CACHE + SSL/TLS

(@thierrymarianne | thierrym@theodo[point]fr)

Objectifs à atteindre

1. Mettre en cache du contenu dont la génération est coûteuse
2. Protéger les utilisateurs ayant accès aux ressources cachées

(@thierrymarianne | thierrym@theodo[point]fr)

Pourquoi une mise en cache des contenus ?

- HTTP 1.1 et son « Accélération » [RFC 2616]
- Plus grande capacité d'accueil des visites
- Meilleure tolérance aux pannes (relative)
- Réponses retournées plus rapidement

(@thierrymarianne | thierrym@theodo[point]fr)

Pourquoi sécurise-t-on le trafic ?

- Écoutes sur le réseau (MITM)
- Usurpation d'identité
- Altération des données échangées

(@thierrymarianne | thierrym@theodo[point]fr)

Toujours pas convaincu ?

(@thierrymarianne | thierrym@theodo[point]fr)

Comment se prémunir des risques ?

- Par le chiffrement des communications
- => Confidentialité des échanges
- => Authentification des interlocuteurs
- => Intégrité des données échangées

(@thierrymarianne | thierrym@theodo[point]fr)

Protocoles sécurisant HTTP

- ~~SSL v1.0, SSL v2.0~~
- SSL v3.0 [RFC 6101]
- TLS v1.0 [RFC 2246]
- TLS v1.1 [RFC 4346]
- TLS v1.2 [RFC 5246]

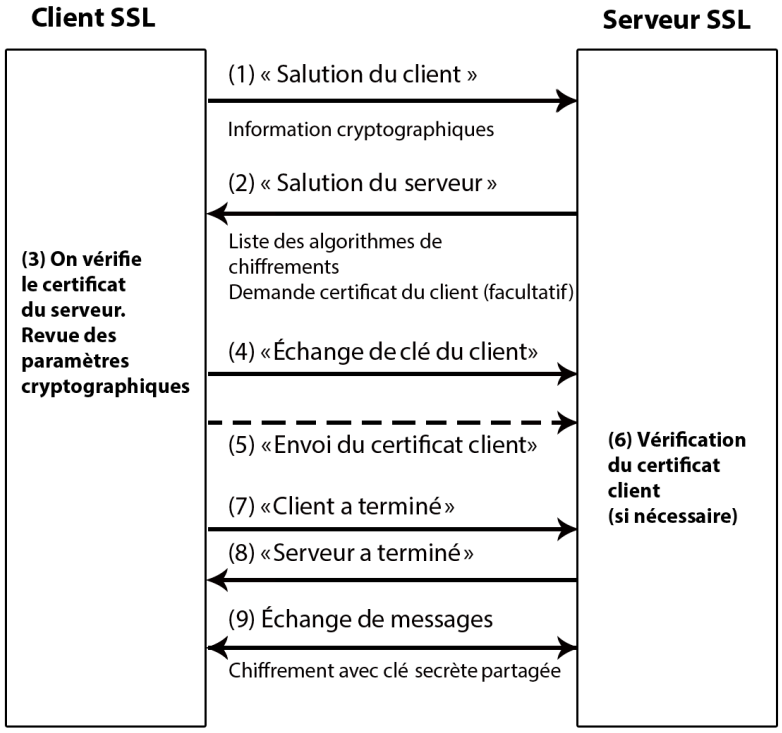
(@thierrymarianne | thierrym@theodo[point]fr)

Performances avec SSL ?

> *In January this year (2010), Gmail switched to using HTTPS for everything by default. [...]*
>
> *In order to do this we had to deploy no additional machines and no special hardware. [...]*
>
> *SSL/TLS is not computationally expensive any more.*
>
> ***Adam Langley***

(@thierrymarianne | thierrym@theodo[point]fr)

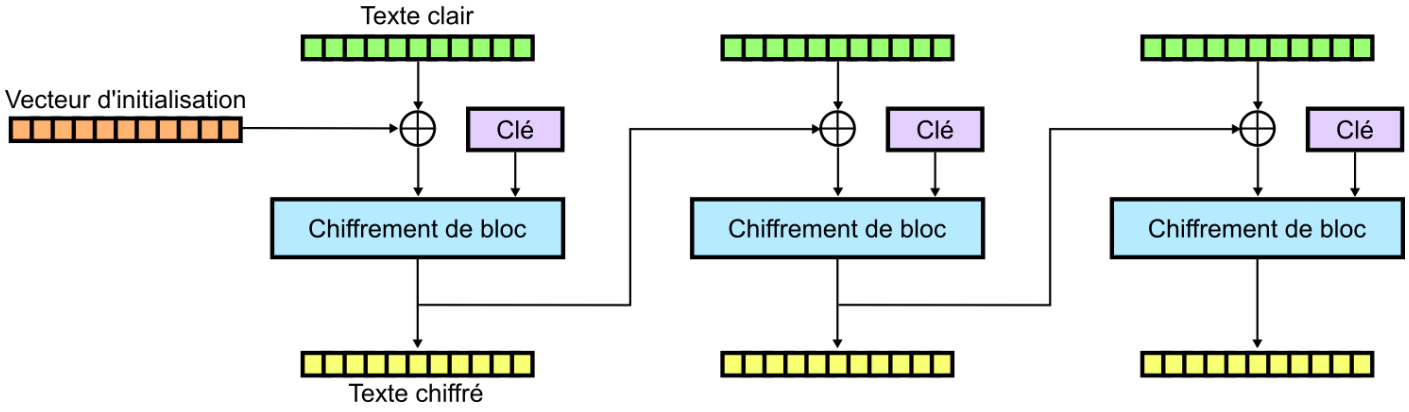
Handshaking



- Client
  - valeur pseudo-aléatoire
  - id de session
  - liste de chiffrements
- Serveur
  - valeur pseudo-aléatoire
  - id de session
  - certificat
  - liste de chiffrements

(@thierrymarianne | thierrym@theodo[point]fr)

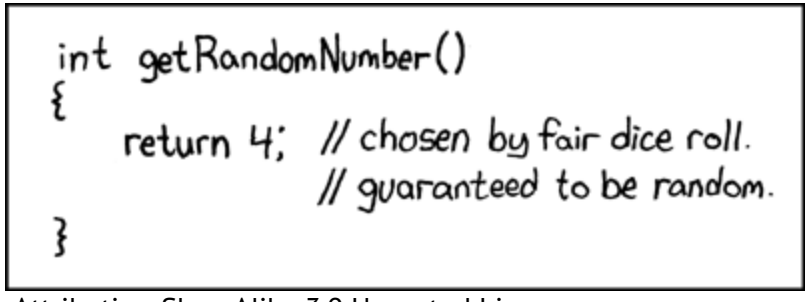
Chiffrement par bloc (CBC)



- Découpage des données
- Chiffrement des blocs
- *Exemple*: AES, Blowfish

(@thierrymarianne | thierrym@theodo[point]fr)

Chiffrement par flot

- Un générateur de nombres pseudo-aléatoires
- XOR entre bit de la sortie du générateur et un bit de la donnée
- Aucune contrainte sur la longueur des données
- *Exemple*:
  - RC4
  - 

(@thierrymarianne | thierrym@theodo[point]fr)

Vulnérabilités 1/4

- CRIME (Compression Ratio Info-leak Made Easy)
  - Détournement de session
  - Désactiver la compression SSL/TLS

(@thierrymarianne | thierrym@theodo[point]fr)

Vulnérabilités 2/4

- BEAST (Browser Exploit Against SSL/TLS)
  - Récupération du cookie de session
  - Utiliser RC4 comme chiffrement avec SSL v3.0 et TLS v1.0

(@thierrymarianne | thierrym@theodo[point]fr)

Vulnérabilités 3/4

- BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext)
  - Prolongement de l'attaque CRIME
  - Désactiver la compression HTTP pour diminuer les risques (solution la plus drastique)

(@thierrymarianne | thierrym@theodo[point]fr)

Vulnérabilités 4/4

- StripSSL / CSRF / XSS
- => HSTS (HTTP Strict Transport Security)

(@thierrymarianne | thierrym@theodo[point]fr)

Vulnérabilités 4/4

```
# Nginx
add_header Strict-Transport-Security max-age=63072000;

# Lighttpd
server.modules += ( "mod_setenv" )
$HTTP["scheme"] == "https" {
    setenv.add-response-header  = ( "Strict-Transport-Security" => "max-age=63072000")
}

# Apache
# Optionally load the headers module:
LoadModule headers_module modules/mod_headers.so
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"
```

Gnothi seauton (Know Thyself)

1. SSL Server Test (by SSL Labs)
2. Extension navigateur proposée par Netcraft

(@thierrymarianne | thierrym@theodo[point]fr)

Preuve de concept

1. Backend - Apache (2.2.22) + PHP (5.5) + Symfony (2.3)
2. Reverse proxy cache - Varnish (3.0.2)
3. SSL proxy - Nginx (1.4.2)
4. Nginx <--> Varnish <--> Apache

(@thierrymarianne | thierrym@theodo[point]fr)

Backend Server (Apache) 1/3

```
<VirtualHost 127.0.0.1:80>
  ServerAdmin host@ed-by.me
  ServerName 127.0.0.1
  DocumentRoot /var/www/symfony
  <Directory />
      AllowOverride None
  </Directory>
  ErrorLog ${APACHE_LOG_DIR}/error.symfony2.log
  CustomLog ${APACHE_LOG_DIR}/access.symfony2.log combined
  # Préparer vous au pire et à creuser
  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  # httpd 2.4.6
  # LogLevel debug
  # Loglevel alert rewrite:trace8
  # httpd 2.2
  # RewriteLog "/usr/local/var/apache/logs/rewrite.log"
  # RewriteLogLevel 9
</VirtualHost>
```


(@thierrymarianne | thierrym@theodo[point]fr)

Backend Server (Apache) 2/3

```
01.     <Directory /var/www/symfony2>
02.         AddCharset utf-8 .*
03.
04.         Order allow,deny
05.         # [2] Allow access from localhost only
06.         Allow from 127.0.0.1
07.         <IfModule mod_rewrite.c>
08.             RewriteEngine on
09.             RewriteCond %{REQUEST_URI}::$1 ^(/.+)/(.*)::\2$
10.             RewriteRule ^(.*) - [E=BASE:%1]
11.             RewriteCond %{ENV:REDIRECT_STATUS} ^$
12.             RewriteRule ^app\.php(/(.*)|$) %{ENV:BASE}/$2 [R=301,L]
13.             RewriteCond %{REQUEST_FILENAME} -f
14.             RewriteRule .? - [L]
15.             RewriteRule .? %{ENV:BASE}/app.php [L]
16.         </IfModule>
17.     </Directory>
```


(@thierrymarianne | thierrym@theodo[point]fr)

Backend Server (Apache) 3/3

```
01. # [1] Redirects to secured-front-server.net:443
02. # Nginx et Apache ne peuvent pas écouter sur le même port
03. <VirtualHost *:80>
04.     ServerAdmin host@ed-by.me
05.     ServerName ssl-termination.net
06.
07.     <IfModule mod_rewrite.c>
08.             RewriteEngine on
09.             RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [L]
10.     </IfModule>
11. </VirtualHost>
```


(@thierrymarianne | thierrym@theodo[point]fr)

Entêtes proxy SSL 1/2

- Trusting Proxies (doc Symfony2)

```php
<?php
// /web/app.php
// [...]
Request::setTrustedProxies(array('127.0.0.1'));
// [...]
$request->setTrustedHeaderName(Request::HEADER_CLIENT_PROTO, 'X-Proxy-Proto');
$request->setTrustedHeaderName(Request::HEADER_CLIENT_IP, 'X-Proxy-For');
$request->setTrustedHeaderName(Request::HEADER_CLIENT_HOST, 'X-Proxy-Host');
```


(@thierrymarianne | thierrym@theodo[point]fr)

Entêtes proxy SSL 2/2

```
01.     location / {
02.         add_header            Front-End-Https   on;
03.
04.         proxy_pass            http://127.0.0.1:8080;
05.
06.         proxy_next_upstream   error timeout invalid_header http_500 http_502 http_503 http_504;
07.
08.         proxy_set_header      Accept-Encoding   "";
09.         proxy_set_header      Host              $host;
10.         proxy_set_header      X-Real-IP         $remote_addr;
11.         proxy_set_header      X-Forwarded-For     $proxy_add_x_forwarded_for;
12.         proxy_set_header      X-Forwarded-Host    $host;
13.         proxy_set_header      X-Forwarded-Proto   $scheme;
14.
15.         proxy_hide_header     X-Varnish;
16.         proxy_hide_header     X-Powered-By;
17.         proxy_hide_header     Via;
18.
19.         proxy_redirect        off;
20.     }
```


(@thierrymarianne | thierrym@theodo[point]fr)

Forcer HTTPS avec Symfony2

```
01. # security.yml
02. # http://symfony.com/doc/current/cookbook/security/force_https.html
03. access_control:
04.     - path: ^/login
05.       roles: IS_AUTHENTICATED_ANONYMOUSLY
06.       requires_channel: https
07.
08. # routing.yml
09. # http://symfony.com/doc/current/book/routing.html
10. secure:
11.     pattern:  /secure
12.     defaults: { _controller: AcmeDemoBundle:Main:secure }
13.     requirements:
14.         _scheme:  https
```


(@thierrymarianne | thierrym@theodo[point]fr)

Forcer HTTPS avec Symfony2 ou pas

- Risques de boucles de redirection sous certaines conditions
- Varnish est seul à communiquer avec le backend sur 127.0.0.1:80

(@thierrymarianne | thierrym@theodo[point]fr)

SSL Proxy (Nginx)

```
01. server {
02.     listen      443;
03.     ssl         on;
04.     server_name ssl-termination.net;
05.     # [...]
06.
07.     ssl_certificate             /etc/ssl/private/signed-certificate.crt;
08.     ssl_certificate_key         /etc/ssl/private/private.key;
09.     # réduction des versions de SSL / TLS proposées par le serveur
10.     ssl_protocols               SSLv3 TLSv1 TLSv1.1 TLSv1.2;
11.     # réduction de la liste algorithmes de chiffrements proposés par le serveur
12.     ssl_ciphers                 RC4:HIGH:!aNULL:!MD5;
13.     ssl_prefer_server_ciphers   on;
14.
15.     keepalive_timeout    60;
16.     ssl_session_cache    shared:SSL:10m;
17.     ssl_session_timeout  10m;
18.     # [...]
19. }
```


(@thierrymarianne | thierrym@theodo[point]fr)

Compression déléguée au proxy SSL

```
01. server {
02.     // [...]
03.     gzip                on;
04.     gzip_disable        "msie6"; # Please, let it rest in peace
05.
06.     gzip_min_length     20;
07.     gzip_vary           on;
08.     gzip_proxied         any;
09.     gzip_comp_level     6;
10.     gzip_buffers        16 8k;
11.     gzip_http_version   1.1;
12.     gzip_types          text/plain text/css application/json application/javascript application/x-javascript \
                                  text/xml application/xml application/xml+rss text/javascript;
13.     // [...]
14. }
```


(@thierrymarianne | thierrym@theodo[point]fr)

Compression déléguée au Backend

```
01. # See also http://symfony.com/doc/current/cookbook/cache/varnish.html
03. sub vcl_recv {
04.
05.     if (req.http.Accept-Encoding) {
06.         if (req.url ~ "\.(jpg|png|gif|gz|tgz|bz2|tbz|mp3|ogg)$") {
07.             # No point in compressing these
08.             remove req.http.Accept-Encoding;
09.         } elsif (req.http.Accept-Encoding ~ "gzip") {
10.             set req.http.Accept-Encoding = "gzip";
11.         } elsif (req.http.Accept-Encoding ~ "deflate" && req.http.user-agent !~ "MSIE") {
12.             set req.http.Accept-Encoding = "deflate";
13.         } else {
14.             # unkown algorithm
15.             remove req.http.Accept-Encoding;
16.         }
17.     }
18.
19.     # [...]
20. }
```


(@thierrymarianne | thierrym@theodo[point]fr)

...ou au Reverse-Cache Proxy

```
01. sub vcl_fetch {
02.     if (req.url ~ "\.(css|js|min|)$") {
03.         set beresp.do_gzip = true;
04.     }
05.
06.     # ESI
07.     if (beresp.http.Surrogate-Control ~ "ESI/1.0") {
08.         unset beresp.http.Surrogate-Control;
09.         set beresp.do_esi = true;
10.     }
11. }
```

Conclusion 1/2

- Le monde (de la sécurité) n'est pas figé
  - ImperialViolet
  - GRC (Gibson Research Corporation)
  - TechSNAP
  - « Il était une fois SSL/TLS » par Benjamin Sonntag (co-fondateur de La Quadrature du Net) à la Cantine le 20 Septembre 2013

(@thierrymarianne | thierrym@theodo[point]fr)

Conclusion 2/2

- Rien ne vaut l'expérimentation !
  - Extensions PHP
  - CryptoJS
  - PyCrypto

(@thierrymarianne | thierrym@theodo[point]fr)

Une journée ne compte que 24h (approximativement)…

- Benchmarks (JMeter)
- Autres solutions de mise en cache nginx HttpProxyModule
- Autres solutions de chiffrement SSL/TLS stunnel

(@thierrymarianne | thierrym@theodo[point]fr)

Merci pour votre attention !

- Et merci à
  - L'AFSY
  - Yoopies
  - Theodo
  - @paulgreg & @michaelc

(@thierrymarianne | thierrym@theodo[point]fr)

Questions ?

(@thierrymarianne | thierrym@theodo[point]fr)

Sources

- https://www.trustworthyinternet.org/ssl-pulse/
- https://www.grc.com
- http://www.codinghorror.com/blog/2012/02/should-all-web-traffic-be-encrypted.html
- http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/
- http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html
- http://vincent.bernat.im/en/blog/2011-ssl-benchmark.html
- http://breachattack.com/
- http://news.netcraft.com/archives/2013/06/25/ssl-intercepted-today-decrypted-tomorrow.html
- https://raymii.org/s/tutorials/HTTP_Strict_Transport_Security_for_Apache_NGINX_and_Lighttpd.html
- https://github.com/nealharris/BREACH
- http://xkcd.com/221/
- http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/
- http://en.wikipedia.org/wiki/Certificate_authority
- http://en.wikipedia.org/wiki/Secure_Sockets_Layer
- http://en.wikipedia.org/wiki/Message_authentication_code
- http://en.wikipedia.org/wiki/Stream_cipher
- http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://speakerdeck.com/yassl/tls
- http://takingnote.blogs.nytimes.com/2013/07/18/yes-we-can-to-yes-we-scan/

(@thierrymarianne | thierrym@theodo[point]fr)