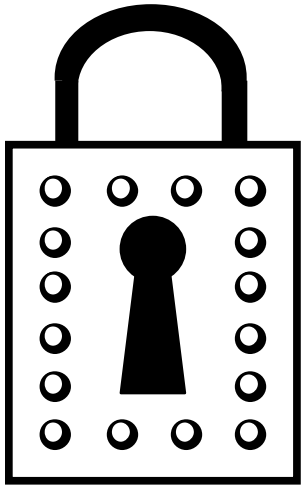
Introduction to LDAP



License

What is LDAP?

- LDAP = Lightweight Directory Access Protocol
  - Let's look at each of those words
- A *directory* is a collection of information you can look up to find a person, organization, …
- You have probably encountered many directories:
  - A "telephone directory" book
  - A "directory enquiries" telephone service
  - A directory of sports clubs, embassies, local businesses, …
- UNIX uses the term *directory* in the same way that Windows uses the term *folder*
  - Enables you to look up a file by its name

What is LDAP? (cont')

- LDAP is *lightweight* in comparison to its predecessor (the X.500 directory service)
  - Implemented on top of TCP/IP rather than with the 7-layer OSI stack
  - Omits many operations that were rarely used in X.500
- LDAP is a *protocol,* that is, a specification for how clients communicate with servers
  - You can implement LDAP clients and servers in many programming languages and on many operating systems
- So, LDAP is a *lightweight protocol* that enables clients to *access directory* services.

Relevance of LDAP to security

- Some knowledge of LDAP is useful when working with secure communications
- An X509 certificate contains a *distinguished name*
  - This term comes from LDAP
- Some organizations use LDAP to centralize:
  - Usernames and passwords
  - Public key certificates
  - User → role mappings (for access control lists)

Typical use of LDAP

- Multi-user systems require access to directory information:
  - Operating system: usernames and passwords, user-specific information (home directory, default shell, …)
  - Mail client: usernames and passwords, email addresses
  - Wiki
  - Bug-tracking application
- It is error-prone to update a user's details if each system has its own directory service
- If each system can act as an LDAP client then:
  - You can centralize directory information → easier administration
  - Applications can use LDAP to:
    - Check login details
    - Perform auto-completion of, say, names or email addresses
    - Retrieve user → role mappings for access control lists

Typical use of LDAP (cont')

- LDAP is of limited benefit if you have just one multi-user system
  - The multi-user system might provide its own built-in directory service that is easier to use
- Benefits of LDAP grow quickly as an organization gets several multi-user systems
  - As already discussed, LDAP offers centralized administration
  - LDAP also offers replication and federation (splitting a directory's contents over several, inter-connected LDAP servers)
- Because of this:
  - People with a standalone computer, for example, home users, are unlikely to use LDAP or even know what it means
  - Administrators in large organizations are more likely to be familiar with it

LDAP schemas

- A schema is meta-information:
  - Often written in the syntax of the thing it describes
- Example:
  - A database schema describes the structure of a database:
  - Names of tables
  - Names and types of columns within each table
- LDAP uses schemas:
  - You can define an LDAP schema for the information you want to store
  - The schema syntax is a bit obscure and outside the scope of this course

LDAP and databases

- LDAP and databases have some characteristics in common:
  - They can perform searches quickly
  - They have extensible schemas
- However, there are some differences:
  - LDAP assumes that reads are much more frequent than updates
    - In contrast, a database assumes that reads and updates occur with similar frequency
  - LDAP does not support transactions
- However, remember that LDAP is an on-the-wire protocol
  - An LDAP server can use any technology it wants to store its data
  - It might use text files
  - It might use a database
    (but it won't expose the database's transaction capability to clients)

Summary

- LDAP = Lightweight Directory Access Protocol
- LDAP is useful when you have *several* multi-user systems
  - Use LDAP to centralize directory information → easier administration
- LDAP is relevant to security because:
  - An X509 certificate contains an LDAP *distinguished name*
  - LDAP can be used to centralize usernames, passwords, public key certificates and user → role mappings