CAMP Enterprise Authentication Workshop
Web Applications Track: Open-Source Web Initial Sign-On Packages

Presenters: Nathan Dors, Robert Banz, Keith Hazelton, Kevin McGowan

Date: Thursday, November 18, 2004 at 2:30 p.m. – 3:45 p.m.

Scribe: Todd Piket

Discussion

I. Essential Functions of a WebISO system
   a. Authenticate people
   b. Deliver credentials

II. Drive behind a WebISO system
   a. Protect credentials
   b. Normalize/standardize web authentication
   c. Reduce costs through integration
   d. Increase productivity
   e. Improve security

III. WebISO Prerequisites
   a. Know who your users are…Identity Management System
   b. An existing authentication service.
   c. Balance requirements with broader objectives.

IV. Common Open-Source ISOs
   a. Yale CAS (Central Authentication Service)
      i. Many campuses use it
      ii. Has good uPortal ties
   b. Cosign (University of Michigan)
      i. NMI component
      ii. Kerberos integration
      iii. Distributed session management
   c. PubCookie (University of Washington, Carnegie Mellon, University of Wisconsin)
      i. NMI component
      ii. Many campuses use it
      iii. Kerberos V and LDAP integration
      iv. Simple application integration
   d. A-Select
      i. NMI component
      ii. Supports authentication plugins
      iii. Used in more than just U.S.A.
   e. Shibboleth
      i. Standard SAML tokens, protocol
      ii. Attribute exchange and privacy
      iii. Simple application integration
      iv. Current version has a fairly complicated install and configuration
v. Must have an authentication system in place already.

V. Leading WebISO Planning Sessions
   a. Where does it fit in the campus strategy
      i. Determine requirements
      ii. Get stakeholders in a room
      iii. May help to “score” things as critical desired, or optional in order to focus on what the actual and/or beginning requirements should be. Keith Hazelton (Univ. Wisconsin) has a useful scoring system.
   b. Authentication Requirement from University of Wisconsin
      i. Protect against replay attacks
      ii. Protect against man-in-the-middle attacks
   c. Politics at University of Wisconsin
      i. Didn’t have to “fight” to do WebISO
      ii. Thought about what was needed in the future.
   d. Should be easy to use and deploy.
   e. Question: Is NetID public information?
      i. The consensus of those in the room was that it is public.
      ii. Shibboleth doesn’t “lead with identity” so it begs the question should it be public or not.
   f. FERPA and NetID based on name are arguments in favor of making NetID/Userid secret.

VI. Cosign Perspective from University of Michigan
   a. Services register centrally with ISO server
   b. Can only keep logs for a week because they contain identity
   c. Can logout on central server or from specific application
   d. People will probably already have their own WebISO systems in place so tread lightly.
   e. Questions about Cosign can go to cosign@umich.edu

VII. “Legacy”/Home grown WebISO Perspective
   a. Consensus of the room was to use an existing WebISO system or Shibboleth if they could do it over.
   b. History of this Legacy WebISO
      i. Started as API model
      ii. Moved to a .htaccess model
      iii. Application wanted student ID exposed
         1. Developed a way to provide more than just student ID.
         2. Developed a way to turn off student ID exposure to make it “pseudonymous”.
      iv. Gives you control
         1. Can do what you want, but you have to do it.
         2. Creates ongoing development costs.
         3. Can be difficult to provide code for other operating systems and architectures.
         4. Generally put a small group or single person in control.
            This is bad if that small group or person becomes unavailable.
5. Once deployed visibly users will drive application compliance across campus.

VIII. Future
   a. Multiple authentication methods work in unisons
      i. Client certificate failover to WebISO.
      ii. HTTP/Spnego failover to WebISO
   b. Shibboleth
      i. May get web login features.
      ii. WebISO may move to SAML
      iii. SAML can provide useful vendor integration