Web Security Requirements: A Phishing Perspective

What is Usability? How are we failing?

Ian C. Fette, Norman Sadeh, Lorrie Cranor

March 15, 2006
{icf,sadeh,lorrie}@cs.cmu.edu

http://cups.cs.cmu.edu/
The Phishing Problem

- It's easy to fake a page and collect user information
Overview

- What does it mean for security to be usable?
- What security features do we currently have?
- Why what we have has failed (or will fail)
- Where our group is looking
- Concluding Remarks
What is usable security?

• Any interactions with the user should be at a level understandable by said user

• Required user interaction (both input and attention) should be kept minimal

• Should be “hard” for a user to commit a serious mistake

• Should be usable from wherever the user may be (public cafe, mobile device)

• Should consider users' disabilities
Current Security Features

- The Lock
  - Ignored by many
  - Confusion as to what it means
  - Mis-used by websites (next slides) so as to diminish power

- RSA SecurID

- PassMark SiteSecure

- Various chrome extensions
We've Failed The Lock

- We started with something ill-designed
- We made it worse by confusing the issue “The lock means you're secure”
- We started using the indicator outside of its normal location, and now people look for it outside of its normal location.
RSASecurID

- Moving beyond the browser to hardware assistance
- Usable at home or on the road
- ... but vulnerable to man in the middle attacks
Passmark SiteSecure

- Attempt at two-factor mutual authentication using properties of the computer as the second factor

- Enrollment process to 'sign up' a computer

- Once enrolled, user authenticates in part based on the computer they are using

- Bank authenticates itself by displaying a shared secret (picture)

- Enrollment process can be spoofed
Phishing Toolbars

- Overall, fail to protect users from high quality spoofs
- Users ignore indicators, as security is not their primary objective
- Pop-up warnings are slightly more effective, but overuse and false positives lead to the “just-click-ok” syndrome.

Where Our Group is Looking

- **Heuristic Detection**
  - Link Characteristics and HTML tricks
  - Header Information
  - Domain Age
  - “Inbox context”

- **Collaborative Approaches**
  - Leverage economies of scale
  - Publish warnings, or “vaccines” (think virus definitions)
  - Issues of trust in reporting, detecting misinformation
Where Our Group is Looking (2)

- **Semantic Approaches**
  - User's environment knows more about the user than the ISP does
  - Detect deviance from normal user behavior
  - Semantic approaches, including digital wallets or federated identity management systems

- **Leveraging Out-Of-Band Communications**
  - Salvaging PKI
  - Building on current relationship establishment procedures
  - Facilitating support technologies
Where Our Group is Looking (3)

Understanding the Users: Interviews

- People misunderstand many cues the browser provides:
  - Some are alarmed by 'warnings' that they are entering a secure site
  - Certificates, especially self-signed, and encryption are confusing to users: “I guess I'm not fully sure what 'encrypted' means.” - user
- Some are highly affected by targeted attacks
- Past “experience” doesn't necessarily help
Where Our Group is Looking (4)

- Educating the User
  - Providing training in the context of the user's inbox
  - Tailoring the training to the specific user's needs, adapting to strengths and weaknesses
  - Creating an educational game to teach anti-phishing skills
Concluding Remarks

- New solutions must take usability into account

- Security should be analyzed from a holistic perspective, including user analysis
  - What do we rely upon the user doing?
  - Can the user be tricked into doing a “bad” action at any stage?

- Expectations for user action should be minimal

- Active, positive indicators of problems
Questions?

- Thank you

- Ian Fette, Norman Sadeh, Lorrie Cranor
  Carnegie Mellon University
  School of Computer Science – COS
  5000 Forbes Ave.,
  Pittsburgh PA 15217

{icf,sadeh,lorrie}@cs.cmu.edu