

Heimdal

Making Kerberos 5, AFS, and Windows 2000 work together

Love Hörnquist-Åstrand
Royal Institute of Technology
lha@stacken.kth.se

<http://www.stacken.kth.se/~lha/afstreffen2000/heimdal.ps>

Kerberos 4

- Created at Project Athena, MIT
- Exported without crypto in Bones.
- Eric Young put encryption back, eBones.
- Picked up at KTH, cleaned up, some parts rewritten.
- Cross realm.
- Vulnerable to offline attack.
- Limited to single des only.

Kerberos 5

- Pre-authentication.
- Support for smartcards (PKINIT).
- Public key authentication between realms (PKCROSS)
- Any encryption-type types you want.
- Uses ASN.1 to encode messages.
- Ticket forwarding.
- Crossrealm trust can be specified.
- Transit realms (realm jumping)

rx and rxkad

- R_x is the RPC subsystem in AFS.
- rxkad is the Kerberos authentication module.
- rxkad uses fcrypt, not des.
- rxkad only support Kerberos 4.

kaserver

- Kerberos 4 based, but using R_x rpc-calls.
- Pre-authentication.
- KAA, KAT, KAM.
- KAM uses rxkad for security.
- kpasswd uses KAM !

Salts

- Salts is is used to harden password.
- Appended or prepended to password.
- Kerberos 4 uses no salt ("")
- kserver uses salt (cell).
- Server specifies salt in Kerberos 5, depends on string2key function (principal).

Heimdal

- Kerberos 5 implementation using RFC1510 (and drafts).
- Written from scratch by Assar Westerlund and Johan Danielsson.
- GSS-API.
- arcfour-hmac-md5 (windows 2000 compatibility).
- Pluggable database backend (distributed database support ?).
- Kerberos 4 kdc and kaserver emulation.

Windows 2000

- Kerberos 5 only.
- SSPI, almost GSS-API, Kerberos and NTLM.
- Authorization-data in the ticket.
- Support for SSPI in most applications (Explorer!).
- Uses Active Directory as database.
- Stores PAC in authorization-data field.

Authorization data

Ticket

Server principal: host/mim.e.kth.se

Realm: E.KTH.SE

Encrypted part (Encrypted by server principal)

Key: session key

Endtime: 2000-12-24

Principal: lha

Realm: E.KTH.SE

Authorization-data: PAC

Put in the TGT, inherited to all “children”
if not else specified.

PAC

- Used to authorize the user.
- Contains the groups and id of the user.
- Signed by the kdc.
- Specification released, but not for implementation!

Kerberos 5 in a W2K workstation

- User mapping specified in the registry.
- Can not be part of a domain.
- Stores the kdc/realms db in the registry.

Crossrealm trust with a W2K domain

- User mapping written in the AD.
- Must be part of a domain.
- Stores the kdc/realm db in the registry.
- Windows KDC adds PAC.

Windows 2000 tips and tricks

- Microsoft forgot checksum algorithms 'rsa-md4-des' and 'rsa-md5-des'.

- /etc/krb5.conf

```
[libdefaults]
default_etypes = des-cbc-crc
default_etypes_des = des-cbc-crc
[kadmin]
default_keys = des3:pw-salt des:pw-salt
des:pw-salt:
```

- Need to add the realm to all workstations (ksetup or regedit).
- Account mapping.
- Heimdal texinfo (info) documentation.

What we use

- Unix users log in to a Windows 2000 Citrix' Metaframe server and run Microsoft Office.
- They use their kerberos password.
- Files are accessed throu the Ica-client.

AFS and Kerberos

- The key in **KeyFile** is the same as
afs@my.cell (afs/my.cell@MY.REALM)
- A token is a striped down ticket + cred.
- Can use Kerberos 5 (still fcrypt!)
Check out des-cbc-crc version of afs@MY.REALM
Convert it to a token
Push it into the kernel
- KTH-KRB and Heimdal is AFS-aware
and will do the right things.
- Heimdal (hprop) can read a ka-database

Kerberos AFS tools

- **afslog** will get you tokens from a ticket.
- **pagsh** will get you a new PAG.
- **ktutil** can convert between srvtab, KeyFile, and keytab.

```
ktutil -k KEYFILE:/usr/afs/etc/KeyFile list
```

- **kadmin** is the admin interface (-local exists).
- Arla has a **klog** that uses Kerberos 4.
- **krb-forward** forward Kerberos 4 request to the real server.

Gross hacks with Samba

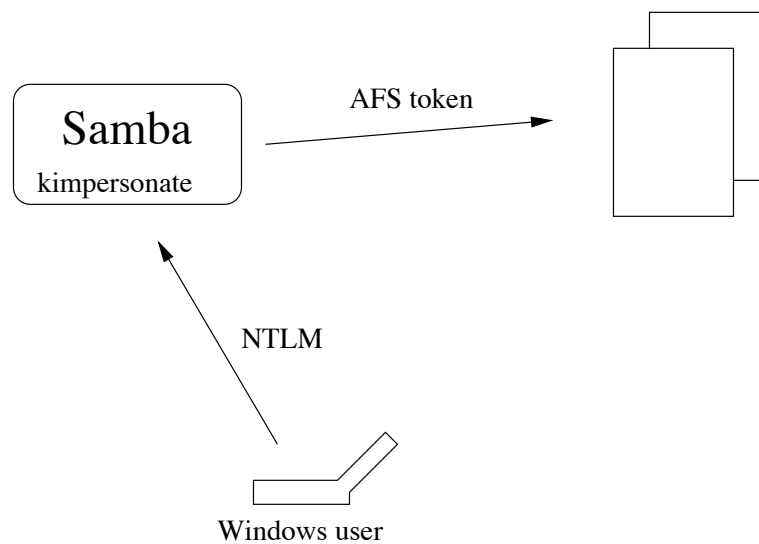
- User needs token to read/write files.
- To get token the password is needed.
- Using cleartext password is not acceptable.
- Need a solution that scales.

Other solutions

- Umich did KSamba that send a token over an encrypted channel to the Samba server on the side.
- Other people store a srvtab on the samba server with the users password.

The gross hack

Store the AFS KeyFile on the server and generate a ticket on the fly.



When the user is logged a script is run that fetch the user a token and install it into the kernel.

Things that might be done better

Windows NTLM is a delegation service, only used by Microsoft. Somewhat works like Kerberos, but it require the server to talk to the **password server** for each request.

The samba-server should check the password against the Kerberos database. **arcfour-hmac-md4** is the same Windows hash, due tp there must be a way for old Windows NT 4 users to convert their domain.

What it.kth.se use

- A round 250 mobile users use it daily to access their files.
- They have two password
- The timelimit on the token i 12 hour.

So when do you change/Migrating

Missing native support for AFS, zephyr and kpop.

Solutions:

- Does not matter
- Kerberos 4 kdc emulation
- Kerberos 5 to 4 service

So when do you change/Migrating

- Try to build the software.
- Run a Kerberos 5 slave for a while.
- Figure out if it does everything you want it to.
- Burn the bridge and change the master.
- Let a small number of controlled users use Kerberos 5 tools.
- Let all users use the Kerberos 5 tools by default.
- Turn off services that doesn't need Kerberos 4 auth.

Questions ?