

CS393/CS682 Lab 5

Security Vulnerabilities in SSL/TLS

Introduction:

SSL/TLS is an application security protocol that is used widely to secure electronic transactions on the Internet. Although most of the protocol is secure, there have been several attacks on earlier versions of SSL (esp. SSL 2). This assignment has two goals:

- 1) Demonstrate truncation attack on *both* SSL2 and SSL3
- 2) Implement a test-bed and demonstrate the timing attack against CBC mode

Requirements:

Read and understand the following material:

- **SSL/TLS:** You must understand the differences between SSL3 and SSL2 connection termination sequences and how one would use a truncation attack effectively.
- **SSL Timing Attack:** A new timing attack on SSL/TLS was uncovered recently and a tool, named Omen, can be found at <http://omen.vuagnoux.com/> Familiarize yourself with the tool, how it works, why it works, and what type of network topology is required for the tool to work. Although it is optional to read the research paper, CBC Padding: Security Flaws in SSL, IPSEC, WTLS..., which describes the attack a light-reading of the paper is recommended for understanding the question. Paper can be found at: http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Vau01
- **SSL Tools:** Familiarize yourself with OpenSSL, stunnel, Omen
- **Use the man:** man is your friend. Do a man openssl, man stunnel etc. when you need help.
- **Hint:** For Part II, make sure you install proper version, the one with the bug, of OpenSSL.

Your Task:

Part I: Demonstration of Truncation Attack: (30 Points)

- 1) Explain in detail the differences between SSL3 and SSL2 termination sequences.
- 2) What is truncation attack? Give an example, where truncation attack would be very effective. Be precise in your description of the attack, explain which application is being attacked, how the victim perceives the attack etc. (Be creative in answering the second question but be practical.)
- 3) Does SSL3 prevent the attack? (Meaning you *cannot truncate the data* at all) If yes, describe a solution. If no, is it possible to detect the attack? Explain. (Explain how one can detect the attack or why one cannot detect the attack.)

4) Modify the program you wrote, henceforth referred to as *proggy*, for the first assignment such that it waits for a remote connection and when a connection is established (say, via `telnet`) it echoes the characters sent to it from the remote connection to the screen where *proggy* is running (not the remote screen, where you `telnet` from). Use `stunnel`, install it if necessary, so that an SSL connection can be established to *proggy* via port forwarding. See http://www.stunnel.org/examples/encrypt_services.html for details on how to do port forwarding via `stunnel`. Now that *proggy* is capable of using SSL connections install OpenSSL, if necessary, and use `openssl` command to establish a connection to *proggy* and test it thoroughly. Details about the topology of the network and where to install what are left out intentionally. (Hint: Obviously, you will need at least two machines for this assignment. One from which you establish the SSL connection, using `openssl`, and the other where *proggy* is listening via `stunnel`. Always compartmentalize your assignment and test if each step works.)

5) Once you are convinced *proggy* is accepting strings/key strokes via SSL demonstrate the truncation attack. Note that you must demonstrate the attack on **both SSL2 and SSL3**. Details of implementing truncation attack are left out intentionally. Include enough detail, including source code, screenshots, explanations, etc., to convince graders that you have implemented the attack (on both SSL2 and SSL3) properly.

Part II: Demonstration of Timing Attack: (20 Points)

1) Read the slides documentation about Omen, found at <http://omen.vuagnoux.com/>, (and the research paper, if necessary). Using two machines (from the testbed) assigned to you and an additional workstation (in the work-area) construct a network topology to exploit the Timing Attack. (Hint: You need one machine to run Omen, another providing IMAP services and a third one for mail-client.) Clearly mark which services are running on which machines and explain how the timing attack will proceed using these machines.

2) Setup all necessary machines and install all necessary packages on appropriate machines. Demonstrate the attack. Include screenshots of Omen in your answer, preferably with cracked password (for full credit). (Note that sometimes you may not be able to crack the password, in which case explain the reason. Attach a screenshot of Omen, which shows various messages of SSL session. See the Omen website for such an image.)

3) Explain the following:

- a. Explain Bleichenbacher attack. (Esp. the weakness that was exploited and how.)
- b. What was the weakness that led to the Timing Attack?
- c. What is the fix?