TLS

CIS-3240 Homework #TLS

Peter Chapin, Vermont State University

This homework covers TLS. In the text TLS is covered in section ?. See also RFC-8446 [https://tools.ietf.org/html/rfc8446] for details about TLS.

The questions below are intended, in part, to force you to look at the TLS RFC and get experience with reading such documents.

1. When the TLS record protocol is using a block encryption algorithm, it must normally pad the last block in each record to make it the right size for the algorithm. Exactly how is that done? HINT: Look at section 5.4 of RFC-8446. Extra padding beyond what is necessary is allowed. Since extra padding increases the overall amount of data sent on the network without any additional information being sent, why might extra padding be used?

2. RFC-8446, Section 6.1 says that TLS connections are ended by the parties first exchanging "close_notify alert" messages. The RFC further comments that this is to prevent "truncation attacks". What is a truncation attack and how does the use of close alert messages avoid it?

3. It is possible to direct client HTTP traffic through a proxy server so that pages can be cached on an institution-wide basis. However, it is not possible to cache the data in a TLS connection in any useful way. Why not? Is it even possible to proxy TLS connections at all?

4. How does TLS protect against a replay attack? In other words, what stops an attacker from recording the outgoing client traffic during a legitimate connection and then connecting to the server and replaying the recorded client data? It is understood that the attacker won't necessarily understand the data being replayed, but in some cases that might not matter to them.