Heimdal—Kerberos 5 for the world

Johan Danielsson
Parallelldatorcentrum, KTH
joda@pdc.kth.se

Assar Westerlund
Swedish Institute of Computer Science
assar@sics.se

Heimdal—Kerberos 5 for the world

free

independent

internationally available

What is Kerberos?

authentication system

trusted third party system

in widespread use since many years

Heimdal general overview

includes most commonly used applications:

- Kerberos server
- kinit, klist, kdestroy
- telnet, ftp, rsh, and pop servers and clients
- administration system

Heimdal general overview (cont.)

reasonably compatible with MIT API

tries to be portable

PAM, SIA, and afskauthlib

support for Kerberos 4 and OTP

Heimdal extras

authenticated and encrypted X11 sessions

incremental database propagation

3DES

IPv6-support

firewall tools

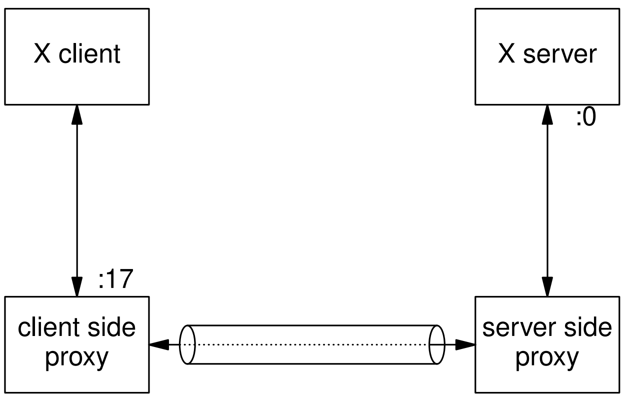
Authenticating X11

mechanism	advantages	problems
xhost	easy to use	trusts IP addresses host granularity
xauth	more secure	cumbersome vulnerable to snooping
krb5	secure easy to use	not deployed only initial authentication no encryption

X11 authentication with kx

How it works

- proxy-based
- encrypts whole session



X11 authentication with kx (cont.)

Advantages

- easy to use
- secure

Problems

- requires some preparation
- breaks with some applications

Kerberos servers

There are reasons for having more than one Kerberos server:

- reliability
- load sharing
- geographic distribution

Database propagation

consistency is required

single master, several slaves

database is copied every hour

Problems

database could be up to one hour old

uses machine resources and network bandwidth

propagation delay cannot be too small

Incremental database propagation

assign a version number to every change

log all changes

propagate changes as soon as possible

slaves keep track of latest version

Firewalls

a number of problems with firewalls

- unusable protocols
- unusable ports
- unknown addresses

Firewalls (cont.)

a few solutions

- use protocols and ports that work—TCP, HTTP
- ignore addresses
- add more addresses

Portability

Requirements:

- an ANSI/ISO C compiler (such as gcc)
- awk
- lex/flex
- yacc/bison
- sh, make, sed, & c:o
- Posix libraries
- Berkeley sockets
- ndbm or Berkeley DB (only server)

Portability (cont.)

AIX

*BSD

Digital UNIX

HP-UX

Irix

Linux

SunOS

Ultrix

Unicos

UXP/V

Windows 95/NT with cygwin32

Compatibility

Tested with:

- MIT Kerberos
- OSF DCE
- Cisco IOS
- Microsoft NT 5 beta1

Future work

- more ways of handling firewalls
- ports to other systems (Windows, Macintosh, VMS)
- public-key support

Mythology

Kerberos is a monster that guards the exit from Hades (the Greek underworld).

Heimdal is a watchman on the bridge Bifrost that leads to Asgard (the realm of gods in Nordic mythology).

Acknowledgments

Supported by Parallelldatorcentrum, KTH

Lots of other people (see the documentation)

Availability

Source and documentation is available from
`http://www.pdc.kth.se/heimdal/`