Identity as a Platform Service

Sam Hartman (Painless Security)
Josh Howlett (JANET(UK))

Identity in the Browser
May 25, 2011

Platforms Help Identity Management

The platform is in a position to improve browser identity because it has information that cannot be shared with applications:

- ➜ List of identities
- ➜ Cached credentials
- ➜ security policy
- ➜ Channel bindings

No Single Mechanism will Win

- ➜ We will not settle on a single mechanism for conveying identity
- ➜ Enterprise, consumer portals, government all have different requirements
- ➜ The platform can make mechanisms available so applications need not support everything

Best Practices Beyond the Web

- Platform provides security services; applications may pick up and use new mechanisms without any code changes
- Example: IETF's Common Authentication Technology supports OpenID, OAuth, SAML, Kerberos and public-key
- Moonshot: new mechanism taking advantage of platform to drive federation
- Application is in control of how much mechanism knowledge it needs

Application and Platform Together

- Platform provides mechanisms and identities to application
- Application can supplement these possibly even adding new mechanisms
- Application can feed in credentials and identities it knows about
- Application controls the UI

Recommendations

- ➜ Provide platform extensions for identity management
- ➜ Provide web application libraries to facilitate identity management with or without these extensions
- ➜ Where present take advantage of platform security beyond the browser