Strengthening Password-based Authentication

SCOTT RUOTI
JEFF ANDERSEN
KENT SEAMONS

BRIGHAM YOUNG UNIVERSITY
Problems with Passwords

POOR SECURITY AT THE SERVER

• Servers have access to password plaintext
• Users trust that servers salt+hash before storage
• Many servers are vulnerable to password theft

VULNERABILITY TO PHISHING

• Web pages have access to password plaintext
• Phishers impersonate legitimate site
• Credentials immediately vulnerable

Password re-use compounds both problems
What can be done?

- Strong password protocols
- Safe password entry
Strong Password Protocols

Client -> HTML + JS -> Password "Handshake" -> Remote Server

HTML + JS <-> HTTPS

Password Handshake
Safe Password Entry

- Spoof-resilient password-entry interfaces
- Interfaces that indicate they are privileged
  - Position on screen
  - OS features
  - SiteKey
Dynamic Security Skins, Dhamija [2005]

- Over 500 citations
- SiteKey
- Strong password protocol
- Visual hashes provide site authentication
Our Ideas

• Safe Password Entry
  • Browser chrome
  • Operating system prompt

• Site Authentication
  • Browser detects handshake failure
Next Steps

1. Build our systems

2. Design a user study using good methodologies
Improving User Studies

PRESENT METHODOLOGY

• Too short
• Occurs in a lab
• Participants are primed
• Lab-assigned credentials

PROPOSED METHODOLOGY

• Long-term
• “Take-home”
• Deception
• Personal credentials
Preliminary Study Design

• Assign user to one safe password entry tool
• Playtesting a new game suite
  • Access via BYU Single Sign-On
• Daily testing, over 10-day period
  • Game links delivered over email
• On day 7, users are phished for their SSO password

Work Needed

• Introduce safe password entry without priming for security
• Ensure study is safe for participants
Points of Discussion

• Where should safe password entry be implemented?
  • Browser window, browser chrome, or operating system

• How can safe password entry effectiveness be accurately evaluated?
  • Ensuring both deception and safety for users