About

- principles
- usage & application
- ticket flow
NotAbout

- writing applications
- cryptography
- number theories
WhatIs

- MIT developed
- implementations
  - MIT krb5
  - Heimdal
  - Windows AD
WhatIs #2

• AUTHENTICATION
  • act of verifying identity
  • process of proving identity to service

• Benefits
  • Standards based strong authentication system
    – AES-256 -128, arcfour, 3DES
  • Various OS support
  • No password sent thru the network
  • Single sign-on
WorksWith
(included in MIT implementation)

- eklogin
- gssftp
- krsh
- kshell
- ksu
- telnet
WorksWith (supported)

- ssh
- httpd + modules (perl, python, ruby)
- nfs
- versioning (git, svn, cvs)
- bind
- cups
- proxy
- mail (smtp, pop, imap)
How Works

- Client wants to prove his identity to AS
- User ID = name + realm
- AS checks the database
  - Krb (berkleydb)
  - ldap
HowWorks #2

Client enters the password to decrypt the TGT
HowWorks #3

- Client ID
- Client network address
- Ticket validity period
- client/TGS session key
HowWorks #4

- The client submits the ticket-granting ticket mentioning the service name to the ticket-granting server (TGS), to get authenticated.

- **KDC**
  - key distribution center
  - KDC shares a key with each of all the other parties
  - The KDC produces a ticket based on a server key.
How Works #5

- The TGS creates an encrypted key with a timestamp, and grants the client a service ticket
- The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service
HowWorks #6

- The service decrypts the key, and makes sure the timestamp is still valid.
How Works #7

- The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server.
- After the communication is made between the client and server, no further need of transmitting logon information is needed. The client is authenticated until the session expires.
What Is Not

AUTHORIZATION

Disadvantages

- The only KDC handles authentication (might be solved by propagation to slaves)
- Clock synchronization – up to 10 minutes (might be solved by proper time synchronization)
- No unencrypted service should be used
Thank you

- questions