Advanced Unix System Administration

Lecture 22
April 19, 2007

Steven Luo
<sluo+decal@OCF.Berkeley.EDU>

Directory Services

- What do directory services do?
  - Classically, a directory service stores information about users and computers on a network
    - Internal address/telephone/email directories were some of the earliest applications for LDAP
  - In a system administration world, you frequently hear about it in the context of providing name and address lookups
    - Directories are optimized for fast read access via the network – hence the suitability

Directory Services

- Network Information Service (NIS/YP)
  - Another Sun RPC based service
  - Simple request-reply protocol, types of data available limited (passwd, hosts, etc.)
    - A limited generic “map” facility is available
  - Data is stored in flat files, with separate flat files needed for each field which can be looked up
  - No over-the-wire security

Directory Services

- NIS+
  - Looks sort of like NIS, but isn't NIS
  - Supports arbitrary key lookups and (weak) over-the-wire security
  - Also allows arbitrary data to be stored
  - Not known for its reliability and support
- Netware Directory Services, Windows NT domains
  - Similar design and scope as NIS

Directory Services

- Lightweight Directory Access Protocol
  - Originally intended as a lightweight, non-OSI-stack based method of accessing X.500 directories
  - Protocol quickly was implemented standalone
  - Can store any type of data, in any organization
    - The data types and the structure are defined in “schemas”
    - With flexibility comes complexity
  - Lots of implementations

Directory Services

- LDAP con't
  - Lifecycle of an LDAP connection
    - The client “binds” to the server, authenticating and negotiating protocol version
    - Stream of requests issued
      - Various search operations and compare operations – LDAP mandates powerful built-in filters
      - Add, modify, delete entries
      - New operations can be defined via the “extended operation” operation
    - “Unbind” is the connection close
  - The use of TCP imposes some overhead

Directory Services

- LDAP con't
  - LDAP security
    - LDAP itself provides no over-the-wire security; connection security is usually managed via SSL/TLS
    - Secure authentication methods are provided by SASL, if both client and server support it
  - Use for Name Service Switch lookups
    - RFC 2307 (and later drafts) defines a standard schema for storage of this data that fits in with the standard schemas for other uses of LDAP
    - Overhead is considerable – use a caching service!

Directory Services

- Active Directory
  - Embrace-extended version of LDAP and Kerberos
    - Standard (if buggy) LDAP and standard Kerberos – but Microsoft uses a proprietary Kerberos-over-LDAP protocol to provide security
  - Can be used to store standard LDAP schema data, as well as M$-proprietary schema data
  - Interoperability with Unix can be difficult, but is possible