SunSoft

A Sun Microsystems Company

NFS Security Topics: Kerberos V5 as an NFS security mechanism

March 9, 1998

Ram Marti

RPC/NFS Engineering Group

ram.marti@Eng.Sun.Com

CONTENTS

- **Why Kerberos V5?**
- **Kerberos Overview**
- **Kerberos Deliverables**
- **Issues**
- **References**

WHY KERBEROS V5?

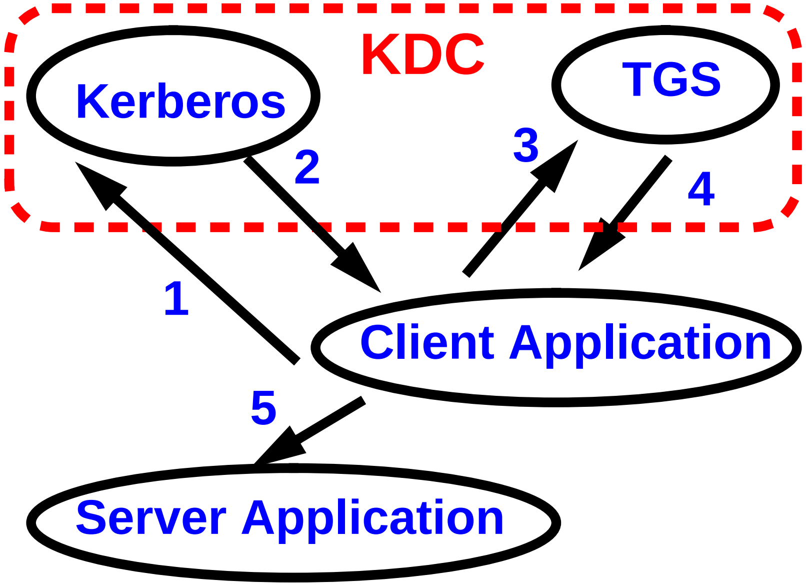
(Or, why not "public key"?)

- **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**
- **Authentication server provides a centralized audit trail of what services are being accessed**
- **Kerberos V5 will (someday) support public key certificates**

Kerberos Overview

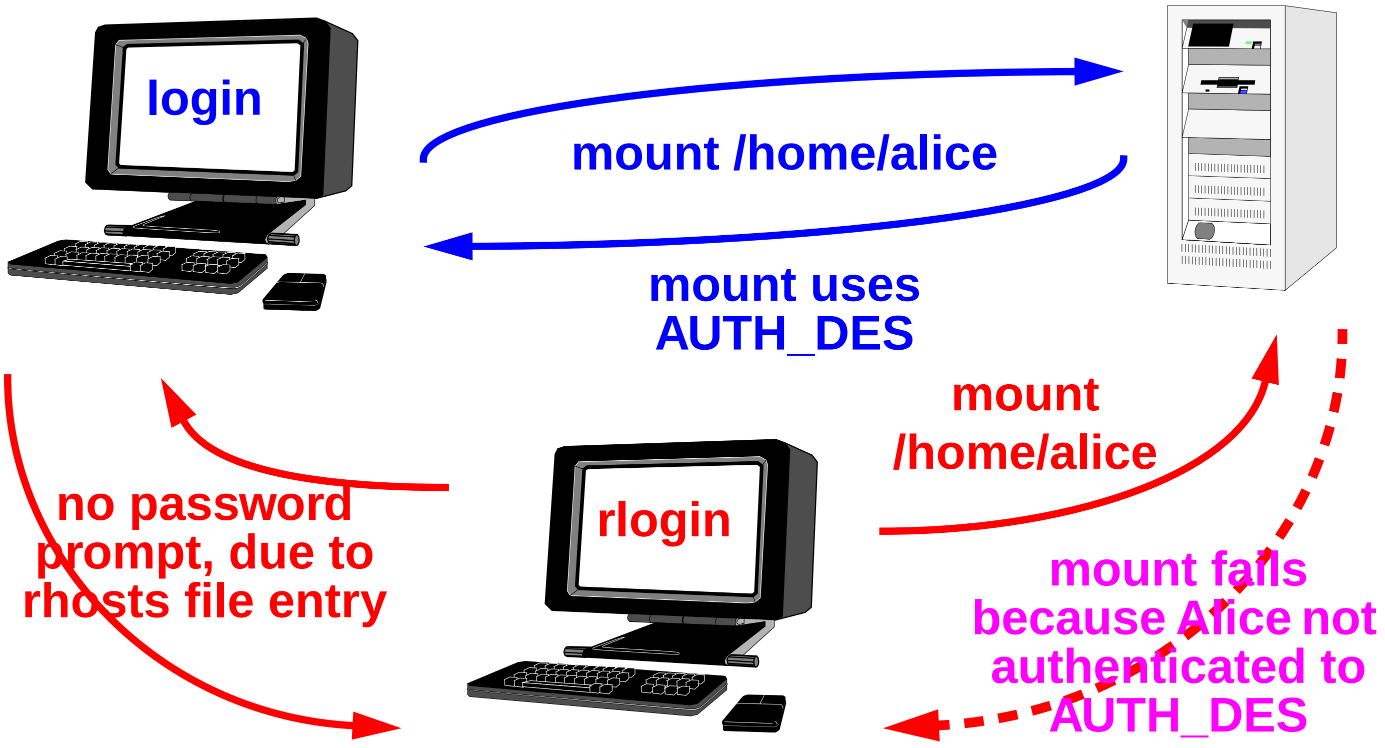
- **Based on trusted third-party authentication service**
- **Participants trust Kerberos' judgement as to the identity of the participants**
- **Database of all participants and their private keys**
- **Can provide three levels of protection**
    - Authentication of connection
    - Message integrity
    - Message privacy

How does Kerberos V5 work?



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

Auth_DES File Sharing/Remote Login Scenario



login

mount /home/alice

mount uses AUTH_DES

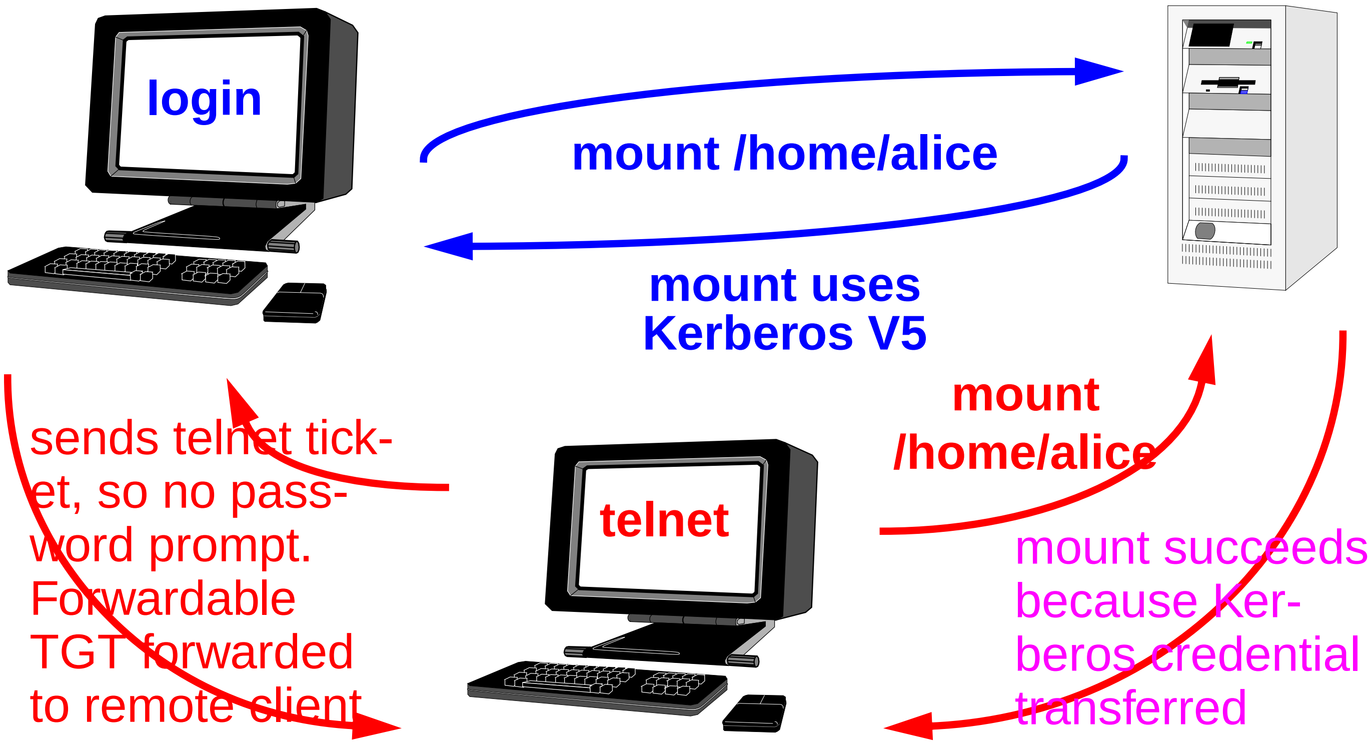
no password prompt, due to rhosts file entry

rlogin

mount /home/alice

mount fails because Alice not authenticated to AUTH_DES

Kerberos File Sharing/Remote Login Scenario



sends telnet ticket, so no password prompt. Forwardable TGT forwarded to remote client

mount succeeds because Kerberos credential transferred

Kerberos Deliverables

- Clients (Kinit, Klist, Kdestroy and Kpasswd)
- Kerberized Applications (Telnet, FTP, R*)
- Kerberos Servers (AS and TGS)
- KADMIN Client and Server
- JAVA-based GUI Tool for Kerberos Administration
- GSS-API plug-in support

ISSUES

- **Kerberos V5 interoperability**
- **GSS-API portability**
  - definition of default quality of protection is Kerberos implementation specific
- **Export control**

References

- Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems", USENIX Mar 1988. [athena-dist.mit.edu:pub/kerberos/doc/usenix.PS]
- RFC 1510 PS J. Kohl, B. Neuman, "The Kerberos Network Authentication Service (V5)", 11/21/97