SAML et services hors web

SAML en bref

- Security Assertion Markup Language
- Fédération d'identités pour le web
- SingleSignOn (SSO) et SingleLogout (SLO)
- Diffusion contrôlée d'informations personnelles
- Ne requiert pas de fonctionnalité particulière dans les navigateurs

Terminologie SAML

- Fournisseur d'identité (IdP): service authentifiant l'usager
- Fournisseur de service (SP): service rendu à l'usager
- Assertion SAML: message XML produit par l'IdP, validant l'identité de l'usager
- ProviderId: identifiant unique d'un SP ou d'un IdP, souvent l'URL d'un fichier de métadonnées SAML décrivant le service

Échanges SAML

- Le client s'adresse au SP
- Redirection vers l'IdP
- Authentification par l'IdP
- Renvoi vers le SP (requête POST contenant l'assertion SAML)
- Nombreux autres mécanismes possibles dans la norme: requêtes GET ou POST, SOAP direct entre SP et IdP sans intervention du client...

Assertion SAML

- Message XML indiquant l'identité de l'usager
- Signature cryptographique par l'IdP
- Spécification du SP récipiendaire
- Fenêtre temporelle de validité
- Comprends des attributs personnels, typiquement extraits de l'annuaire LDAP

Services hors web

- Exemple canonique: le webmail
- Le webmail est le SP, mais le client doit s'authentifier au serveur IMAP
- SAML prévoit le mécanisme enhanced client or proxy (ECP), mais basé sur HTTP
- Implémentation libres de ECP: ?
- Faire parler HTTP aux serveurs IMAP: bof...
- Même problème pour l'annuaire LDAP

CrudeSAML

- L'assertion SAML est signée, précise le SP et la fenêtre temporelle de validité
- Connue uniquement de l'IdP, du client et du SP
- Elle est donc utilisable comme jeton de sécurité
- CrudeSAML: module PAM et plugin SASL validant les assertions SAML
  - Signature cryptographique, IdP émetteur
  - Fenêtre temporelle

Intégration avec mod_auth_mellon

- mod_auth_mellon: module Apache 2 implémentant un SP SAML
- Option pour inclure l'assertion SAML dans l'environnement Apache

```
<Location /webmail>
    MellonSamlResponseDump On
</Location>
```

- Pas de compromission si des usagers ont accès au serveur web

Service hors web: OpenLDAP (1)

- Utilisons le plugin SASL
- Client en PHP

```
$error = ldap_sasl_bind($ds, NULL,
                        $_SERVER["MELLON_SAML_RESPONSE"],
                        "SAML", NULL, $user, NULL, "none");
```

- Sur le serveur web, seul notre client a accès à `$_SERVER["MELLON_SAML_RESPONSE"]`

Service hors web: OpenLDAP (2)

- Sur le serveur LDAP, /usr/lib/sasl2/slapd.conf

```
saml_grace: 600
saml_userid: uid
saml_idp0: /etc/openssl/certs/idp.saml
saml_trusted_sp0: https://sp/saml/metadata
```

- Et enfin /etc/openldap/slapd.conf

```
authz-regexp uid=([^,]*),cn=saml,cn=auth
        ldap:///o=example??sub?(uid=$1)
```

Service hors web: Squirrelmail (1)

- Usage du module PAM
- Surcharges dans le fichier de configuration de Squirrelmail, cf README de CrudeSAML

```
saml_data = $_SERVER["MELLON_SAML_RESPONSE"];
$bin_data = base64_decode($saml_data);
$secretkey =
    base64_encode(gzcompress($bin_data));
$_POST["login_username"] =
    $_SERVER["REMOTE_USER"];
$_POST["secretkey"] = $secretkey;
```

Services hors web: Squirrelmail (2)

- Sur le serveur IMAP, /etc/pam.d/dovecot

```
auth            sufficient      pam_saml.so
                grace=600 userid=uid
                idp=/etc/openssl/certs/idp.saml
                trusted_sp=https://webmail/saml/metadata
```

Services hors Web: SSH

- Comme le webmail, on envoie l'assertion SAML comme mot de passe
- Cohabitation avec les accès SSH usuels: appel de pam_saml puis pam_ldap, ou l'inverse
- Pas de système de sélection du mécanisme dans PAM: erreurs dans les journaux...

Conclusions

- WebSSO sur tous les services
- Pas d'application web privilégiée
- Développement d'application interne simplifié
  - Authentification gérée par Apache
  - Informations personnelles dans $_SERVER
- Fonctionne exceptionnellement bien ...
- … mais pas du tout remarqué par les usagers!