Kerberos and Related Technologies

Tom Yu

MIT Kerberos Consortium

SIPB “Cluedump” Series
02 December 2008
Overview

- Kerberos
- GSS-API
- SASL
- Resources
Kerberos

- Secure network authentication
- General features
- Applications
- Protocol description
- Version 4 (krb4) – legacy
- Version 5 (krb5) – current
- Microsoft and Kerberos
Kerberos: Network Auth.

- Project Athena
- Security in an adverse environment
- Attacker network capabilities
  - Listen to anything
  - Modify anything
- Trusted third party
  - Based on Needham–Schroeder
  - KDC (Key Distribution Center)
Kerberos: General Features

• Single sign-on
• Simplified key management
• Symmetric cryptography
• Centralized administration
• Widely implemented and deployed
Kerberos: Applications

- Login
  - PAM, SSH, FTP
- Mail
  - POP, IMAP
- Filesystems
  - NFS, AFS
- Instant Messaging
  - Zephyr, Jabber
Kerberos Participants

- Key Distribution Center (KDC)
  - Authentication Service (AS)
  - Ticket Granting Service (TGS)
- Client
- Service
Kerberos: Shared Secrets

- **Client**
- **KDC**
- **Server**

Key exchange:
- Client password
- Service key
- Session key
Kerberos Protocol

- Client
- KDC
- Server

Messages:
- AS_REQ
- AS_REP
- TGS_REQ
- TGS_REP
- AP_REQ
- AP_REP
Getting Kerberos Credentials

**AS_REQ:** C → TGS: C, TGS

**AS_REP:** TGS → C: \{k_{(C,TGS)}, \text{TGS}, \{C, \text{TGS}, t_{KDC}, k_{(C,TGS)}k_{\text{TGS}}\}k_{\text{TGS}}\}k_{C}

**TGS_REQ:** C → TGS: \{C, \text{TGS}, t'_{KDC}, k_{(C,TGS)}k_{TGS}, \{C, t_C\}k_{(C,TGS)}, \text{S}\}

**TGS_REP:** TGS → C: \{k_{(C, \text{S})}, \text{S}, \{C, \text{S}, t'_{KDC}, k_{(C,\text{S})}k_{\text{S}}\}k_{\text{S}}\}k_{(C,TGS)}

Ticket-Granting Ticket (TGT)

Service ticket
Using a Kerberos Ticket

AP_REQ: $C \rightarrow S$: $\{C, S, t'_KDC, k_{(C,S)}\} k_S$, $\{C, t'_C\} k_{(C,S)}$

Service ticket

Authenticator
krb4

• First publicly released version
• Known limitations
  – Single-DES
  – “Weird” (PCBC) cipher mode
  – Exploitable protocol vulnerabilities
  – Single-hop cross-realm
krb5

- IETF standards track
- Improved crypto
  - Improved integrity protection
  - Algorithm-agile
- More extensible
- More features
  - Transitive cross-realm
  - User-to-user
  - Credential forwarding, renewing, etc.
Microsoft and Kerberos

• PAC – Privilege Attribute Certificate
• Nonstandard extensions
• Active Directory
  – Kerberos, LDAP, DNS, etc.
GSS-API

- Generic Security Services API
- IETF standards track
- Abstracts details of underlying security mechanism
- Abstract API; C and Java bindings
GSSAPI: Details

• Context setup
  – GSS_Init_sec_context
  – GSS_Accept_sec_context

• Message protection
  – GSS_Wrap, GSS_Unwrap
  – GSS_GetMIC, GSS_VerifyMIC

• Others
  – Credential and name handling, etc.
GSS-API: Context Setup

Client

Init

App. prot.

Init

App. prot.

Init

App. prot.

Server

Accept

Accept

Accept

CONTINUE

CONTINUE

CONTINUE

CONTINUE

SUCCESS

SUCCESS

SUCCESS
SASL

• Simple Authentication and Security Layer
• IETF standards track
• Generalizes preexisting app. practices
  – IMAP
  – POP
  – etc.
Using Kerberos in Applications

• Client-server authentication
• Password validation
  – Beware the Zanarotti attack!
• User-to-user authentication
Choosing an API

- API mostly determines protocol
- Existing protocol: use matching API
- New protocol: it depends...
MIT krb5 API

• Pro:
  – Most flexible
  – Most protocol features

• Con:
  – Most complicated
  – Somewhat limited portability
GSS-API

• Supposedly a generic security API
  – In practice, often used for krb5
• Very portable
• Non-krb5 mechs
  – SPNEGO negotiation mechanism
    • Microsoft usage (NTLM)
    • HTTP authentication
  – SPKM (X.509 certificates)
GSS-API

- Context setup loop can be tricky
- Doesn’t expose all krb5 capabilities
SASL

• Pro:
  – Can use krb5 “GSSAPI” mech.
  – Variety of other auth. mechs.
  – Negotiation capability

• Con:
  – General GSS-API support still pending
  – Tends to get re-implemented from scratch
Specifications

• Kerberos
  – RFC 4120 (current spec.)
  – RFC 3961 (crypto spec.)

• GSS-API
  – RFC 2743 (abstract spec.)
  – RFC 2744 (C lang. bindings)
  – RFC 1964, RFC 4121 (krb5 mech.)
Specifications

• SASL
  – RFC 4422 (general spec.)
  – RFC 4505 (anonymous mech.)
  – RFC 4616 (PLAIN mech.)
  – RFC 4752 (krb5 mech.)
Resources

• Kerberos Consortium
  – http://kerberos.org/

• MSDN Library
  – Note MS-KILE and MS-SPNG

• Solaris Security for Developers Guide
  – http://docs.sun.com/app/docs/doc/816-4863/
  – GSS-API programming guide