Web Authentication and Phishing

Sam Hartman
Massachusetts Institute of Technology July 14, 2006

hartmans@mit.edu

Starting with Local UI

- The local browser needs to distinguish cryptographically strong protocols from passwords sent over the web in its UI.

- This UI cannot be spoofable.

- One possible mechanism is for users to brand computers when they install them.

Requirements for Web Authentication

- Support for passwords and potential other credentials
- Password equivalents never sent across the net
- Mutual authentication of the server
- Binding of the returned web page to the authentication

What These Requirements Bring Us

- One mistake does not lead to compromise of credentials
- Servers know they are talking to clients not phishers.
- Confidential information held by servers with existing relationships can increase confidence you got the right server.