Tequila

Overview

Claude Lecommandeur

EPFL - KIS

claude.lecommandeur@epfl.ch

Table of Contents

Overview

Tequila is a Web authentication and authorization system. It provides all the nuts and bolts to setup a federated, cross organizations system. It is user friendly, simple and powerful. The main points to consider are :

- Accessible from any Web application that require users authentication.
- Very careful about personal data protection. Users can override server policy for attribute release via a powerful tool *tape).
- Only the Tequila server can authenticate and has access to users information and it is very careful with these data.
- Several Tequila servers can establish a mutual trust. In this case users from one organization can access services from another.
- The Tequila server is independent of the local authentication system and local identity management databases, it provides a software connector system that can connect to any specific external software. The default distribution offers connectors to LDAP directories both for authentication and user attributes.
- It is very versatile, you can set it up to be very permissive and easy to use, or very strict, requiring cross authentication and strong encryption.
- Single sign support : users authenticate only once for all Tequila aware applications.
- Portal support : portals have very special needs, they should be a to impersonate users.
- Can protect static pages easily, but also offers a strong API to achieve complex tasks for applications.
- Interface to Shibboleth authentication system. Tequila can insert itself seamlessly in a Shibboleth federation.
- The mutual system is much more versatile than just federation. Each couple of Tequila servers decides which kind of trust they will use.

Prerequisites

Installing Tequila supposes you already have a users base, a way to authenticate them, either via username/password or with a PKI infrastructure, and a repository for users attributes. Users attributes can be anything with a name, and can be expressed in some way with a string, for example photos are well supported.

To access the authentication and users attributes systems, Tequila uses a generic interface that can be plugged in virtually any external information system. LDAP connectors are in the standard distribution, if you are using LDAP for local authentication users data distribution, it will be very easy to install Tequila.

From the secured application side

There is 2 cases : protecting static pages and protecting applications. We’ll first examine the static pages protection. There is an Apache module (actually 2, one in Perl and one in C) that you can use. After installing one of these modules, it is just a question of Apache configuration, either in .htaccess, or in the server wide Apache configuration files.

A short example with the C module :

```
<Location /restricted>
    TequilaAllowIf  firstname=claude
    TequilaService  A simple test
</Location>
```

Simple, isn’t it ? This means that you want to protect with Tequila the location /restricted (and everything inside), that access will be allowed only to people whose first name is Claude. (I know, I should have chosen a better example, but you can replace with your first name).

With the Perl module, this is almost the same :

```
<Location /perlteqmod/>
  PerlAccessHandler Apache::AuthTequila
  PerlSetVar TequilaAllowIf  firstname=solene
  PerlSetVar TequilaService  A simple test
</Location>
```

You can also protect CGI with method :

```
<Location /cgi-bin/perlteqenv>
  PerlAccessHandler          Apache::AuthTequila
  PerlSetVar TequilaAllowIf  group=myfriends
  PerlSetVar TequilaRequest  "name firstname unit"
  PerlSetVar TequilaService  "Another test"
  Options +ExecCGI
</Location>
```

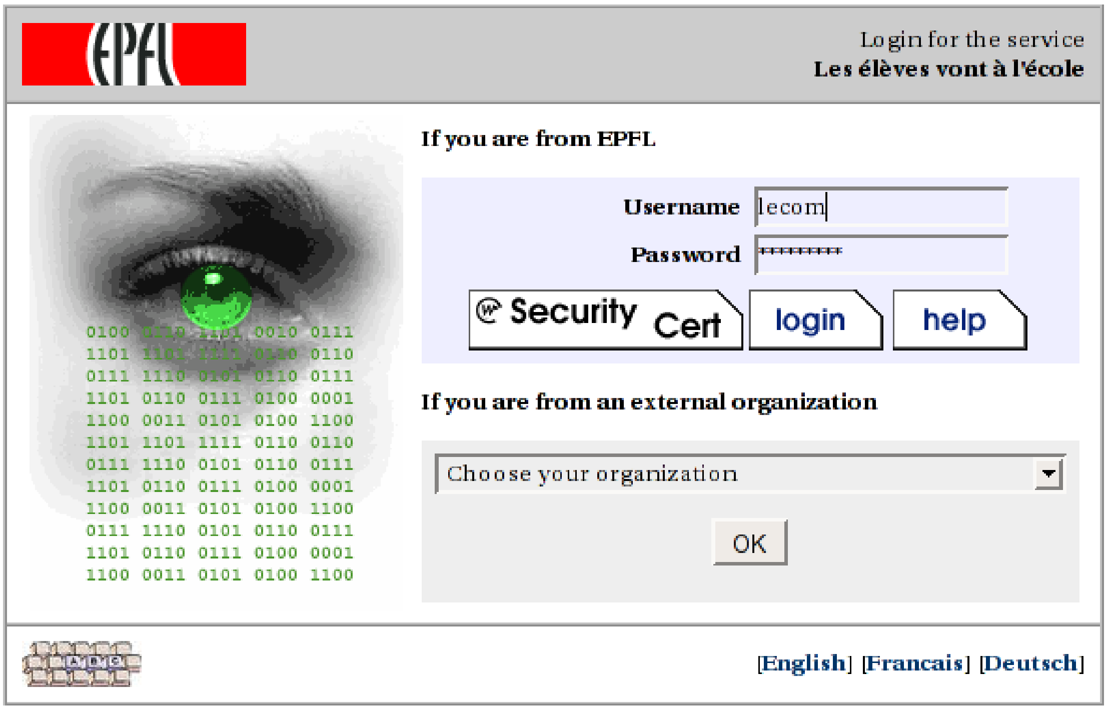
You get exactly the same effect, but there is a bonus, a set of environment will be defined in your script, in this case : REMOTE_USER, HTTP_TEQUILA_USER, HTTP_TEQUILA_NAME HTTP_TEQUILA_FIRSTNAME and HTTP_TEQUILA_ORG (plus a few others more technical).

Tequila won’t let the user step in if she doesn’t fit the AllowIf condition. In the example above, you don’t even know who is in the group myfriends (I suppose you know), the Tequila server will do the job for you.

Now the script interface, if you want do access more advanced feature of Tequila, you can use one of the modules provided in the distribution. There is modules for Java, Perl, PHP and ASP. I won’t explain here how it works, you should refer to the corresponding documentation.

From the user side

When accessing a protected area, the incoming user will be redirected to the Tequila server and will see something like this :



Login for the service
Les élèves vont à l'école

If you are from EPFL

Username lecom

Password *********

If you are from an external organization

Choose your organization

One can argue on the graphical design but this should be pretty easy to understand and use. The user can log in either with her username/password or with an SSL certificate. She can choose a different organization.

Personal data protection

As we have seen, the Tequila server can check the value and deliver personal user attributes values to applications that use it.

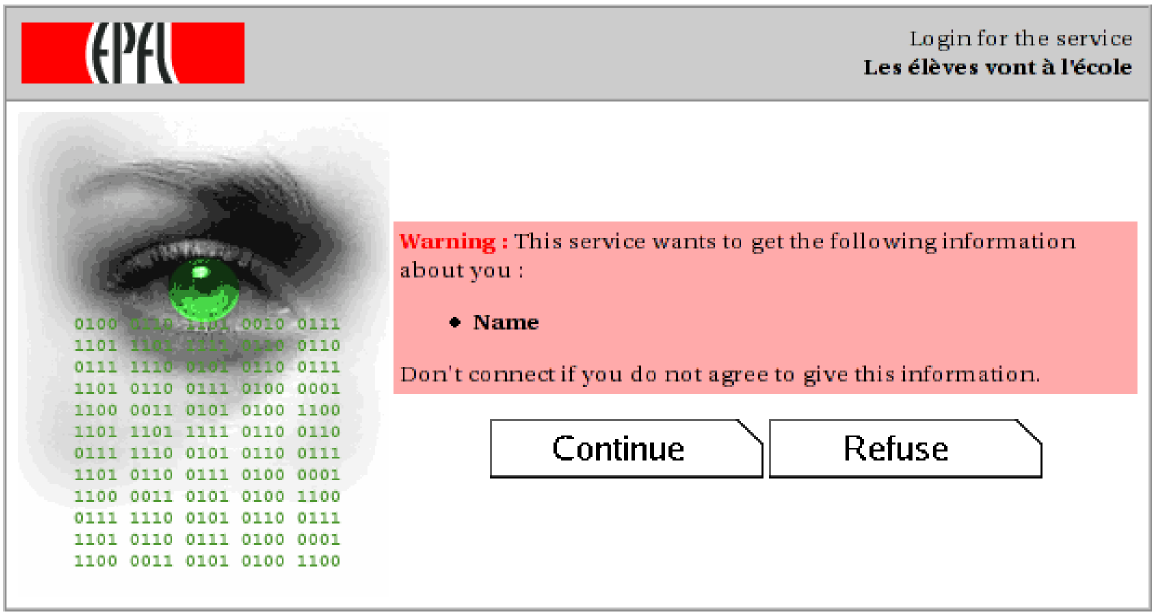
But it is possible that there is very private information served by Tequila (salary, photo), in this case the end user should be able to control herself who is able to access these data and in which condition. This is possible. All attributes have a delivery policies. A server wide policy that the server manager sets up, and a user defined policy that can be fully controlled by the user. The **tape** tool is used for this purpose.

If you log into **tape**, you can ask information about what the server knows about yourself, what is the default server policy used to control the delivery of this information, what are the other Tequila servers trusted by your server, and you can see and change the delivery policy for each and every attribute value about yourself.

There are 2 kinds of client applications, 'resources', and 'anonymous' applications. A resource is a trusted application, known to the organization Tequila manager, during a transaction, it is fully authenticated by the server. Anonymous applications are more volatile, they are any application that uses the services of this particular Tequila server. Note that the server can be configured to allows anonymous applications to be only on certain subnets, or even completely disable them.

The end user can use these specifications to make her decision on her attribute policy.

There is 3 possible values for an attribute policy : 'Yes', 'No' and 'Ask'. If set to 'Yes' the value will be delivered to the corresponding application without warning. If set to 'No', it won't be delivered, and it set to 'Ask' the user will be asked when the application tries to fetch the value. She will see something like this :



Login for the service
Les élèves vont à l'école

Warning : This service wants to get the following information about you :

- **Name**

Don't connect if you do not agree to give this information.

Goodies

- A plugin system than can be use to extend the features of the Tequila server.
- Portal support. Portal cam impersonate users, ask Tequila to check digests. To be used with care.
- A distributed session manager, to be used when your Tequila server runs on redundant servers.
- Seamless integration in a Shibboleth federation.
- A software keyboard to defeat key loggers.
- Multiple identities for usernames. If a user works in several places in the same organization, she can choose on which place she is logging on.
- Support for applications local users. If an application uses the Tequila services but has it's own set of local users, it can ask Tequila to let unknown users logs in and do the password check itself.
-