Kerberos on the Web
Thomas Hardjono
MIT Kerberos Consortium

MIT Kerberos Conference
October 20-21, 2009
Kerberos Today

- Enterprise, B2B, B2C
- Kerberos & Identity Infrastructure
Intra-Enterprise Kerberos

- Large presence of Kerberos in Enterprise space
  - AD, “AD-Clones”, MIT code base, Intel AMT

- Desire to re-use Kerberos infra for web security
  - Increase security of web logins
    - Address authentication in Web-SSO
  - Simplification of security management

- Require Kerberos integration into web systems
  - Web-services typically already a separate infrastructure
  - Kerberos administration must also be integrated into web systems
  - Unified management of infrastructures
Kerberos for B2C & B2E Security

• Forms/SSL primary authentication method:
  – Passwords, HTML Forms, no client certs
  – HTTP-Negotiate underutilized
    • Limitations to current version of HTTP-Nego/SPNEGO

• B2E Web-SSO needs strong access control:
  – Intra-network services & business access only
    • Locally-scoped identities
  – HTTP-Negotiate deployed in many Enterprises

• B2C Web-SSO a harder problem:
  – Need standard interfaces
  – Part of Identity Management & Federation problem
  – HTTP-Negotiate limitations (today)
Kerberos in Identity Management

- Largely absent from SAML based Identity stacks
  - Liberty, Shibboleth, etc

**WS Security:**
- Oasis WS-S Kerberos Token Profile (AP_REQ)
- CardSpace/InfoCard, Geneva (Microsoft)

**Kerberos and Providers:**
- Authentication to IdP still using Pwd/Forms/SSL
- Providers (IdP/SP/OP) have limited Kerberos large-scale operational experience
Current Efforts

- Interoperability with SAML
- Web back-end security
Kerberos Interoperability with SAML

• Kerberos support in SAML (2.0) Systems:
  – Profiles: Web-SSO & Web Services
  – Subject Confirmation method:
    • Confirm the SAML attesting entity using Kerberos (Holder of Key)
  – Collaboration with Josh Howlett

• Authentication to Kerberized Web Service:
  – Delegation of Kerberos credential to a web-application to access Kerberized service
  – Authentication using S4U Extensions (constrained delegation)
Confirming SAML Attesting Entity

![Diagram of SAML authentication process]

1. Client requests service from Service Provider (SP)
2. SP forwards request to Identity Provider (IdP)
3. IdP authenticates client and requests service
4. IdP issues SSO (Single Sign-On) ticket to client
5. Client can now interact with SP

Kerberos KDC
- Kerberos Authentication Service (AS)
- Kerberos Ticket Granting Service (TGS)

Identity Provider (IdP)
- Authentication Authority
- Attribute Authority

Service Provider (SP)
- Assertion Consumer Service
- Resource
Authentication to Kerberized Web Service

• Use-Case:
  – SAML system entity requires access (via a Web-Service) to a local/remote Kerberized Service on a behalf of a Client (user) Principal.
  – SAML Requestor may not be able to request a service-ticket directly from the KDC since it is an entity that is not recognized by the KDC

• Possible Solution:
  – Use of the SAML2.0 Assertion Query Protocol and Request Protocol
  – Combined use of S4U2self and S4U2proxy
    • See next slides
Authentication to Kerberized Web-Service

Kerberos KDC | Identity Provider (IdP)
---|---
Kerberos Authentication Service (AS) | Kerberos Ticket Granting Service (TGS)
Authentication Authority | Attribute Authority

User Principal (eg. Web-Mail)

SAML Requestor

(eg. home IMAP Server)

SAML2.0 Assertion Query Protocol and Request Protocol

S4U2self

[1] → [2] → [3] → [4]


S4U2proxy
Kerberized Web Service: S4U2self

• Goal: IdP asks authorization from the KDC (for the user) to access itself (the IdP)
  – IdP requests the TGS for a service-ticket to itself on behalf of the user (Client Principal).
  – IdP assumed already a Kerberized entity
• SAML Requestor send <AttributeQuery> msg to IdP:
  – Identifying the Client Principal (ie. the user) and target Kerberized Service
• TGS returns a service-ticket to the IdP
  – As if the ticket had been requested from the user using her own TGT
Kerberized Web Service: S4U2proxy

- Goal: IdP seeks authorization to request access to other services (eg. IMAP server) on the user's behalf
  - Requestor sends query to IdP
  - IdP uses client name & realm from S4U2self
  - IdP requests service ticket from KDC/TGS to access service (eg. IMAP server)
  - TGS issues a forwardable service-ticket, placing the Client Principal’s name (instead of the IdP name) within the service-ticket.
Kerb-Web: Other Related Work

• HTTP-Negotiate (SPNEGO):
  – GSS-API handshake with HTTP Server
    • RFC4559 & RFC4178
  – Active Directory environments
  – “Open Internet” deployment unproven

• Some open/related issues:
  – Lack of protection of HTTP request
  – Support for multi round-trips of GSS-API mechanisms over TLS
  – State management at end-points
Related Work (cont)

• Future work at MIT-KC:
  • Kerberos interoperability in WS-Federation systems
    • Oasis WS-Federation architecture
  • Kerberos to secure back-end web infrastructure

• MashSSL (startup):
  • Based on MIT Kerberos
  • Promising “open-internet” deployment solution
  • Go to: www.safemashups.com

• MIT-KC Whitepaper:
  • Towards Kerberizing Web Identity and Services
    • http://www.kerberos.org/software/kerbweb.pdf
Thank You & Questions
Contact Information

The MIT Kerberos Consortium
77 Massachusetts Avenue
W92-152
Cambridge, MA 02139 USA

Tel: 617.715.2451
Fax: 617.258.3976

Thomas Hardjono
Lead Technologist & Strategic Advisor

Web: www.kerberos.org

MIT Kerberos Consortium

Lead Technologist & Strategic Advisor
Thomas Hardjono (hardjono@mit.edu)
Mobile: +1 781-729-9559