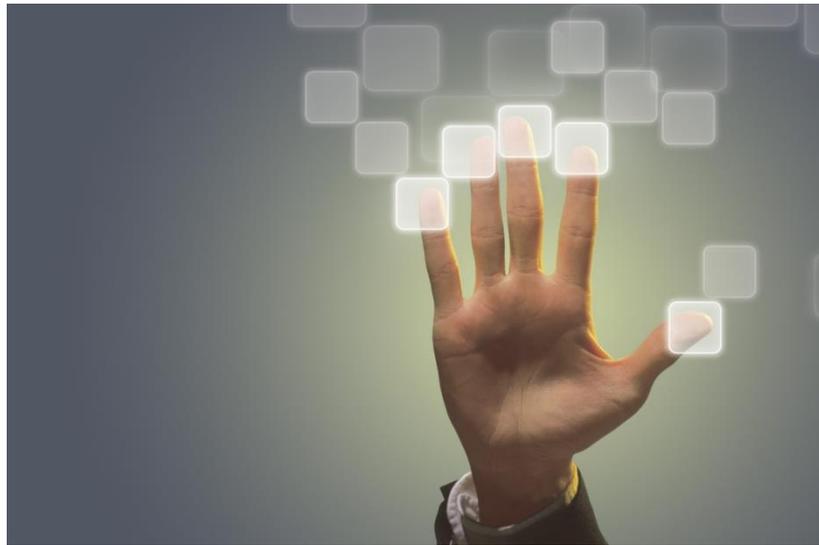


Requêtes Multi-parties Sessions HTTP Authentification et Contrôle d'accès

Département Sciences Informatiques
Jean-Yves Tigli – tigli@polytech.unice.fr
<http://www.tigli.fr>

SI 3^{ème} année



Authentification avec HTTP

L'authentification dans HTTP

- ✓ Indiqué dans les ACL
- ✓ Modes d'authentification
 - BASIC
 - nom d'utilisateur et mot de passe échangé en clair (base64) !
 - base des mots de passe dans un fichier htpasswd utilitaires de gestion du fichier
 - DIGEST
 - sécurisation de BASIC
 - hachage sécurisé MD5 du (nom,password,URI, méthode,nombre aléatoire fourni par le serveur)
 - SSL
 - Secure Socket Layer (TLS : Transport Layer Security)
 - authentification avec CA du serveur (2.0) et du client (3.0)
 - confidentialité avec DES
 - puis dialogue HTTP sur la connexion SSL

L'authentification applicative

- ✓ **Motivations**
 - interface de login
 - identification externe
 - BD, Annuaire LDAP, ...
 - authentification plus forte
- ✓ **L'application gère l'authentification de l'utilisateur**
 - formulaire d'accueil HTML (nom, password)
 - attention le mot de passe peut-être est en clair
 - gestion des tables d'utilisateur
 - une session est ensuite ouverte associé à un utilisateur authentifié (ou non : par exemple rejet au bout de 3 tentatives)

Contrôle d'Accès dans HTTP

- ✓ **ACL (Access Control List)**
 - spécifie les autorisations (**ALLOW**) ou les interdictions (**DENY**) d'accès à une arborescence virtuelle du serveur
 - en fonction :
 - de l'authentification
 - de la localisation du client sous domaine DNS, réseau ou adresse IP
- ✓ **ACF (Access Control File)**
 - fichier regroupant les ACL
 - global : `access.conf` dans Apache
 - par arborescence : `.htaccess`
 - combinaison des **ALLOW** et des **DENY**

Audit des Requêtes

- ✓ **Journaux des requêtes**
 - les accès (access.log, refferee.log), et les erreurs (error.log),... sont journalisés
- ✓ **Exploitation des Journaux**
 - erreur dans les liens, ...
 - clientèle, analyse d'activité, ...
- ✓ **Reporting (Présentation Synthétique)**
 - Pour Apache
 - AccessWatch, Wusage, Analog, wwwstat
 - IIS, NS
 - intégré et visualisé par un script
 - Généraux
 - Net Analysis (Net Genesis), Enterprise Suite (Web Trends)