

VOUS AIMEZ (LE) GASPAR, VOUS ALLEZ AIMER (LA) TEQUILA

CLAUDE.LECOMMANDEUR@epfl.ch, SIC



Uous connaissez tous **Gaspar**, le merveilleux outil d'authentification et de contrôle d'accès pour les applications Web sécurisées de l'EPFL. **Tequila** est une approche complémentaire de Gaspar, portable, multi-institutions et plus riche en outils côté client.

Tequila offre la possibilité de mettre en place un ensemble de serveurs qui collaborent pour offrir une solution d'authentification globale à un ensemble d'institutions qui gèrent elles-mêmes leurs bases d'utilisateurs sans qu'il y ait besoin de regrouper ces utilisateurs (et les attributs qui vont avec) dans une base de données centrale. En ce sens Tequila est un outil d'authentification et de contrôle d'accès fédéré.

Tequila a été proposé lors de l'appel d'offre de SWITCH pour la mise en place d'un système d'authentification global pour toutes les universités et hautes écoles Suisses, mais, bien qu'infiniment supérieur à tous ses concurrents, il n'a malheureusement pas été retenu (le choix s'est porté sur Shibboleth).

COMMENT FONCTIONNE CETTE FÉDÉRATION DE SERVEURS TEQUILA?

Chaque institution participante doit posséder sa propre base d'utilisateurs qu'elle gère elle-même, en général dans un serveur LDAP, mais Tequila peut utiliser d'autres sources via un système de *plug-in*.

Lorsqu'un utilisateur tente d'accéder à une application sécurisée, l'application le redirige vers le serveur Tequila de l'institution locale (à l'application). Si l'utilisateur est lui aussi de cette institution, il s'authentifie normalement avec son *username/password*. Mais s'il est membre d'une autre institution participante à la fédération (c'est là où ça devient rigolo), Tequila lui offre la possibilité de s'authentifier sur son propre serveur via une redirection. S'il le fait correctement, l'application sécurisée initiale recevra les données de cet utilisateur et le nom de son institution mère. Elle pourra alors en toute sécurité donner les droits adéquats à cet utilisateur.

A aucun moment l'utilisateur ne dévoile son mot de passe à un autre serveur que celui de son institution mère. L'application sécurisée initiale peut demander des précisions sur cet utilisateur (nom, prénom, unité, ...), mais l'interface Tequila le prévient qu'elle va divulguer ces informations et lui offre la possibilité de ne pas le faire (au risque de se voir refuser l'accès à l'application). L'utilisateur reste le maître de ses données personnelles.

VOYONS LE CÔTÉ CLIENT

Ici le client est une application Web qui doit être sécurisée. Tequila offre une palette d'outils pour le client. Comme pour Gaspar, l'application peut gérer seule et à ras les pâquerettes son dialogue avec Tequila, ainsi tout CGI, quel que soit son langage, peut y avoir accès. Mais la distribution standard contient des modules Perl et Java qui simplifient considérablement l'accès pour ces langages. Il y a aussi un module Apache (1.x pour l'instant, 2.x bientôt) qui permet de protéger automatiquement, via une configuration simple des documents html, des répertoires entiers, voire même des serveurs WWW entiers sans la plus petite ligne de programme.

Un article plus détaillé suivra dans le prochain Flash informatique.

POUR EN SAVOIR PLUS

Une seule adresse: tequila.epfl.ch ■

**ABONNEZ-VOUS À LA VERSION ÉLECTRONIQUE DU
FLASH INFORMATIQUE EN ENVOYANT UN COURRIER
À: fi-subscribe@listes.epfl.ch**

Flash informatique

Les articles ne reflètent que l'opinion de leurs auteurs. Toute reproduction, même partielle, n'est autorisée qu'avec l'accord de la rédaction et des auteurs.

Rédacteur en chef: Jacqueline Dousson, fi@epfl.ch

Mise en page &
graphisme:

Appoline Raposo de Barbosa

Comité de rédaction: Omar Abou Khaled, Jean-Daniel Bonjour, Nicolas Bouche, Milan Crvcenin, Jean-Damien Humair, Pierre Kuonen, Jacques Menu, Maciej Macowicz, Philippe Pichon, Daniel Rappo, François Roulet, Christophe Salzmans & Jacques Virchaux

Impression: Atelier de Reprographie EPFL

Tirage: 4000 exemplaires

Adresse Web: <http://sic.epfl.ch/publications/>

Adresse: SIC-SA EPFL, CP 121,

CH-1015 Lausanne

Téléphone: +41 21 69 32246 & 32247