

# LDAP and authentication



Stig Venaas, UNINETT

2001-10-30

# Overview

---

- What is LDAP?
- LDAP authentication
- LDAP based authentication

## What is LDAP?

---

- Lightweight Directory Access Protocol
- Simplified access to X.500 directory
- Today a typical LDAP server has its own database, where most (all) database access is through LDAP
- Anonymous and authenticated access
- Powerful ACLs/ACIs for fine-grained access control (not standardized)

# LDAP authentication

---

- Simple authentication with username/password (should use SSL/TLS)
- LDAPv2 offers simple and Kerberos
- LDAPv3 offers simple and by use of SASL, many other mechanisms including Kerberos
- RFC 2829 Authentication Methods for LDAP

# SASL (RFC 2222)

---

- Simple Authentication and Security Layer
- Framework for authentication with connection-based protocols and optional security layer that offers integrity and/or privacy
- Client sends an authorization identity that may differ from authentication identity. Useful for proxies
- Cyrus SASL library supports anonymous, CRAM-MD5, Kerberos, plain, GSSAPI, DIGEST-MD5 and external mechanisms. With external one can use auth.id. from client certificate used for TLS

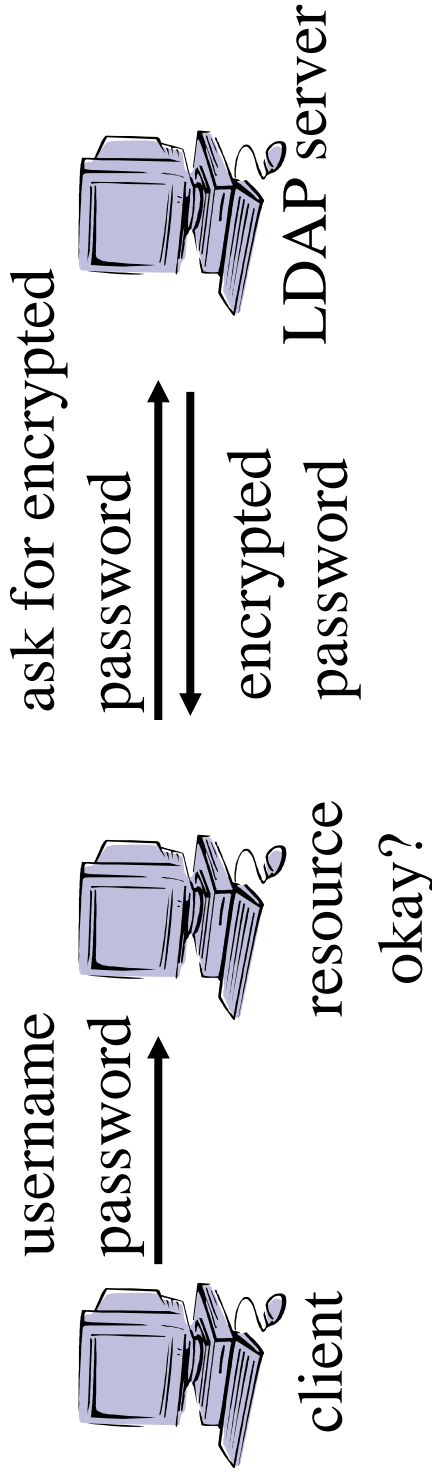
# LDAP based authentication

---

- LDAP is being used as a component in many authentication solutions
- Basically two ways to use LDAP
- LDAP as data store
  - Decision maker uses LDAP to access data necessary for the authentication decision
- LDAP as decision maker
  - Authentication decision is delegated to the LDAP server by relying on authenticated LDAP bind

# LDAP as data store

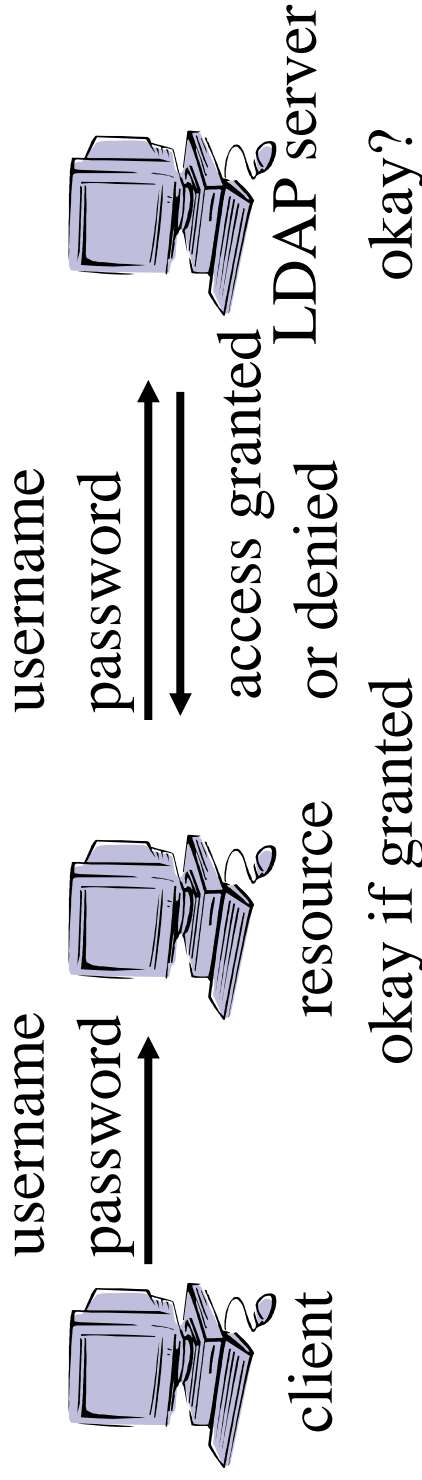
---



- All communications might be through secure channels, maybe SSL
- Resource might also retrieve other information necessary to authenticate and authorize client
- Resource might have to authenticate itself to get access to the necessary data

# LDAP as decision maker

---



- All communications might be through secure channels, maybe SSL
- LDAP server does authentication and authorization based on its own data and rules
- Resource might retrieve information and also do additional authorization

## LDAP as decision maker (2)

---

- Resource acts as a proxy
- Resource might authenticate itself before binding on behalf of user
  - If SSL/TLS is used, resource authentication based on certificate can be done as part of session initiation
- That SASL allows `author.id` different from `authent.id` is useful for proxy solutions, but proxy needs to authenticate user first