The Increasing Importance of Proof-of-Possession to the Web

W3C Workshop on Authentication, Hardware Tokens and Beyond

Michael B. Jones

September 10, 2014

Abstract

- *A number of different initiatives and organizations are now defining new ways to use proof-of-possession in several kinds of Web protocols.*
- *These range from cookies that can't be stolen and reused, identity assertions only usable by a particular party, password-less login, to proof of eligibility to participate.*
- *While each of these developments is important in isolation, the pattern of all of them concurrently emerging now demonstrates the increasing importance of proof-of-possession to the Web.*

Existing Uses of Proof-of-Possession

- TLS (https) most common use of PoP
- *PoP internal to TLS implementations and not exposed to applications*

TLS Channel Binding Work

- Enables non-replayable cookies
  - Already deployed in Chrome
- Channel ID values can be used in higher-level protocols, such as OpenID Connect
  - Prevents replay of ID Tokens, Access Tokens, etc.
- tools.ietf.org/html/draft-balfanz-tls-channelid

- *Brining the benefits of TLS PoP to applications*

Current OAuth PoP Work

- Authorization Code PoP
  - tools.ietf.org/html/draft-ietf-oauth-spop
- PoP Key Distribution
  - tools.ietf.org/html/draft-ietf-oauth-pop-key-distribution
- PoP JSON Web Token (JWT) Representation
  - tools.ietf.org/html/draft-ietf-oauth-proof-of-possession
- OAuth PoP Architecture
  - tools.ietf.org/html/draft-ietf-oauth-pop-architecture

- *Lots of work for PoP-enabled applications happening*

PoP for Login

- Login by proving possession of a private key
  - Instead sending a password
- Key ideally held in secure storage
  - TPM, tamper-resistant device, etc.
- Solutions for this being explored platform vendors, FIDO Alliance

- *Can be both more convenient and secure than passwords*

Proving Eligibility to Participate

- Using platform-held key as proof of eligibility to participate in an online interaction
  - Mechanism essentially same as PoP-based login
- JavaScript support for using platform keys needed for JavaScript apps to participate

- *WebCrypto Key Discovery our starting point*

Conclusions

- The number of independent initiatives working on enabling PoP demonstrates increasing importance of PoP for the Web
- PoP being surfaced to applications
- WebCrypto specs will need to enable use of platform and device PoP keys for JavaScript applications to be able to participate

- *Result will be more secure, usable Web*