



# Authentication

## Prouver qui on est

Thibaut HENIN

[tbowan@arsouyes.org](mailto:tbowan@arsouyes.org)

# Petite définition

Identification

« *Qui on est* »

Authentication

« Le prouver »

# Facteurs d'authentification

**Je sais**

(Mot de passe)

**Je suis**

(Biométrie)

**Je possède**

(Téléphone, carte à puce, ...)

**Je sais faire**

(Signature manuscrite)

# Méthode d'authentification

**Simple**

(1 facteur)

**Forte**

(au moins 2)

# Contextuelle

Adresse IP, HTTP Referer, HTTP Host, Cookies

N'est pas sûr

# Adresse IP

```
<VirtualHost *:80>

    ServerName  secured.example.com

    <Location />
        Require ip 87.98.129.198
        Require ip 192.168.0.0/24
        Require host trusted.example.com
        Require forward-dns other.example.com
        Require local
    </Location>

</VirtualHost>
```

# Géolocalisation

```
<VirtualHost *:80>  
  
    ServerName  secured.example.com  
  
    GeoIPEnable On  
    GeoIPDBFile /path/to/GeoIP.dat  
  
    <Location />  
        Deny from GEOIP_COUNTRY_CODE=CN  
        Deny from GEOIP_COUNTRY_CODE=RU  
    </Location>  
  
</VirtualHost>
```

# Limitations sur les adresses

Man In the Middle

IP & DNS Spoofing

Proxy sortant

En-tête « x-Forwarded-For »

Mise à jour des bases de données

# En-tête HTTP : HOST

```
<VirtualHost *:80>
```

```
    ServerName  intranet.example.com
```

```
    Require expr "%{HTTP_HOST} == 'intranet.example.com'"
```

```
</VirtualHost>
```

# En-tête HTTP : Referer

```
<VirtualHost *:80>  
  
    ServerName    intranet.example.com  
  
    Require expr  
        "%{HTTP_REFERER} -strmatch '*://%{HTTP_HOST}/*'"  
  
</VirtualHost>
```

# En-tête HTTP : User Agent

```
<VirtualHost *:80>
```

```
    ServerName  intranet.example.com
```

```
    Require expr "! %{HTTP_USER_AGENT} -strmatch '*NESSUS*'"
```

```
</VirtualHost>
```

# Cookies

```
<?php

function setAsAdmin() {
    $_COOKIES['admin'] = true ;
}

function isAdmin() {
    return @$_COOKIES['admin'] === true ;
}
```

# Limitations sur les en-têtes

Forgées par le client

# Secret partagé

Mots de passes, OTP, cryptographie

# Mot de passe

## Principe

Stockage « identifiant / mot de passe »

## Sécurité spécifique

Stockage & choix

# Stockage du mot de passe

**Défense en profondeur**

(en cas de compromission de la base)

**Assurer la confidentialité**

(même si la base est lisible)

# Stockage du mot de passe

Niveau 0

Attaque

En clair

Triviale

# Stockage du mot de passe

**Niveau 1**

Hacher le mot de passe

`sha512(password)`

**Attaque**

Dictionnaires

(dont google)

Rainbow tables

(dictionnaire compressé)

# Stockage du mot de passe

**Niveau 2**

Saler le mot de passe  
`sha512(sel + password)`

**Attaque**

Brute force  
(hashcat)

# Stockage du mot de passe

## Niveau 3

### Hachage ralenti

`Bcrypt(sel + password)`

`Password_hash(password)`

## Attaque

### Brute force

(hashcat mais bien plus lent)

# Choix du mot de passe

## Résistance au brute force

Quantité d'information (de Shannon, en bits)

## Limitations

Cognitives, psychologiques, ...

# XKCD

<p>MoT BASIQUE (EXISTANT) PEU COMMUN</p> <p>ORDRE INCONNU</p> <p>Trøub4dor &amp; 3</p> <p>MAJ? SUBSTITUTIONS COMMUNES CHIFFRE PONCTUATION</p> <p>(VOUS POUVEZ AJOUTER QUELQUES BITS EN PLUS DANS LA MESURE OÙ CE N'EST QU'UN DES QUELQUES FORMATS LES PLUS COMMUNS.)</p>	<p>~28 BITS D'ENTROPIE</p> <p><math>2^{28} = 3 \text{ JOURS À } 1000 \text{ ESSAIS/SECONDE}</math></p> <p><small>CATTARQUE PLAUSIBLE SUR UN SERVICE WEB FAIBLE ET ISOLÉ. OUI, CA VA PLUS VITE DE CRAQUER UNE FONCTION DE HACHAGE VOLÉE, MAIS C'EST PAS CE DONT UN UTILISATEUR NORMAL SE SOUCIE.</small></p> <p>DIFFICULTÉ À DEVINER: FACILE</p>	<p>C'ÉTAIT TROMBONE ? NON, TROUBADOUR. ET UN DES 0 ÉTAIT UN ZÉRO ?</p> <p>ET IL Y AVAIT DES SYMBOLES ...</p>  <p>DIFFICULTÉ À MÉMORISER: DIFFICILE</p>
<p>CHEVAL EXACT AGRAFE PILE</p> <p>QUATRE MOTS COMMUNS AU HASARD</p>	<p>~44 BITS D'ENTROPIE</p> <p><math>2^{44} = 550 \text{ ANS À } 1000 \text{ ESSAIS/SECONDE}</math></p> <p>DIFFICULTÉ À DEVINER: DIFFICILE</p>	<p>C'EST UNE AGRAFE À PILE</p> <p>EXACT!</p>  <p>DIFFICULTÉ À MÉMORISER: TU L'AS DÉJÀ RETENU</p>
<p>EN VINGT ANS D'EFFORTS, NOUS AVONS RÉUSSI À ENTRAÎNER TOUT LE MONDE À UTILISER DES MOTS DE PASSE QUI SONT DIFFICILE À MÉMORISER POUR LES HUMAINS MAIS FACILE À DEVINER POUR LES ORDINATEURS.</p>		

<https://xkcd.lapin.org/index.php?number=936>

# OTP - One Time Password

Mot de passe à usage unique

(dans la pratique, on génère une liste)

*e.g.* ENIGMA

# OTP - One Time Password

## Basés sur le temps

```
hash(graine + timestamp / interval)
```

## Liste chaînée

```
hash(precedent)
```

## Challenge / response

```
hash(graine + challenge)
```

# Sessions

Suivre une activité répartie sur plusieurs requêtes

# Sessions IP

« Identification Number »

(Défragmenter à l'arrivée)

# Sessions TCP

« sequence » et « ack number »

(Acquittement des messages reçus)

# Sessions TLS

**Session ID**

(paramètres déjà négociés)

# Sessions Web

Identifiant dans un cookie

(PHPSESSID, JSESSIONID, ...)

# Vulnérabilités spécifiques

## Stealing

(voler l'ID d'une victime)

## Guessing

(deviner l'ID d'une victime)

## Fixation

(forcer l'ID d'une victime)