.

# Some Overlaps are Not Useful

- Overlap of browser plugins and client agents between protocol families are counter-productive.
- Perceived “protocol wars” in the press are distracting.
- Semantic clashes (impedance mismatches) between protocol families are an insidious problem.
  - For example, there are various approaches and meaning as to how to transfer a SAML token via OpenID.
  - Syntax and protocol are easy for specific use cases.
  - Synchronizing schema and semantics of a general (and good) underlying identity model is hard.
  - But that's what we should do.

# Gaps 1

- Terms and conditions should be attached to claims
  - If your service asks for identity information, make it clear to the user (and attach it to the data) the terms and conditions to which the user agreed, e.g. did you promise not to sell it to spammers?
- User-agent string pollution
  - Some identity selectors are advertising themselves in inappropriate ways.
  - The user agent string is for diagnostic messages, not client capabilities.
  - Show some respect to granny. Offending vendors, you know who you are.
- Multiple information card support
  - Many real-word information card use cases involve multiple sources of identity information (or cards), yet the user interface does not support this.

# Gaps 2

- Auditing instrumentation, standards, tools
  - Who did what, when?
  - Appears to be surprisingly little interest from vendors and implementors
  - However, XDAS is active and viable.
- Receipts
  - When granny buys something (a transaction involving a more powerful entity) she gets a receipt.
  - Allows her recourse in case of a dispute
  - Allows her to mercilessly harangue the unfortunate kid at the returns counter

# Questions?

For me: Dale Olds <dolds@novell.com>

For Granny: Are you sure you want to ask? If so send them to me, I will relay them.


Novell®