TECHNISCHE UNIVERSITÄT CHEMNITZ

Managing Users and Permissions in a LDAP Directory

Karsten Petersen

kapet@informatik.tu-chemnitz.de

Introduction

- personalized user environments
  - central storage of documents
    => users must be authenticated
- computer networks
  - people use several machines
  - restricted and free-to-use computers
    => authorization of users must be checked

Scenarios of Use

- Computing Center of the TU Chemnitz
  - Unix Servers and Workstations
  - Windows Workstations
- Chair of Computer Networks
  - Unix Workstations
- André-Gymnasium Chemnitz
  - Unix Servers and Workstations
  - Windows Workstations

Linux

- Logging In:
  - PAM dispatches authentication and authorization
  - flexible, modular system
- Information Requirements:
  - UID and GID lookups
  - NSS handles several information sources
  - also flexible and modular

Windows

- Logging In:
  - GINA presents graphical login screen
  - LSA authenticates and authorizes
  - although modular it is inflexible, hard to extend
- Information Requirements:
  - SID lookups
  - process badly documented, bound to the LSA

Information Technologies

- Local File Based
- Hesiod
- YP / NIS / NIS+
- NT4 Domains
- LDAP
- Active Directory (NT5 Domains)
- others

Integrating AFS and LDAP

- LDAP directory
  - stores information about users
  - used by systems to lookup IDs
  - used for authorization
- AFS distributed filesystem
  - includes Kerberos authentication service
  - used for authentication and to store files

Linux

- PAM modules for LDAP and AFS exist
- NSS module for LDAP exists
  => easy solution

- successfully used
- proved stable and powerful

Windows

- no modules exist
- extension requires several new elements
- solution: Authentication Framework

- successfully used at André-Gymnasium
- proved stable
- but: other comparable packages emerged

Thank you for your attention!

Questions?