Norges teknisk-naturvitenskapelige universitet

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

TTM4100 – Kommunikasjon – Tjenester og nett

Praksisøving 4

Wireshark Lab: SSL Security

Denne praksisøvingen er én av sju praksisøvinger i emnet. Du må levere og få godkjent minst fire av disse praksisøvingene, og tilsvarende for teoriøvingene, for å kunne gå opp til eksamen. Hvis du lurer på noe angående øvingen kan du stille spørsmål på Piazza.

Lever svarene dine på spørsmålene under **som én PDF** på Blackboard. Inkluder forklarende skjermbilder dersom du ønsker det, men det er ikke påkrevd.

Innleveringsfristen er **søndag 07. mars 2021, kl. 23:59.**

This lab uses Wireshark. It is an open source packet analyser used for network troubleshooting, analysis, software and communications protocol development and, education. Wireshark can be downloaded from https://www.wireshark.org/#download.

The questions in this lab assignment are taken from the Wireshark Labs at http://www.pearsonglobaleditions.com/Sitemap/Kurose/. It contains questions from the SSL lab. Some of them have been updated, since there have been some changes in the use of SSL/TLS.

If you did not do the earlier Wireshark lab, you might have to look at the "How to Run Wireshark" section before starting this lab. You should read chapter 8.6 in Kurose and Ross: Computer networking a top-down approach before starting this lab.

SSL

Secure Socket Layer (SSL) is a way to provide a security service for TCP. All the popular browsers and server support some version of SSL/TLS. Transport Layer Security (TLS) is a modified version of SSL version 3. You can identify when SSL is being used by the https, rather than http in the beginning of the URL in your browser (Chrome, Safari and Firefox uses a green/grey padlock to show that a website uses https). SSL is used when sending credit card information over the Internet. In this lab, we are going to look at SSL by analyzing the beginning of purchasing something online.

Capture Trace

For this exercise, refer to the "SSL Lab" trace from Blackboard. There is a lot of excess traffic in this trace file, so be sure to sort on the "Protocol" column and use the "Info" column to find the packets in question.

Questions

SSL Record Types

1. For each of the first 6 SSL/TLS packets (consider the **client Hello** packet as packet number 1):
   i. specify the source of the packet (client or server)
   ii. list the SSL record types for the packet
   Answers for packet 1-6 should be on the form:
   "From client/server: record type(s) of packet"

2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is "content type" and has length of one byte. List all three fields and their lengths. To find the length of each field, mark it and look at the hexadecimal window.

Client Hello

3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?
4. The ClientHello record advertise the cipher suites it supports, a total of 13 plus reserved. Be sure to read page 664 in Top Down (7^{th}) to understand the cipher suite. In the first listed suite, what is:
   i. the public-key algorithm
   ii. the symmetric-key algorithm
   iii. the hash algorithm?

Client Key Exchange

5. Locate the client key exchange record. How long is the public key included in this record?

Application Data

6. Inspect the packets from the handshake to decide how the application data is being encrypted.
7. Do the records containing application data include a MAC?
8. Does Wireshark distinguish between the encrypted application data and the MAC?