HP and Kerberos

Kerberos case studies:
from large to small (or even none)

Jakub Urbanec
HP Czech republic

Why me?

Great guys in HP Czech (believe it or not)

- Detailed, topical, …. in czech
- In English – by me

HP

- Printers
- Hardware

  PC

  Servers

  Big servers, storage, network equipment …
- Software
  - Consulting and Support
    - Security
      - My managers manager
        - My manager
          - me

Use cases

- You have been through UC million times
- We can not reveal the customer names :-(

UC 1

Customer1 - pharmacy

needed JUST central auth service

- Linux (RHEL, directory server)
- MIT Krb code compiled from source
- No patches, no X-realm auth
- Anything interesting?
- Boring (but still it is business ;-)!

UC 2

Customer2 big telco - central auth for services

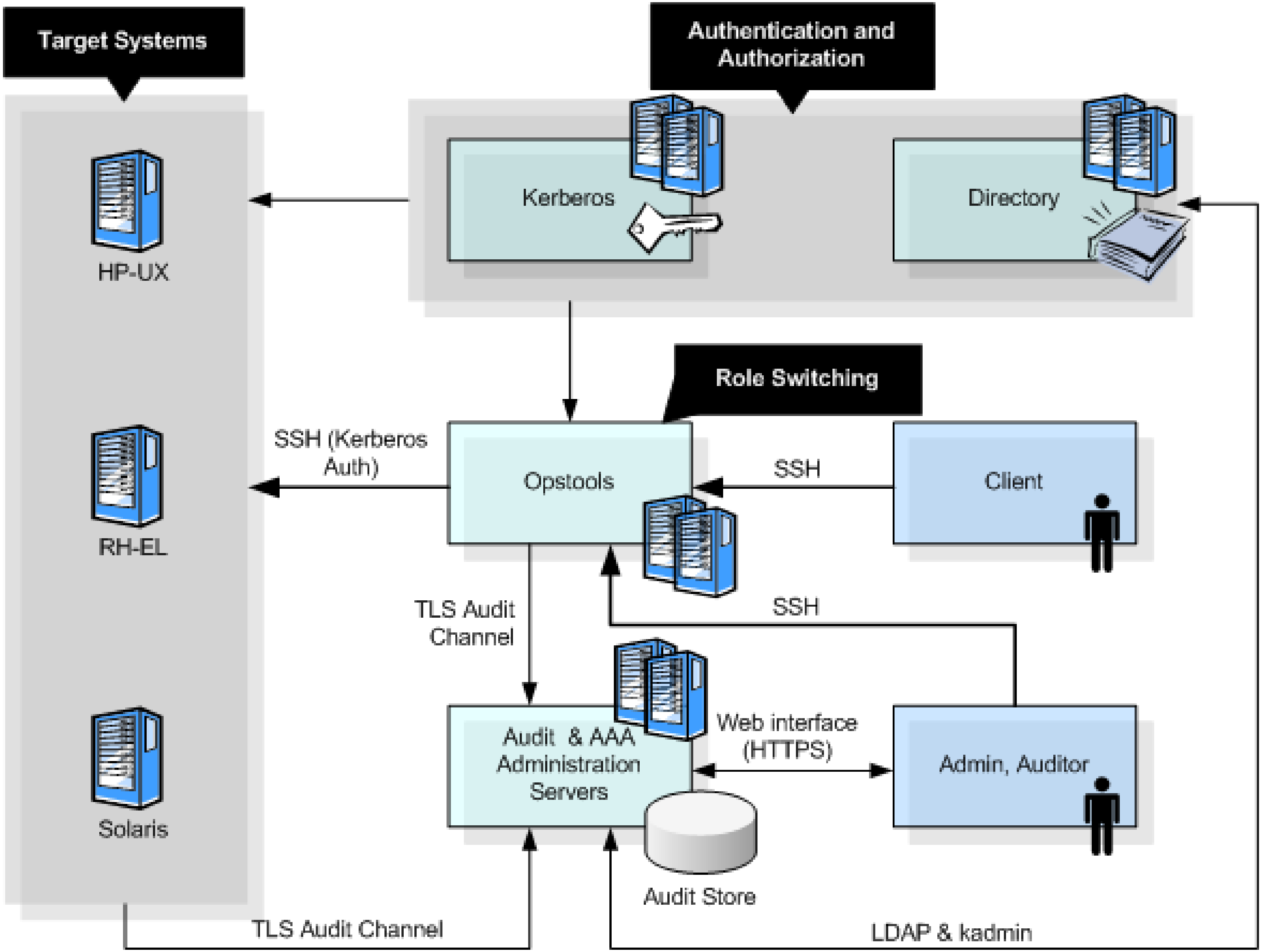
- Solaris, HP-UX, Linux
- MIT Krb code 1.2.x era + delta level replication patch (HPUX 11.11)
- X-realm with Microsoft AD for users
- Anything interesting?
    - At least the patches and X-realm

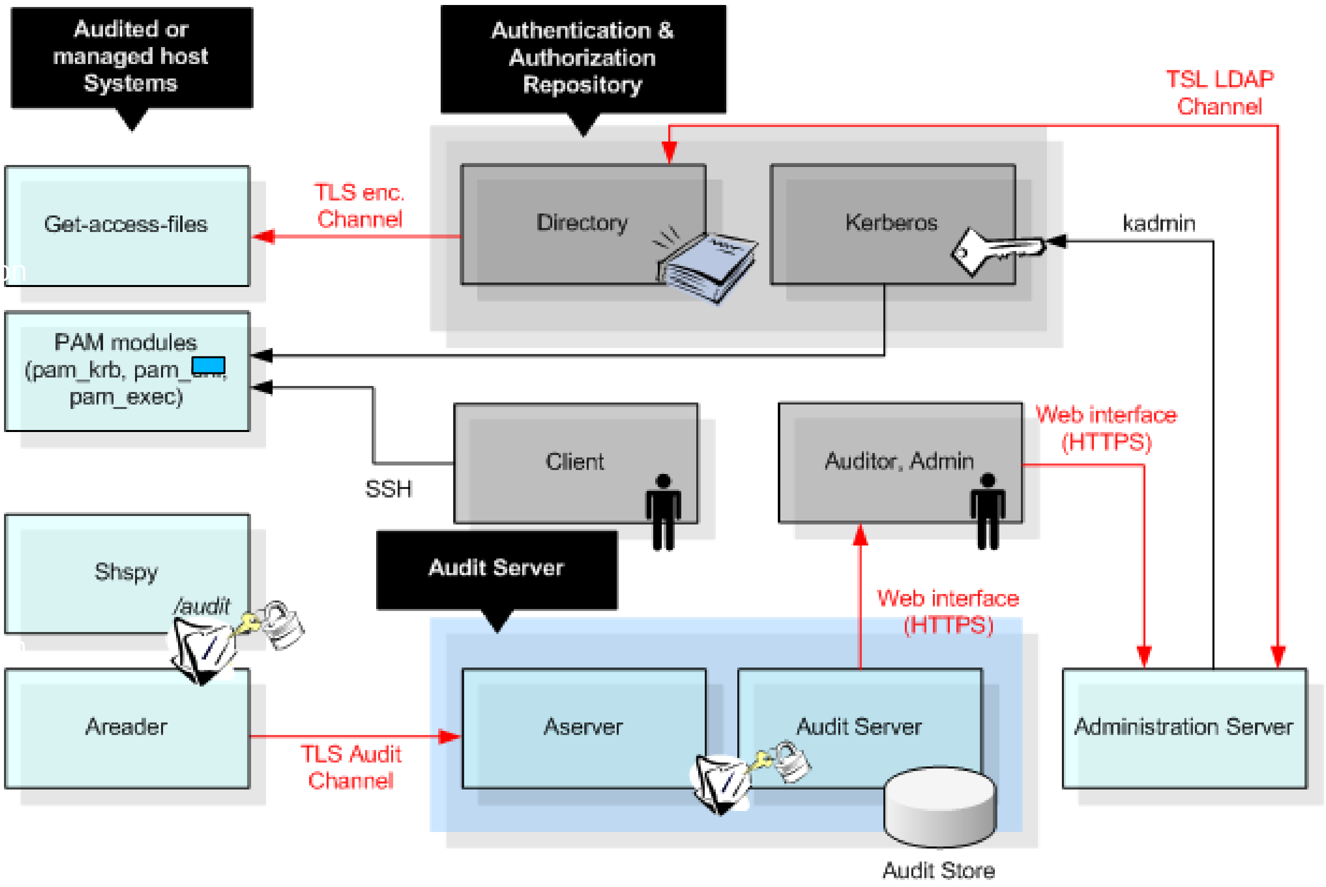
UC 3

Customer3 – large 3letter logistic organization

- 800+ servers
  - HPUX (IA, PA-RISC)
  - Linux (RHEL v 3,4,5)
- Project to enable **unified** access control and **accounting** for **admin** users
- AAA solution

UC 3 II


Target Systems
Authentication and Authorization
Kerberos
Directory
HP-UX
RH-EL
Solaris
Role Switching
SSH (Kerberos Auth)
Opstools
SSH
Client
TLS Audit Channel
SSH
Audit & AAA Administration Servers
Web interface (HTTPS)
Admin, Auditor
Audit Store
TLS Audit Channel
LDAP & kadmin



MIT Kerberos

- Standard Kerberos clients
- Standard Kerberos server
- Custom build of MIT Kerberos utilities and libraries used by custom AAA components

OpenSSH

- Standard SSH client (HP rebuild)
- Support of customer required Kerberos encryption types back-ported to RHEL3

LDAP

- RHEL Directory Server
- Custom schema added
- LDAP-UX client used for Access ctrl
- OpenLDAP libraries with TLS support used in cust. AAA components

Custom AAA components

- Audit server
- Shspy
- PAM modules
- Areader/Aserver
- Get-access-files
- Admin server GUI
- Automatic Principal Lockout

UC 3: Authentication – Kerberos

Single Sign On available to users authenticated on host

Support of customer required AES 256 required own HP-UX library build

Proper time synchronization is required

Principal Management available via kadmin utility or via custom administration GUI

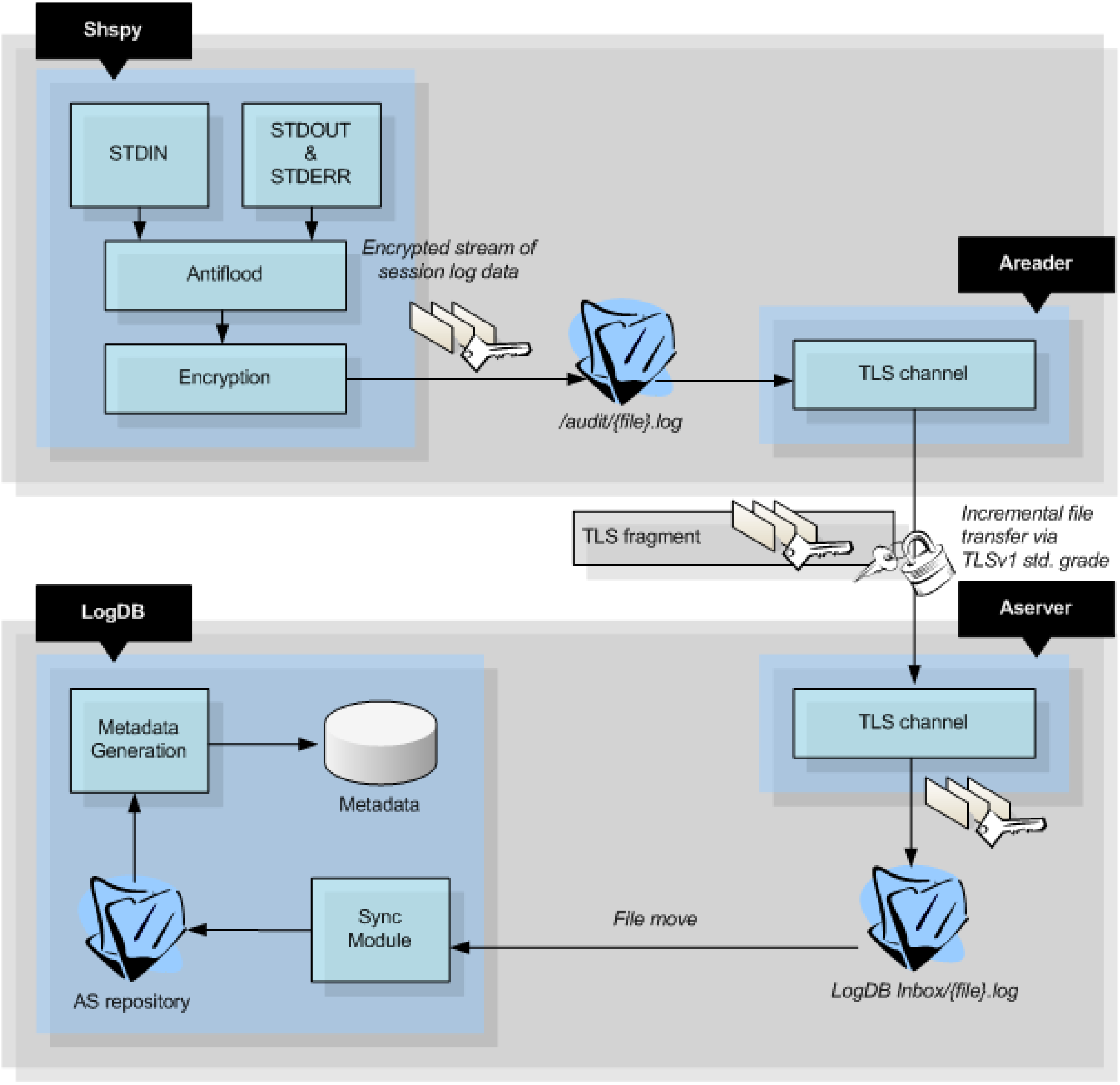
Principals may be administratively locked etc.

Custom automatic principal lockout script added

UC 3: Authorization

- Utilizes Standard features of NSSWITCH for LDAP
- Suite of PAM modules
  - PAM Kerberos (custom build for HP-UX required)
  - PAM XXX (based on pam access driven by local XXX_access.conf file, KRB or localy)
  - PAM Exec (custom built for HP-UX required)
  - PAM Env (custom build for HP-UX required)
- Get-access-files
  - Utility for synchronization of target host configuration files from AAA admin server (LDAP)

UC 3: Audit


Shspy
STDIN
STDOUT & STDERR
Antiflood
Encryption
Encrypted stream of session log data
/audit/{file}.log
Areader
TLS channel
TLS fragment
Incremental file transfer via TLSv1 std. grade
LogDB
Aserver
Metadata Generation
Metadata
TLS channel
Sync Module
File move
AS repository
LogDB Inbox/{file}.log

UC 3: Audit II

Stream cipher allows immediate transfer

- Stored blocks of streams are enciphered with chained cipher – allows integrity check and independence of blocks if some block of session has been removed
- Stream contains timestamps of each input/output separated that allows better/custom heuristics implementation used to user issued command detection
- When connection is temporary unavailable, sessions are locally cached (till enough cache space is available. If not, you win).

UC 3: Audit III

Search for stored session by

- Date/time of start/end or session was active
- Kerberos principal name
- Process/Shell running
- PID
- User name
- Command issued

Replay or pause stored part of session (or whole) in real or virtual time (faster or without idle times)

Auditor has a special access to full user input, binary dump of stored session possible

UC 4

Customer4 – large czech bank

- Call from sales manager:

They need to get a rid of ssh keys!

```
rm –fr ~/.ssh
find / -iname “id_rsa.*” –exec rm {};
```

UC 4 ssh keys bad bad bad

SSH keys are somewhere on the FS, unprotected. The access via ssh key does not show identity

SSH Keys for users, but mostly for services (cron…)

What they wanted:

- Cheap, secure and fast solution
- Based on the UNIX system components
- Windows access would be nice to have
- Easily integrated into the bank systems

UC 4 Kerberos?

Bank has already large Microsoft AD deployment

But the AD guys are ***s (not to mention we needed instance principals)

There is planned KRB5 architecture in other project, which ***s (not to be managed by IT sec guys, no user principals (PCIDSS limit))

We want brand NEW REALM!

UC 4 Kerberos??

Summary: in order to remove ssh keys we will:

- Start new KRB infrastructure (3servers, HA, backup, procedures, paper work,...)
- Name people responsible for this realm
- Change a lot of system scripts to obtain the tickets before calling ssh/scp

UC 4 – HP way

50+ Man Days project

- Testing, deployment and production environment (it is a bank, you know the drill)
- Rewriting scripts
- Training for the staff
- Lots of work, lots of fun but:
- **Will it really increase the security?**

UC 4

SSH keys on the FS

KRB keytab on the FS

Will it really increase the security?

The End

Thank you guys @147.228.0.0/16

No more killall -9 httpd on Digital UX fileserver