

---

# Kerberos use in Web Authentication

Paul B. Hill, Consulting Technical Architect

The Kerberos Conference, October 21, 2009



# Current landscape

---

- Since 1996 MIT has issued X.509 soft certificates to its traditional user community
- Roughly 100 to 150 servers accepting MIT user certificates
- MIT Shibboleth deployment started in Fall of 2007
- Roughly 15 applications in operation today



# Driving factors

---

- The community that our applications must interact with is larger than the MIT community, and includes people that do not have an account with any KDC.
- There was no organization building a *large* cross realm community, similar in scope to some of the growing Shibboleth federations.
- It is not always appropriate to release a student's name to a third party application.



# MIT as a federation: Current Shibboleth IdPs

---

- Core IdP for people that have an MIT Kerberos principal (idp.mit.edu)
  - Central administration
- Collaboration Account IDP for people that don't have an account at a site with a Shibboleth IdP (idp.touchstonenetwork.net)
  - Self registration

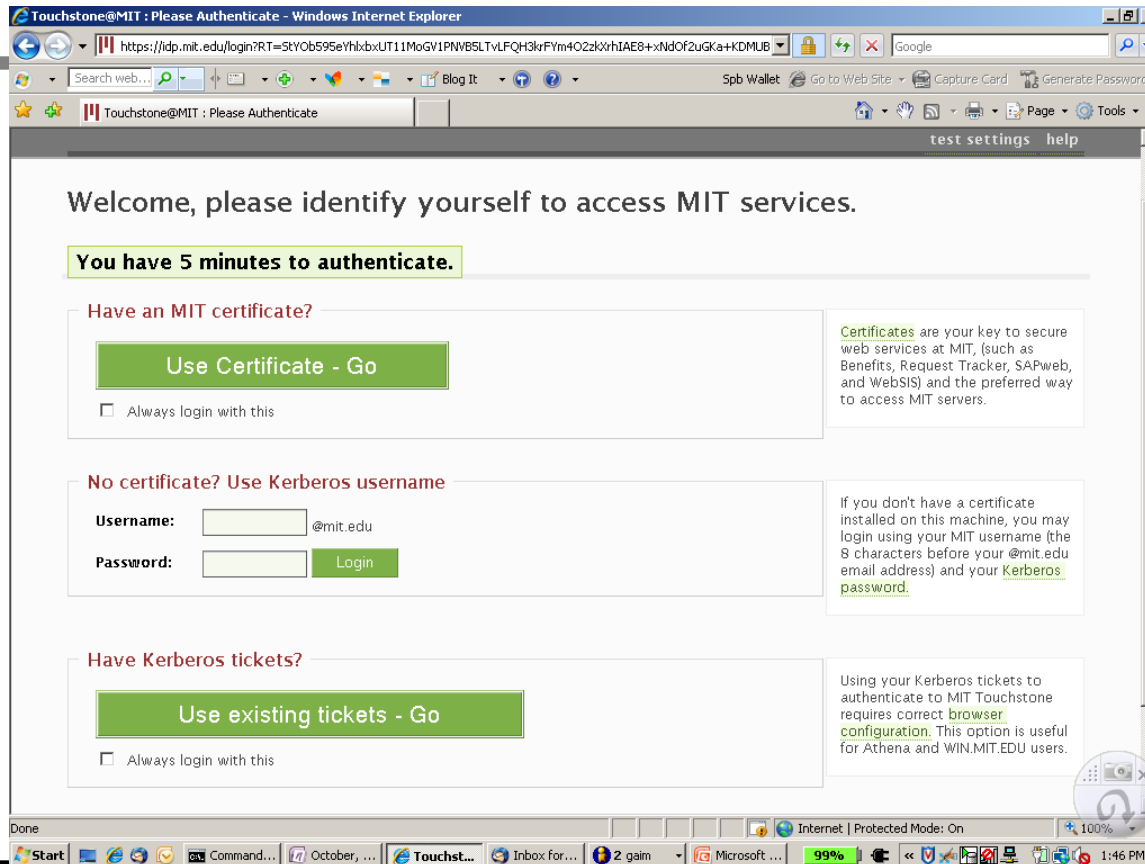


# IdP initial authentication mechanisms

---

- Core MIT (idp.mit.edu)
  1. MIT issues X.509 certificates
  2. MIT Kerberos principal and password
  3. Kerberos via HTTP-SPNEGO
    - Internet Explorer, FireFox, Safari

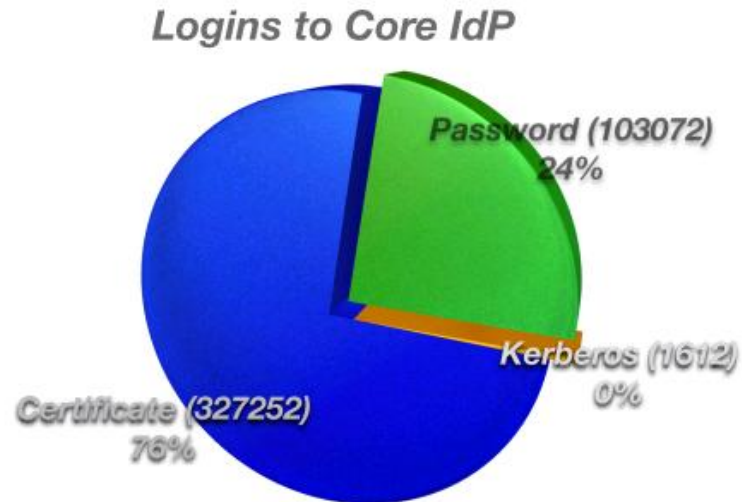




## Metrics: core IdP, July 10 – Oct 8

Logins, by authentication method:

- certificate 327252 (75.76%)
- username/password 103072 (23.86%)
- Kerberos 1612 (0.37%)



# IdP initial authentication mechanisms

---

- Collaboration Accounts ([idp.touchstonenetwork.net](http://idp.touchstonenetwork.net))
  1. Username / password
  2. OpenID
  3. Kerberos via http-spnego
    - was available during beta, and some time in the future, not currently turned on in production





Touchstone Collaboration Account Login - Windows Internet Explorer

https://idp.touchstonenetwork.net/shibboleth-idp/AuthSSO?shire=https%3A%2F%2Fwikis.mit.edu%2FShibboleth.sso? Google

Search web... Blog It Spb Wallet Go to Web Site Capture Card Generate Password

Touchstone Collaboration Account Login Page Tools

# Touchstone Collaboration Account Login

[help](#)

Choose one of the following methods to login:

**Your email & password**

Email:

Password:

[Forgot password?](#)


[Not registered?](#)

You can login by entering the email address and password with which you registered your MIT Touchstone collaboration account. If you have not yet registered for your account, you may do so [here](#).

**Your OpenID**

OpenID:

This option is available if you have registered an [OpenID](#) as an alternate security ID for your Touchstone collaboration account.

 **MIT** IST massachusetts institute of technology

Done Internet | Protected Mode: On 100%

Start Command... October, ... Touchst... Inbox for... 2 gaim Microsoft ... 99% 1:48 PM

## Metrics: TouchstoneNetwork IdP, July 10 – Oct 8

---

Logins, by authentication  
method:

- username/password

12,372

- OpenId 1



# Shibboleth and Cross realm interactions

---

- Shibboleth Attribute Resolution issue
  - idp.mit.edu maps well with the Athena.mit.edu realm and ldap.mit.edu.
    - What happens when someone from another realm authenticates?
    - Where do we perform the attribute resolution?



# Identity transformations

TouchstoneNetwork IdP addresses this via self registration of alternate security identifiers

 P. B. Hill:pbh41@hotmail.com

## Manage Alternate Security Accounts

[↔ Add Alternate Security Id](#)

## Active Alternate accounts

Alternate ID	ID Type
http://auth.mit.edu/pbh	OpenId
pbh@ATHENA.MIT.EDU	Kerberos

## Inactive Alternate accounts

Alternate ID	ID Type
--------------	---------



# Future directions

---

- Add Kerberos mechanism back into Touchstone
- “KAML” raises privacy concerns when extending across the border of the enterprise.
  - Ticket in the SAML assertion
  - SAML assertion in the ticket
  - In both cases the username is likely to be exposed

