La mémorisation des mots de passe dans les navigateurs web modernes

Didier Chassignol

Frédéric Giquel

6 décembre 2005 - Congrès JRES

INRIA

La problématique

- Multiplication des applications web nécessitant une authentification
- Multiplication des saisies de mots de passe pour l'utilisateur
- Les navigateurs proposent une fonction de mémorisation des mots de passe

➔ Question : peut-on raisonnablement utiliser cette fonctionnalité ?

- Point vue ergonomie
- Point vue sécurité

Les navigateurs étudiés

- Mozilla 1.7.3 (Windows, Linux, Mac OS)
- Netscape 7.1 (Windows, Linux, Mac OS)
- Firefox 1.0 (Windows, Linux, Mac OS)
- Internet Explorer 6.0 (Windows)
- Internet Explorer 5.2.3 (Mac OS)
- Safari 1.2.4 (Mac OS)
- Konqueror 3.4.2 (Linux)

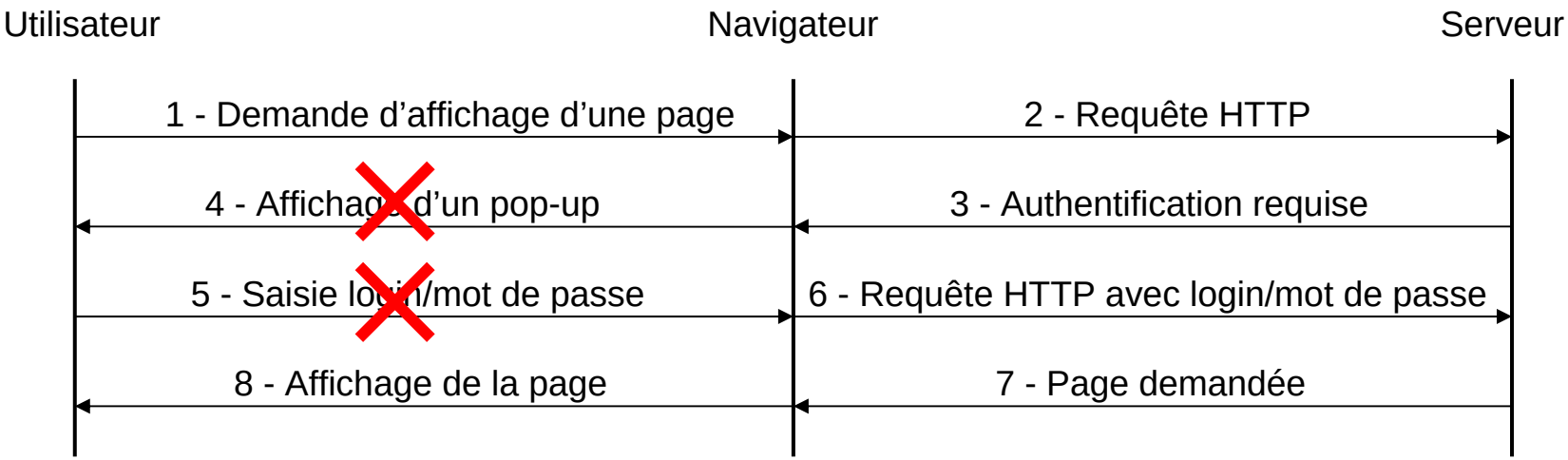
Plan de la présentation

➔ Rappel sur les méthodes d'authentification sur les serveurs web

- Résultat des tests
  - Disponibilité de la fonctionnalité et de l'ergonomie
  - Sécurité de la mémorisation sur les postes clients
  - Sécurité du point de vue réseau
- Conclusion

Authentification au niveau du protocole HTTP

- Protocole normalisé (RFC 2617)
  - Facilement détectable par le navigateur
- 2 variantes : Basic (et Digest)



- Suivi de session authentifiée : rejeu automatique par le navigateur
- Utilisation d'un « realm » pour délimiter la zone protégée

Authentification applicative par formulaire

- Pas de normalisation
  - Détection partielle par le navigateur
- Page web avec un formulaire
  - Entrée de formulaire de type `text` pour le login
  - Entrée de formulaire de type `password` pour le mot de passe
  - Transmission, généralement en clair, du login et du mot de passe par la méthode HTTP POST (parfois GET)
- Suivi de session authentifiée : généralement avec un cookie (RFC 2965)

Plan de la présentation

- Rappel sur les méthodes d'authentification sur les serveurs web

➔ Résultat des tests

  - Disponibilité de la fonctionnalité et de l'ergonomie
  - Sécurité de la mémorisation sur les postes clients
  - Sécurité du point de vue réseau

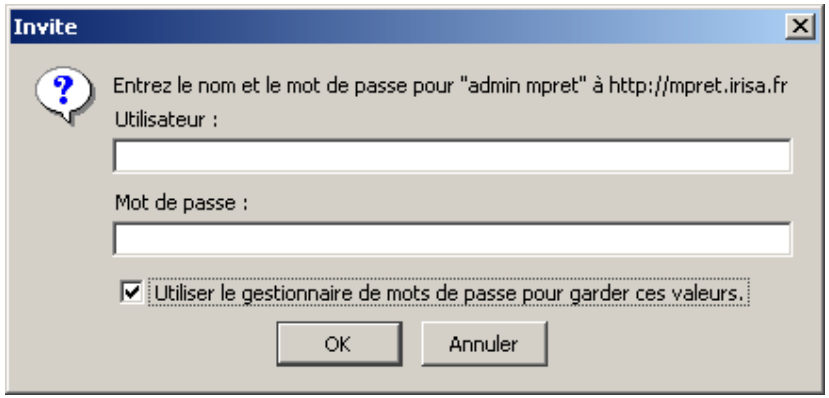
- Conclusion

Disponibilité de la fonctionnalité sur les navigateurs web

	HTTP/HTTPS
Authentification HTTP Basic	Tous les navigateurs
Authentification applicative par formulaire	Tous les navigateurs sauf Internet Explorer Mac OS

Contrôle de la mémorisation

• L'utilisateur contrôle la mémorisation des mots de passe lors de la 1ère authentification



Authentification HTTP Basic avec Firefox

Authentification applicative par formulaire avec Safari

Automatisation de l’authentification

- L’automatisation est-elle complète ?

  - Quasi automatisée (préremplissage + validation de l’utilisateur)
  - Entièrement automatisée pour l’authentification HTTP Basic avec Safari

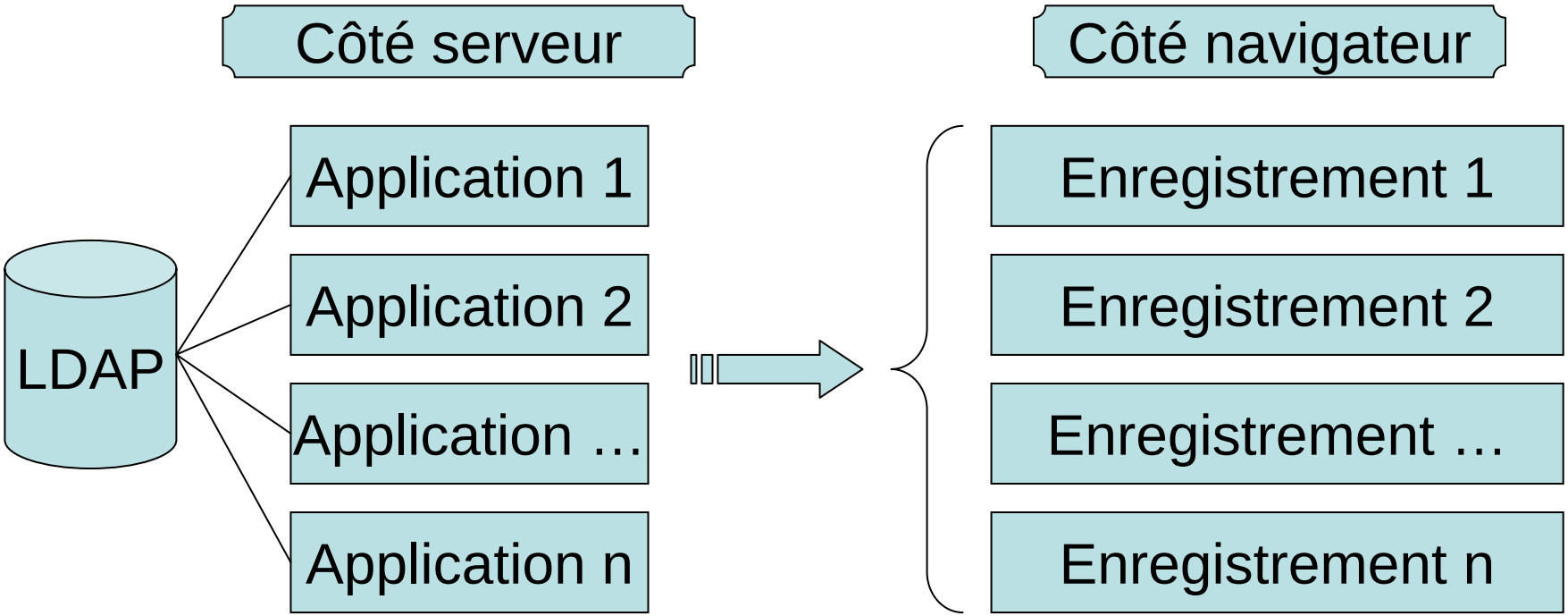
- Eléments complémentaires concernant l’authentification applicative par formulaire
  - Choix dans une liste déroulante
  - Propriété « autocomplete off »

Cas où le mot de passe mémorisé diffère de celui attendu par l'application

- Authentification HTTP Basic :
  - Détection par le navigateur
  - Légères différences de comportement entre les navigateurs (préremplissage ou non du champ « Mot de passe »)

- Authentification applicative par formulaire :
  - Pas de détection par le navigateur
  - Lié aux choix du programmeur de l'application web

Mot de passe commun à plusieurs applications



- Peut-on en une seule opération modifier la mémorisation du mot de passe commun ?
- Aucun des navigateurs ne propose cette fonctionnalité

Plusieurs applications sur un même site web

- Problématique : des URLs très proches
  - http://serveur.etablissement.fr/appli1/
  - http://serveur.etablissement.fr/appli2/
- Authentification HTTP basic :
  - Les navigateurs proposent la bonne authentification si des realms différents sont fournis
  - Exception lors de nos tests : Mozilla
- Authentification applicative par formulaire
  - L'application fournit ou ne fournit pas des noms différents pour les entrées de formulaire de type `text`
  - Internet Explorer et Konqueror mémorisent l'URL complète

Visualisation des mots de passe

- Un utilisateur peut-il retrouver un mot de passe mémorisé ?

- Oui, directement dans l'application pour Mozilla et Firefox
- Oui, à l'aide d'un outil externe fourni pour Safari et Konqueror
- Oui, à l'aide d'outils tiers pour Internet Explorer Windows et Netscape
- Non pour Internet Explorer Mac OS

Plan de la présentation

- Rappel sur les méthodes d'authentification sur les serveurs web

➔ Résultat des tests

  - Disponibilité de la fonctionnalité et de l'ergonomie
  - Sécurité de la mémorisation sur les postes clients
  - Sécurité du point de vue réseau

- Conclusion

Stockage des mots de passe

Les mots de passe mémorisés sur le disque dur sont-ils chiffrés dans un but de protection en cas d'accès physique ?

➔ Pas de stockage en clair quelque soit le produit

- Chiffrement 3DES : Mozilla, Netscape, Firefox et Safari
- Chiffrement Blowfish : Konqueror
- Méthode de chiffrement/codage non documentée : Internet Explorer (Windows et Mac OS)

Note : Internet Explorer Windows stocke les données dans le registre de l'utilisateur (fichier NTUSER.DAT)

Clé de chiffrement / « master password »

Comment la clé de chiffrement est-elle créée ? Est-elle dérivée d'un « master password » ?

➔ Utilisation d'un « master password »

- En option pour Mozilla, Netscape et Firefox
- Obligatoire pour Konqueror
- Obligatoire pour Safari : par défaut, le mot de passe de session Mac OS
- Durée de vie paramétrable

➔ Pas de « master password » pour Internet Explorer

- Chiffrement cassable en cas d'accès physique

Stockage des cookies

• Les cookies permettent un suivi de session authentifiée pour l'authentification applicative par formulaire

- Importance de les protéger

• Risque moins important que pour les mots de passe

- Durée de vie souvent limitée par le serveur
- Tous les cookies ne sont pas stockés sur le disque dur

➔ Aucun des navigateurs n'intègre un mécanisme de protection du stockage des cookies

Sauvegarde et restauration

Risque d'oubli par l'utilisateur des mots de passe mémorisés par le navigateur

➔ Simple pour les navigateurs qui stockent les données dans un fichier (Mozilla, Netscape, Firefox, Safari, Konqueror et Internet Explorer Mac OS)

➔ Compliqué pour Internet Explorer Windows car nécessite un outil de sauvegarde du registre

Solution transparente de chiffrement externe

• Une alternative au chiffrement proposé par le navigateur et à l'utilisation d'un « master password »

• Peut être une solution pour la protection des cookies

➔ Solution par système d'exploitation et non par navigateur

- EFS sous Windows
- CryptoAPI sous Linux
- FileVault sous Mac OS

➔ Difficultés pour Internet Explorer Windows à cause du stockage dans le registre

Plan de la présentation

- Rappel sur les méthodes d'authentification sur les serveurs web

➔ Résultat des tests

  - Disponibilité de la fonctionnalité et de l'ergonomie
  - Sécurité de la mémorisation sur les postes clients
  - Sécurité du point de vue réseau

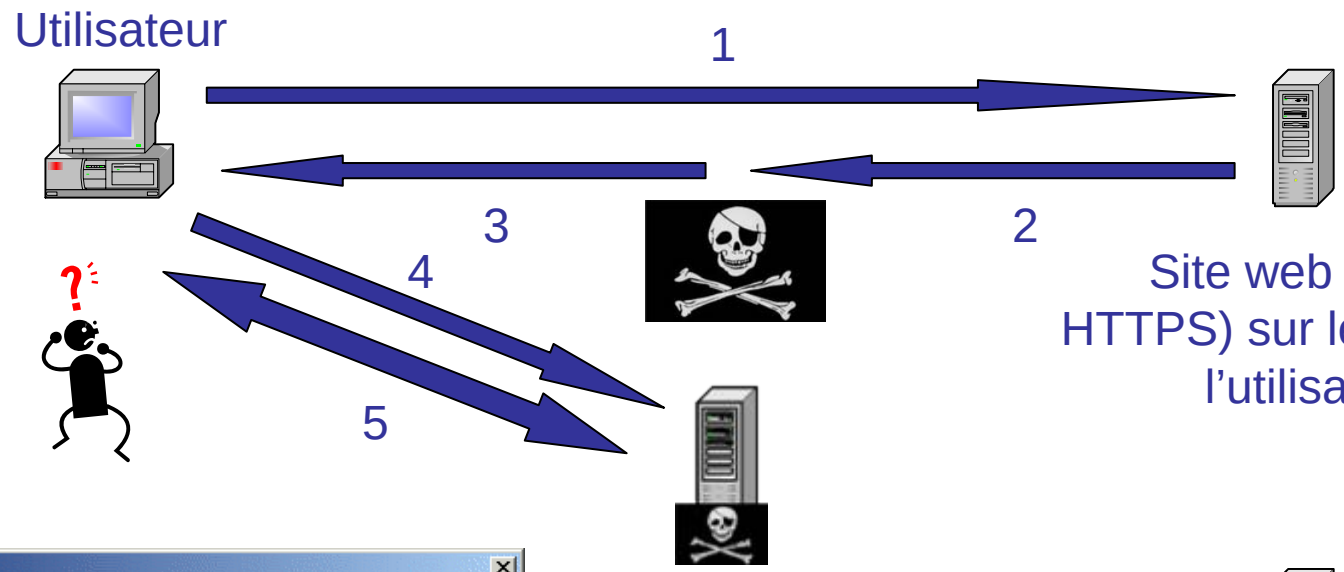
- Conclusion

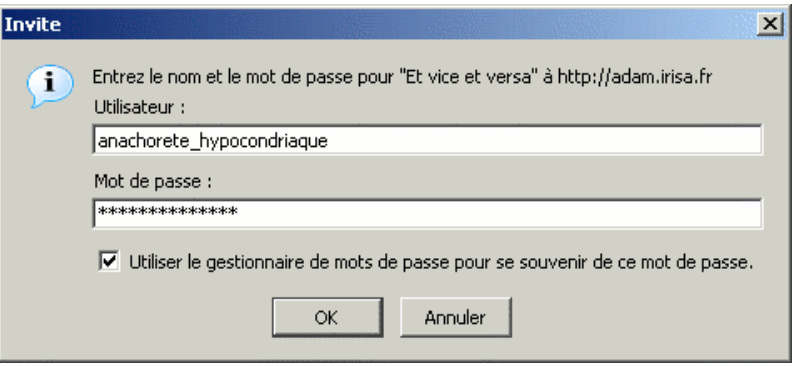
Idées développées

- Les « webbugs »
  - Code HTML utilisé par les spammeurs
  - Force le navigateur à faire une requête HTTP
    - Utilisable pour déclencher une authentification HTTP Basic
  - Image factice, invisible par l'utilisateur
  - Exemple : <img src="http://serveur_a_contacter/image.jpg" width=1 height=1 border=0>

- Non utilisation de HTTPS
  - Risque d'usurpation d'identité du serveur
  - Pas de confidentialité pour la transmission du mot de passe
  - Pas de vérification d'intégrité

Scénario possible de vol de mot de passe





Ordinateur

Site web B (non HTTPS) pour lequel l'utilisateur à mémorisé un mot de passe de l'authentification HTTP Basic

Authentification à l'insu d'un utilisateur de Safari

Avec Safari, l'authentification HTTP Basic est entièrement automatisée

➔ Pas d'apparition de pop-up à la suite du « webbug » visant les sites avec mot de passe mémorisé

➔ Risque supplémentaire lié à la mémorisation :

- Automatisation complète du vol de mot de passe

➔ Limitation du risque :

- Le nom des sites est chiffré dans le stockage sur le poste client

Limitation de la mémorisation et du préremplissage aux seules pages HTTPS

L'utilisateur peut-il globalement désactiver les fonctionnalités de mémorisation et de préremplissage pour les pages non HTTPS ?

➔ Quelque soit le navigateur, pas de désactivation globale

- Limitation de la mémorisation aux seules pages HTTPS à la discrétion de l'utilisateur
- Préremplissage d'une page HTTPS par le navigateur seulement si la mémorisation a eu lieu en HTTPS
  - Sauf cas particuliers …

Réutilisation en HTTP des mots de passe mémorisés en HTTPS

Cas rencontrés :

- Famille Mozilla et Internet Explorer pour l'authentification HTTP Basic en HTTP sur port TCP 443. Exemple :
  - URL lors de la mémorisation : https://serveur.etablissement.fr/page.html
  - Informations mémorisées : `serveur.etablissement.fr:443`
  - URL valide pour le préremplissage : http://serveur.etablissement.fr:443/page.html
- Safari pour l'authentification applicative par formulaire

➔ Risque supplémentaire lié à la mémorisation :

- Vol d'un mot de passe d'un site HTTPS par attaque réseau

➔ Limitation du risque :

- Nécessite une action de l'utilisateur

Plan de la présentation

- Rappel sur les méthodes d'authentification sur les serveurs web
- Résultat des tests
  - Disponibilité de la fonctionnalité et de l'ergonomie
  - Sécurité de la mémorisation sur les postes clients
  - Sécurité du point de vue réseau

➔ Conclusion

Conclusions générales

- Résultats des tests significatifs à instant T. La grille d'analyse est importante
- Coûts faibles
- Ergonomie améliorée malgré quelques inconvénients
- Risques supplémentaires de vol de mot de passe
- Internet Explorer à déconseiller si accès physique non protégé
- Des précautions à prendre :
  - Utilisation d'un « master password »
  - Sauvegarde/restauration
  - Verrouillage de session
  - Portables : éviter le mode hibernation et chiffrer la zone de swap

Contextes d'utilisation

- Base de compte commune
  - Situation actuelle à l'INRIA
  - Annuaire LDAP central
  - 2 gros inconvénients
    - Ergonomie mal adaptée
    - Risque de vol du mot de passe unique

- Ensemble hétérogène d'applications web
  - Webmail, forum, inscription à une conférence
  - Utilisation adaptée si choix de mots de passe différents (idéalement aléatoires)

Questions / Réponses