# Using History, Collaboration, and Transparency to Provide Security on the Web

Mary Ellen Zurko, Dave Wilson
IBM Software Group,
Workplace, Portal and Collaboration Software

# What I'll Talk About

- **The problem space**
- **Trustworthiness of web sites from the people perspective**
- **Metadata for reality based assurance of web sites**
  - Personal history
  - History of others with personal connections
  - Mediators and authorities

# The Problem Space

- **Semantic attacks via the combination of mail (push) and web sites (pull) on individuals**
- **Web site authenticated name is only a computer artifact (DNS domain)**
  - Multiple DNS domains legitimately act on behalf of a single wetspace institution
- **Worth of data stolen may be global or targetted**
  - Credit card vs. Bank account + password

# Trustworthiness of web site

- **Users use attributes not tied to any notion of computer security**
  - Ease of use
  - Attractive and professional design
  - Consistency, familiarity, predictability
  - Seals of approval
  - Explanations

# Metadata for Reality Based Assurance of Web Sites

- **Personal history**
- **History of others with personal connections**
- **Mediators and authorities**

# Personal History

- **Pattern of previous accesses**
  - How often, over what time period
    - Most recent – when
  - How the user got there and gets there
    - Typed, linked, or followed from another program
      - Can help with transition to outsourced areas
    - Bookmarks exist?
  - If the site was authenticated previously
    - Previously authenticated with same site key
    - Cookies for that site
  - Data posted previously
    - Values new or repeated?
    - P3P policy association would help

# History of Others with Personal Connections

- **Issues of usable authentication and trust are moved from authenticating web sites to trusting (meta) data from others**
- **XML Digital Signature standard can help**
  - Key management to sign and trust in signers become the issues
  - Linkage with public keys in user's address book provides one solution
  - Wetware communities can solve this problem with shared trusted infrastructure
    - For example, enterprise directories
  - Public key certificate from OpenID URL associated with the person you believe you want to trust also possible

# Mediators and Authorities

- **Can minimize the trust issues if gatekeepers, mediators or authorities can be used**
  - Not a strong tradition in P3P, PICS, or SSL
    - Slightly better with spam blacklists
      - Still issues with false positives and vigilantism
    - Works if the trust comes pre packaged
      - Browser shipped trust in SSL certificates for servers
  - OpenID servers may provide useful information on what others have done with a site
    - Which OpenID servers do you trust?
  - Time remains a critical component to avoid brief, intense scams

# In Summary

- **Metadata tied to past personal actions, past community activity, and authority recommendations can combat large categories of web site scams**
  - Integration with mail infrastructure can provide additional benefits
- **More potential issues**
  - Bootstrapping
  - Roaming, multiple computers
  - Design that makes all the metadata consistently usable
  - Attacks on both technical and social aspects of metadata
  - Gaps from anything not absolute
  - Human ingenuity x human naiveté
- **Just need to make some other scam easier and more profitable**