

15 Authentication

Sessions, 2FA, délégation

Thibaut HENIN

www.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)

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)

Choix du mot de passe


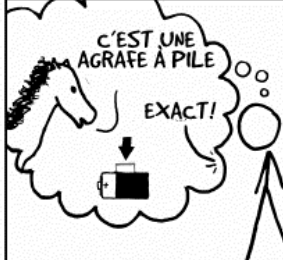
Résistance au brute force

Quantité d'information (de Shannon, en bits)

Limitations

Cognitives, psychologiques, ...

XKCD

<p>MoT BASIQUE (EXISTANT) PEU COMMUN</p> <p>ORDRE INCONNU</p> <p>Trøub4dor & 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>$2^{28} = 3 \text{ JOURS À } 1000 \text{ ESSAIS/SECONDE}$</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>$2^{44} = 550 \text{ ANS À } 1000 \text{ ESSAIS/SECONDE}$</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>

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.

<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)

Annuaire

Fournisseurs d'identités

(oauth, openid, kerberos, ldap, ...)

IAM

Identity and Account Management

(gestion des identités et des comptes)

Principes

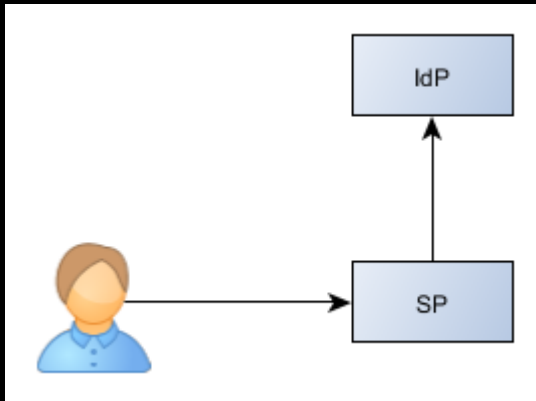
Fournisseur de Service

SP « Service Provider »

Fournisseur d'identité

IdP « Identity Provider »

Délégation



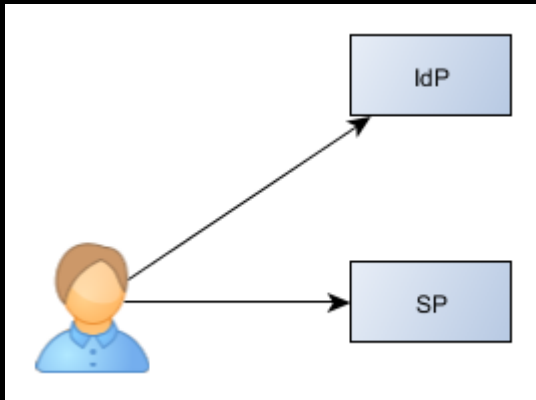
Base de donnée

.htpasswd, PHP + mySQL

Annuaire

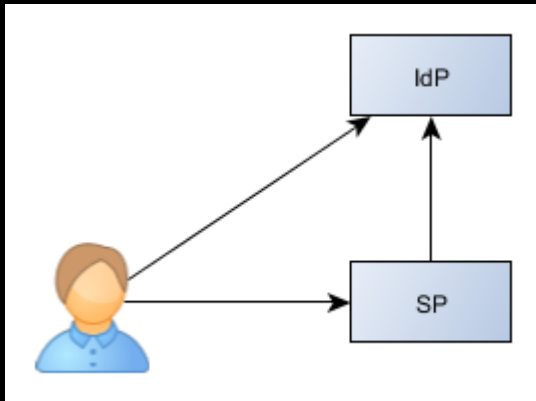
LDAP, Active Directory

Jeton et assertions



Kerberos
SAML

Principe

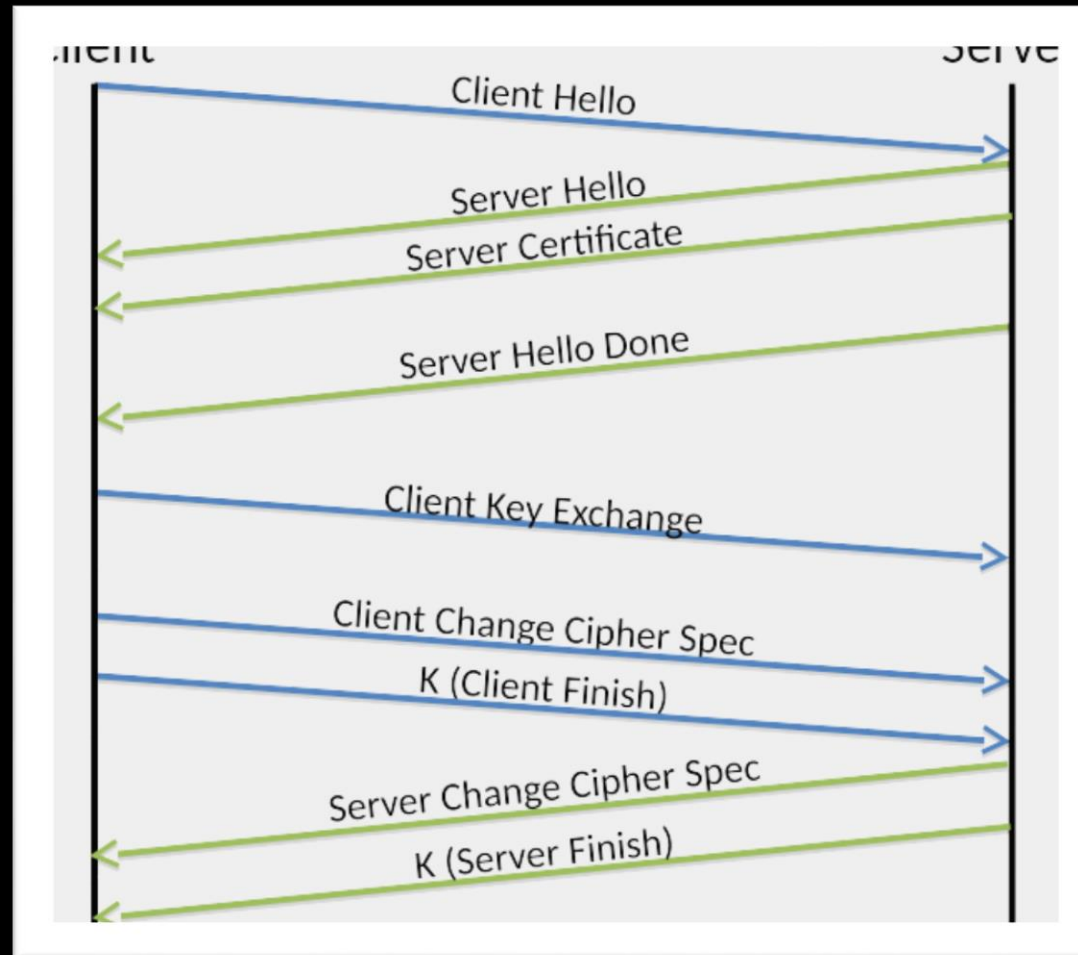


- Oauth
- OpenID
- Tiers de paiement en ligne

Authentication cryptographique

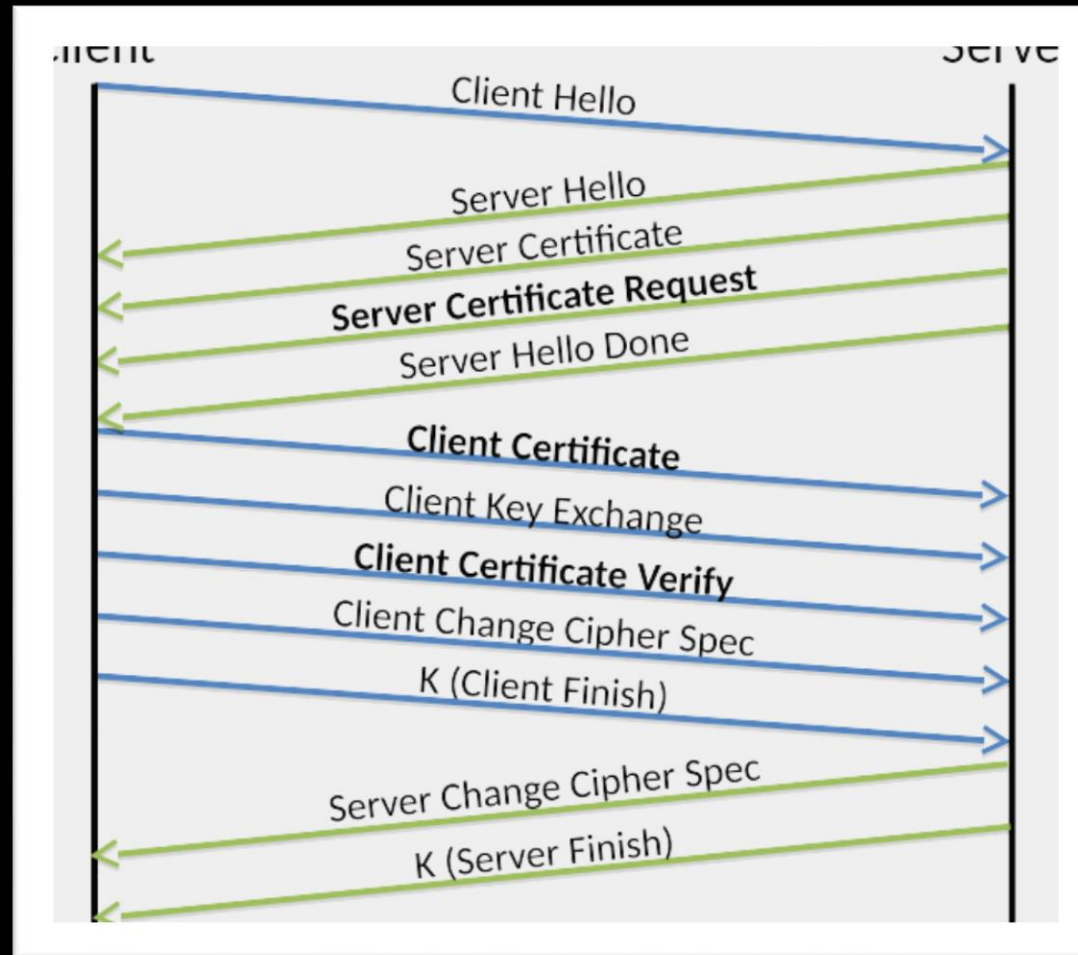
SSL/TLS, SAML, JWT

SSL/TLS : serveur



Source : <http://www.allanbank.com/blog/security/tls/x.509/2014/10/13/tls-x509-and-mongodb/>

SSL/TLS : mutuelle



Source : <http://www.allanbank.com/blog/security/tls/x.509/2014/10/13/tls-x509-and-mongodb/>

Signature des requêtes

SAML

Security assertion markup language

JWT

Json Web Token

Exemple SAML

```
<samlp:Response ...>
  <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
  <samlp:Status>...</samlp:Status>
  <saml:Assertion ID="pfxcaa3deda-f4a7-863c-5d83-b714652c352c" ...>
    <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#pfxcaa3deda-f4a7-863c-5d83-b714652c352c">...</ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>TYGJ1Z8+jGNpQuRcNAWTbk2.....En8IYtAUjsrSVsr4=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIICajCCAdOgAwIBAgIBAD.....Gyc4LzgD0CROMASTWNg==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>...</saml:Subject>
    <saml:AuthnStatement ...>...</saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```