Kerberos On The Web

Pete Bosanko
bosanko@cornell.edu

Kerberos Consortium Conference
October 21, 2009
Web Authentication @ CU

- CUWebAuth – Kerberos 5
- 400+ Web Sites Using CUWebAuth
- Heterogeneous – Apache, IIS, Others
- Multiple Kerberos Realms
  - Active Directory
  - MIT KDC
  - Inter-campus Federation
- Shibboleth
- Most Services Use Single-Factor (ID/Password)
CUWebAuth

- Kerberos 5
- N-Tier Delegation
- Fat (Kerberos) Client
- Cross Realm
- Multiple Platforms
- Integrated Authorization
CUWebAuth – Service Model

- Distributed Implementation & Deployment
- Many Campus Units
- ~200 Site Admins

- Open source – BSD License
  - Departmental development
Self-Service

- Users
- Website Administrators
Protected Web Applications

- 400+ Virtual Hosts
- Roughly Half in Shared Hosting
- >1M Logins / Month
Cross Realm Applications

- Primary Student/Staff/Faculty Accounts
- Exchange
- Distance Learning (Blackboard)
- Applicants
- Medical College
Realms / Domains

- **NetID & ServiceID**
  - MIT KDC
- **NetID & LocalID**
  - Active Directory
- **GuestID & ApplicantID**
  - MIT KDC
- **CMID – Weill Medical**
  - Active Directory
  - NYC – Qatar
<Directory c:/Inetpub/wwwroot/Services/Projects>
    AuthName CORNELL
    AuthType all
    require permit cu.employee cu.medical cu.affiliate.cumc
    require netid ar74
    require valid-user@A.WCMC-AD.NET
    CUWAwaK0Realms "CIT.CORNELL.EDU,A.WCMC-AD.NET"
    CUWAwaak2Name "NetID or CMID"
</Directory>
Federation

- Shibboleth (Single CUWebAuth IdP)
  - InCommon
- Harris Connect (Cornell connect)
- SciQuest (Purchasing)
  - under development
- Videonote.com (online course lectures)
- Library research sites
  - JSTOR & Sciencedirect.com & others
- Illiad (Inter library loan)
Kerberos with WebDAV

• Kproxy
  ➢ Kerberos Proxy Service
  ➢ SSL + Basic Auth
  ➢ Integrated with CUWebAuth

• DAV Portal
  ➢ Integrated with CUWebAuth
  ➢ Establishing a Session is Less User Friendly

• SPNEGO
  ➢ Under development
  ➢ Some DAV client issues
N-Tier Web Applications

• CUWebAuth
  ➢ Kerberos Credentials

• Delegation Constraints
  ➢ Applications must be Authorized
  ➢ WebLogin is Gatekeeper

• Target System Authenticates...
  ➢ User
  ➢ Mid-Tier
Future

• Improve AD Integration – IIS Impersonation
  ➢ Under development
• Token – Multi-factor
  ➢ Early Planning Stage
• Realms / Domain Consolidation
• Client Certificates
• Simplify our Federation
More Information

CUWebAuth  https://confluence.cornell.edu/display/CUWAL

bosanko@cornell.edu