MIT Kerberos Consortium

Kerberos on the Web: Update

Thomas Hardjono

March 30, 2009

www.kerberos.org

MIT-KC Strategic Pillars

- We propose to make steady progress in then following areas:

1. Kerberos on the Web
2. Kerberos on Mobile Devices
3. Maintaining and Securing Kerberos
4. Vendor Independence

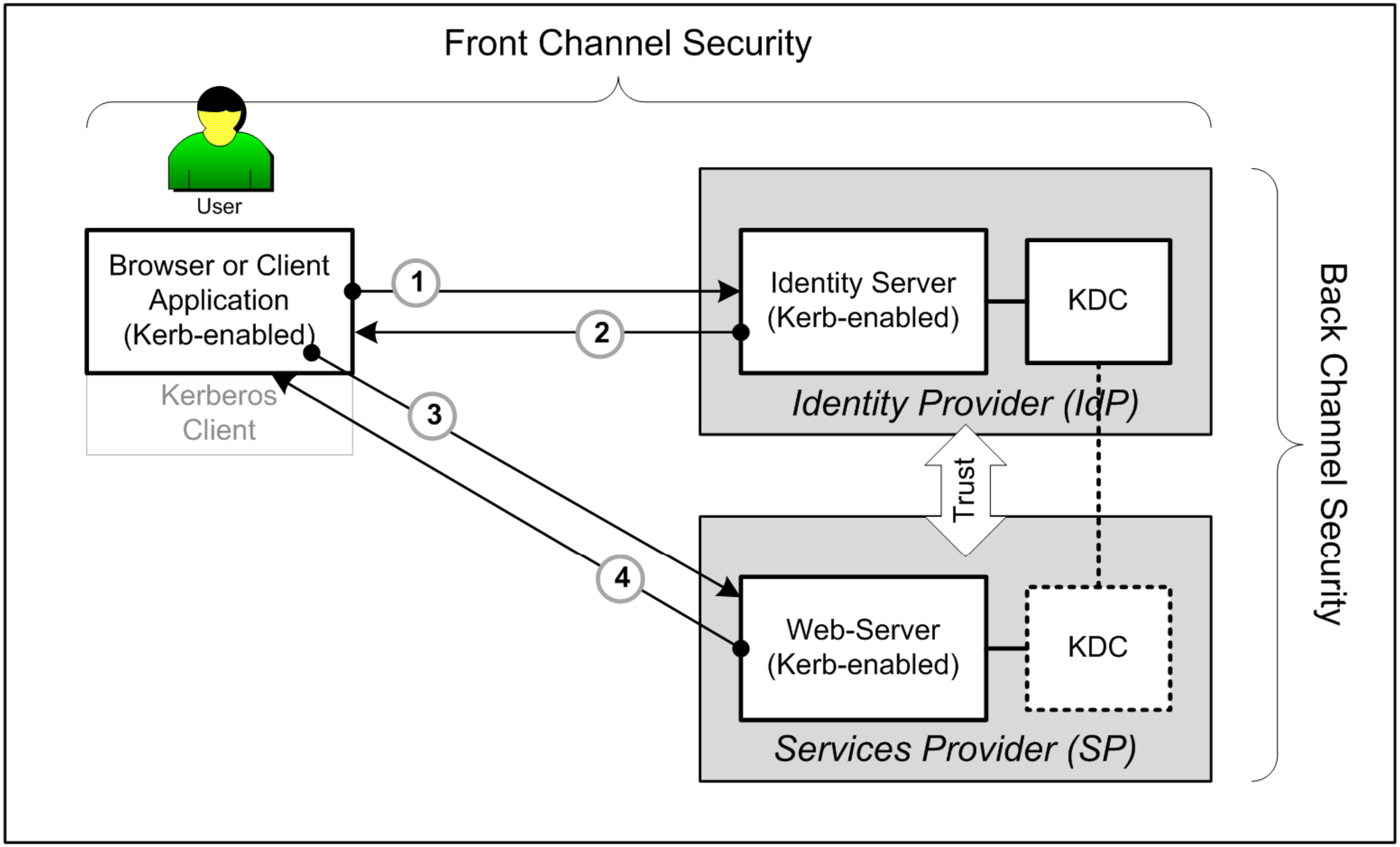
Why Kerberos on the Web

- Why Kerb-Web:
  - Web-services core to future Internet economy
  - Strong Kerberos presence in SMB to Large Enterprises
    - Expand enterprise Kerberos infrastructure to support web-services transactions
- Benefits:
  - Re-use enterprise investment
  - Enterprise-grade security for consumer transactions

Kerb-Web Problem Space

- Broadly a 3-sided problem space:
  I. Client to Web-Server/App (IdP) authentication
  II. Authenticated service request to SP
    - aka “Web-SSO”
  III. IdP-to-SP trust (key) establishment
- Kerberos and Certificates:
  – Both Kerberos and a certificate infrastructure are foundation for web-services security
  – Certificate support relevant for Kerberos inter-domain/realm trust establishment

Kerb-Web Problem Space



MIT Kerberos consortium
www.kerberos.org

I. Client/User Authentication

- Goal: User on Kerb-enabled client performs authentication against IdP
  - – Kerberized IdP
    - Eg. web-server/app retrofitted with a KDC.
  - – Kerberos messages within HTTP and/or SSL/TLS (or other suitable transport)
  - – Pre-authentication mechanisms (FAST)
  - – Provide leap in security quality compared to current web form+password.

I. Client/User Authentication (cont)

- Some key issues:
  - No clear leading standard
    - GSS-TLS, PKU2U, etc. etc.
    - Desire minimal (or no) change to apps & browsers
  - Support in current browser (chicken & egg)
    - Browser vendors reluctant if no server-side support
- What we can do:
  - Influence standardization efforts
  - Identify use-cases & develop server support
    - Web-SSO use case (e.g. Shibboleth)
  - Outreach to browser vendors

II. Service request to SP

- Goal: use Kerberos service ticket to obtain web-services
  - Wrap standard Kerberos ticket in XML-based format
    - WS-Security token, Kerb-in-SAML or SAML-in-Kerb
    - Claims
  - Interoperability with identity management
  - Support Client-to-SP mutual authentication
    - When required by SP
  - Support automated service-requests
    - No human present

II. Service request to SP (cont)

- Some issues:
  - – WSS Token profile v1.1 covers AP_REQ only
  - – Designed for WS-S* over SOAP
    - Need to address SAML-based SPs and IdPs
- What we can do:
  - – Update WS-S Kerb Token profile spec
  - – Develop spec for SAML equivalent
  - – Investigate interoperability with identity standards/frameworks
    - Liberty, Shibboleth, CardSpace/Geneva, etc

III. IdP-to-SP Trust Establishment

- Goal:
  - – IdP/kdc and SP/kdc to share keying material
- Some issues:
  - – The “Back Channel” problem area
  - – Automated KDC-to-KDC key establishment
- What we can do:
  - – Investigate Kerberizing CAs or adding X509 certificate capability to KDC
    - KX509 or similar
  - – Implement & promote PKCROSS or similar.

Conclusions

- Great interest in Kerb-Web notion:
  - Recognized need to bring Kerberos to the web
- Seek support from MIT-KC Members:
  - Standards front
  - Architectural inputs
  - Code contributions
  - Engineering resources

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
Strategic Advisor

Web: www.kerberos.org

MIT Kerberos Consortium

Strategic Advisor
Thomas Hardjono(hardjono@mit.edu)
781-729-9559