Privacy enabled directory services

Jose A. Accino[1] Victoriano Giralt[1] Javier Masa[2]

[1]Central Computing Facility
University of Malaga

[2]RedIRIS

TERENA Networking Conference, 2005

Outline

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to. . .

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to...

- Offer information about themselves

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to...

- Offer information about themselves
- Offer information about their members

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to...

- Offer information about themselves
- Offer information about their members
- Collaborate amongst them

Users' needs

Users want

Users' needs

Users want

- To find others for communicating

Users' needs

Users want

- To find others for communicating
- To be found by possible partners for projects

Users' needs

Users want

- To find others for communicating
- To be found by possible partners for projects

but they do not want

Users' needs

Users want

- To find others for communicating
- To be found by possible partners for projects

but they do not want

- their data exposed

Legal matters
in the problem

- People's right to privacy

Legal matters
in the problem

- People's right to privacy
  Persons have the right to conceal their data

Legal matters
in the problem

- People's right to privacy
  Persons have the right to conceal their data
- Internet searchable directories may be international transfers of personal data

Technical requirements
that are part of the problem

- The directory may be accessed directly

Technical requirements
that are part of the problem

- The directory may be accessed directly
- Enforce the policy regardless the access method

Technical requirements
that are part of the problem

- The directory may be accessed directly
- Enforce the policy regardless the access method
- Different treatment for

Technical requirements
that are part of the problem

- The directory may be accessed directly
- Enforce the policy regardless the access method
- Different treatment for
  - Inside searches

Technical requirements
that are part of the problem

- The directory may be accessed directly
- Enforce the policy regardless the access method
- Different treatment for
  - Inside searches
  - Outside searches

Technical requirements
that are part of the problem

- The directory may be accessed directly
- Enforce the policy regardless the access method
- Different treatment for
  - Inside searches
  - Outside searches
- Reduce the administrative burden

Different approaches
for solving the problem

- Lawyers approach

Different approaches
for solving the problem

- Lawyers approach

Ditch the directory

Different approaches
for solving the problem

- Lawyers approach

Ditch the directory

- Users approach

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None, they just want *it* to work

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None, they just want *it* to work

- Technicians approach

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None, they just want *it* to work

- Technicians approach

  Ditch the lawyers

Points to find a solution

- Put control on the hands of the user

Points to find a solution

- Put control on the hands of the user
- Policy is defined by the organization

Points to find a solution

- Put control on the hands of the user
- Policy is defined by the organization
- Abide by the law

Two sides of a coin
user side / server side

- User side

Two sides of a coin
user side / server side

- User side
  The user must have control of her data

Two sides of a coin
user side / server side

- User side
  The user must have control of her data
- Server side

Two sides of a coin
user side / server side

- User side
  The user must have control of her data
- Server side
  The solution must work whichever the interface.

The user decides about his data

- Interface for setting user preferences

The user decides about his data

- Interface for setting user preferences
  We know what to do

The user decides about his data

- Interface for setting user preferences
  We know what to do create a nice web form

The user decides about his data

- Interface for setting user preferences
  We know what to do create a nice web form
- Directory attribute for holding the preferences

The user decides about his data

- Interface for setting user preferences
  We know what to do create a nice web form
- Directory attribute for holding the preferences

irisUserPrivateAttribute

The institution sets the policy

- Policy enforcement whatever the interface

The institution sets the policy

- Policy enforcement whatever the interface
  Application level control is discarded

The institution sets the policy

- Policy enforcement whatever the interface
  Application level control is discarded
- Policy enforcement at server level

The institution sets the policy

- Policy enforcement whatever the interface
  Application level control is discarded
- Policy enforcement at server level
  using OpenLDAP ACLs

Summary

- The user has control of personal data

Summary

- The user has control of personal data
- The policy is enforced at the server

Summary

- The user has control of personal data
- The policy is enforced at the server
- Lawyers seem happy

Summary

- The user has control of personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple

Summary

- The user has control of personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

Summary

- The user has control of personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

Summary

- The user has control of personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

WORKS

Summary

- The user has control of personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

WORKS

do you want me to show you how?

irisUserPrivateAttribute may have a value of *all* or may be empty, denying or allowing access to ALL optional attributes, defined in *attrs*. Actually, our present policy for student personal data, denies access to the whole entry.

Deny access to all attributes

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(&(eduPersonAffiliation=student)
                  (irisUserPrivateAttribute=all))"
        attrs=entry
        by * none
```

If a student clears her irisUserPrivateAttribute, then the system allow access to the entry and, then, to the policy permitted attributes, so they may be shown.

Allow access to permited attributes

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(eduPersonAffiliation=student)"
        attrs=entry,displayName,mail,telephoneNumber
        by * read
```

The organization may decide that an entry should not appear in searches. Then irisUserPrivateAttribute receives the value *entry*.

Blocking all access

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=entry)"
        by * none
```

The user may decide which attributes should be hidden to anonymous searches, from a set defined by the organization's policy. irisUserPrivateAttribute holds the names of such attributes. In case the search is done by a bound user, the attribute is shown.

Blocking access to the phone number

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=telephoneNumber)"
        attrs=telephoneNumber
        by users read
        by * none
```

The user may decide to hide all attributes in the set defined by the organization's policy. In such case, irisUserPrivateAttribute holds a value of *all*. If the search is done by a bound user, the attributes are shown.

Blocking access to all attributes

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=all)"
        attrs=mail,telephoneNumber,facsimileTelephoneNumber
        by users read
        by * none
```