Regina : un *credential provider* LDAP pour Windows 7 et Vista

François Dagorn

15 février 2011

Introduction

L'authentification des utilisateurs dans les environnements `Windows` peut être réalisée de différentes manières, parmi celles-ci citons les suivantes :

1. utilisation d'un service `kerberos` [1] ;
2. utilisation d'un annuaire `Active Directory` ;
3. utilisation d'un annuaire `LDAP`.

C'est la 3ème solution qui est utilisée à l'université de Rennes 1. L'outil `pGina` est nécessaire pour la mettre en oeuvre dans les environnements `Windows XP`.
`Windows 7` et `Vista` ne proposent pas de solutions natives concernant l'usage d'annuaires LDAP. Par ailleurs, `pGina` tel qu'il se présentait à la fin de l'année 2009 n'était pas utilisable. Souhaitant déployer rapidement `Windows 7` dans ses salles de TP, l'IFSIC a développé son propre outil : `Regina`.

Principes techniques

`Regina` a été conçu sur la base des *credential providers* d'exemples dont les programmes sources[2] sont fournis par `Microsoft`. Le principe est d'enregistrer[3] une bibliothèque en la déclarant de type *credential provider*, elle sera utilisée dans la phase d'ouverture de session de `Windows`. Elle a pour rôle de procéder à l'acquisition d'un couple *usager/passwd* et de le transmettre à `Windows` pour vérification et ouverture potentielle de session. Dans le principe, c'est ce qui est fait par le *credential provider* installé par défaut sur tous les systèmes. Alors pourquoi en écrire un autre ?

[1] cf. la note technique *Authentification des utilisateurs - de LDAP à Kerberos* (Aubry - Dagorn).

[2] Ils sont accessibles en cherchant les mots suivants à l'aide d'un moteur de recherche : *Windows Vista Credential Provider Samples.*

[3] HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers

Le fait de disposer des sources d'un programme qui va s'intercaler dans le processus d'ouverture de session de `Windows` (avec des droits élevés) permet d'envisager plusieurs scénarios. Comme le *plugin* `LDAP` de `pGina` le faisait, nous avons décidé de vérifier la validité du couple *usager/passwd* par l'intermédiaire d'un annuaire LDAP. Si le mot de passe est correct, avant de rendre la main à `Windows`, on crée l'usager dans la base locale et l'ouverture de session va pouvoir s'opérer.
Lorsque `Regina` est installé, une ouverture de session se déroule de la manière suivante :

Début de la phase d'ouverture de session
↓
Entrée dans le code du *credential provider* (regina.dll)
↓
Acquisition du couple usager / mot de passe
↓
Accès à l'annuaire LDAP pour vérifier le mot de passe
↓
Si le mot de passe est bon, créer l'usager dans la base locale et stocker son mot de passe pour utilisation par les scripts de connexion.
↓
Retour à Windows (sortie du code de regina.dll)
↓
Fin de la phase d'ouverture de session. Si le mot de passe a été validé, la session va s'ouvrir et des scripts de connexion vont se dérouler ...

Installer, personnaliser ...

`Regina` comprend les composants suivants :

- `regina.dll`, `regina.pl`, quelques modules `.pm` et `Register.reg` qui permettent de mettre en place le *credential provider* `LDAP`. Il convient d'installer `regina.dll`, `regina.pl` et les modules `.pm` dans `c :\windows\system32\regina` (tout ceci est fait automatiquement par l'installeur). Avant d'effectuer un test il faut :
  - configurer les paramètres dans `conf_regina.pm` (serveur LDAP, comptes locaux à préserver, emplacement des logs, ...) ;
  - redémarrer le poste.
- `scriptlogin.pl` et `explorer.pl` sont les scripts de connexion de l'ISTIC (positionner des lecteurs réseaux, choix de l'imprimante par défaut, ...). Le rôle d'`explorer.pl` est expliqué dans La bogue des lecteurs réseaux sous `Windows 7` [4].

[4] http ://doc-admin.ifsic.univ-rennes1.fr/bogue.pdf

- l'image et le texte d'invite de connexion sont personnalisables :
  - l'image doit s'appeler `regina.bmp` et se trouver dans `c :\windows\system32\regina` (format BMP 128x128) ;
  - le texte d'invite de connexion doit se trouver dans le fichier `banniere.txt` également situé dans `c :\windows\system32\regina`

Télécharger `Regina` : http ://regina.ifsic.univ-rennes1.fr/Install.exe.

Compiler une nouvelle bibliothèque : les sources de `regina.dll` peuvent être installés (ils sont accessibles via l'installeur), il convient de disposer de `Microsoft Visual C++`.

sécurité

`regina` est dédié à l'authentification via un serveur `LDAP` mais surtout à permettre l'utilisation de ressources contrôlées par un service `LDAP` (serveurs de fichiers, imprimantes, ...). La partie authentification `LDAP` pourrait être sécurisée via l'usage de `LDAPS` (à suivre bientôt), ce n'est toutefois pas possible concernant concernant l'accès aux ressources (le mot de passe doit arriver en clair jusqu'au service qui lui pourra faire du `LDAPS` ensuite).

Comment `regina` permet-il de ressortir un mot de passe en clair pour un usage dans un script de connexion ?

Tant qu'on se situe sous le contrôle du *credential provider* on bénéficie de privilèges très élévés. On peut donc créer un fichier qui va contenir le mot de passe de l'utilisateur dont on est en cours d'acceptation de la connexion. Ce fichier créé avec les `ACL` de `Windows 7` (en lecture exclusive pour l'utilisateur) contient le mot de passe chiffré en `3DES` avec une clef tirée aléatoirement. Un service est alors démarré, il a pour rôle de fournir la clef de chiffrement symétrique lorsque nécessaire (lorsque le script de login va se dérouler).En quittant le Credential Provider on rend la main à `Windows` qui va ouvrir la session de l'utilisateur (*Bienvenue*, *Préparation du bureau*, ...) et appeler un script de connexion qui a la charge de monter les lecteurs réseau nécessaires. Cette phase nécessite de disposer du mot de passe de l'utilisateur en clair, il faut alors interroger le service de fourniture de la clef de chiffrement `3DES`. Ce service ne peut servir qu'une fois.