HTTP Origin Bound Authentication (HOBA)

Providing a way to Displace Passwords

draft-farrell-httpbis-hoba-02

Stephen Farrell, stephen.farrell@cs.tcd.ie
Paul Hoffman, paul.hoffman@vpnc.org
Mike Thomas, mike@phresheez.com

IETF-85

Problem, Goals & Solution Overview

- Web sites have password verifier databases and those frequently leak out exposing (literally) millions of (maybe hashed, maybe not) passwords every year – pick your favourite example
  - **MANY** bad effects
- Goal: Replace password verifier database entries with something that can safely leak, in a way that can easily be “dropped in” to a site
  - Non goal: solve all web authentication problems
- HOBA Solution:
  - Password verifier replaced with public key used only for that site
  - Private key used in signature based challenge-response protocol as an HTTP authentication Method ***or*** from Javascript
    - Private key storage in browser (HTTP Auth) or LocalStorage (Javascript)
    - Javascript aspects of the solution are non-normative but a good example to follow
  - Usual cookie based session stuff can follow authentication
  - Admin (enroll/mobility/etc.) fully controlled by application in a process triggered via .well-known URLs.

Picture

TBD

A Few Details

- Enrollment via .well-known/hoba/ means that HOBA has NO user interface, all is left to the application, e.g. no username needed
  - Account/Authentication separation is crucial
- Mike's Javascript implementation is live:
  - http://mtcc.com/
- Things needing work:
  - Challenge response crypto detail
  - Level of harmonisation between HTTP auth and Javascript
  - Handling of off-site re-directs during e.g. enrollment
  - Details details...

Summary

- Loss of password databases is a key problem that is costly, serious, fairly widespread, getting worse and any site can be affected by any other given password re-use patterns
  - HOBA solves **this** problem, which is our goal
- It is (way past) time that the IETF offered the Internet community something usable and more secure
  - We think HOBA does this too