www.skills-1st.co.uk

Skills 1st

Best Practices in LDAP Security

Andrew Findlay
Skills 1st Ltd
October 2011

What is "Security"?

- ISO/IEC 27000:2009 Information Security is...
  - Confidentiality
  - Integrity
  - Availability
  - And some other things

Controls

- A means of managing risk
  - Technical
  - Organisational
  - Legal
- Should be appropriately chosen

Accounts

- Must have automated update from an authoritative source
- Should never be deleted
- DNs should never be changed

Authentication

- Never let the password leave the client
  - The network is not to be trusted
  - The server may be compromised
- Use client-side certificates with TLS
  - Zero-knowledge proof
  - Can hold key in secure hardware
- Use TLS + Kerberos

If you *must* use passwords

- Use TLS + SASL SCRAM
  - Avoids exposing password to server
- Use TLS + simple bind
  - This really is the minimum acceptable
- Beware of non-ASCII passwords
  - LDAP treats passwords as binary blobs

Storing Passwords in LDAP

- Don't
- Don't store clear-text password
- AES256 is no better
- Always use a strong hash
  - SHA-1 OK for now
  - SHA-2 family current, SHA-3 coming
- Always use lots of salt

www.skills-1st.co.uk

Skills 1st

Enforcing Password Policies

- Draft-Behera
- Policy often conflicts with human factors
  - Humans are smart: they will win if you fight
  - Don't upset the good guys
- Don't do "n-strikes lockout"
  - Easily triggered by client config errors
  - Attackers are more subtle these days
  - Lockout and replication don't mix
- Password reset is often the weak link

Access Control

- Not standardised
- Even the simple schemes are complex
- Programmer territory
  - Use source-code control
  - Write test suites (and do it *first*)
  - Treat ACL change like software upgrade
- ACLs may not be enough
  - Limits, Structure Rules etc.

DIT Design

- Common DIT structure is bad:
  CN=Smith,OU=Sales+L=Ipswitch,O=Telecom,C=UK
- Cannot hide DN content!
- Most servers cannot even hide entries

Replication

- Good for Read Availability
  - Resilience
  - Performance
  - Lower network round-trip time
- Less good for Write Availability
  - All servers must process all writes
  - Multi-master is a risk to Integrity
- Subset-replica – good for Confidentiality

Network

- Assume the network is compromised
- Firewalls are evil
  - Also necessary
  - Typically paranoid, breaking TCP rules

LDAP over SSL

- Don't do it
  - Never standardised
  - SSL is cryptographically weak
  - ~~Deprecated~~
- Port 636 is no more 'secure' than 389
  - If policy requires encryption then enforce with ACLs or server config
- SSL is still better than nothing :-(
  - Many clients *still* cannot do TLS

www.skills-1st.co.uk

TLS

- Use it – always
- Run your own Certification Authority
- Clients *must* check server certs
- Use client-side certs for high-value accounts (server admin, replicator...)
- Don't trust any data obtained before TLS is established – re-read it

Server Setup

- Harden the OS
- Don't run LDAP server as root
  - CAP_NET_BIND_SERVICE
- Check file permissions
- Check backend DB permissions
- Check open-files limit
- Check add-on security settings (SELinux, AppArmor, etc)

www.skills-1st.co.uk

Skills 1st

Testing

- Build a permanent test suite
  - Access Control
  - Limits
  - Authentication
  - TLS
- Run all tests frequently during development
- Test the production service regularly
- Build a *large* set of dummy data for dev

Constant Service

- Design for 100% availability
- That includes non-stop through software upgrades
- Client machines may need proxies

www.skills-1st.co.uk

Skills 1st

Human Factors

- Legitimate users are a big risk
  - Educate them
  - Don't fight them
- Tight password policy is often bad
- LDAP server can only enforce simple policy – users must do the rest

www.skills-1st.co.uk

Skills 1st

Future Work

- Collect best practices
- Produce a checklist
  - Minimum requirements for all LDAP services
  - List of optional controls for higher security
- Submit checklist to SANS
- I need your help
  - www.ldap-best.org

www.skills-1st.co.uk

Best Practices in LDAP Security

www.ldap-best.org

Andrew Findlay

Skills 1st

LDAP Best Practice