Kerberos 101

Basic knowledge for Kerberos users

Red Hat Czech s.r.o.

Jan Zelený

16. února 2012
Section 1

Introduction
What is Kerberos, why to use it

- Kerberos (SW suite) vs. Kerberos (protocol)
- usage on unsecure network
- secure authentication, creating secure channels
- symmetric cryptography (3DES, AES)
- Single Sign On
- passwords not transferred through the network
Section 2
Basic concepts
Important definitions and terms

- realm
- KDC, AS, TGS
- ticket
- principal
- key, keytab
Communication schema

1. AS: request
   Reply: TGT

2. Request for service
   Response: use KRB

3. TGS request
   Reply: service ticket

4. Request for service with the ticket
Section 3
MIT Kerberos
Kerberos implementation

- MIT Kerberos vs. others
- server, client libraries, GSSAPI
- kadmin, kadmin.local, database backends
- kinit, klist, keytabs
Server

- `/var/kerberos/krb5kdc`
- database backends (db2, hdb, ldap)
- kadmin
- kadmin.local
Client

- `/etc/krb5.conf`
- `kinit`, `kdestroy`
- `klist`
- `keytabs`
- `pam_krb5`, SSSD
Section 4

Some interesting extensions
Some interesting extensions

- PKINIT
- pre-authentication
- FAST
- OTP pre-auth using FAST
- AuthHub
The end.

Thanks for listening.