Automatic CRL Updates for the Apache Web Server

Pascal Buchbinder

AdNovum Informatik AG
pascal.buchbinder@adnovum.ch
+41 44 272 6111

OWASP
Zurich, June 14, 2011

The OWASP Foundation
http://www.owasp.org

Certificate-Based Authentication

- Becomes popular again thanks to SuisseID
- One of the issues to consider is the revocation of certificates:
  - User has lost his private key
  - User's name has changed
  - Other attributes within a certificate have changed
  - User has left the company
- We may use OCSP (Online Certificate Status Protocol) or CRL (Certificate Revocation List)

Certificate Revocation List (CRL)

- Serial number of certificates that have been revoked:
  - Regularly updated (daily, couple of hours)
- Usage at client side (browser):
  - Not really (nine fraudulent digital certificates issued by Comodo can't be revoked by CRL)
- Usage at server side (Web server):
  - **Yes! But how do we load updated CRLs into the server on a regular basis?**

mod_sslcrl

- Module for the Apache Web server
- Extension to mod_ssl which verifies the validity of client certificates against the CRLs
  - Obsoletes the SSLCARevocationFile and SSLCARevocationPath directives
- Loads CRL information automatically via HTTP or HTTPS from the Certification Authorities (CA)
- It's an open source software available at

  http://opensource.adnovum.ch/

mod_sslcrl: how-to

- Download the module and compile it, e.g. by using apxs, the Apache extension tool
- Load the module into the Apache Web server
- Configure the module
  - Specify a cache to store the fetched CRL files to
  - Specify one or multiple URLs to load CRLs from
  - Specify the update interval (optional)