W3C Security Update

IETF 75, Stockholm

Yves Lafon <lafon@w3.org>
Thomas Roessler <tlr@w3.org>

XML Security WG

- XML Signature 1.1, XML Encryption 1.1
  - hash algorithms: SHA1 → SHA256
  - mark-up for ECC keying material (to supersede RFC 4050)
  - under discussion: ECDSA, ECDH as mandatory to implement
- Updated WDs due 2009-07-30

XML Security WG

- Generic Hybrid Cyphers
  - FPWD due 2009-07-28
- XML Signature 2.0
  - attempt at simplifying transform and canonicalization model
- http://w3.org/2008/xmlsec/

XML Signature HMAC truncation

- XML Signature has mark-up for HMAC truncation as part of the signature, but no explicit minimum truncation length - oooops
- Erratum and software updates 2009-07-14
- CVE 2009-0217

Widget Signatures

- HTML + JavaScript as portable application platform du jour
- Put into zip archive, add configuration file, call “widget”
- Code-signing: XML Signature profile http://www.w3.org/TR/widgets-digsig/

Upcoming: Device APIs

- Business driver: Convergence between Web applications and native applications; mobile market.
- e.g., application launcher, camera, contacts, messaging, device status, ...
- Challenges: security and privacy

Upcoming: Device APIs

- December 2008: W3C workshop http://w3.org/2008/security-ws/
- Upcoming: Device API and Policy WG
  - APIs for both applications (widgets) and Web sites
  - security policy expression
- http://w3.org/2009/dap/

Web Security Context

- Usability and consistent behavior of TLS related user interactions, error handling
- Wrapping up final set of Last Call comments
- Lesson learned: Standards that deal with usability are *hard*.
- Group to end 2009-12-31

Questions?

- Yves Lafon <lafon@w3.org>
- Thomas Roessler <tlr@w3.org>
  <xmpp://roessler@does-not-exist.org>