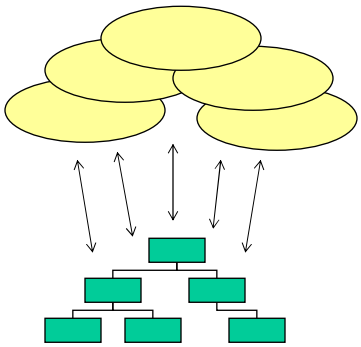
Deploying Corporate LDAP-directory

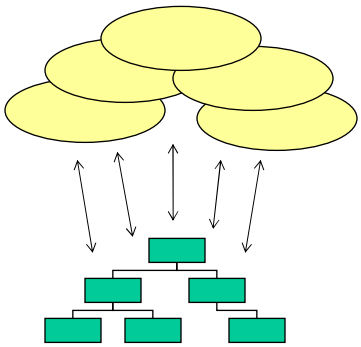


Data Security ´99

12.10.1999
Jari.Pirhonen@atbusiness.com
Project manager, CISSP
AtBusiness Communications
http://www.atbusiness.com/

AtBusiness Communications Oy / Jari Pirhonen © 1999

Deploying Corporate LDAP-directory



Introduction to directories & LDAP
Building corporate LDAP-directory
Directory Guided IT
case: Finland Post

Directory is...

…specialized database tuned for reading and searching. Directory supports wide variety of information and schema is easy to extend. Directory can be distributed in large scale and is usually replicated to ensure availability and performance.

AtBusiness Communications Oy / Jari Pirhonen © 1999

Directories

- Proprietary solutions
  - Windows NT 4.0
- NOS-based (OS specific, standard API)
  - Windows NT 2000 ADS, Novell NDS, Banyan StreetTalk
- Purpose specific
  - DNS
- Application specific
  - Lotus Notes, MS Exchange
- General-purpose, standard based
  - X.500, LDAP
- Meta-directories
  - synchronize different solutions

LDAP

- Lightweight Directory Access **Protocol**
- Developed in University of Michigan
- Commercialized by Netscape
- Simplified **TCP/IP**-based protocol to use X.500
- 90% of X.500 DAP functionality with 10% of resources
- LDAP-only directories available
- LDAPv2 - RFC 1777, 1778
- LDAPv3 - RFC 2551-2256 (proposed standard)
- LDAP-directories are optimized for **searching**
- Not a general-purpose database

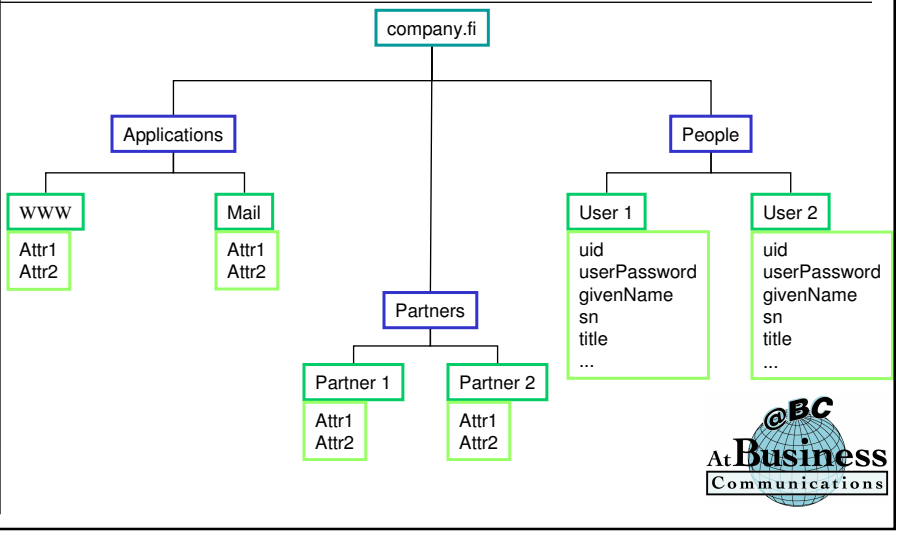
AtBusiness Communications Oy / Jari Pirhonen © 1999

LDAP <> X.500

LDAP	**X.500**
• TCP/IP	• OSI
• protocol	• protocol,replication,security
• simple	• complicated
• lightweight	• heavyweight
• corporate directory	• global directory
• strings only	• several data types

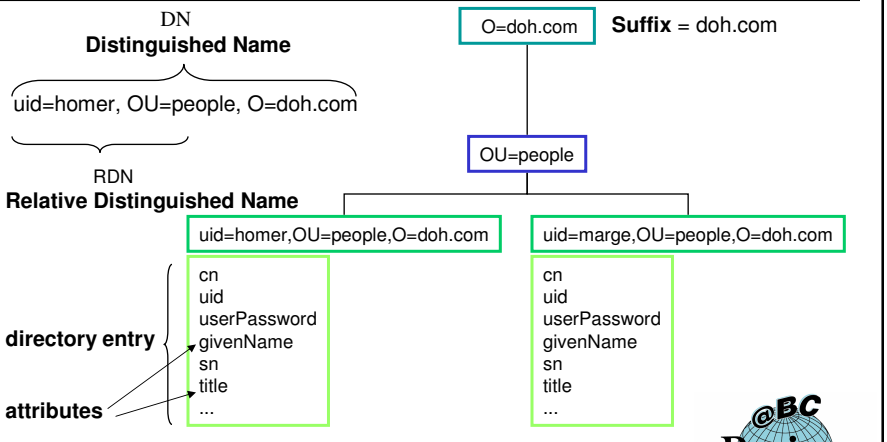
Common
- organization of data
- object classes
- naming standard
- distribution

Directory tree

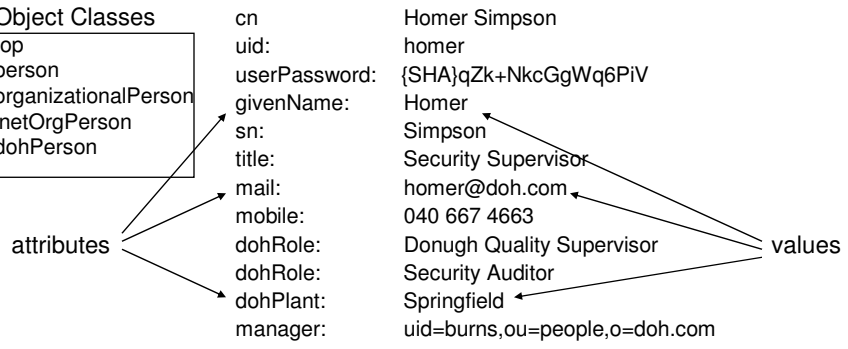


AtBusiness Communications Oy / Jari Pirhonen © 1999

Terminology



Directory entry



Schema = defines object classes & attributes

API

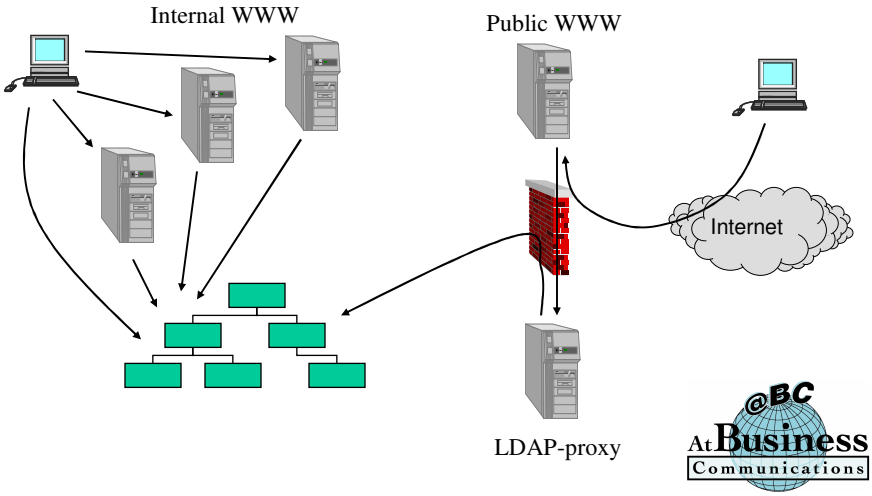
- LDAP API
  - *bind(), unbind(), search(), compare(), modify(), add(), delete(), rename(), result(),...*
  - C, C++, Java, JavaScript, Perl, VB
  - LDAP C-API RFC 1823
- URL
  - *ldap://server/searchbase?attributes?scope?filter*
  - *ldap://ldap.doh.com/ou=people,o=doh.com?sn?sub?uid=homer*
    find surname of person, whose uid is homer
  - *ldap://ldap.doh.com/ou=people,o=doh.com?sn?sub?dohPlant*=Springfield
    find surnames of all users, who are located in Springfied

LDAP-possibilities

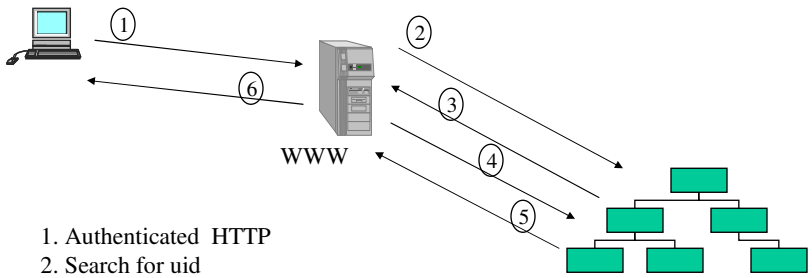
- Centralized user database for authentication
- Authorization information: roles, groups, department,...
- Storage for digital certificates
- Voice over IP
- Hardware configuration, directory enabled networks
- Netscape Communicator administration - roaming access
- Information storage for corporate applications
- PKI
- LDAP-support of COTS-applications
  email, firewalls, VPNs, web-server, authorization servers

AtBusiness Communications Oy / Jari Pirhonen © 1999

Authentication with LDAP



Authentication with LDAP



1. Authenticated HTTP
2. Search for uid
3. Get response (DN)
4. Bind to user's entry using uid & passwd
5. Response OK or failed
6. Page returned or error

AtBusiness Communications Oy / Jari Pirhonen © 1999

Directory <> database

- Directories are tuned for best possible *read*-performance
- Directories are usually easier to extend
- Directories are designed for distribution
- Directories are easier to replicate
- Performance meters are different
  - thousands of *searches* / s <> hundreds of *transactions* / s
- LDAP standard <> SQL "pseudo-standard"
  - real communication standard between client and data source

When NOT to use directory

- You want store large pieces of information
- Attribute-based information model is not suitable
- Information is updated a lot
- Search capability is not important
- You need support for transactions

AtBusiness Communications Oy / Jari Pirhonen © 1999

LDAP-directory products

- Netscape Directory Server
- Innosoft PowerDirectory
- OpenLDAP
- IBM SecureWay Directory
- SUN Directory Services
- MS Windows NT 2000 Active Directory
- Oracle Internet Directory
- Novell Directory Services

LDAP project design phase

- Evaluate directory needs (applications, people)
- Find data sources
- Design directory schema
- Design directory namespace
- Topology
- Replication
- Security

AtBusiness Communications Oy / Jari Pirhonen © 1999

LDAP project deployment phase

- Choose directory software
- Pilot
- Performance testing
- Tuning & handling feedback
- Go to production

LDAP project maintenance phase

- Data maintenance
- Backups
- Schema extensions
- Monitoring
- Directory data and use expansion

AtBusiness Communications Oy / Jari Pirhonen © 1999

FACT

http://www.aberdeen.com/ab%5Fabstracts/1999/08/0899fact.htm

- Aberdeen Group 1999
- Fine-frained Access Control and Trust infrastructure
  - PKI - authentication
  - XML - exchange of the data
  - Directories - data stores
  - LDAP - directory access protocol

“Both XML and PKI will have a huge impact on the Internet, but the real catalyst for change - the technology that will leverage these two technologies to create something larger - is the directory.”

“Building a sound directory-guided IT architecture is not a luxury, but a necessity.”

POSTI

Case Finland Post Ltd

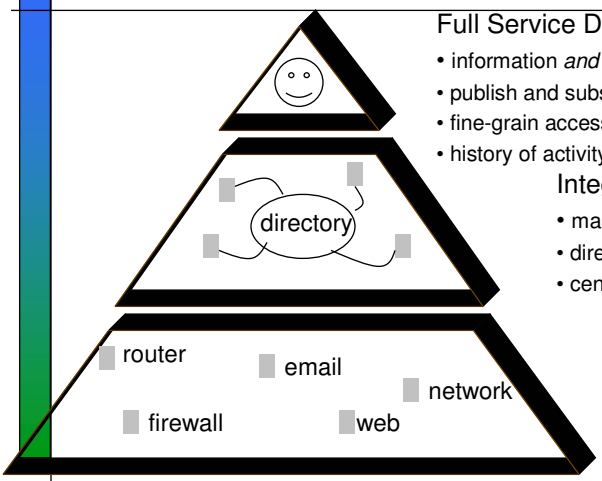
- AtBusiness Communications helped Finland Post to build corporate LDAP-directory
  - project management
  - LDAP-knowledge
  - application development
- First version is in use
- Corporate phonebook application uses directory
- Lots of plans for future

AtBusiness Communications Oy / Jari Pirhonen © 1999

POSTI

Directory Guided IT

http://www.aberdeen.com/ab_company/researchareas/netsvc/directory.htm



Full Service Directory
- information *and* status
- publish and subscribe
- fine-grain access control
- history of activity

Integrated directories
- master-directory (links to data)
- directory synchronization
- centralized LDAP-directory

Tightly coupled directories
- local directories
- data is not shared

Aberdeen Group 1999

POSTI

Environment

- +26.000 employees
- +6000 NT-users in two separate domains
- Unix-servers
- Netscape and Microsoft Web-servers
- Netscape Communicator
- Lots of outsourced services (firewall, Internet/extranet web-servers, Unix-server administration)
- Tuxedo + Oracle

@BC AtBusiness Communications

AtBusiness Communications Oy / Jari Pirhonen © 1999

POSTI

Projects

- Q4 1997: Internet/extranet-apps requirements study
- Q1 1998: Evaluation of user administration methods
- Q2 1998: LDAP evaluation
- Q4 1998: LDAP pilot
- Q1 1999: LDAP deployment phase 1

@BC AtBusiness Communications

POSTI

Where directory can help

- Administration of user information
- Application development
- Information integrity and availability
- Extranet services
- Customer services

AtBusiness Communications Oy / Jari Pirhonen © 1999

POSTI

Goals

- Centralized authentication and authorization
- One user db & one password per user
- User db for Extranet applications
- Strong authentication & digital certificates
- Evolution towards Single Sign-On
- Good performance & scalability
- Security platform for web-applications
- Standards-based solution

POSTI

Background

- Tuxedo-applications had their own db for user authentication and authorization
- Many passwords per user
- Intranet web-servers used NT filesystem ACL
- Lots of Internet/extranet plans & projects
- No common authorization method

AtBusiness Communications Oy / Jari Pirhonen © 1999

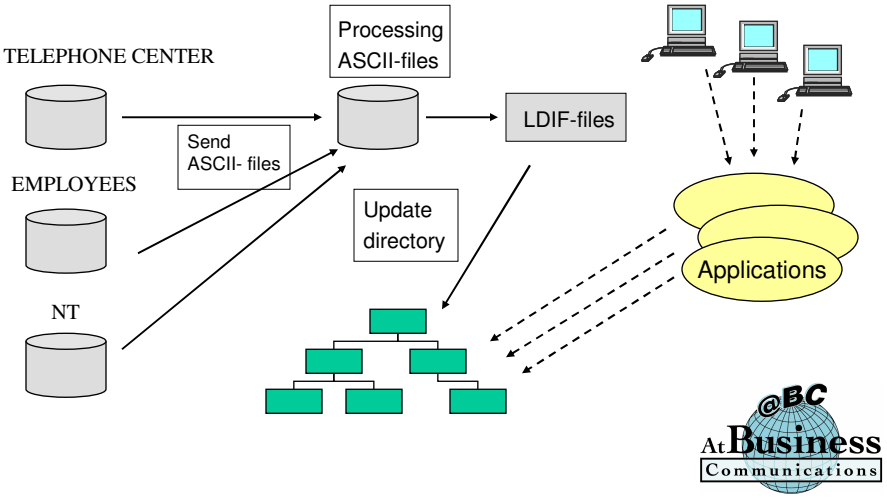
POSTI

Deployment

- LDAP-hierarchy and required attributes were planned in evaluation and pilot phase
- Choosing LDAP-product, platform and location
- Internal web-based phone-app will use LDAP
- Programming LDAP-update tools (Perl)
- Installing and configuring LDAP-directory
- Setting up update process
- Administration

POSTI

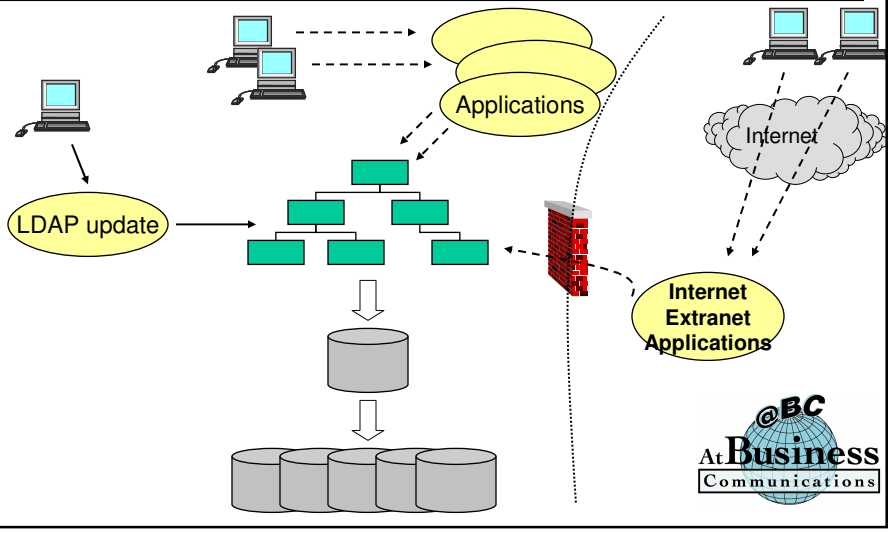
Current architecture



AtBusiness Communications Oy / Jari Pirhonen © 1999

POSTI

Some day?



POSTI

Challenges/surprises

- New requirements during deployment
  => extending the planning phase
- No unique key to identify user in different dbs (employeenumber, name, uid)
  => employeenumber added in every db
- Update-process was more complicated than excpected
  => more time spent in Perl-programming
- Outsourced server admin & services
  => lots of time spent in “waiting-mode”

@BC AtBusiness Communications

AtBusiness Communications Oy / Jari Pirhonen © 1999

POSTI

Challenges/surprises

- Product prices, different licensing methods
  => negotiations take time
- Many different interest groups
  => communicate, evangelize
- Administration: data sources, Perl scripts, LDAP-directory
  => communicate, find right persons
- LDAP-based phone-app gave tight schedule
  => phone-app related problems solved first

@BC AtBusiness Communications

POSTI

Lessons learned

- Don't underestimate the time required for handling data sources and populating LDAP
- Communications and co-operation with service providers requires lots of time
- Developers were very interested in LDAP
- Not too much LDAP-knowledge available
- Spread the word. LDAP is not a threat, but it's not the Silver Bullet either.

AtBusiness Communications Oy / Jari Pirhonen © 1999

POSTI

Next phase

- Directory usage policy & guide
  => directory available for applications
- Add more information in the directory
- Add more data sources
- NT to LDAP passwd sync
- SSO for web-apps
- Phonebook => employee directory
- Ensure availability