Tour d'horizon des différents SSO disponibles

L. Facq, P. Depouilly, B. Métrot, R. Ferrere

ANF Les systèmes d'authentification dans la communauté ESR : étude, mise en oeuvre et interfaçage dans un laboratoire de Mathématique
Angers, 22 - 26 septembre 2014

Plan

Introduction

Définitions

CAS : Exemples et périmètre d'utilisation

Kerberos : Exemples et périmètre d'utilisation

SSO multi-établissements (Shibboleth, OpenIDConnect)

Quelques références...

Progression

La problématique ?

- Un besoin : comment authentifier les utilisateurs de façon unique et sécurisée ?
- A partir de n'importe quelle ressource informatique (fixe, mobile) et avec tout système d'exploitation, navigateur internet ;
- Pour leurs applications et profils d'utilisation (droits/accès) ;
- La réponse : un mécanisme/système d'authentification unique par serveur SSO-CAS et/ou kerberos

Enjeux du côté utilisateur

- Répondre à un besoin de la culture du citoyen d'aujourd'hui : toujours pressé et demandeur ;
- Souhaite accéder à son ENT, ses multiples applications web n-tiers
- En utilisant un seul login/mot de passe (plus de mot de passe noté !)
- Plus de mot de passe noté ! et plus de prolifération de mots de passe !
- Une seule saisie du mot de passe par session de travail
- Connexion en fonction de son profil .

Enjeux du côté laboratoire/UFR/Université

- Apporte de la sécurité au système d'information mais sécuriser également l'authentification
- Accès à partir d'un seul point d'entrée pour l'authentification des utilisateurs
- Centralisation des informations d'authentification et délégation à un système de type CAS, Kerberos
- Les applications web déchargées de la tâche d'authentification des utilisateurs $\rightarrow$ serveur dédié type CAS
- Utilisation de techniques de synchronisation entre différents domaines d'authentification et annuaires LDAP

Progression

Introduction

Définitions

CAS : Exemples et périmètre d'utilisation

Kerberos : Exemples et périmètre d'utilisation

SSO multi-établissements (Shibboleth, OpenIDConnect)

Quelques références...

Qu'est ce qu'un SSO ?

- Single Sign-On, acronyme SSO ;
- Mécanisme de centralisation et de propagation de l'authentification (informations utilisateurs) ;
- Web-SSO : accès aux applications et services Web avec présentation automatique des mots de passe ;
- Un seul login/mot de passe pour de multiples ressources ;
- Simplification par un seul login/mot de passe en liaison souvent avec un annuaire LDAP ;
- En pratique : nom du service ou URL présentée à l'utilisateur.

Identification

Définition

Attribuer un numéro à un utilisateur de façon à pouvoir l'associer facilement aux différents objets du système qu'il sera amené à manipuler (fichiers, périphériques, processus...).

- Unicité du numéro d'identification au sein du système
- Informations complémentaires
  - Nom, prénom
  - Expiration du compte
  - Appartenance de groupes
  - ...
- Problématique de cohérence et de distribution des informations complémentaires

Authentification (*authentication*)

Définition

Garantir que l'utilisateur qui se présente est bien celui qu'il prétend être.

- L'utilisateur ou système présente un couple login, mot de passe ou un certificat ;
- Le serveur renvoie une réponse par l'affirmative ou par la négative
- La réponse affirmative s'accompagne d'attributs propres à la session utilisateur (adresse IP, niveau de droits...)

Autorisation

Définition

Permettre ou interdire l'accès à une ressource pour un utilisateur ou un système.

- Une requête d'autorisation du client au serveur ;
- Que si la réponse d'authentification est affirmative ;
- Gestion centralisée des commandes ou des actions autorisées ;

Accounting

Définition

Comptabilisation des accès aux ressources et suivi des opérations effectuées, en vue d'auditer les performances, les erreurs...

- Requêtes de comptabilisation suite à différents événements liés à l'utilisateur ;
- Quand il y a : début/fin de connexion, exécution d'une action/commande ;
- Qu'est-ce qui a été fait, à quel moment et par qui ?
- Reste optionnel et peut être activé à tout moment
- Détection d'attaque, de surcharge, de tentatives d'accès non autorisées

Solutions libres SSO possibles

centralisées

- CAS

fédératives

- Shibboleth
- OpenSSO/OpenAM (solution d'authentification et de fédération), Openstack

coopératives, décentralisées

- SAML
- OpenID (Yahoo, Google,...)
- Liberty Alliance (SUN, NOVELL, IBM avec jetons SAML)
- LemonLDAP : :NG (complète AAA)

Progression

Introduction

Définitions

CAS : Exemples et périmètre d'utilisation

Kerberos : Exemples et périmètre d'utilisation

SSO multi-établissements (Shibboleth, OpenIDConnect)

Quelques références...

CAS - Central Authentication Service

CAS selon Wikipédia :

Système d'authentification unique (SSO) pour le web développé par l'Université Yale, partenaire majeur dans le développement de uPortal. Ce logiciel est implanté dans plusieurs universités et organismes dans le monde

Sous licence JA-SIG type BSD, écrit en Java

Avantages et périmètre de CAS

- S'authentifier une seule fois pour de multiples applications
- Mot de passe ne circulant que du navigateur au serveur CAS sur un canal sécurisé (https)
- Authentification sur une source centralisée faisant autorité : Utilisateurs annuaire LDAP, royaume Kerberos, domaine Windows, serveur nis (panachage possible) ...
- Tickets dans les entêtes HTTPS
- Pour des applications Web ou non Web
- CAS-ification des applications grâce à de multiples librairies clientes disponibles
- Limité à une authentification locale (pas de multi-établissements)
- Ne répond qu'à la problématique d'authentification : pas de gestion de droits ou d'attributs supplémentaires

Quelques exemples d'utilisation SSO avec CAS

- Accès restreint à des pages web,
- Applications PHP, JAVA,
- Webmail, ENT,
- IMAP, Cyrus-Imap

Progression

Introduction

Définitions

CAS : Exemples et périmètre d'utilisation

Kerberos : Exemples et périmètre d'utilisation

SSO multi-établissements (Shibboleth, OpenIDConnect)

Quelques références...

Kerberos

Qu'est que Kerberos ?

Système d'authentification sécurisé et centralisé, où il n'est nécessaire de saisir son identifiant/mot de passe qu'une seule fois pour accéder à de multiples ressources. Il garantit l'authentification mutuelle entre l'utilisateur et la ressource visée.

Systèmes compatibles [1]

- Distribution Linux (Ubuntu, Debian, Fedora)
  - Intégré dans les paquets
  - Deux implémentations du protocole : Heimdal ou MIT
- FreeBSD, NetBSD
- Mac OS X (intégré au système)
- Produits Windows
  - XP, 7, 2003 Serveur, 2012 Serveur
  - Protocole d'authentification d'ActiveDirectory

1. Liste non exhaustive

Périmètre

- S'exécute au niveau système d'exploitation
- Concerne un groupe d'ordinateur d'un réseau local : clients/serveur
- S'applique sur une ogranisation/utilisateurs, service d'un domaine
- Serveur KDC (Key Distibution Center) –> tickets/mots de passe
- Ne prend pas en charge la diffusion des informations d'identification

Quelques exemples

- Ouverture de sessions graphiques ou textes
- Partage de fichiers
- Propagation d'authentification (à partir d'une session)
  - Rebond de machine en machine
  - Messagerie électronique (IMAP, POP)
  - Pages internet

Progression

Introduction

Définitions

CAS : Exemples et périmètre d'utilisation

Kerberos : Exemples et périmètre d'utilisation

SSO multi-établissements (Shibboleth, OpenIDConnect)

Quelques références...

Notion de fédération / Possibilités

- Les fédérations d'identités permettent une gestion « propre » et « secure » du multi établissements, composants hébergés par entités différentes

découplage des composants

- choix d'un établissement (« aiguillage », Where Are You From)
- notion d'identité (fournisseur d'identité, IdP)
- services avec authentification (fournisseur de service, SP)
- fourniture d'attributs (email, nom, prénom, civilité, ...)

propagation d'attributs IdP –> SP

- « à la tête du client (SP) »
- pas tout ou rien, adapté au cas par cas
- attributs opaques

« Fédérations » : SAML vs OAuth/OpenID**

- 2 grandes familles

SAML (XML) Security Assertion Markup Language

- Complexe (XS, ...)
- Notion forte de fédération (métadonnées centralisées & signées)
- *« Implémentations » :* **Shibboleth, EduGain**

OAuth (+JSON/REST) JWT (JSON Web Token)

- Simple
- Pas de fédération (confiance via certificat/AC habituelles)
- *« Implémentations » :* **OAuth (Facebook, Twitter, ...), OpenIDConnect (Google, ...)**

Récapitulatif : Tour d'Horizon MultiEtab - Shibboleth / OpenIDConnect

Usages: Systèmes	SSO?	Mono établissement	Multi établissement	Attributs propagés	Simple	Féd.°	Cas d'usage classique
LDAP	Non	Oui	Non	« Oui »	Oui	-	base
CAS	Oui	Oui	Non	Non	Oui	-	web+, mono établissement
Kerberos	Oui	Oui	*Peut*	Non	Non	Non	quelques établissements, comptes unix ? multi protocoles
OpenID	Oui	*Peut (2much)*	Oui	Oui	Oui (JSON REST)	Non	Web+? groupe ouvert d'établissements, identités sociales
Shib	Oui	*Peut (2much)*	Oui	Oui	Non (XML)	Oui (méta données)	Web+, groupe fermé d'établissements
802.1X radius	Non	Non	Oui	Oui	Non	Non	eduroam

Progression

Introduction

Définitions

CAS : Exemples et périmètre d'utilisation

Kerberos : Exemples et périmètre d'utilisation

SSO multi-établissements (Shibboleth, OpenIDConnect)

Quelques références...

liens internet et articles

- Shibboleth - Démo Shibboleth
- Wiki Shibboleth Déploiement Shibboleth
- Intérêt de la fédération Education-Recherche - Renater
- Site de internet2
- Protocole CAS
- Gestion des identités CNRS
- "Kerberos, le SSO universel", Guillaume Rousse - GNU/Linux Magazine numéro 143
- "SSO et authentification web centralisée avec CAS-Toobox ", Christophe Borelly - GNU/Linux Magazine numéro 113
- Authentification Kerberos Microsoft

- Merci pour votre attention.
- Avez-vous des questions ?