Lab 3: SSL/TLS + Heartbleed Bug

(Due 26 Feb at 23:59)

1. Overview

We have two sections for this lab. One is to review the SSL/TLS handshake through Wireshark pcap file. The other is to study the famous Heartbleed bug in SSL and try to fix it.

2. Section 1: Review the SSL/TLS handshake

Step 1: Download the 'trace-ssl.pcap' from eDimension

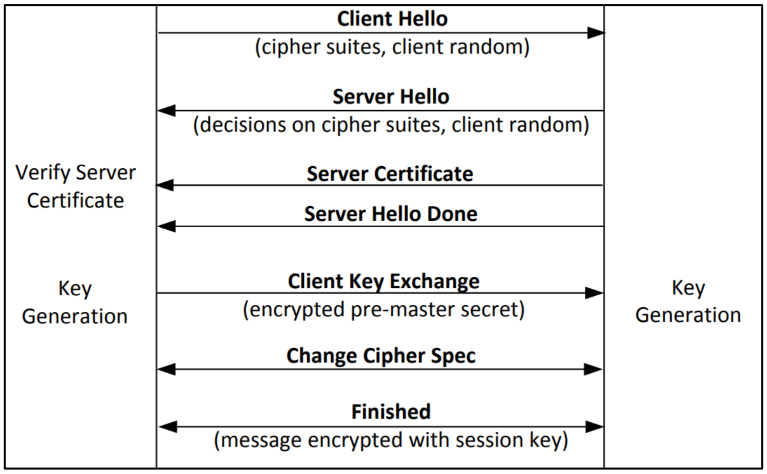
Step 2: Filter the 'ssl' packets, find the 'Application Data' & expand its Secure Sockets Layer block

Application Data is a generic TLS message carrying contents for the application, such as the web page. It is a good place for us to start looking at TLS messages. The lower layer protocol blocks are TCP and IP because SSL runs on top of TCP/IP. The SSL layer contains a "TLS Record Layer". This is the foundational sublayer for TLS. All messages contain records.

Q1: What's the Content-Type for a record containing "Application Data"?

Q2: What's the version of the TLS protocol?

Step 3: The SSL Handshake


Client Hello
(cipher suites, client random)
Server Hello
(decisions on cipher suites, client random)
Verify Server Certificate
Server Certificate
Server Hello Done
Key Generation
Client Key Exchange
(encrypted pre-master secret)
Key Generation
Change Cipher Spec
Finished
(message encrypted with session key)

3.1 Client Hello Messages

For these initial messages, an encryption scheme is not yet established so the contents of the record are visible to us. They contain details of the secure connection setup in a Handshake protocol format.

Q3: What are the time (GMT seconds since midnight Jan 1, 1970) and random bytes (size 28) which are used later to generate the symmetric encryption key?

Q4: What is the list of cipher suites, which dictate the key exchange algorithm, bulk encryption algorithm (with key length), MAC, and a psuedo-random function?

Q5: How is the compression methods set? Why is it set like that?

3.2 Server Hello Messages

Q6: What's the Cipher method chosen by the Server?

3.3 Certificate Messages

As with the Hellos, the contents of the Certificate message are visible because an encryption scheme is not yet established. It should come after the Hello messages. Note it is the server that sends a certificate to the client, since it is the browser that wants to verify the identity of the server. It is also possible for the server to request certificates from the client, but this behavior is not normally used by web applications.

Q7: What's the certificates messages in this step?

3.4 Client Key Exchange and Change Cipher Messages

The key exchange message is sent to pass keying information so that both sides will have the same secret session key. The change cipher message signals a switch to a new encryption scheme to the other party.

Q8: What's the Content-Type for Change Cipher Spec message?

Both sides send the Change Cipher Spec message immediately before they switch to sending encrypted contents. The message is an indication to the other side.

Q9: What's the Change Cipher Spec message? What's its size?

3. Section 2: The HeartBleed Bug

Referring to SeedLab document

Download the Ubuntu 12.02 VM and the attack file from
https://seedsecuritylabs.org/Labs_16.04/Networking/Heartbleed/