A Customer's Perspective on Directories

Skip Slone
Principal Architect
Lockheed Martin

October 16, 2002
Cannes, France

THE Open GROUP

In This Presentation

- Some Heretical Assertions
- Business Drivers
- A Look at Accounts
- What About Protocols?
- A Focus on LDAP
- Sample Scenario
- Some Challenges for the Industry

Some Heretical Assertions

- There is no business justification for directories
- Businesses don’t care about directory protocols
- LDAP is a failure

Business Drivers

- Although there is no business justification for directories, there are business drivers that lead to directories as a technical solution:
  - We need to manage access to systems
  - We need to prevent unauthorized access to systems
  - We need to be able to find computing resources
  - We need to facilitate information sharing among individuals
  - We need to be able to find information about our trading partners and to make information about ourselves available to trading partners

A Look at Accounts

- An account is a representation of a relationship (e.g., system/authorized user, employer/employee, business/customer)
- An account must specify both parties in the relationship (if not specified explicitly, it is clear from context)
- For the purposes of system efficiency, an account is often reduced to a bit string, for example:
  - SID pair in Windows
  - UID/GID in UNIX
- Account information is ideally suited to directories
- Accounts are the primary driver behind directories

What About Protocols?

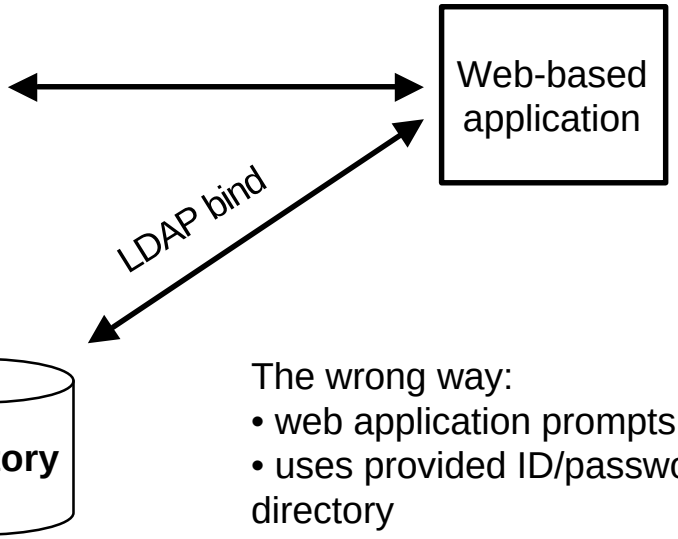
- Businesses don't care about directory protocols; however, businesses do care:
  - That the system works
  - That the system works efficiently
  - That the technology does not get in the way of doing business
- LDAP was not designed for account access; other protocols have been around longer and are perhaps better suited to the task:
  - NTLM
  - NIS
  - Kerberos
- Sometimes a protocol is not the answer, e.g., GSS-API may be much better suited to certain tasks

A Focus on LDAP

- A directory should support more than just LDAP:
  - LDAP provides *a* view of directory information – not necessarily *the* view
- LDAP's greatest strength is that it inherited X.500's distributed naming concept
  - An LDAP distinguished name should be as easy and efficient to resolve as a DNS domain name – put a name in and get an answer back
- LDAP's greatest weakness is that it has failed to deliver distributed naming
  - No one has delivered a top level name registration authority / service (comparable to "." in DNS)
  - LDAP servers typically view themselves as the center of the universe – not as part of a bigger picture

Example Scenario

User – logs into home system



The wrong way:

- web application prompts user for ID and password
- uses provided ID/password to perform LDAP bind to directory

Example Scenario

User – logs into home system

A better way:

- web application uses GSS-API to obtain user credential without prompting user to log in again
- the user's operating system and the web app's operating system communicate transparently to make this happen

Some Challenges to the Industry

- Make operating systems talk to one another
  - GSS-API is of limited value if they don't
- Deliver directory products that truly interoperate
  - LDAP certification can help achieve this goal
- Deliver a distributed naming solution that works
  - LDAP referrals provide a place to start
- Provide a globally unambiguous representation of the parties to an account:
  - Issuer UUID / Subject UUID pair makes sense