

Privacy enhanced directory services

TERENA EuroCAMP
Turin, March 2rd 2005

Victoriano Giralt
Systems Manager
University of Málaga

Directory uses in academic institutions

- General public
 - Finding a public service
- Between organizations
 - Researchers can find each other
 - Find possible partners for projects
- Inside the organization
 - Authentication
 - Authorization
 - Mail routing
 - Sky is the limit

Why a privacy enhanced directory

The problem

(if there isn't one there is no need for a solution)

Directories provide information that some people consider private.

Directory privacy problems

- spam
- confrontation of interests
privacy vs the need to be found
- The Law
Directories that can be searched via Internet may be considered international transfer of personal data

First approach to solve the problem

- The lawyers propose to ditch the directory
- The users offer no solutions
 - They like to find others' data
 - Some of them don't want to be found
- The technicians propose to ditch the lawyers.

A second approach

- Put control on the hands of the users
- Keep policy controls on the hands of the organization
- The technicians abide to the Law
- The lawyers seem happy
- Looks like we have *The Solution*

Why a privacy enhanced directory

Because our mission is to provide
useful services for our users

Implementing the solution

There are two parts to the solution

- Giving control to the user in an easy way
- Making the solution work via all its interfaces

The easy part: end user control

- A nice web interface for the user to decide the data about herself that is to be publically accesible
- A directory attribute to hold such preferences

irisUserPrivateAttribute

Hard part: implementing the policy

- The policy must be enforced whatever the interface to the directory
- Application level control is discarded
- OpenLDAP ACLs come to the rescue
- Policy can be enforced at server level

Best of all

despite how simple it seems

It works!

and I'll show you how

ACL technicalities

- I may show you these later
- I may make you suffer with some terminal output.