

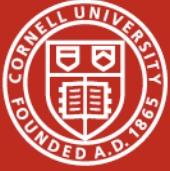


Cornell University
Cornell Information Technologies

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

Cornell University

CUWebLogin

NetID:

Password:

[What is this?](#)
[I forgot my password!](#)
[I don't have a NetID, now what?](#)

To log out, you must Exit or Quit your browser.

Cornell University

CUWebLogin

NetID or CMID:

Password:

Realm:

[What is this?](#)
[I forgot my password!](#)
[I don't have a NetID, now what?](#)

To log out, you must Exit or Quit your browser.



Cornell University
Cornell Information Technologies

CUWebAuth – Service Model

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

- Open source – BSD License
 - Departmental development



Self-Service

- Users
- Website Administrators

- Use IDM Team Privs
- My ServiceIDs
- Update ServiceID
- Create K5 keytab
- Delete ServiceID
- Request SSL Certificate
- Permit Management
- Contact Us

Update ServiceID HTTP/aaddev.cit.cornell.edu

An asterisk (*) indicates required fields.

Basic Config

Owner NetID:

Department:

Remove Admin NetIDs:

- mfi2
- em268
- mas18
- nl85
- elr32
- jsu1
- ral274

Add Admin NetID:

Service Hostname:

*Service Description:

Kproxy Config

Enable kproxy: Check this box to enable kproxy for this ServiceID.

kproxy port:

kproxy over SSL: Check this box if your kproxy uses SSL.

Kproxy service info:

kproxy request status:

Enable Delegation Config

Enable delegation: This service needs to make requests on behalf of users to other services.

Delegation request status: TBD

Accept Delegation Config

Accept delegation: Allow other applications to obtain delegated credentials for this service.

Add application ServiceID:

Save Changes

Manage Your NetID

[About Passwords](#) | [About NetIDs](#) | [About Identity Management](#) | [Contact Help Desk](#)

Manage Your NetID

This site will help you manage your NetID and NetID password, which are necessary for you to access many of Cornell's online services.

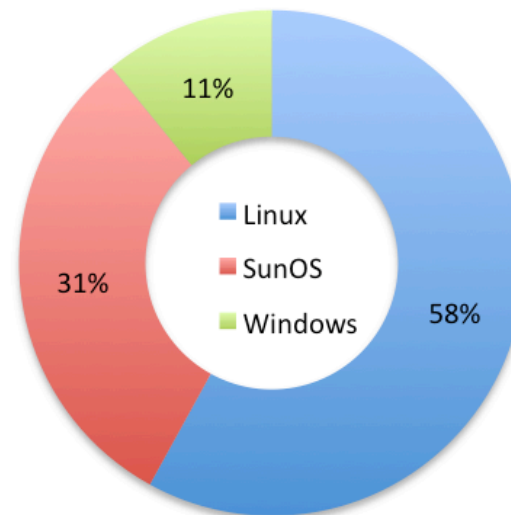
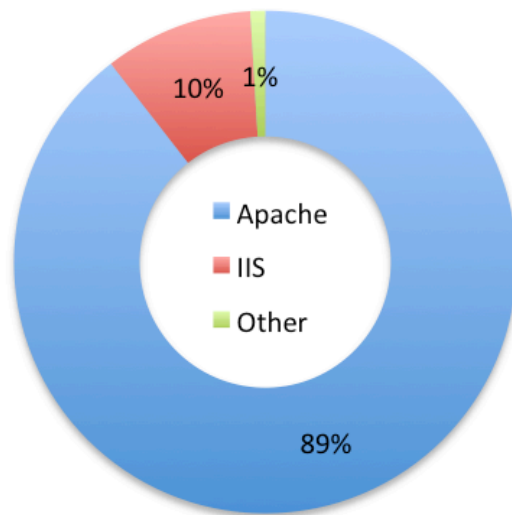
- **Activate your NetID** - Start here if you are new to Cornell or just received your NetID.
- **Change your Password** - Start here if you know your password and want to change it.
- **Reset your Password using your Security Questions** - Start here if you forgot your password and want to reset it by answering your Security Questions.
- **Set your Security Questions** - Start here if you know your NetID and password and want to set your Security Questions so you can reset your password should you ever forget it.
- **Do you have a strong password? Click here to find out.**

After your NetID has been activated, Cornell alumni who wish to set up Email forwarding, or Cornell students and staff who need to set up their Cornell Email address, can do so by clicking on [WhoIAm](#).



Protected Web Applications

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

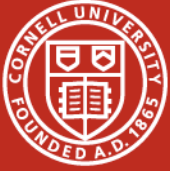




Cornell University
Cornell Information Technologies

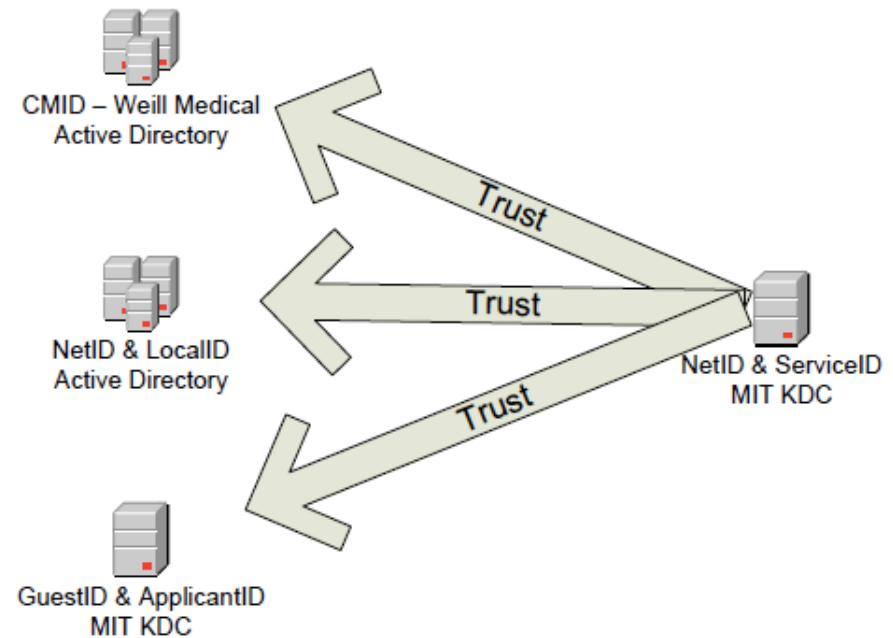
Cross Realm Applications

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



Realms / Domains

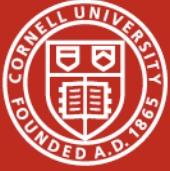
- NetID & ServiceID
 - MIT KDC
- NetID & LocalID
 - Active Directory
- GuestID & ApplicantID
 - MIT KDC
- CMID – Weill Medical
 - Active Directory
 - NYC – Qatar





Access Control

```
<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"  
CUWAwak2Name "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)



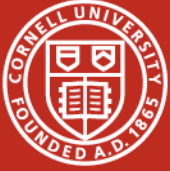
Kerberos with WebDAV

- 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



Cornell University
Cornell Information Technologies

More Information

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

bosanko@cornell.edu