Experiment 2

Chinmay Parikh A059

Questions and Answers

1. What is the Content Type for a record containing Application Data?

   Ans: Application Data (23).

2. What version constant is used in your trace, and which version of TLS does it represent?

   Ans: TLS 1.0 (0x0301).

3. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data to allow the establishment of session keys.

   Ans: 28 bytes.

4. How long in bytes is the session identifier sent by the server? This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value.

   Ans: 32 bytes.

5. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

   Ans: TLS_RSA_WITH_RC4_128_SHA (0x0005).

6. Who sends the Certificate, the client, the server, or both? A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.

   Ans: Server.

7. Who sends the Change Cipher Spec message, the client, the server, or both?

   Ans: Both.

8. What are the contents carried inside the Change Cipher Spec message?

   Ans: The value `1` which signals a change in the communications protocol.

9. Explain minimum two attacks against SSL/TLS.

   Ans:

   A. Renegotiation attack – A vulnerability of the renegotiation procedure was discovered in August 2009 that can lead to plaintext injection attacks against SSL 3.0 and all current versions of TLS. For example, it allows an attacker who can hijack an https connection to splice their own requests into the beginning of the conversation the client has with the web server. The attacker can't actually decrypt the client-server communication, so it is different from a typical man-in-the-middle attack. A short-term fix is for web servers to stop allowing renegotiation, which typically will not require other changes unless client certificate authentication is used. To fix the vulnerability, a renegotiation indication extension was proposed for TLS. It will require the client and server to include and verify information about previous handshakes in any renegotiation handshakes. This extension has become a proposed standard and has been assigned the number RFC 5746. The RFC has been implemented by several libraries.

B. Beast Attack – On September 23, 2011 researchers Thai Duong and Juliano Rizzo demonstrated a proof of concept called BEAST (Browser Exploit against SSL/TLS) using a Java applet to violate same origin policy constraints, for a long-known cipher block chaining (CBC) vulnerability in TLS 1.0. Practical exploits had not been previously demonstrated for this vulnerability, which was originally discovered by Phillip Rogaway in 2002. The vulnerability of the attack had been fixed with TLS 1.1 in 2006, but TLS 1.1 had not seen wide adoption prior to this attack demonstration.