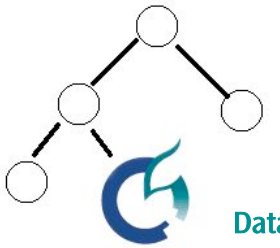
Introducing Kerberos

Æleen Frisch
aefrisch@lorentzian.com

NUUG, Oslo, 13 April 2010



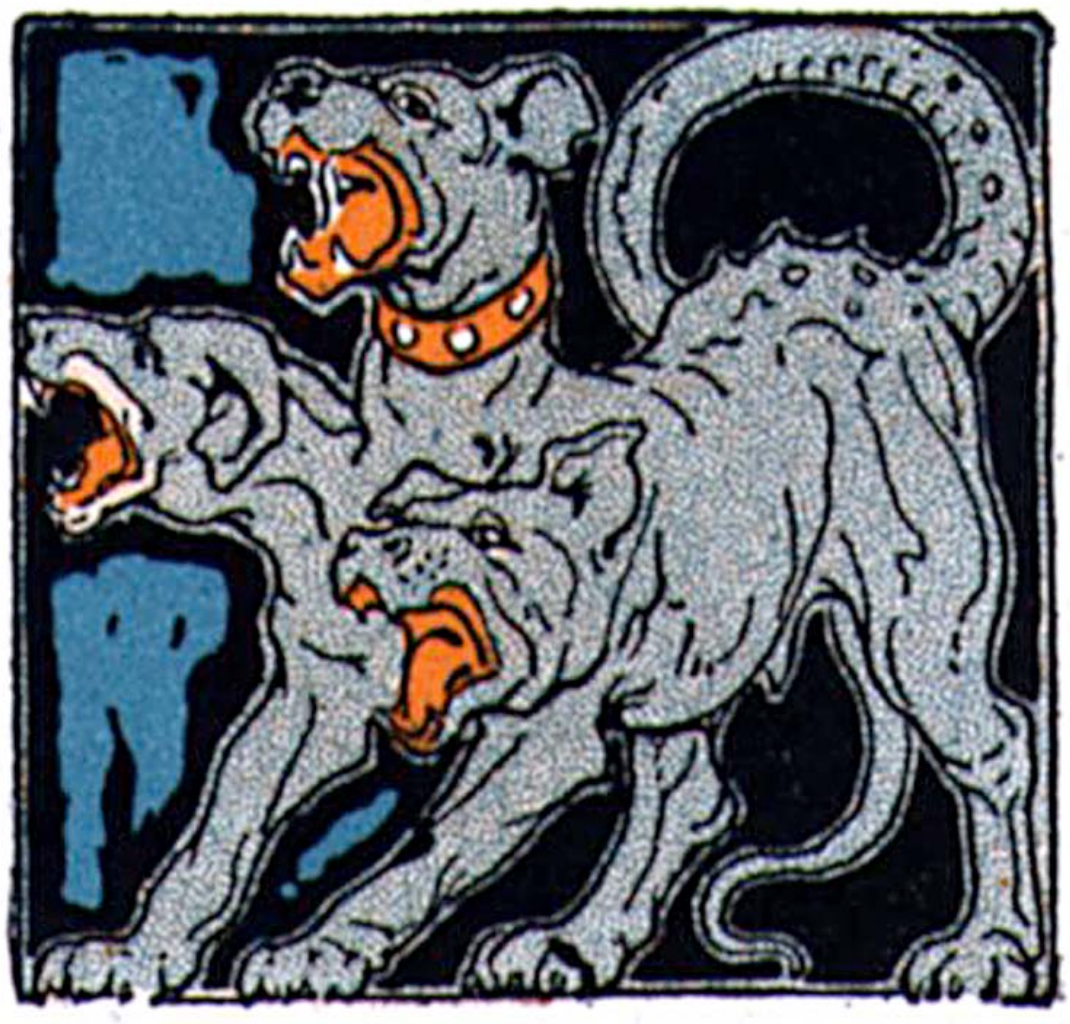
Data, Avdeling for ingeniørutdanning, Høgskolen i Oslo

Κερβεροσ

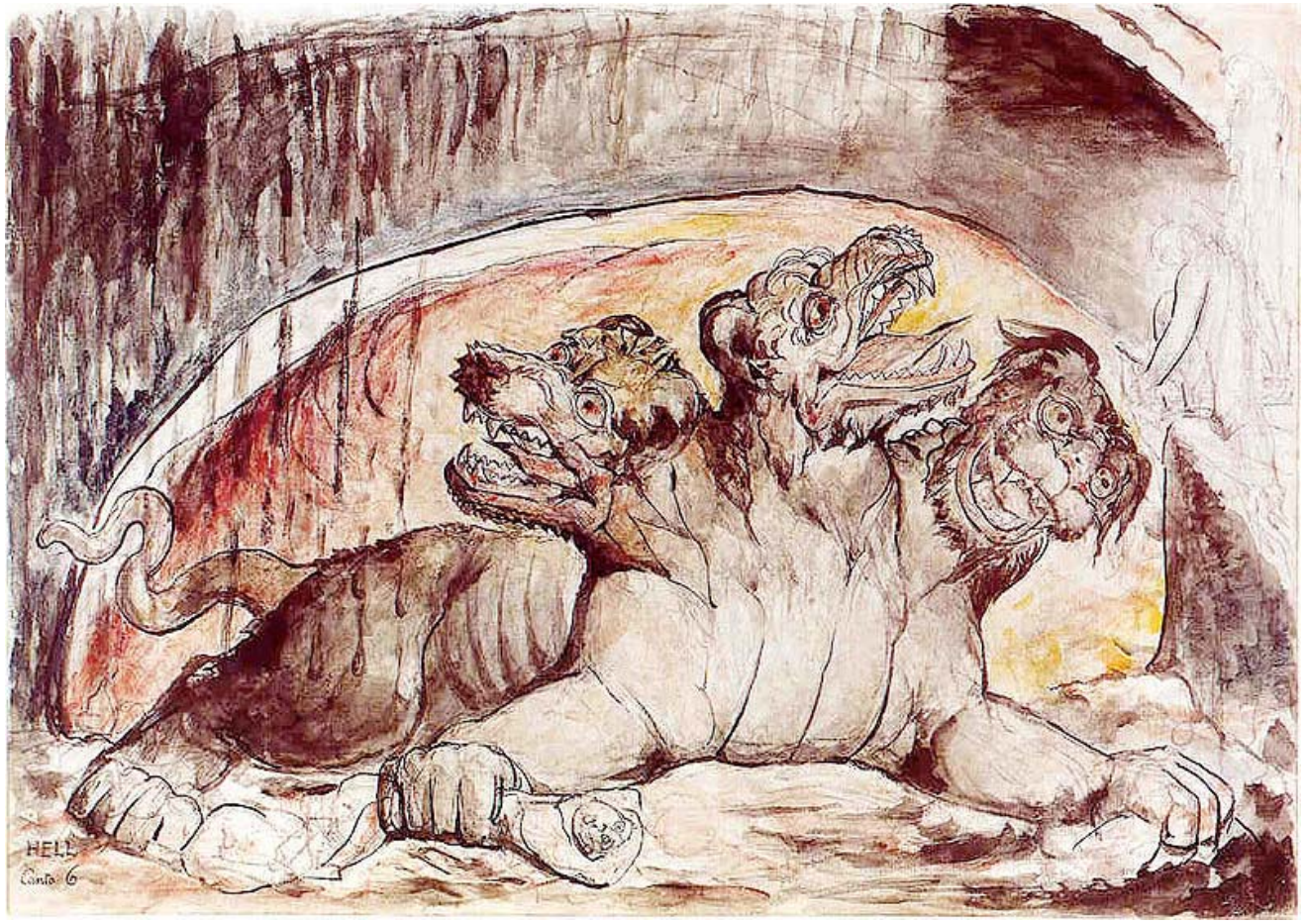
Høgskolen i Oslo

- Latin: Cerberus
- 3-headed dog serving as the gatekeeper to hell

Contemporary Illustration



William Blake's Dante



Anatomically Correct

Cerberus

Before the Beginning ...

Høgskolen i Oslo

- rsync /etc/hosts /etc/passwd ...
- /etc/hosts.equiv
- rlogin & rcp

A Little History

Høgskolen i Oslo

- MIT, 1983, Project Athena:
  - Single sign on
  - Secure remote access
  - Network file sharing
  - Graphical UI
  - Naming conventions and directory service
- Kerberos 4, late 1980s
- MIT Kerberos 5, 1993
  - RFC 4120

Fervor

We forsee a day when Kerberos-based authentication and authorization will be as ubiquitous as TCP/IP-based networking itself.

OMG There's a Munition in There!

- Until 2000, 56-bit DES cannot be exported from USA
- Kerberos 4p9 =>
  eBones =>
  Swedish Institute of Technology's KTH-KRB =>
  Heimdal Kerberos 5 (17/03/1997)

Heimdall

- Guards the Bifrost Bridge between Åsgard and Midgard
- Will blow the Gjallarhorn signaling the start of Ragnarok

But There Are Always 3 ...

Høgskolen i Oslo

- MIT Kerberos 5
- Heimdal Kerberos 5
- Active Directory

Why Kerberos

Høgskolen i Oslo

- Single sign-on
- No password data across the network
  - Not even in encoded/encrypted form
- Scales to even the largest sites
- Excellent support for heterogeneous environments

Kerberos Server

Høgskolen i Oslo

- Known as a KDC: Key Distribution Center
  - Think *Kerberos Domain Controller*
    - Database server handling keys
    - Authentication Server
    - Ticket Granting Server

Infrastructure Features

Høgskolen i Oslo

- Scales very well on even modest hardware
  - Tiny network messages
  - Only one access per user per service
- “Master” and “slave” servers
- Server-to-server replication

Kerberos Jargon

Høgskolen i Oslo

- Realm: Single Kerberos infrastructure implemented by a designated set of servers
  - Name=Upper(DNS domain)
- Principal: User account or host in a Kerberos database
- Ticket: Encrypted message authenticating user identity and authorization for access to a host, network or service
  - Ticket Granting Ticket (TGT): Entrance to Disneyland
    - Some things in the park are free
  - Service Ticket: Entrance to Pirates of the Caribbean

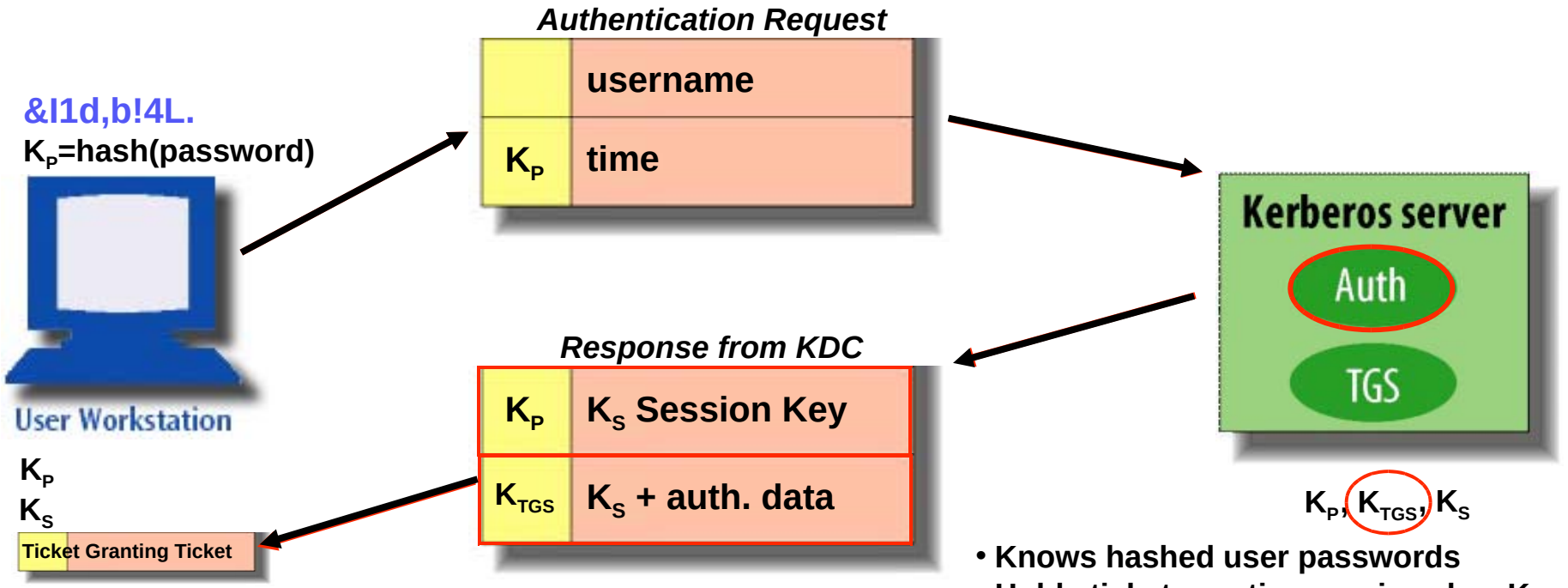
High Level Views

Høgskolen i Oslo

- User authentication
- Service access

Kerberos: Initial Authentication

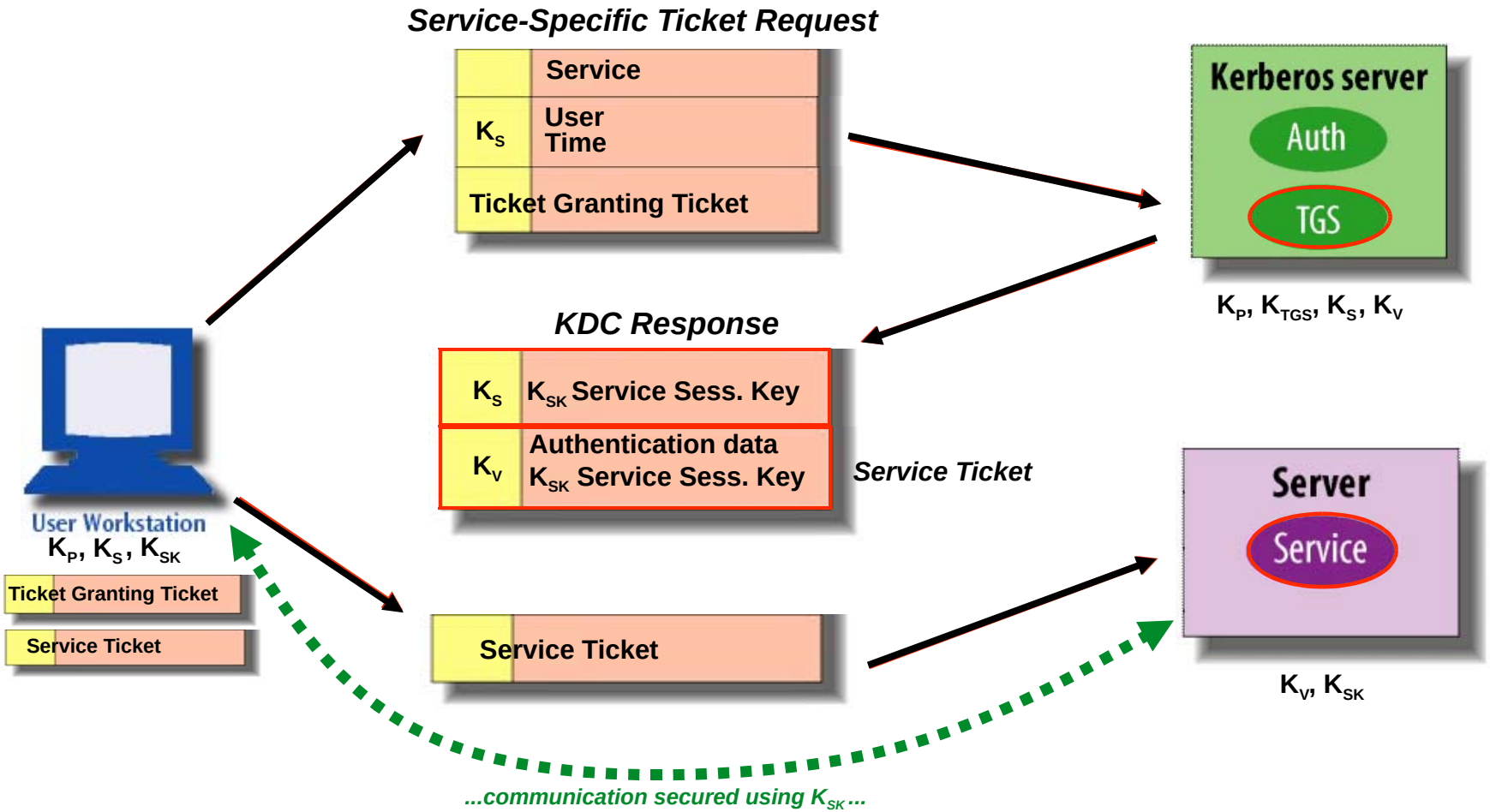
Høgskolen i Oslo



- Knows hashed user passwords
- Holds ticket granting services key K_{TGS}
- Checks time is within window to avoid replay attacks
- Creates session key K_S

Using a Kerberized Service

Høgskolen i Oslo



Additional Details

- Pre-Authentication: Requiring the user to prove knowledge of the key before granting TGT
  - Other option: PKI
- Ticket properties:
  - Renewable:
    - Initial expiration time (10 hours)
    - Maximum lifetime (7 days)
  - Forwardable: Ticket follows user to new clients
  - Proxiable: Ticket can be used by service directly for user
  - Postdated: For batch jobs

Security Safeguards

Høgskolen i Oslo

- Replay attacks
  - Using the time as the encrypted data prevents most of them
  - KDC can also maintain a replay cache
- Man-in-the-Middle attacks
  - Client responsibility
  - Secure DNS servers

Installing a Kerberos Server

- Prerequisites
- Install and configure KDC
  - Add principals to DB
  - Expand the infrastructure
- Install and configure client computers
- Install and configure server for services

- Example: MIT on Debian for AHANIA.COM (VMs)

Prerequisites

Høgskolen i Oslo

- DNS
  - A and PTR records for all hosts
  - Hostnames are FQDNs (e.g., /etc/hosts, /etc/hostname)
- NTP
  - At least ntpdate *server* in cron and at boot (rc.local)
- LDAP v3 (optional)

DNS SRV Records

Høgskolen i Oslo

```
@ORIGIN ahania.com.

_kerberos._udp.AHANIA.COM.        IN SRV 1 0  88 kdc
_kerberos._tcp.AHANIA.COM.        IN SRV 1 0  88 kdc
_kerberos-adm._tcp.AHANIA.COM.    IN SRV 1 0 749 kdc
_kpasswd._udp.AHANIA.COM.         IN SRV 1 0 464 kdc
```

Build the Software ...

Høgskolen i Oslo

- Or install packages:
  - krb5-kdc
  - libkrb53*
  - krb5-config*
  - krb5-admin-server
  - krb5-user*
  - krb5-doc

  - krb5-clients*
  - libpam-krb5*

Configuration Files

Høgskolen i Oslo

- /etc/krb5.conf: General settings
- /etc/krb5kdc/kdc.conf: Configures the servers
- /etc/krb5kdc/kadm5.acl: Administrative access control

/etc/krb5.conf

Høgskolen i Oslo

```
[libdefaults]
    default_realm = AHANIA.COM

[realms]
    AHANIA.COM = {
        kdc = dyrehagen.ahania.com:88
        admin_server = dyrehagen.ahania.com:749
        default_domain = ahania.com
    }

[domain_realm]
    ahania.com = AHANIA.COM
    .ahania.com = AHANIA.COM

[logging]
    kdc = FILE:/var/log/kdc.log
    kadmin = FILE:/var/log/kadmin.log
    default = FILE:/var/log/krb5.log
```

/etc/kdc.conf

Høgskolen i Oslo

```
[kdcdefaults]
    kdc_ports = 750,88

[realms]
    AHANIA.COM = {
        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
        acl_file = /etc/krb5kdc/kadm5.acl
        key_stash_file = /etc/krb5kdc/stash
        kadmin_port = 749
        kdc_ports = 750,88
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        master_key_type = des3-hmac-sha1
        supported_enctypes = aes256-cts:normal ...
        default_principal_flags = +preauth
    }
```

Creating the Realm

Høgskolen i Oslo

- /usr/sbin/kdb5_util create -s
  - Remember the master key
  - Corresponds to principal krbtgt/AHANIA.COM@AHANIA.COM
  - Database files are in /var/lib/krb5kdc

Adding Principals

- kadmin.local and kadmin
- Naming: aeleen/admin@AHANIA.COM
  - user/context@REALM

```
kadmin.local: addprinc aeleen/admin
WARNING: no policy specified …
Enter password for …:
Re-enter password …:
Principal "aeleen/admin@AHANIA.COM" created.
```

kadmin Subcommands

Høgskolen i Oslo

- {add,delete,modify,list}_{principals,policies}
- change_password
- kt{add,remove}

Granting Administrative Permissions

- /etc/krb5kdc/kadm5.acl

```
root/admin@AHANIA.COM       *
aeleen/admin@AHANIA.COM     *
chavez/admin@AHANIA.COM     AICL    */admin@AHANIA.COM
```

- Permissions: add, delete, inquire, modify, change password, list

Kerberos Server Processes

- krb5kdc: /etc/init.d/krb5-kdc
- kadmind: /etc/init.d/krb5-admin-server
- kpropd

- krb524d
- kadmind4

Kerberos Client Utilities

Høgskolen i Oslo

- kinit
- klist
- kdestroy
- kpasswd

- krb5-ftp
- ksu

Client Configuration

Høgskolen i Oslo

- Install software
- Configure /etc/krb5.conf as on KDC
- Add support for authentication and other services

PAM

- Module comes *before* pam_unix.so

- /etc/pam.d/common-auth

```
auth      sufficient   pam_krb5.so minimum_uid=1000
```

- /etc/pam.d/common-password

```
password sufficient   pam_krb5.so minimum_uid=1000
```

- /etc/pam.d/common-account

```
account  required     pam_krb5.so minimum_uid=1000
```

- /etc/pam.d/common-session

```
session  required     pam_krb5.so minimum_uid=1000
```

OpenSSH

Høgskolen i Oslo

- SSH v2
- /etc/ssh/sshd_config:

```
KerberosAuthentication yes
KerberosOrLocalPasswd yes
KerberosTicketCleanup yes
```

- Non-kerberized versions use the Generic Security Services API:

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

Application Support

Høgskolen i Oslo

- Replacements for insecure LAN services: FTP, telnet, rsh
- NFSv4
- SAMBA 3
- AFS
- Apache (and IIS)

Beyond the Basics

Høgskolen i Oslo

- Keytab(s) and their implications
- PKI integration
- Cross-realm trust
  - Active Directory integration
- Replication and updating
- SASL integration

For More Information

- MIT: web.mit.edu/kerberos/www/
- Heimdal: www.h5l.org
- Jason Garman, *Kerberos:The Definitive Guide* (O'Reilly, 2003)
- Gerry Carter, "Kerberos 5: Revenge of the Three Headed Dog," LISA conference tutorial
- Æleen Frisch, *Essential System Administration,* 4th ed, forthcoming 2011.