Requirements for Coherent Web Security Framework

Jeff "=JeffH" Hodges
IETF-79 Beijing

Chartered Item

- Deliverables
  - A document illustrating the security problems Web applications are facing and listing design requirements. This document shall be Informational.

Motivations

- Multitude of classes of issues
  - “content” aka “a web app”
    - .js embedded or retrieved? From where?
    - User input allowed? Can it subvert web app?
    - XmlHttpRequest, Flash sockets, ...
    - etc.
  - Network
    - Secure transport on or off?
  - Combinations thereof

Motivations, cont'd

- Plethora of Disjoint Approaches
  - Flash policies
    - conveyed by file crossdomain.xml, unique syntax
  - ABE (Application Boundaries Enforcer)
    - conveyed by a file, unique syntax
  - HSTS/CSP/CORS
    - conveyed by unique headers, unique syntaxes
  - STS-ng (others?)
    - conveyed via DNS ?

Question

- What is “policy” ?
  - Is there a difference between “mandate” and “policy” ?
  - Need to answer & define
- Suggestion..
  - Use these terms from RFC 4949..
    - security policy
    - policy rule
  - A “mandate” is a particular “policy rule”

Security Policy Conveyance Mechanisms On Table

- HTTP headers
- DNS (augmented w/ dnssec)
- host-meta / crossdomain.xml (ie "file" (+DNS?))
- TLS extensions
- cert extensions

Policy Scopes On Table

- Policy domains of applicability
  - Web App code/data (aka “content”) policies
    - E.g. CSP
  - HTTP verbs/methods policies
    - E.g. ABE
  - per origin policies
    - HSTS, CSP, ABE
  - Cross-origin policies (e.g CORS)
  - Network operations (e.g. HSTS)
- cookie-based policies
  - Do not necessarily provide isolation via Path attribute, thus don't work well for per-resource policies

Various Issues

- Tension between policy scope expressiveness and deployment models
  - e.g http//example.com/~user/public_html
    - Users can muck with web apps emitted by example.com and other users
  - e.g. mapping keys to domain names in DNS
    - Map keys to “example.com” ?
      - Apply to all subdomains thereof ?
      - What if one's WWW and SMTP keys differ ?
    - Or map only to explicit “mail.example.com”, “ www.example.com”, domains, etc?
    - What about DNS-based name mapping ?
      - Eg DNAME, via SRV, etc.

Various Issues, cont'd

- i.e. "you *have* to use a new host name, eg 'mail.example.com', to make this work”
- ..is suboptimal from some slice of deployers' perspectives

Various Issues, cont'd

- Policy inheritance
  - Cookies “mapping up the tree”, vs
  - HSTS “mapping down the tree”

Various Issues, cont'd

- Policy management on UAs and in intermediaries
  - Caching / persistence
  - design/impl considerations
    - perf/cost in..
      - Additional bits-on-the-wire
      - UA processing overhead
      - # network connections and round trips

How to Proceed?

- Suggestion..
  - Concoct I-D from this session's presos, use to stimulate discussion, iterate