SunSoft
A Sun Microsystems Company

NFS Security Topics: Update on NFS over GSS-API

Mike Eisler

NFS Group

mre@Eng.Sun.Com

CONTENTS

- Status of NFS security project
- Why GSS-API?
- Why Kerberos V5?
- Issues
- Futures

STATUS

- **Goal is to produce NFS client and server using Kerberos V5 security with support for strong:**
  - authentication
  - integrity
  - privacy
- **http://playground.sun.com/~mre/secrpc/ has pointers to design and specifications:**
  - built on draft-ietf-oncrpc-rpcsec_gss-02.txt
  - rpcsec_gss built on GSS-API
  - relevant IETF working groups are ONCRPC, CAT:
    - **http://www.ietf.org/html.charters/oncrpc-charter.html**
    - **http://www.ietf.org/html.charters/cat-charter.html**

- **Prototype of user-level RPC and kernel-level NFS over RPCSEC_GSS/GSS-API/Kerberos V5**
- **Defining a product that includes Kerberos V5, kerberized telnet, ftp, r* in addition to NFS.**
- **Will publish informational RFC for NFS/ RPCSEC_GSS/Kerberos once** draft-ietf-oncrpc-rpcsec_gss-02.txt **goes to proposed standard.**

WHY GSS-API?

(Or, why not SSL? Why not IPSEC?)

- **Why not SSL?**
  - SSL was still proprietary when we started
  - Integrating the SSL model with the RPC authentication model isn’t clean
    - **multiple port number issue**
  - no support for UDP
- **Why not IPSEC?**
  - IPSEC isn’t there yet
  - RPC authentication model (multiple users, one transport end point) is hard to implement in “end-user” IPSEC
    - **especially over Streams**

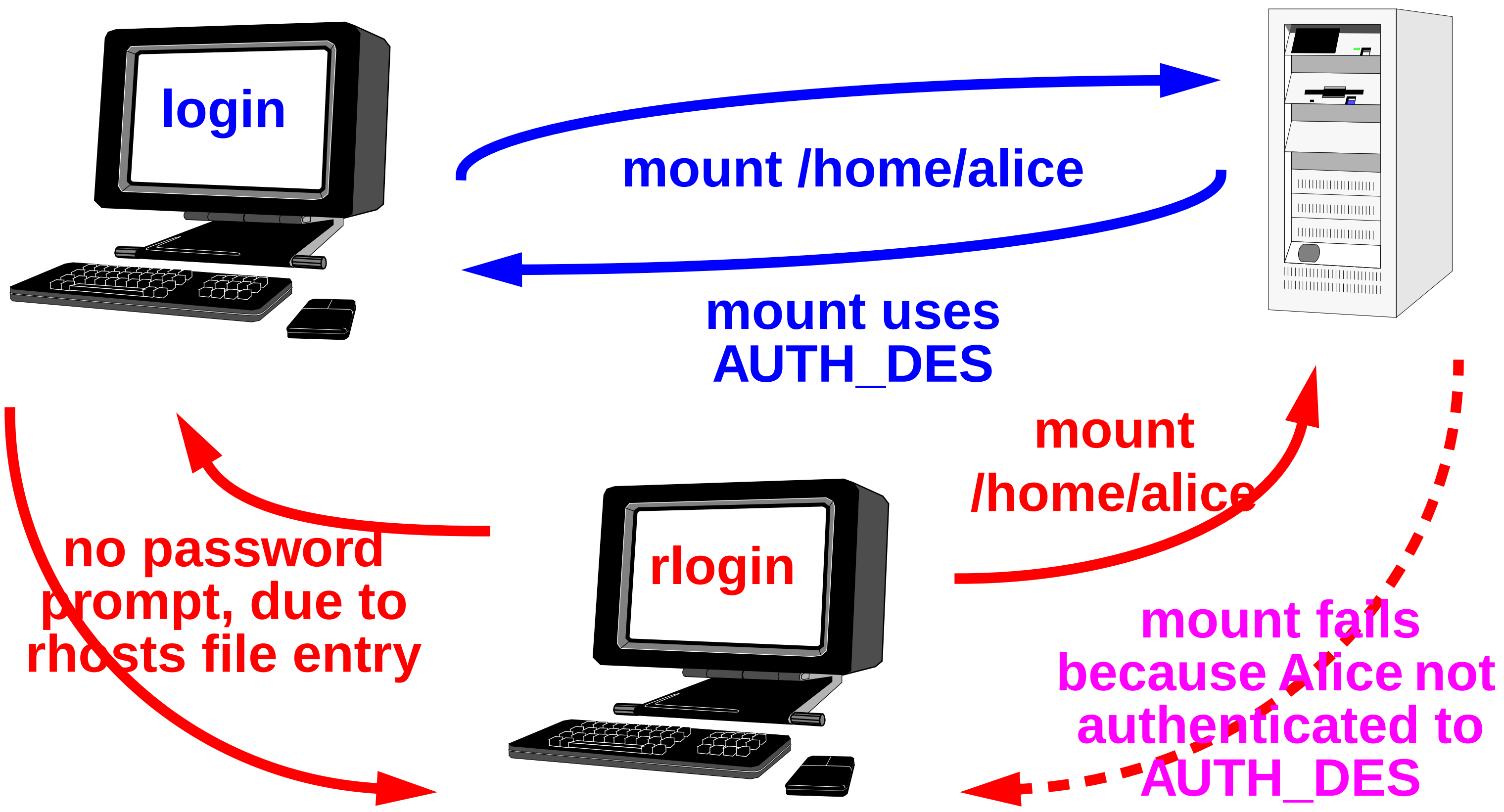
WHY KERBEROS V5?

(Or, why not “public key”?)

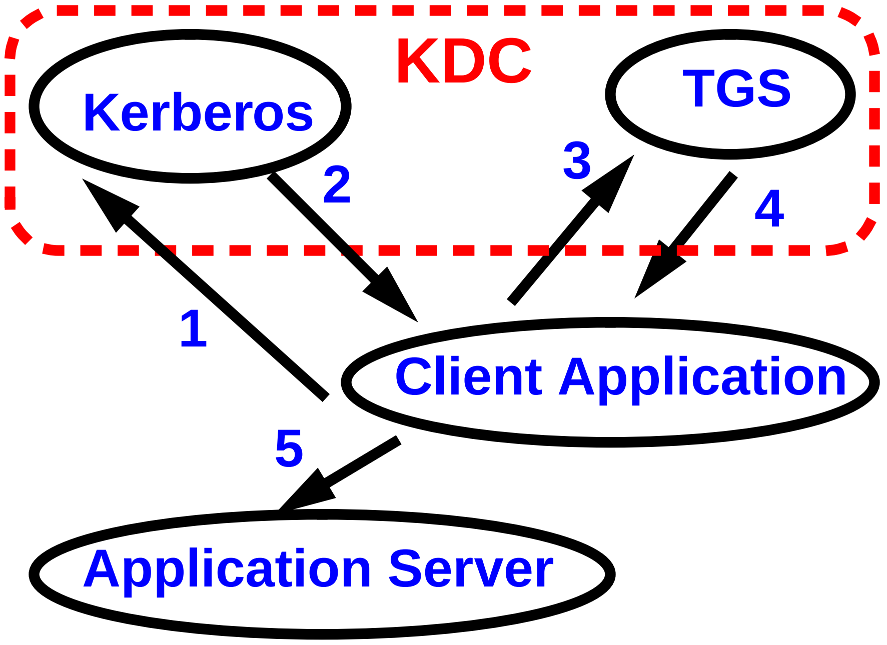
- **Kerberos V5 can provide “single network signon”**
  - log onto your desk top once, and no more password prompts
    - **requires that all the network services be Kerberized**
- **Use a central authentication server provides centralized audit trail of what services are being accessed.**
- **Kerberos V5 will (someday) support public key certificates**

Kerberos V5 versus “public key”

Public-Key File Sharing/Remote Login Scenario

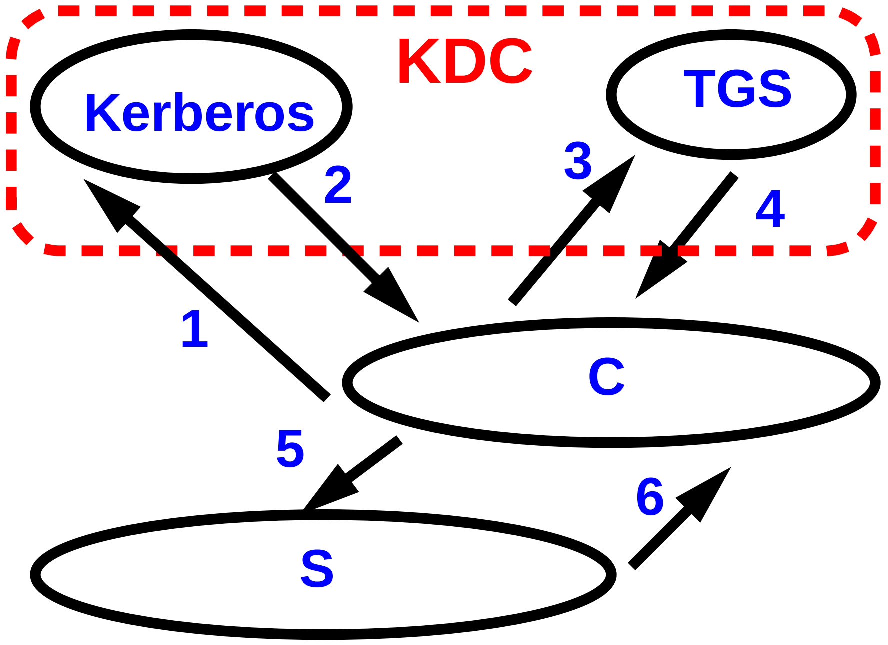

login
mount /home/alice
mount uses AUTH_DES
no password prompt, due to rhosts file entry
rlogin
mount /home/alice
mount fails because Alice not authenticated to AUTH_DES

How does Kerberos V5 work?



Gross Over Simplification

1. Request for Ticket Granting Ticket (in the clear) to Kerberos Authentication Server
2. Session Key (encrypted with client's secret key) for client to TGS session plus TGT (encrypted with TGS' secret key)
3. Request for service ticket: client id (encrypted with session key from step 2) plus encrypted TGT from step 3 plus server id
4. Key (encrypted with session key from step 2) for client/server session plus server ticket (encrypted with server's secret key)
5. Request to server: client id (encrypted with session key from step 4) plus encrypted ticket from step 5



$T_{C,TGS}$ = TGS, {C, timestamp, expiry, $K_{C,TGS}$}K_{TGS}

$T_{C,S}$ = S, {C, timestamp, expiry, $K_{C,S}$}K_S

Over Simplification

1.as_req: C, TGS, ticket expiry

2.as_rep: {$K_{C,TGS}$,TGS, expiry}K_C, {$T_{C,TGS}$}K_{TGS}

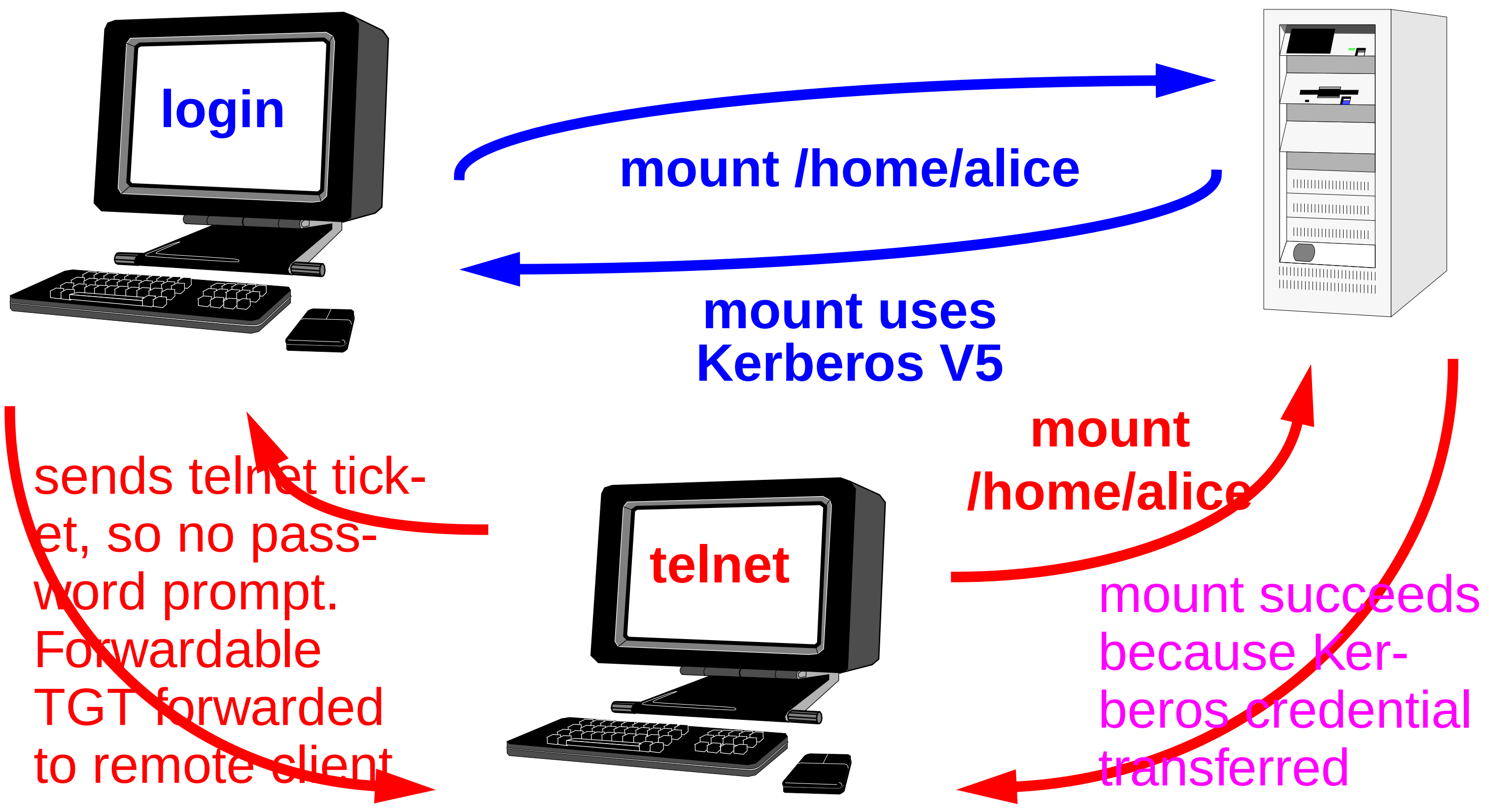
3.tgs_req: {timestamp}$K_{C,TGS}$, {$T_{C,TGS}$}K_{TGS},S, ticket expiry

4.tgs_rep:{$K_{C,S}$,S,ticket expiry}$K_{C,TGS}$, {$T_{C,S}$}K_S

5.ap_rep:{timestamp, C}$K_{C,S}$ {$T_{C,V}$}K_S

6.[optional] ap_req: {timestamp}$K_{C,S}$

Kerberos File Sharing/Remote Login Scenario


login
mount /home/alice
mount uses Kerberos V5
mount /home/alice
telnet
sends telnet ticket, so no password prompt. Forwardable TGT forwarded to remote client
mount succeeds because Kerberos credential transferred

ISSUES

- **Kerberos V5 interoperability**
  - no recent Kerberos “bake offs”
- **GSS-API portability**
  - definition of default quality of protection is implementation specific
- **Export control**
  - packaging may become easier

FUTURES

- **Public-key extensions in Kerberos V5**
- **non-Kerberos public key**
  - SPKM
  - SSL's cipher suites
- **Java classes for GSS-API**