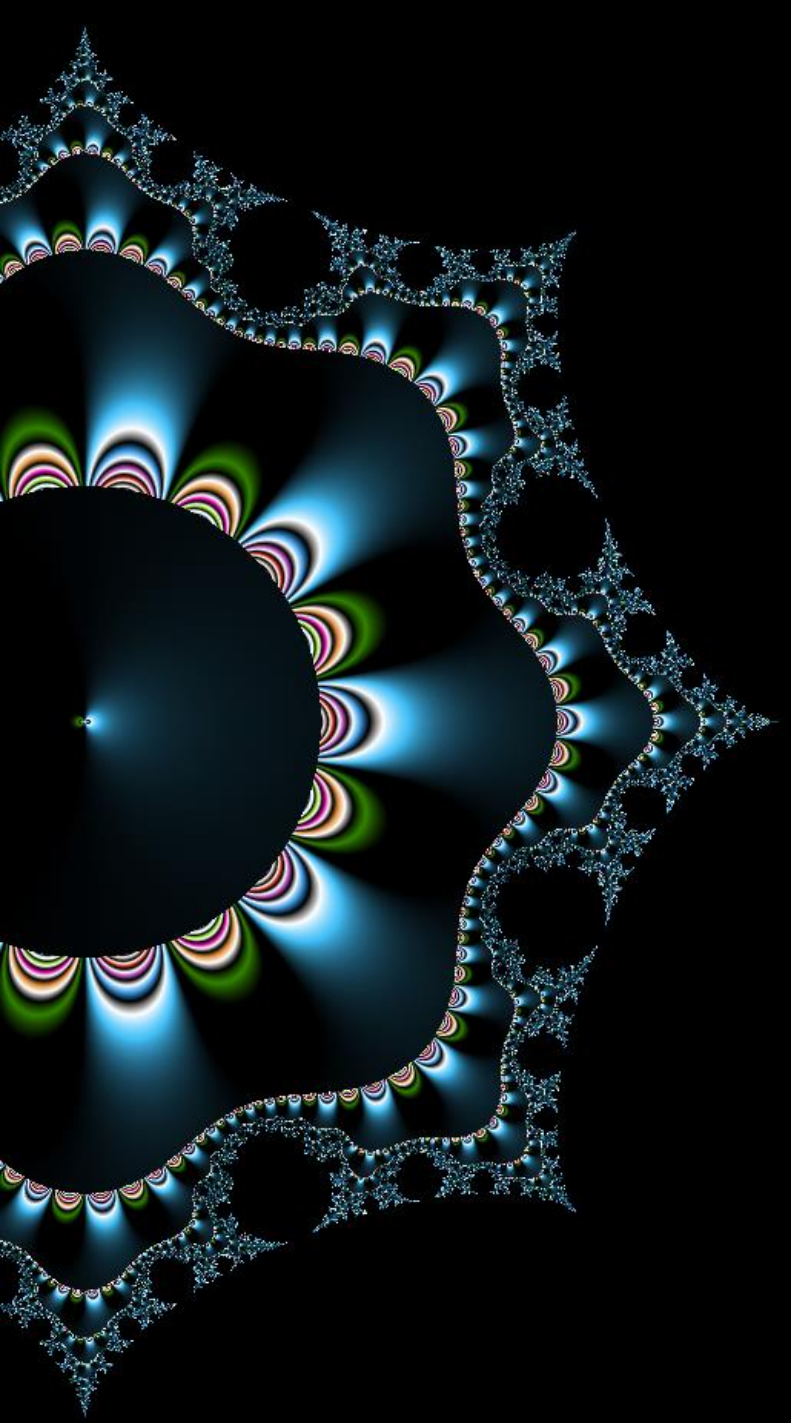


15 Authentification

Sessions, 2FA, déléguation

Thibaut HENIN

www.arsouyes.org

Petite définition

Identification

« Qui on est »

Authentification

« 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

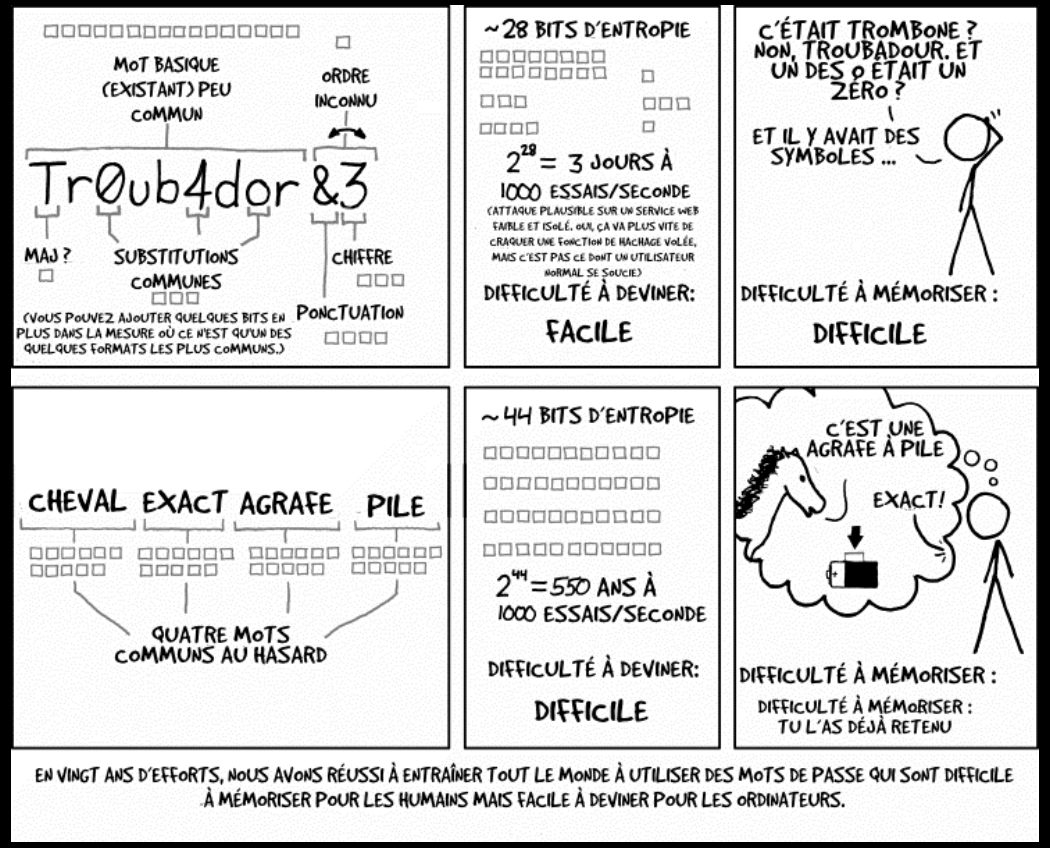
Résistance au brute force

Quantité d'information (de Shannon, en bits)

Limitations

Cognitives, psychologiques, …

XKCD



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 chainée

```
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, JSESSID, …)

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

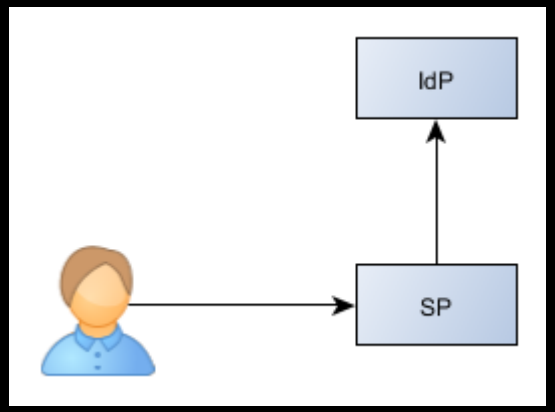
Fournisseur de Service

SP « Service Provider »

Fournisseur d’identité

IdP « Identity Provider »

Délégation



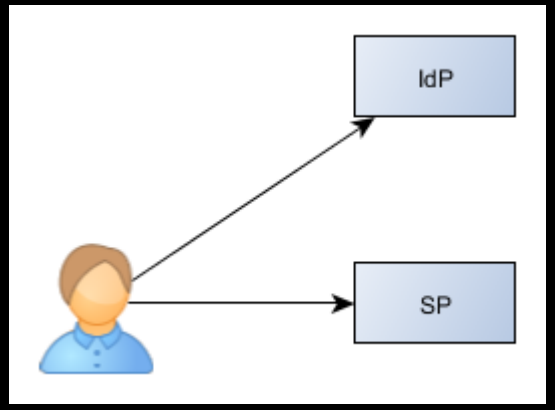
Base de donnée

.htpasswd, PHP + mySQL

Annuaires

LDAP, Active Directory

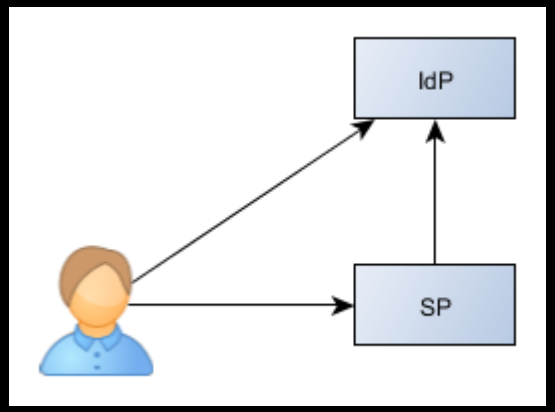
Jeton et assertions



Kerberos

SAML

Principe

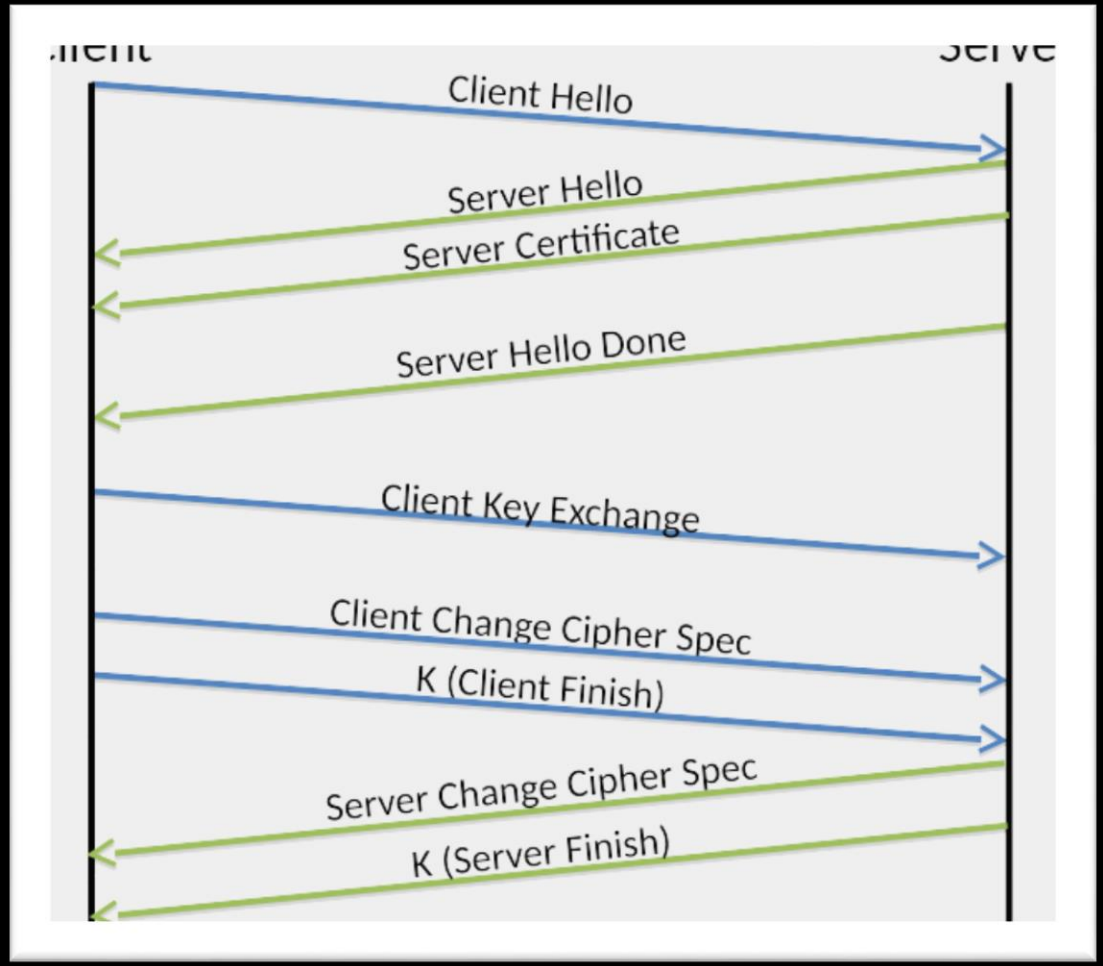


- Oauth
- OpenID
- Tiers de paiement en ligne

Authentification cryptographique

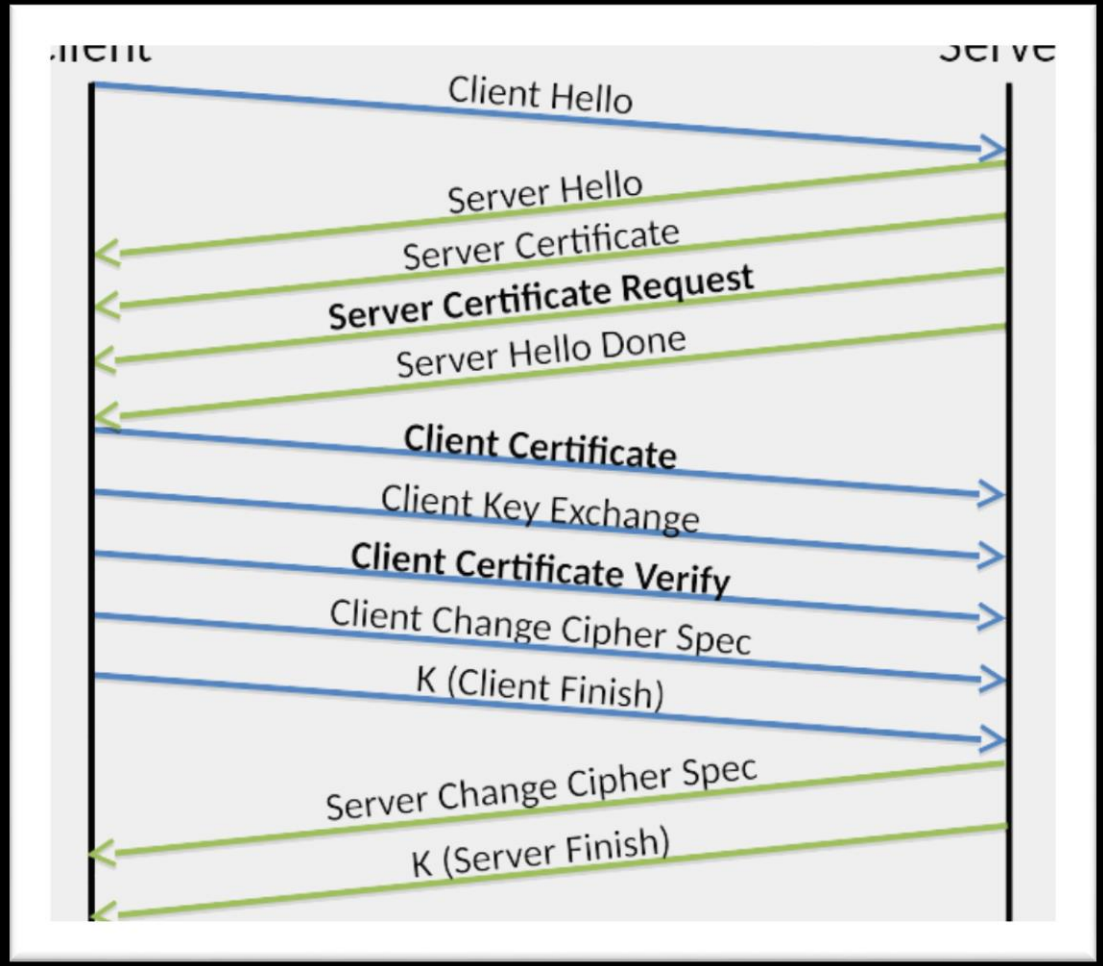
SSL/TLS, SAML, JWT

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>
```