Application access to directories

opening Pandora's box

Victoriano Giralt

Central ICT Services
University of Málaga

Cork
May 18th, 2009

Uses of the directory

what is this good for

Uses of the directory
what is this good for

Most common uses of enterprise directories

Uses of the directory
what is this good for

Most common uses of enterprise directories

1. White pages

Uses of the directory
what is this good for

Most common uses of enterprise directories

1. White pages
2. Credential repository for AuthN

Uses of the directory
what is this good for

Most common uses of enterprise directories

1. White pages
2. Credential repository for AuthN
3. Object classification for AuthR

Uses of the directory
what is this good for

Most common uses of enterprise directories

1. White pages
2. Credential repository for AuthN
3. Object classification for AuthR
4. Object information repository

AuthN

can the user prove his identity?

AuthN

can the user prove his identity?

There are three main ways for checking credentials

AuthN
can the user prove his identity?

There are three main ways for checking credentials

- Binding as the object with the credentials

AuthN
can the user prove his identity?

There are three main ways for checking credentials

- Binding as the object with the credentials
- Retrieving the object and comparing the values

AuthN
can the user prove his identity?

There are three main ways for checking credentials

- Binding as the object with the credentials
- Retrieving the object and comparing the values
- Searching for an object with the proper values

AuthR

is the user allowed to use the application?

AuthR
is the user allowed to use the application?

The object must either

AuthR
is the user allowed to use the application?

The object must either

- possess a certain attribute with a given value
- belong to a certain category of objects

AuthR
is the user allowed to use the application?

The object must either

- possess a certain attribute with a given value
- belong to a certain category of objects

This can be verified either by

AuthR
is the user allowed to use the application?

The object must either

- possess a certain attribute with a given value
- belong to a certain category of objects

This can be verified either by

- retrieving the object and checking the attribute for the value
- searching for an object that has the appropriate values

Attribute source

what does the app need to know about the user?

Attribute source

what does the app need to know about the user?

The directory can store lots of information

Attribute source

what does the app need to know about the user?

The directory can store lots of information

- Unstructured

Attribute source

what does the app need to know about the user?

The directory can store lots of information

- Unstructured
- but syntactically and semantically sound

Attribute source

what does the app need to know about the user?

The directory can store lots of information

- Unstructured
- but syntactically and semantically sound
- bundled together on the object

Attribute source

what does the app need to know about the user?

The directory can store lots of information

- Unstructured
- but syntactically and semantically sound
- bundled together on the object

and all of it can be provided to the applications

Least privilege principle
or the parable of the significant other

Least privilege principle
or the parable of the significant other

Main characters

Least privilege principle
or the parable of the significant other

Main characters

The user

Least privilege principle
or the parable of the significant other

Main characters

The directory

Least privilege principle
or the parable of the significant other

Main characters

The application

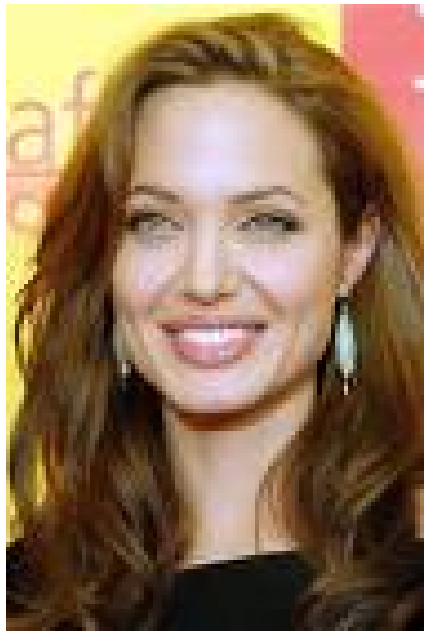
Least privilege principle
or the parable of the significant other

Least privilege principle
or the parable of the significant other

The plot

Least privilege principle
or the parable of the significant other

The plot



Least privilege principle
or the parable of the significant other

The plot

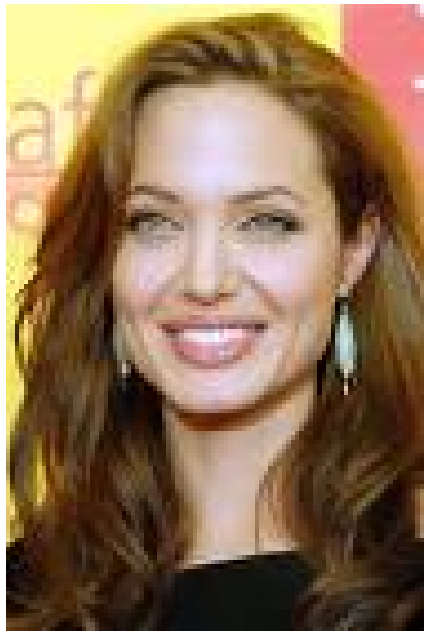
$\Rightarrow$

The user gives his credentials to the application

Least privilege principle
or the parable of the significant other

The plot





The application gives the user's credentials to the directory

Least privilege principle
or the parable of the significant other

The plot

$\Rightarrow$

$\Rightarrow$
$\Leftarrow$

The application gets user's access to the directory

Least privilege principle
or the parable of the significant other

The plot

$\Rightarrow$
$\Leftarrow$

$\Rightarrow$
$\Leftarrow$

The user gets access to the application

Least privilege principle
or the parable of the significant other

The plot

$\Rightarrow$
$\Leftarrow$

$\Rightarrow$
$\Leftarrow$

Everyone is happy

Least privilege principle
or the parable of the significant other

The plot

$\Rightarrow$
$\Leftarrow$

$\Rightarrow$
$\Leftarrow$

Everyone is happy, right?

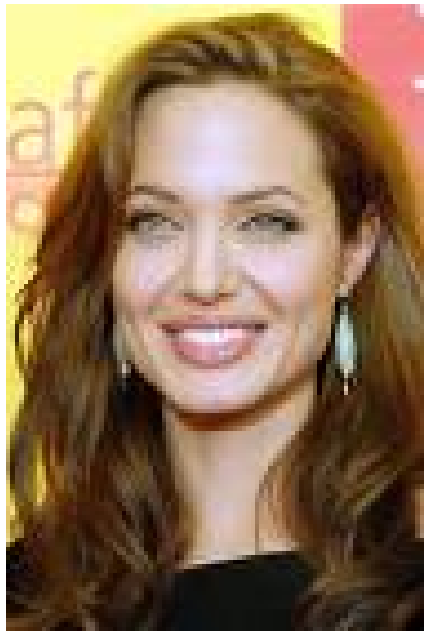
Least privilege principle
or the parable of the significant other

Least privilege principle
or the parable of the significant other

A better plot

Least privilege principle
or the parable of the significant other

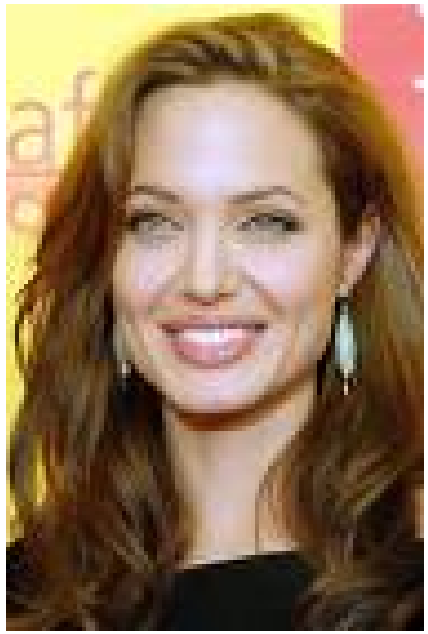
A better plot



Least privilege principle
or the parable of the significant other

A better plot

$\Rightarrow$

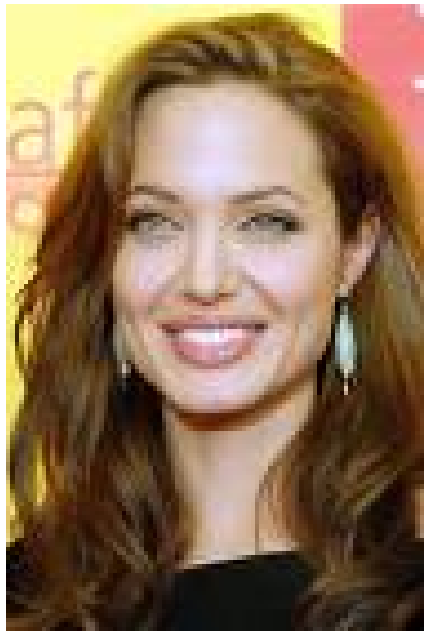


The user gives his credentials to the application

Least privilege principle
or the parable of the significant other

A better plot



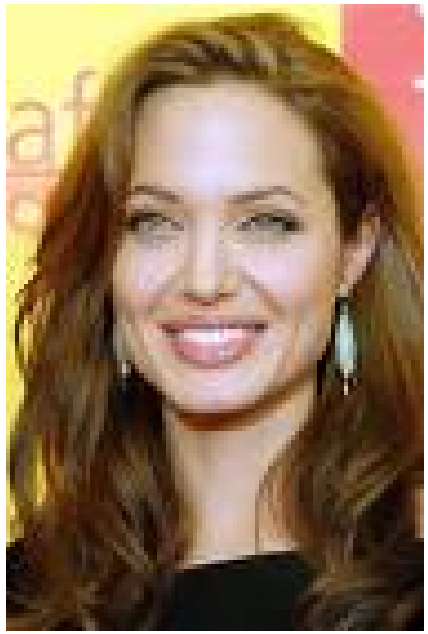


The application gives its credentials to the directory

Least privilege principle
or the parable of the significant other

A better plot

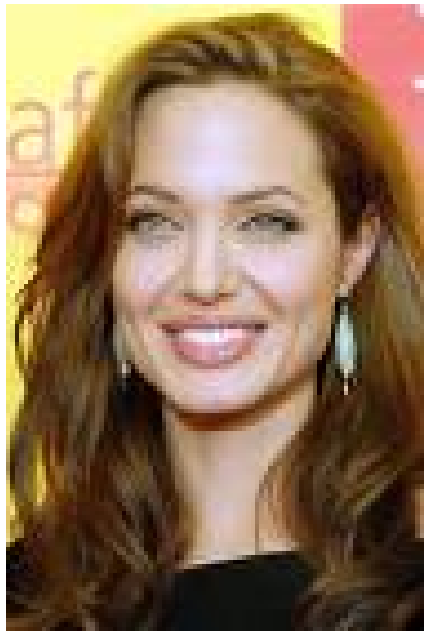




The application gets application's access to the directory

Least privilege principle
or the parable of the significant other

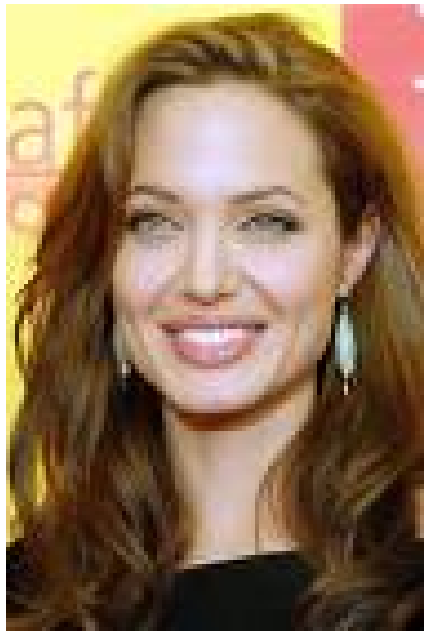
A better plot



The application checks user's credentials with the directory

Least privilege principle
or the parable of the significant other

A better plot



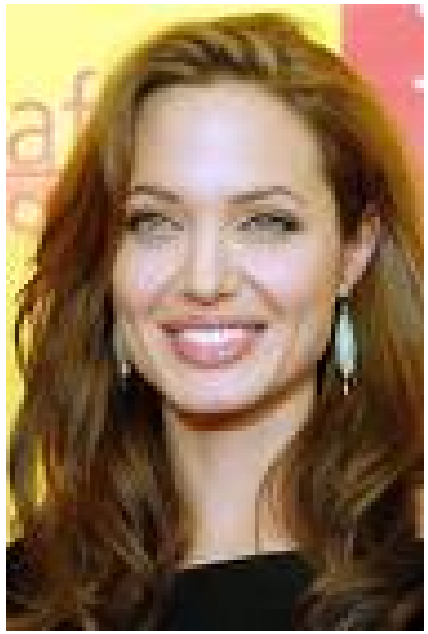
The user gets access to the application

Least privilege principle
or the parable of the significant other

A better plot

$\Rightarrow$
$\Leftarrow$

$\Rightarrow$
$\Leftarrow$
$\Rightarrow$
$\Leftarrow$



Everyone is happy

Least privilege principle
or the parable of the significant other

A better plot

$\Rightarrow$
$\Leftarrow$

$\Rightarrow$
$\Leftarrow$
$\Rightarrow$
$\Leftarrow$

Everyone is happy, or not

Filtering values

who can see what

Filtering values
who can see what

Every attribute and value is not for everyone to see

Filtering values
who can see what

Every attribute and value is not for everyone to see

- User's privacy

Filtering values
who can see what

Every attribute and value is not for everyone to see

- User's privacy
- Application data is not for user consumption

Filtering values
who can see what

Every attribute and value is not for everyone to see

- User's privacy
- Application data is not for user consumption
- Applications should not see data for other applications

Filtering values
who can see what

Every attribute and value is not for everyone to see

- User's privacy
- Application data is not for user consumption
- Applications should not see data for other applications
- Different consumers for different values of an attribute

Controlling access to attributes

applying the least privilege principle

Controlling access to attributes
applying the least privilege principle

This has to be approached from two sides

Controlling access to attributes
applying the least privilege principle

This has to be approached from two sides

The application side An object for each application to bind to the directory

Controlling access to attributes
applying the least privilege principle

This has to be approached from two sides

The application side An object for each application to bind to the directory

The server side ACIs for controlling access to objects, their attributes and their values

Controlling access to attributes
applying the least privilege principle

This has to be approached from two sides

The application side An object for each application to bind to the directory

The server side ACIs for controlling access to objects, their attributes and their values

but...

Controlling access to attributes
applying the least privilege principle

This has to be approached from two sides

The application side An object for each application to bind to the directory

The server side ACIs for controlling access to objects, their attributes and their values

but...

Can we trust our applications?

Controlling access to attributes
applying the least privilege principle

This has to be approached from two sides

The application side An object for each application to bind to the directory

The server side ACIs for controlling access to objects, their attributes and their values

but...

Can we trust our applications? All of them?

The problem is not solved

it has just been mitigated

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

- Applications should not have access to users credentials

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

- Applications should not have access to users credentials
- Applications should not have access to information pertaining to other applications

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

- Applications should not have access to users credentials
- Applications should not have access to information pertaining to other applications
- Applications are not guaranteed to behave as expected

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

- Applications should not have access to users credentials
- Applications should not have access to information pertaining to other applications
- Applications are not guaranteed to behave as expected

in all

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

- Applications should not have access to users credentials
- Applications should not have access to information pertaining to other applications
- Applications are not guaranteed to behave as expected

in all

- Applications should not be trusted

The problem is not solved
it has just been mitigated

It is clear that policies can be enforced at the server, but

- Applications should not have access to users credentials
- Applications should not have access to information pertaining to other applications
- Applications are not guaranteed to behave as expected

in all

- Applications should not be trusted

and, remember, ACIs are a nightmare to manage,
we want few of them

Solution
Single Sign On and IAM technologies

Solution
Single Sign On and IAM technologies

Applications can be forced into behaving

Solution
Single Sign On and IAM technologies

Applications can be forced into behaving

- Blocking access to user credentials

Solution
Single Sign On and IAM technologies

Applications can be forced into behaving

- Blocking access to user credentials $\Rightarrow$ SSO

Solution
Single Sign On and IAM technologies

Applications can be forced into behaving

- Blocking access to user credentials $\Rightarrow$ SSO
- Giving them just the information they need

Solution
Single Sign On and IAM technologies

Applications can be forced into behaving

- Blocking access to user credentials $\Rightarrow$ SSO
- Giving them just the information they need $\Rightarrow$ IAM

Solution
Single Sign On and IAM technologies

Applications can be forced into behaving

- Blocking access to user credentials $\Rightarrow$ SSO
- Giving them just the information they need $\Rightarrow$ IAM

but that is what the rest of this EuroCAMP is about

The End
time for some discussion

Questions?

The End

time for some discussion

Questions?

you might even get answers