Identity in the Browser
-or-
Putting the Cart Before the Horse?

Andy Steingruebl   and   Jeff Hodges
{asteingruebl,jeff.hodges}@paypal.com
PayPal Information Risk Management

Position Paper for W3C Workshop on Identity in the Browser
May 24 and 25, 2011 – Mountain View, CA
Given that...

- Online user credentials today are typically
  - Reusable
  - employ shared secrets (aka “passwords”)
- Users will enter their credentials into most any online form
- People can and will divulge their credentials when nominally prompted
Then...

• Phishing is fun and profitable!
Also, since...

- Mobile handheld ubiquitously Internet-connected third-party programmable devices == “smartphones”
- Smartphones are a different sort of computer
  - Smaller keyboards and screens
  - Power limitations
  - Social connotations
- Smartphone adoption is skyrocketing
Then...

- We **really** need to think differently about user authentication on smartphone platforms, otherwise...
- Phishing will be even more fun and profitable!
And since...

- All sorts of boxes/things feature a web server...
  - ...hosting configuration/management interfaces
- E.g...
  - Network middleboxes
  - Appliances
  - Industrial control systems
  - Vehicles (soon?)
- Vulnerable to Cross-Site Request Forgery (CSRF)
Then...

• Might be even more fun than phishing...
Present Workshop Goal...

- Solutions to be explored are effective enhancements to Web browsers that lead to trustworthy benefits that can be realized in the near term
Rethink/Refine Our Goals...

- User authentication without phishable credentials?
- How to mitigate CSRF?
- Get heads around new world of smartphones?
- New paradigms for security indicators?
- More consistent security characteristics across major browsers?