Goals, constraints, and issues for identity in the browser

John Linn, Sr. Technologist, Office of the CTO, RSA, The Security Division of EMC

W3C Workshop on Identity in the Browser, Mountain View, CA

19 May 2011

Introduction

- Browsers are core Web interaction components, and natural loci for managing identity elements
- Today, browsers are primarily conduits, but they can provide deeper support in active identity agent roles (users' delegates)
  - They can participate in protocols that users can't, directly
  - They can inform users about site characteristics
  - They can enforce user-selected policies
  - They can operate autonomously on behalf of their users
- But, delegation to powerful but untrustworthy browsers would be a Bad Thing!
- Following slides: citing concerns by interface (user, network, platform)

User-facing concerns

- Users must be able to manage what identity elements are shared, and with what sites
  - Privacy and credential usage policies and controls
- Users should be able to authenticate with multiple methods (e.g., per NIST SP 800-63-1), rather than being tied to passwords
  - Mobile devices are important enablers
  - User authentication to browser/platform, distributed authentication protocols to sites
- Users need trusted control and display paths
- All of these interactions need to be usable and comprehensible!

Network-facing concerns

- New or upgraded protocol adoption can be elusive, unless
  - There's value to site operators;
  - There's compelling value to users; and/or
  - There are regulatory mandates
- Proposals must be deployable gradually, and should offer incremental and motivating benefits
  - Challenge: upgrading both of a protocol's peers
- Standardization processes may help to evolve approaches and to filter chaos

Platform concerns

- Browser identity enhancements shouldn't increase credential exposure
  - Either directly, or by enabling credentials to be wielded outside user intent
  - Concentrated data concentrates potential attacks; platform elements can aid credential cache protection
  - Implication: assurance concerns for browser and underlying platform
- Identities (including their credentials) need to be mobile or movable among clients
  - Issue: functionality and trust in supporting servers

Conclusions

- Enhanced browsers can support users' Web interactions with strong security, privacy, and control
- Powerful agents imply increased assurance requirements
- Methods should provide functional value and support incremental adoption
  - Simplicity, capability, and deployability, as well as security
- Challenge: interoperable benefits, not fragmented confusion