Overview

- Digression: XML Signature Authentication, Usability, and the Web
  Thomas Roessler, W3C

- Security Requirements for the Ubiquitous Web
  Dave Raggett, W3C

- Access Control, P.I.
  Charles McCathie Nevile, Opera
  Thomas Roessler, W3C
Digression: XML Signature

- XML Signature is coming of age.
- XML Canonicalization (C14N) has known issues.
  - xml:id - oops
  - xml:base - oops(2)
  - XML Core WG currently preparing C14N 1.1
- We're in listening mode about what the next steps should be for XML Signature.
Web Authentication Today:
A padlock means “secure.”
This is a padlock.
This is not a padlock.

From a recent phishing attack. The attacker’s site was, like the original, serving the form using plain HTTP.
A padlock means “secure.” Not.
Better don't click on the padlock, or else...
Better don't click on the padlock, or else...
Better don't click on "View", either.
A padlock means “secure.” Not.
But it gets worse...

Unable to verify the identity of people.w3.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be people.w3.org, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to accept this certificate for the purpose of identifying the web site people.w3.org?

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this web site
Examine
Or the user could go with the default...
A padlock means “secure.” Not.
Can we do better than this?

- The padlock doesn't make sense.
- X.509 certificates are technical gibberish.
- Current implementation doesn't even help suspicious users.
- Can we make Web authentication more usable?

15/16 March: Workshop in NYC

- 41 position papers, 60 participants, 23 presentations
- banks, browser & security vendors, academics, content providers
Secure Chrome & Secure Metadata

• Show different stuff to users
  – logos?
  – “this is a bank site”? “verified by ***”?

• Show it safely
  – The part of the user interface that displays metadata must be protected from faking through mark-up and scripting.
  – Restrict browsers' abilities.
  – Specific security mode?
Which one is the browser?
What can W3C do here?

- Enable browser vendors to restrict functionality in a concerted way.
- Enable content providers to connect security features to their brands.
- Specify data to be displayed.
  - could be “please use the logoType extension”
  - could be more complex than that - think content labels
Forms and authentication

- HTTP authentication isn't used widely
Forms and authentication

- HTML forms, POST and Cookies are the state of the art
HTML Forms and HTTP Authentication

• If user agents could recognize that an HTML form is used for credentials....
  – user agents could manage credentials, reliably
  – user agents could give the current user interfaces and combine them with HTTP-level authentication
  – user agents could trigger intelligent user interface behaviour - this could be a hook for login rituals

• New tags v. microformats / annotations?
Where do we go from here?

- Next step: charter draft(s).
- Please join the discussion: [http://lists.w3.org/Archives/Public/public-usable-authentication/](http://lists.w3.org/Archives/Public/public-usable-authentication/)
- Nearby:
  - IETF is discussing possible future developments on HTTP authentication
  - Online Identity (dix, Infocard, OpenID, ...)