Beyond Phishing

Simson Garfinkel

James Foley

Susan Landau

Beyond Phishing Session 1

Whose "usability" are we talking about?

- Programmers
  - *Can good HCI-SEC patterns be built into an IDE or a library?*
- End-users
- System Administrators
  - *Admins of large-scale websites (revert doesn't work for them)*
  - *Admins of home-networks (everybody)*

Beyond Phishing Session 1

Identified Research Problems:

- Which security properties should be transparent (i.e.: easy to see), and which should be transparent (i.e.: invisible)?
- How do we understand the user models currently used for secure operation?
    - *Can we foster better user models?*
- How would we certify a platform as aligning security, privacy & usability?
- Usable methodologies for designing systems that are secure.
- Usable methodologies for designing systems that are secure and usable.
- How do usability & security properties compose?
- Are there situations where usability & security really are tradeoffs?
    - *(Brooks accidental vs. inherent complexity)*
- What kind of regulation might help?
- Can we develop a model to help trade-off risk vs. usability?
    - *How do people perceive the risk tradeoffs?*

Beyond Phishing Session 2

What are the barriers to adopting non-password authentication tech?

- Fear of "Big Brother" (a technology that allows correlation across multiple websites.)
- Lack of drop-in software?
- Cost of implementation?
- Lack of awareness?

What are the prerequisites to firms accepting identification credentials issued by other firms?

- Legal requirements?
- Technical requirements?

Are there alternatives to "fact-based authentication" for bootstrapping identification systems?

How do we educate about privacy and security trade-offs?

Beyond Phishing Session 2

What has been the barrier to adoption of federation-based authentication schemes? Would standardizing rigor of systems used for authenticating help?

How do we go beyond fact-based authentication schemes? What might we use for authentication?

Suppose we consider authentication schemes by needs of users: how do we even begin to classify what the different sets of users are?

Suppose the user has a strong authenticator, e.g., the government Common Access Card. What has prevented the adoption of usage outside the workplace?

Suppose users had a single authenticator that could be used universally. Would they prefer to have that supplied by the government or by private industry?

Beyond Phishing Session 2

What has prevented the adoption of Brands' zero-based knowledge system of authentication, a single authenticator that provides privacy by allowing authentications in different sites to remain unlinked?

Would users prefer a single authenticator as described above, or multiple ones, even though the single one provides unlinkability between sites?

- The Europeans use stronger forms of authentication than the Americans. What in European society has enabled the adoption of stronger form of bank ID (with smart card), chip and pin (is that actually really stronger), etc.?
- Has Europe’s purpose limitation on commercial data collection played a role?