Kerberos – MIT protocol

December 11th 2009

Amit Shinde
Kerberos – MIT protocol

- Motivation behind the design
- Overview of Kerberos Protocol
- Kerberized applications
- Attacks and Security analysis
- Q & A
Motivations behind the design

- The user's password must never travel over the network.
- The user's password must never be stored in any form on the client machine.
- The user's password should never be stored in an unencrypted form.
- Single Sign-On.
- Centralized Authentication information management.
- Mutual authentication.
- Establish an encrypted connection.
Kerberos overview

- A network authentication protocol.
- Client/server authentication by using secret-key cryptography.
- Developed at MIT in the mid 1980s.
- Available as open source or in supported commercial software.
- Symmetric key encryption.
- Two versions V4 and V5.
Components and terms

- **Realm** - authentication administrative domain

- **Principal** - entries in the authentication server database
  - Name[/Instance]@REALM
  e.g. pippo@EXAMPLE.COM, admin/admin@EXAMPLE.COM
  imap/mbox.example.com@EXAMPLE.COM

- **Authenticator** - user principal and time stamp encrypted with the session key.

- **Salt** - $K_{\text{pippo}}$
  - string2key ($P_{\text{pippo}}$ + "pippo@EXAMPLE.COM")
Think “Kerberos Server” and don’t let yourself get mired in terminology.
XYZ Service

Represents something requiring Kerberos authentication (web server, ftp server, ssh server, etc…)

Susan's Desktop Computer

Key Distribution Center

Ticket Granting Service

Authentication Service
AS_REQ - “I’d like to be allowed to get tickets from the Ticket Granting Server, please.”
AS_REP – (TGT + session key)
“Okay. I locked this box with your secret password. If you can unlock it, you can use its contents to access my Ticket Granting Service.”
Ticket

- **Ticket** - The requesting user's principal (generally the username);
- The principal of the service it is intended for;
- The IP address of the client machine from which the ticket can be used. In Kerberos 5 this field is optional and may also be multiple in order to be able to run clients under NAT or multihomed.
- The date and time (in timestamp format) when the tickets validity commences;
- The ticket's maximum lifetime
- The session key (this has a fundamental role which is described below);
"Let me prove I am Susan to XYZ Service. Here’s a copy of my TGT!"
Hey XYZ:
Susan is Susan.
CONFIRMED:TGS

TGS_REP- (service session key + service ticket)
You’re Susan.
Here, take this.

TGT

Susan’s Desktop Computer

XYZ Service

Ticket Granting Service

Key Distribution Center

Authen-Tication Service
Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

AP_REQ- (Service ticket + authenticator)
I’m Susan. I’ll prove it. Here’s a copy of my legit service ticket for XYZ.
Hey XYZ:
Susan is Susan.
CONFIRMED:TGS

AP_REP-I’m AP. I’ll prove it.

Susan’s Desktop Computer

App Server -“AP” XYZ Service

Ticket Granting Service

Key Distribution Center

Authentiction Service
That’s Susan alright. Let me determine if she is **authorized** to use me.
Authorization

- Authorization checks are performed by the XYZ service...

- Just because Susan has authenticated herself does not inherently mean she is authorized to make use of the XYZ service
Reuse of ticket TGT

- Tickets (your TGT as well as service-specific tickets) have expiration dates configured by your local system administrator(s). An expired ticket is unusable.

- Until a ticket’s expiration, it may be used repeatedly.
Hey XYZ:
Susan is Susan.
CONFIRMED: TGS

ME AGAIN! I’ll prove it. Here’s another copy of my legit service ticket for XYZ.
Hey XYZ:
Susan is Susan.
CONFIRMED:TGS

Hey XYZ:
Susan is Susan.
CONFIRMED:TGS

That’s Susan… again. Let me determine if she is **authorized** to use me.

Susan’s Desktop Computer

Ticket Granting Service

Key Distribution Center

Authen-Tication Service

XYZ Service
Weaknesses in Kerberos

- "Password guessing" attacks are not solved by Kerberos.
- Replay attacks – sniff the network to extract the AP_REQ message.
- Very bad if Authentication Server compromised – steals all of the tickets stored on that machine.
List of Kerberized applications

- NFS (Network File System): Network protocol by allows a client to access files over a network manner similar to how local storage is accessed.
- Telnet.
- Microsoft supports version of Kerberos 5 in Windows 2000.
- Sun ships a basic set of Kerberos 4 utilities with Solaris (kinit, klist, kdestroy), and the RPC that comes with Solaris supports a Kerberos 4 authentication mechanism.
- Cisco routers support Kerberos 5 authentication for incoming and outgoing telnet connections.
- GSS-API, Server message block
Further reading

- An Introduction to Kerberos:  
  http://www.upenn.edu/computing/pennkey/docs/kerbpres/200207Kerberos.htm

- MIT Kerberos Site:  
  http://web.mit.edu/kerberos/

- The Moron’s Guide to Kerberos:  
  http://www.isi.edu/~brian/security/kerberos.html

- Kerberos: The Definitive Guide:  
  http://www.oreilly.com/catalog/kerberos/cover.html
Thank you