# Feeding Practice Back Into Research

Mary Ellen Zurko

mzurko@us.ibm.com

LotusLive Security Architect, IBM

# Integrate Lessons from Practice into Research thinking to achieve Usable Security in Practice

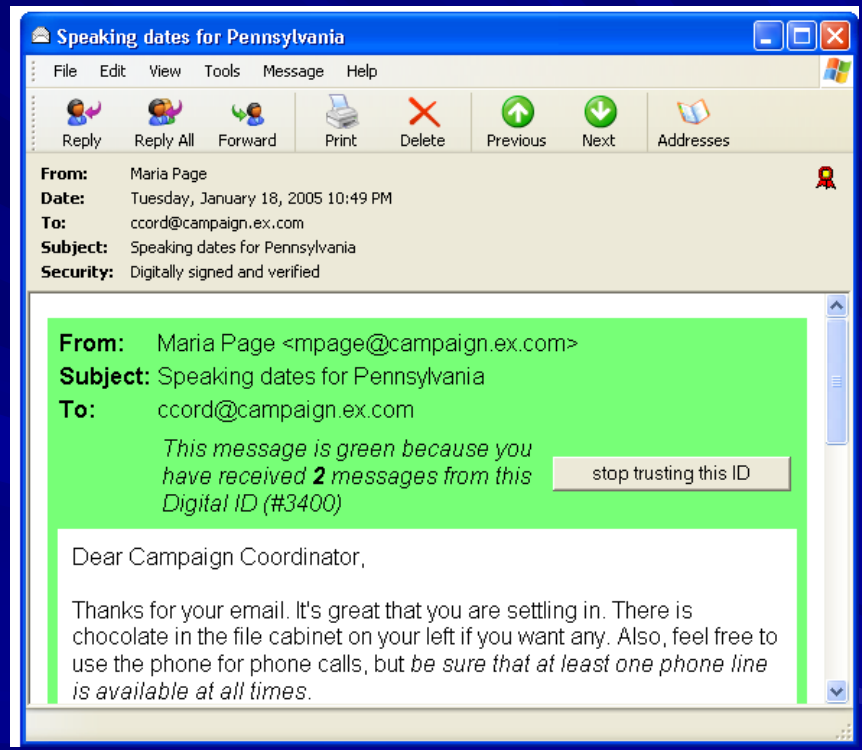
- In theory, there is no difference between theory and practice. In practice, there is.
  - Yogi Berra

- Cyclical approach to feed what we've learned from practice back into research; not just research feeding into practice
  - Making the problem harder makes it different

- Security weaknesses of text passwords were revealed by their use and changes in their use
  - Nostalgia – the days of having just one password
- Generated passwords worked 20 years ago
  - Only professionals needed, used at a computer in an office with a locked door
- Today many passwords,  different strength and management policies
  - Almost all forms of deployed passwords are unusably insecure
- Many of the alternate forms of authentication being researched today have substantial barriers to deployment
  - Scale of enrollment, complex infrastructures only supporting passwords

# Interaction between development concerns and research findings

- Mundane development and deployment concerns can impact the feasibility of technology transfer of user-centered security work
- Many disciplines and features vie for limited design and UI space
- Security dialogs – I can take all the space I want with security concerns
- Not so for the mail display UI
- Tradeoffs that are critical in practice must inform research if research is to successfully transfer to practice and products



# Technology Transfer

- Tools or best practices that allow a larger body of practitioners to incorporate user centered security into their system.
- Criteria or checklists for evaluating how usably secure a system or approach is likely to be.
- Standards (W3C WSC as first example)
- Make Intellectual Property (IP) status clear

# Issue Investigation

- To advance usable security, research needs to actively seek development, deployment, and use experience, and development needs to actively seek deployment and use experience
- Articulation of deployment-specific concerns
  - Scale, performance, usability, accessibility, TCO, ROI, full featured user experience, compliance constraints
- Funding for research that articulates and responds to deployment-specific concerns
- Venue for publishing results
  - e.g.Industry tracks, NSPW for “the other edge”
- Specific use cases, frameworks, and challenges
  - Standards if they are already deployed
  - Walk through a full deployment scenario lifecycle

# How can research get feedback from deployment?

- User studies of deployed technology (e.g. contextual analysis)
- Measure changes in user behavior (change user experience of security in web services)
- Open source, free product betas
- Lightweight iterations and analysis
  - A place for metrics?
- What about deployment characteristics of security? (e.g. tiger teaming)
- Hard to change something that will impact the security of a system
  - Control and oversight (e.g. drug trials)

# Questions?

- Thank you for your time
- Please keep these and other short talk issues in mind during our break out brainstorming