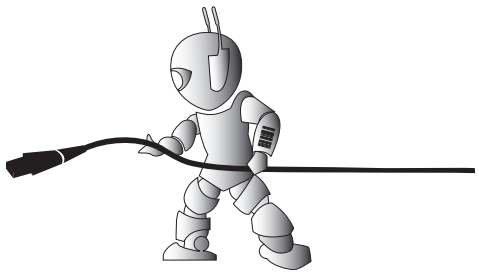
Chiffrement et authentification

Applications de la cryptographie

Tuyêt Trâm DANG NGOC
<dntt@u-cergy.fr>

Université de Cergy-Pontoise

2012–2013



DÉPARTEMENT
Sciences Informatiques

Plan

DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

PGP/GPG

Logiciel de chiffrement et de signature de données utilisant la cryptographie asymétrique et la cryptographie symétrique.

- Transmission de clef symétrique IDEA : chiffré avec clef asymétrique RSA (lente mais sans concertation)
- gros texte rapide à chiffrer/déchiffrer avec IDEA
- Chiffrement des fichiers locaux : avec IDEA.
- Génération de clefs publiques et privées : avec RSA, DSA ou El-Gamahl
- Envoi de fichiers confidentiels : chiffrement avec une clef secrète IDEA générée puis transmise à l'aide de la clef privée.
- Signature électronique : en chiffrant avec la clef privée et vérifiant avec la clef publique.
- Intégrité de messages : hachage du message par MD5 (128 bits) chiffré ensuite avec la clef privée de l'expéditeur.
- Gestion des clefs : 1 trousseau de clefs publiques et 1 trousseau de clefs privées.
- Certification de clefs : ajoute un sceau numérique garantissant

DÉPARTEMENT Sciences Informatiques

Interface ergonomique PGP

- Une interface ergonomique : l'utilisateur n'a pas à connaitre les mécanismes cryptographiques sous-jacents
  - génération aléatoire par mouvement de la souris, clavier, etc.
  - intégration dans les lecteurs/composeurs de mails

DÉPARTEMENT
Sciences Informatiques

Chiffrage et signature avec GPG

1. Créer une paire de clé avec gpg
   - création d'une paire de clé : `gpg --gen-key`
   - connaître la liste des clefs publiques : `gpg --list-key`
   - connaître la liste des clefs privées : `gpg --list-secret-keys`

Toutes les clés existantes sur le système apparaîtrons et auront chacune une ligne avec : `pub 1024D/num_key 2008-01-14`

   - supprimer une clé privée : `gpg --delete-secret-keys num_key`
   - supprimer une clé publique : `gpg --delete-key num_key`
   - exporter une clé publique : `gpg --armor --export num_key > publicKey.asc`
   - exporter une clé privée : `gpg --export-secret-key num_key > privateKey.asc`
   - importer une clé publique sur le système : `gpg --import publicKey.asc`
   - importer une clé privée : `gpg --import --allow-secret-key-import privateKey.asc`
2. Cryptage de fichier avec une clé
   - crypter un fichier : `gpg --recipient num_key --encrypt --armor monfichier`
   - décrypter un fichier : `gpg --decrypt monfichier > nouveaufichier`
3. Signature d'un fichier
   - signer un fichier : `gpg -sa monfichier`
   - vérifier la signature d'un fichier : `gpg --verify monfichier`

DÉPARTEMENT Sciences Informatiques

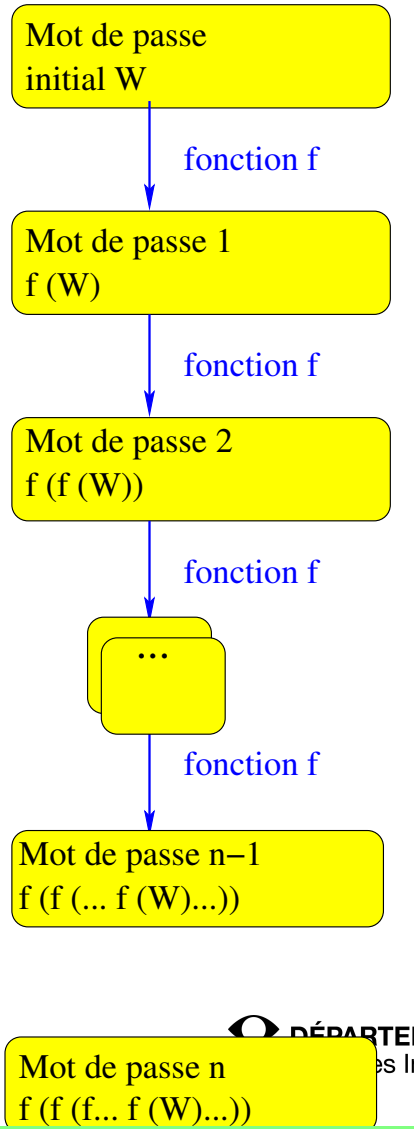
DÉPARTEMENT
Sciences Informatiques

One-Time-Password (OTP) - Mot de passe jetable

f est une fonction à sens unique (difficilement inversible).

Génération :

1. Le serveur génère n mots de passe à partir de celui W donné par l'utilisateur : $p_1, p_2, ..., p_{n-1}, p_n$
2. Il imprime les $n-1$ premiers mots de passe pour le client et ne conserve **que** le n^{ieme} mot de passe.

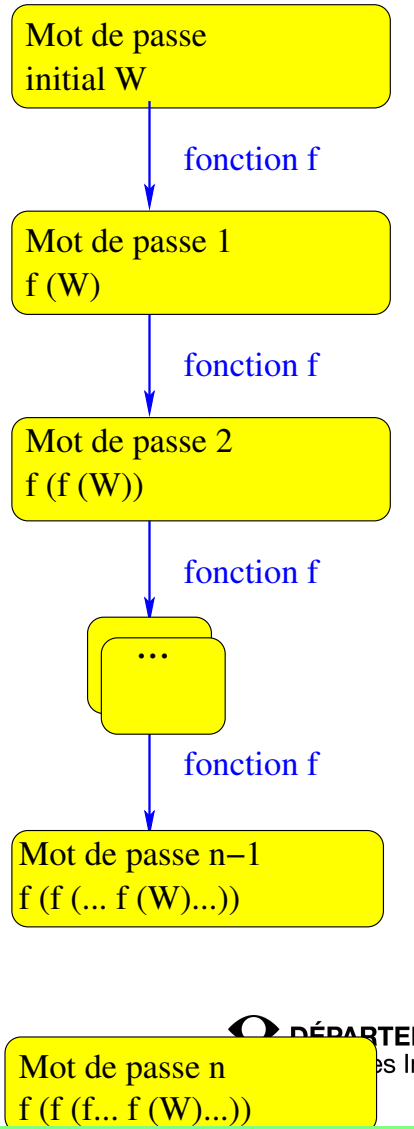


One-Time-Password (OTP) - Mot de passe jetable

f est une fonction à sens unique (difficilement inversible).

Utilisation :

1. Lorsque l'utilisateur souhaite contacter le serveur, il donne le dernier mot de passe de sa liste.
2. le serveur applique la fonction f et compare avec le mot de passe stocké.
3. si c'est OK, autorisation, et le serveur remplace son mot de passe stocké par celui de l'utilisateur
4. l'utilisateur détruit le dernier mot de passe de sa liste.



OTP et S/Key-OPIE

- Fonction f : fonction de hachage type MD4, MD5, DES-MAC
- Mot de 64 bits écrits sous la forme de 6 mots de 2 à 4 caractères

Login : dntt

Mot de passe : toto01

1	ROOF MYTH TOP DESK OATH HURL
2	JOEL GEM SOW SUIT HALO BEY
3	FORE RUNT SELL COWL BEER JOLT
4	EGAN MOO IS RUM BURT KNEW
5	BLOB COY ALEC ROSA LAW FERN
6	DIN SWAT OWNS SLAT WIN DEAR
7	COCK ROE HAY AREA FIR NINE
8	COMB CAKE KNEE MASK GRAY GEAR
9	MART FISH DEAN TIC CRAM BHOY
10	WERT BUN ROY SEAM COW CROW

DÉPARTEMENT Sciences Informatiques

Mot de passe jetable : synthèse

Cette technologie permet de s'authentifier avec un mot de passe à usage unique. Cette technologie est basée sur l'utilisation d'un secret partagé.

- nécessite la rencontre "physique" des deux partis

DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

SSH

- Les données circulant entre le client et le serveur sont chiffrées,
- Le client et le serveur s'authentifient mutuellement

Établissement d'une connexion SSH :

1. le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé
2. le client s'authentifie auprès du serveur pour obtenir une session.

DÉPARTEMENT
Sciences Informatiques

Mise en place du canal sécurisé

Le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).

- phase de négociation entre le client et le serveur : sur les méthodes de chiffrement à utiliser.
- le serveur envoie sa clé publique (*host key*) au client.
- Le client génère une clé de session de 256 bits qu'il chiffre avec la clé publique du serveur, et envoie au serveur la clé de session chiffrée + l'algorithme utilisé.
- Le serveur déchiffre la clé de session grâce à sa clé privée et envoie un message de confirmation chiffré avec la clé de session.
- (si le serveur possède une liste d'hôtes autorisés à se connecter, il va chiffrer un message à l'aide de la clé publique du client (qu'il possède dans sa base de données de clés d'hôtes) $\Rightarrow$ *challenge*
- le reste des communications est chiffré grâce à un algorithme de chiffrement symétrique en utilisant la clé de session partagée par le client et le serveur

Authentification du client

Le client s'authentifie auprès du serveur pour obtenir une session. Deux méthodes :

- Utilisation de mot de passe : Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisé et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide
- Utilisation de clés publiques : Si l'authentification par clé est choisie par le client, le serveur va créer un challenge et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée
- Utilisation de mot de passe jetable : via S/Key

Algorithmes de chiffrement dans SSH

Echange de clefs	SSH1	SSH2
RSA	X	X
DSA	-	X

Chiffrement symétrique	SSH1	SSH2
DES	X	-
3DES	X	X
IDEA	X	-
RC4	-	X
Blowfish	X	X
Cast128	-	X
AES128	-	X
AES192	-	X
AES256	-	X

DÉPARTEMENT
Sciences Informatiques

Utilisation de ssh

```
ssh login@machinedist
ssh machinedist -l login
ssh machinedist
```

-v pour détails des échanges.
La première fois :

```
The authenticity of host 'machinedist' (111.222.333.4)' can't be established.
RSA1 key fingerprint is 1z:2y:3x:4w:56:78:98:78:ab:cd:ef:01:23:45:67:89.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added 'machinedist,111.222.333.4' (RSA1) to
the list of known hosts.
/home/dntt/.ssh/known\_hosts
```

Pas d'avertissement les autres fois. Si attaque (ou simplement changement de clef) :

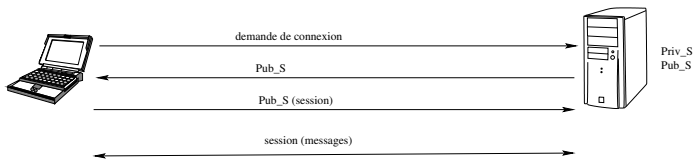
```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: HOST IDENTIFICATION HAS CHANGED!         @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
```

DÉPARTEMENT Sciences Informatiques

Utilisation de ssh

Authentification par mot de passe (du compte utilisateur, ex. /etc/passwd)
Authentification par clef publique

- le client ssh crée une paire de clef (publique, privé)
- le serveur connait les clefs publiques des clients autorisés
- lorsque le client se connecte au serveur, le serveur lance un challenge au client pour vérifier son identité.
- si le challenge réussit, le client est connecté sans avoir besoin de s'authentifier par mot de passe.



DÉPARTEMENT
Sciences Informatiques

- Générer la clef : ssh-keygen -t dsa
- passphrase (optionnelle) : sert à fortifier la clef pour la rendre plus difficilement cassable.
  - si vous tapez une phrase, votre connection sera plus sûre, mais vous devrez utiliser ssh-agent pour ne pas avoir à la retaper à chaque fois (voir plus bas)
  - vous ne tapez pas de phrase (et appuyez seulement sur Enter), votre connexion sera moins sûre

DÉPARTEMENT
Sciences Informatiques

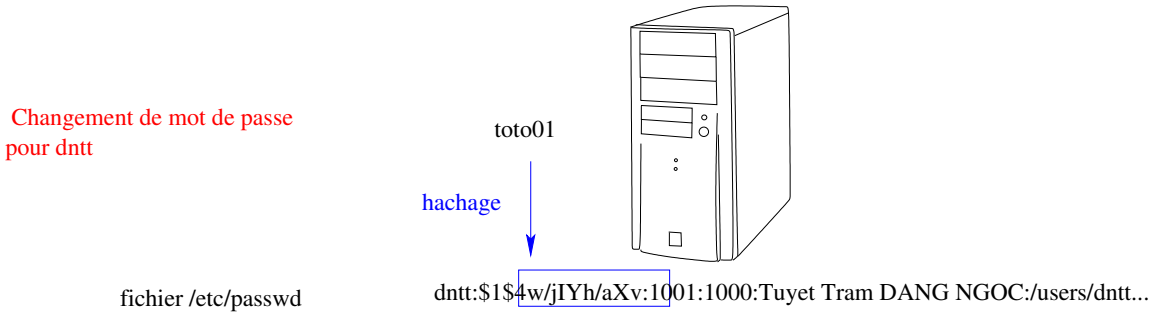
Le fichier /etc/passwd

Le fichier /etc/passwd est en lecture pour tous

```
root:8ofzSt0:0::Le chef:/root:/bin/sh
daemon:x:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:x:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:$1$4w/jIYh/aXv:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:$4$HUcta/uYY:1002:1000:Remy CARD:/users/card:/bin/csh
```

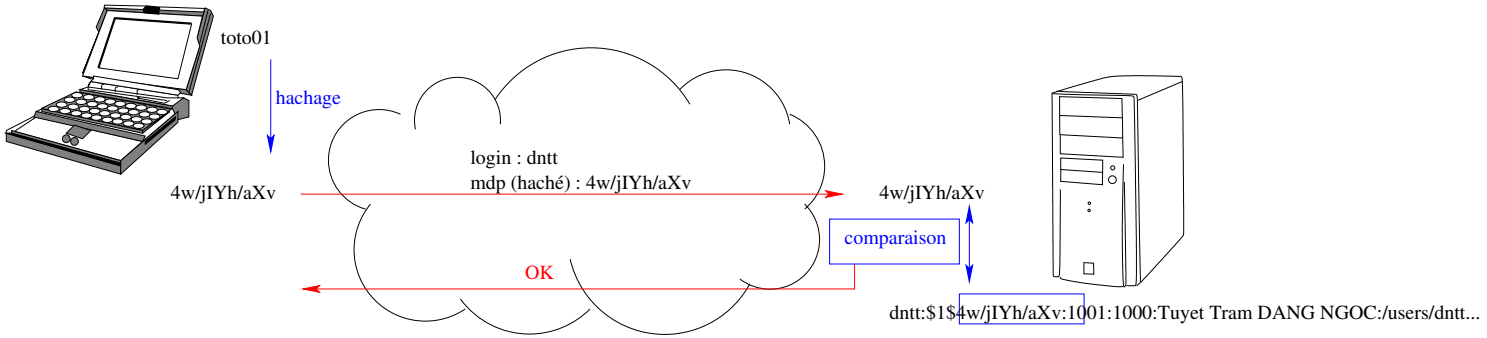
La méthode de hachage par défaut est DES, mais si précédé d'un $, la méthode de hachage sera définie suivant le code :

ID	Methode
1	MD5
2a	Blowfish
5	SHA-256
6	SHA-512



DÉPARTEMENT
Sciences Informatiques

Le fichier /etc/passwd



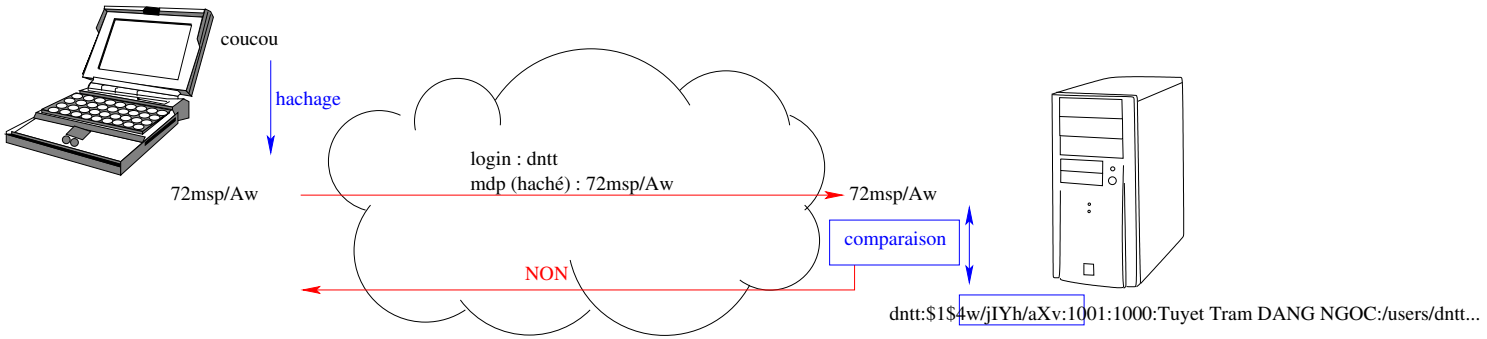
- Le mot de passe chiffré n'est pas déchiffrable ...
- ... mais une attaque brutale à base de dictionnaires peut aboutir (exemple : Crack)

Sous les systèmes récent, la liste des utilisateurs est décomposée en deux fichiers :

- /etc/passwd (sans mots de passe) lisible par tous
- /etc/shadow ou /etc/master.passwd (avec mots de passe) lisible par 'root' uniquement

DÉPARTEMENT Sciences Informatiques

Le fichier /etc/passwd



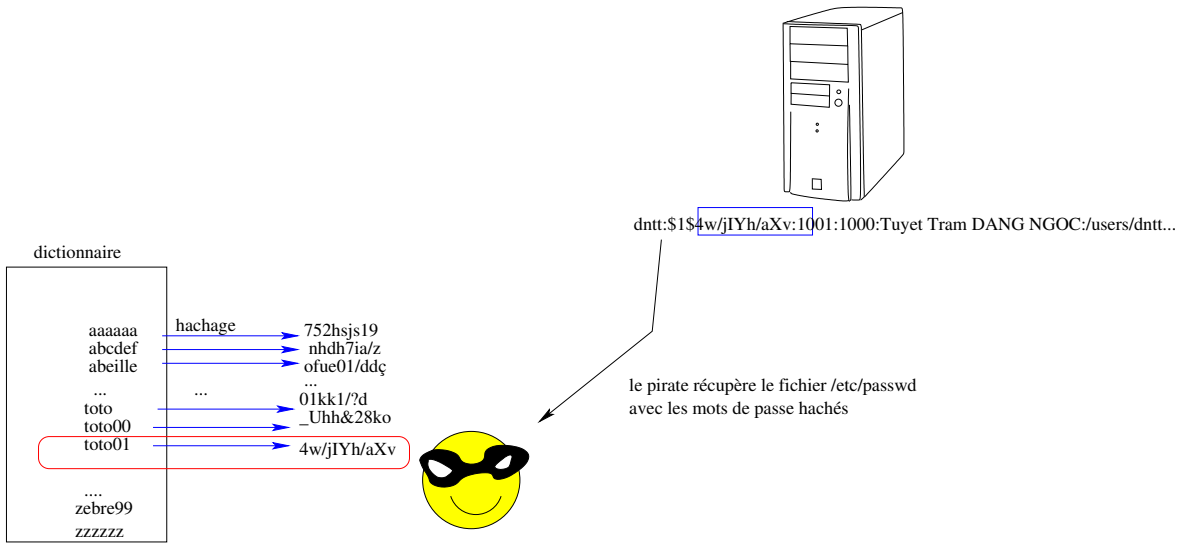
- Le mot de passe chiffré n'est pas déchiffrable ...
- ... mais une attaque brutale à base de dictionnaires peut aboutir (exemple : Crack)

Sous les systèmes récent, la liste des utilisateurs est décomposée en deux fichiers :

- /etc/passwd (sans mots de passe) lisible par tous
- /etc/shadow ou /etc/master.passwd (avec mots de passe) lisible par 'root' uniquement

DÉPARTEMENT Sciences Informatiques

Le fichier /etc/passwd



- Le mot de passe chiffré n'est pas déchiffrable ...
- ... mais une attaque brutale à base de dictionnaires peut aboutir (exemple : Crack)

Sous les systèmes récent, la liste des utilisateurs est décomposée en deux fichiers :

- /etc/passwd (sans mots de passe) lisible par tous
- /etc/shadow ou /etc/master.passwd (avec mots de passe) lisible par 'root' uniquement

DÉPARTEMENT Sciences Informatiques

Le fichier /etc/shadow (System V)

Fichier /etc/shadow (non lisible par les utilisateurs)

```
root:8ofzSt0:12982:0:99999:7:::
daemon:*:12957:0:99999:7:::
webmaster:*:13080:0:99999:7:::
dntt:$1$4w/jIYh/aXv:12977:0:99999:7:::
card:$4$HUcta/uYY:13140:28:30:7:14::
```

Fichier /etc/passwd (lisible par tous les utilisateurs)

```
root:x:0::Le chef:/root:/bin/sh
daemon:x:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:x:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:x:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:x:1002:1000:Remy CARD:/users/card:/bin/csh
```

DÉPARTEMENT Sciences Informatiques

Fichier /etc/master.passwd sous FreeBSD

Fichier /etc/master.passwd (non lisible par les utilisateurs)

```
root:8ofzSt0:0:0::0:0:Le chef:/root:/bin/sh
daemon:*:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster*:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:$1$4w/IYh/aXv:1001:1000::0:0:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin
card:$4$HUcta/uYY:1002:1000:xuser:13140:13168:Remy CARD:/users/card:/bin/cs
```

Fichier /etc/passwd (lisible par tous les utilisateurs) :

```
root:x:0::Le chef:/root:/bin/sh
daemon:x:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:x:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:x:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:x:1002:1000:Remy CARD:/users/card:/bin/csh
```

DÉPARTEMENT Sciences Informatiques

Un bon mot de passe

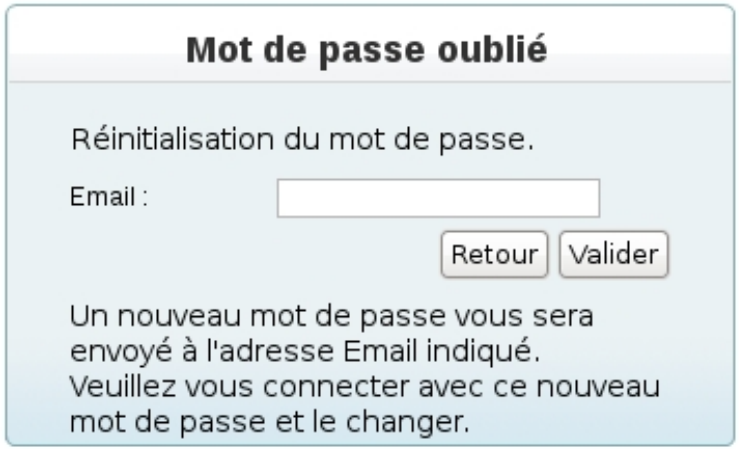
Un "bon" mot de passe doit être :

- composé de lettres majuscules, minuscules, de chiffres et de caractères spéciaux ;
- long (dans la mesure du possible) ;
- dénué de sens (les prénoms et noms propres célèbres sont abolis) ;
- renouvelé régulièrement.
- facile (pour l'utilisateur) à retenir (pour éviter de l'écrire)
- ne pas être le même sur tous les serveurs

DÉPARTEMENT
Sciences Informatiques

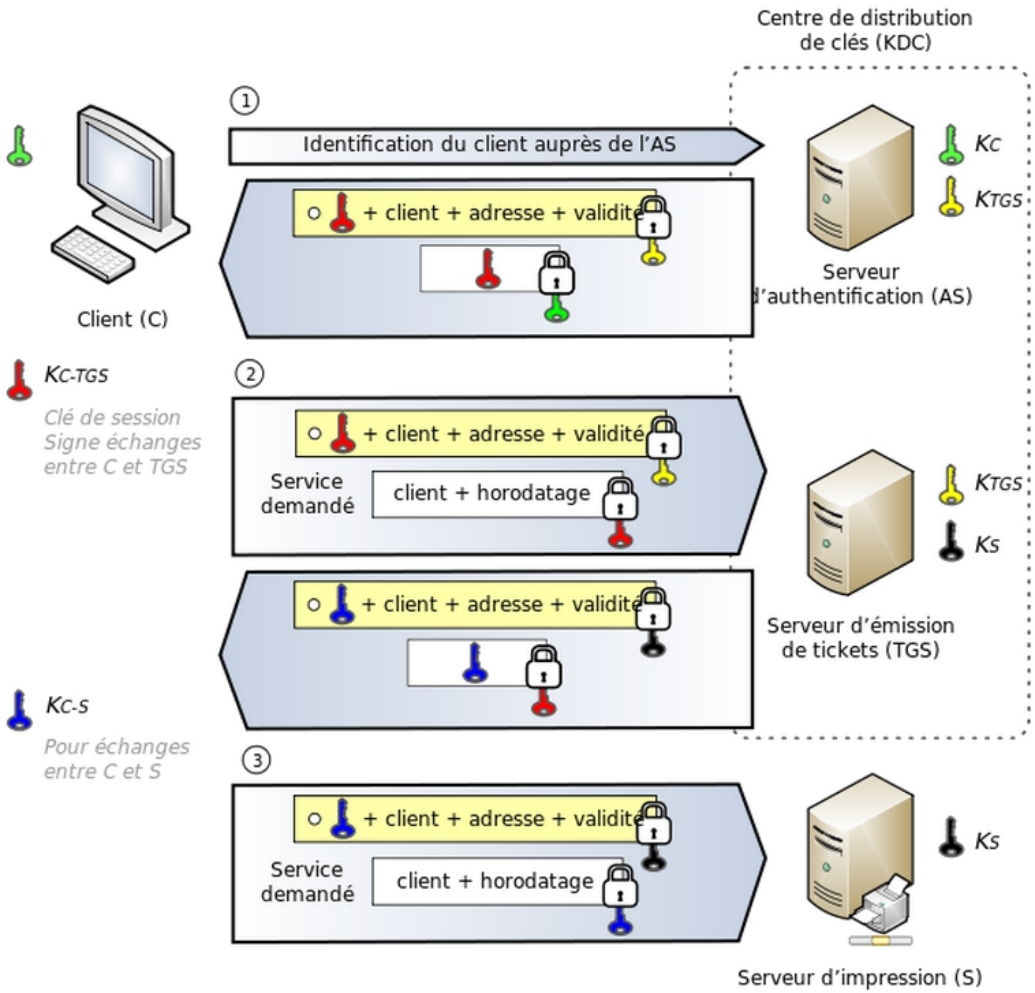
Mot de passe haché

- si système par clef publique/clef privé impossible, utiliser le système de stockage par mot de passe haché.
- personne, même l'administrateur ne devrait avoir à connaitre votre mot de passe
  -
- bannir les logiciels qui stockent les mots de passe de l'utilisateur en clair. Question : sur les sites suivants, lesquels stockent les mots de passe en clair, lesquel stockent le hachage ?



DÉPARTEMENT Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques



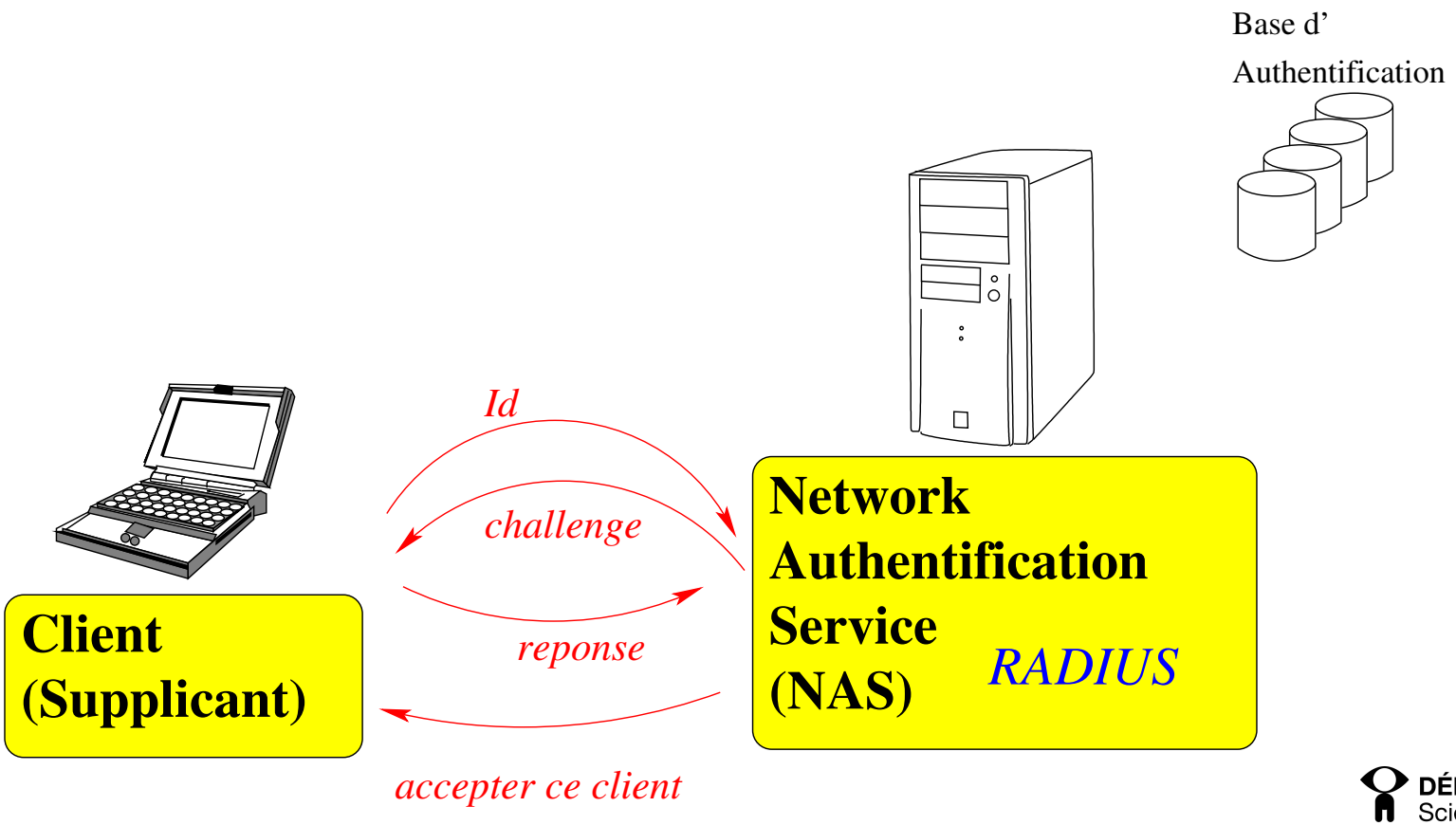
http ://fr.wikipedia.org/wiki/Kerberos

DÉPARTEMENT
Sciences Informatiques

DÉPARTEMENT
Sciences Informatiques

RADIUS

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Il permet d'authentifier un utilisateur souhaitant accéder à un réseau (filaire ou non) grâce à un serveur d'authentification.

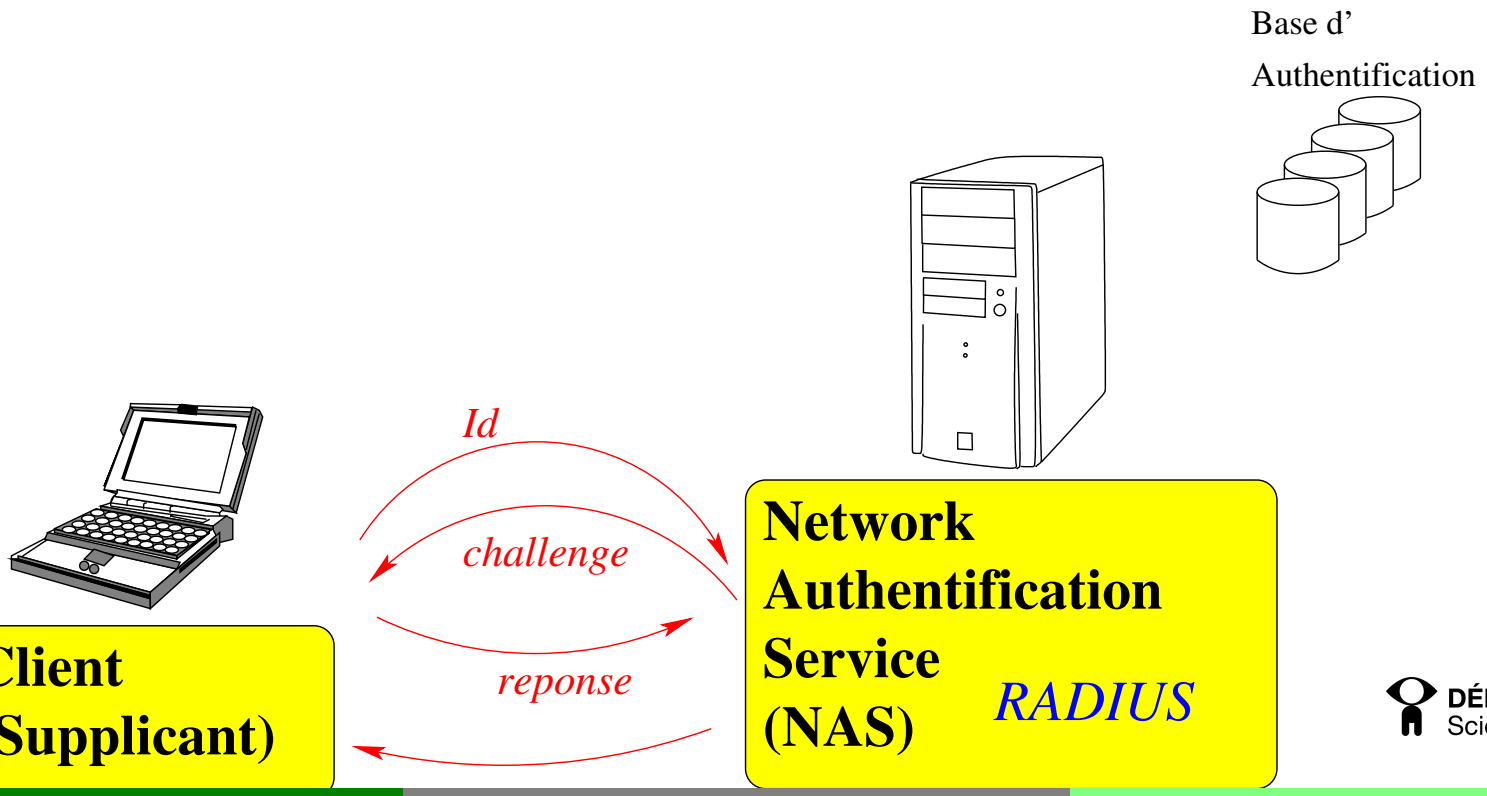


DÉPARTEMENT
Sciences Informatiques

RADIUS

Supplicant :

- boîtier d'accès distant (NAS : Network Access Server)
- un point d'accès réseau sans fil
- un pare-feu (firewall)
- un commutateur
- un autre serveur

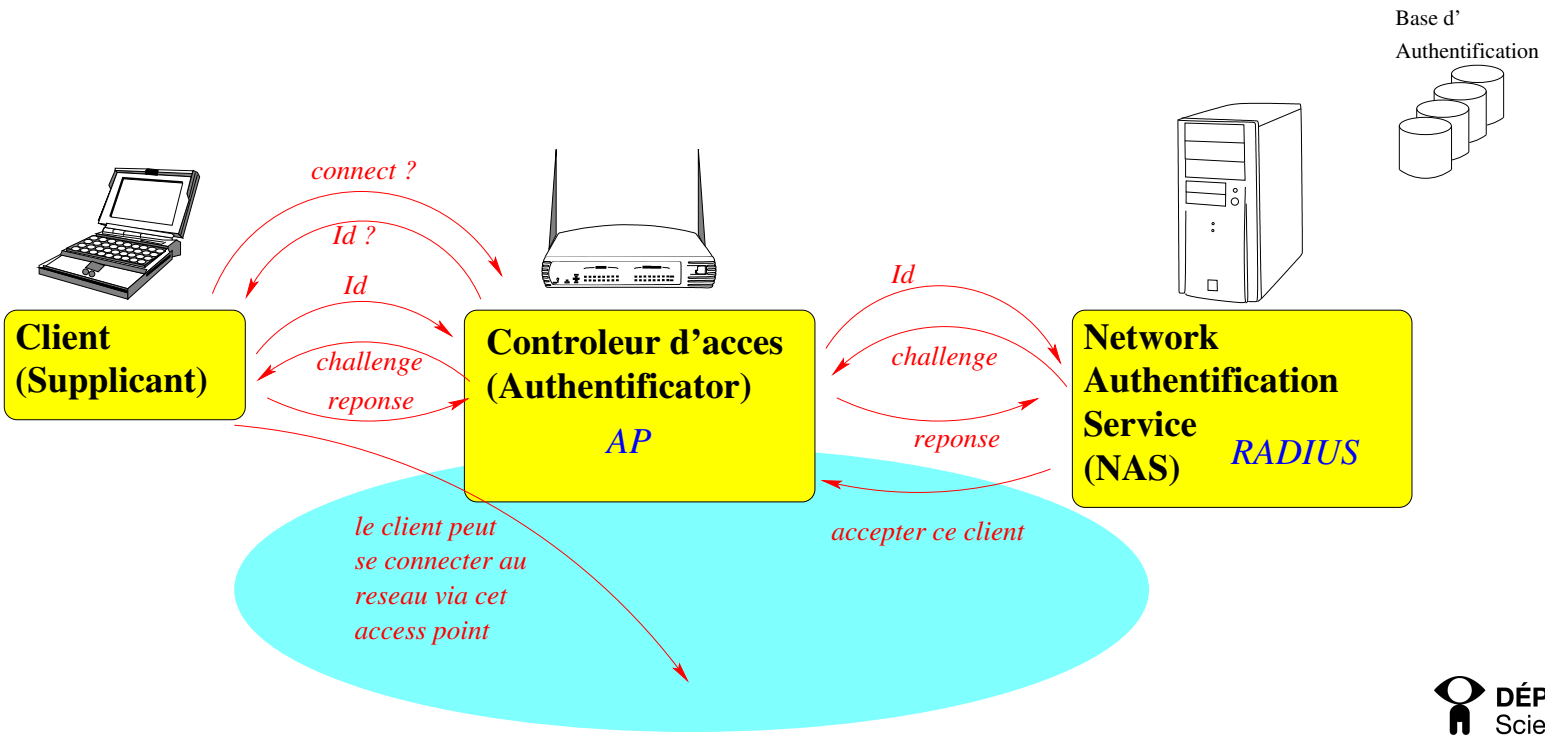


DÉPARTEMENT
Sciences Informatiques

RADIUS

Supplicant :

- boîtier d'accès distant (NAS : Network Access Server)
- un point d'accès réseau sans fil
- un pare-feu (firewall)
- un commutateur
- un autre serveur



DÉPARTEMENT
Sciences Informatiques

Radius : bases d'authentification

- fichier texte (users/mot de passe en clair)
- par adresse MAC
- annuaire LDAP
- base de données SQL (ex. MySQL, pgSQL)
- comptes d'utilisateur de machine ou de domaine
- un autre serveur RADIUS (chainage)

Radius gère également le 802.1X avec l'authenfication via tunnel EAP (PEAP/TLS/TTLS)

DÉPARTEMENT Sciences Informatiques

EAP

EAP (Extensible Authentication Protocol) est un protocole conçu pour étendre les fonctions du protocole Radius à des types d'identification plus complexes ; il est indépendant du matériel du client Radius et négocié directement avec le supplicant (poste client, terminal d'accès).

- LEAP (Cisco) : WEP dynamique, a été cassé
- EAP-TLS : basé sur SSL
- EAP-MD5 : peu utilisé
- EAP-PSK
- EAP-IKEv2
- PEAP (Cisco, Microsoft et RSA Sec.) basé sur TLS, chiffre les échanges EAP
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
- EAP-FAST (Cisco) : utilise PSK. sensible au man-in-the-middle
- EAP-TTLS (Funk Software) similaire à PEAP
- EAP-SIM
- EAP-AKA

DÉPARTEMENT Sciences Informatiques