Assignment 2: Decrypting TLS and HTTP(S) using Wireshark++

Individual Assignment

PART-A: Decrypt TLS handshake and HTTPS messages between your browser and the web server of Bank X

- Set SSLKEYLOGFILE environment variable in your host OS by following the instructions given in References 1-3 and then launch Chrome browser with a blank tab (for surfing the website of bank x) and wireshark (for capturing all the messages exchanged between your browser and bank website/DNS resolvers/CAs).
- Start packet capture in wireshark
- Type in the hostname of the bank X in the address bar of the browser. Let N be your (RollNo % 3 +1). If N==1, X=ICICI. If N==2, X=HDFC. If N==3, X=SBI.
    a. Click on the link that takes you to the online net banking page of the bank.
    b. Enter some arbitrary values against Username and Password so that the login process fails.
    c. Stop the packet capture in wireshark and save it as <RollNo-BankName.pcap>. And also close your browser tab.
    d. Follow the steps in References 1-3 to specify the complete path of SSLkeyLog file in your computer for wireshark to decrypt TLS and HTTPS messages present in <RollNo-BankName.pcap>.
        i. Note that <RollNo-BankName.pcap> should only contain the messages exchanged between your browser and bank website/DNS resolvers/CAs. So, close all background Apps running on your computer to avoid capturing their messages in your wireshark capture. **This is Deliverable-1.**
        ii. Before providing session keys in SSLkeyLog file to wireshark, you should find that all of application traffic (HTTPS) is encrypted and shown as TLS traffic with encrypted application data. Get a snapshot of it. **This is Deliverable-2.**
        iii. After providing session keys in SSLkeyLog file to wireshark, you should find that all of application traffic is decrypted and shown as HTTP traffic along with TLS handshake messages in plain-text. Get a snapshot of it. **This is Deliverable-3.**

Answer the following queries by referring to the (decrypted) messages in your browsing session with the banking site using wireshark GUI. It is important to keep in mind that an Ethernet frame may contain either a partial, one or more TLS records. This is very different from HTTP(S), for which each Ethernet frame contains either one complete

HTTP message or a portion of a HTTP message.

Whenever possible, when answering the questions given below, you should produce a screenshot of the packet(s) within the trace that you used to answer the question asked. Highlight portions of the snapshot to explain your answer. To print a packet in wireshark GUI, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

1. What browser did you use, what's the version number?
2. List out various protocols that you noticed in the column named "Protocol" in the wireshark GUI from the time you keyed in the hostname of the bank in the browser till you start viewing application data. For each such protocol, mention its purpose in brief.
3. Each of the TLS records begins with the same three fields (with possibly different values). One of these fields is "content type" and has a length of one byte. List all three fields and their lengths for the first 10 records in the trace.
4. Cipher Suites in ClientHello Record: Look at the first two cipher suites offered by the client and compare them. What cipher suite the server selected?
5. What is the SNI value in ClientHello Record? What's its purpose? In other words, why is the client advertising it to the server?
6. What is the ALPN value(s) in ClientHello Record? What's its purpose? Which one the server selected?
7. Does ClientHello Record contain the Signature_algorithms extension? What's its purpose?
8. Does the client offer any key share and PSK in ClientHello Record?
9. What TLS versions your browser/client is supporting? Which one the server selected?
10. Look at Certificate Record from the server to the client: How many certificates did the server return and how are they related?
11. Comment on the key exchange algorithm agreed upon, what are the parameters that got exchanged between client and server to derive the session keys.
12. Which certificate type (DV/OV/EV) the bank is using?
13. Which certificate type (single or multi-domain or wild-card) the bank is using?
14. How can the client check whether the certificate is revoked or not: OCSP/CRL? Did OCSP stapling supported by the server?
15. How many log servers logged the certificate of the bank? What role does the log server play in Web PKI ecosystem? Refer: SCT extension.
16. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?
17. Look at various keys logged in the file pointed to by the SSLKEYLOGFILE environment variable in your host OS and describe their usage. Also comment on how they are derived from nonces and other parameters. Which entity in your system does this job on-the-fly?
18. What is the duration of HTTPS session, how many IP packets exchanged in the

browsing session (starting from the first TCP SYN packet till TCP FIN packet)?

19. How many HTTP request/response packets exchanged in the browsing session? Identify the packet(s) that carried the response that included Netbanking LOG-IN page of the bank. Do these response messages carry any security related directives like XSS, sameorigin, HSTS?
20. Identify the HTTP packet(s) that carried LOG-IN credentials supplied by you. Look at the raw bytes displayed in the wireshark GUI and identify strings that carried your LOG-IN credentials. Did you able to find boh user id and password in the raw packet capture?
    a. It's important that you only keyed in some arbitrary user id and password as part of this assignment for more safety!
21. Generate SSL report of the bank using SSL Server Test (Powered by Qualys SSL Labs) and summarize what security features are implemented by the bank's web server for improved online banking by its customers.
22. Comment on and explain anything else that you found interesting in the trace.

Note 1: Bonus 20 marks if you complete TLS and HTTPS decrypting using openssl and shell scripting. Make sure your code is well documented.

Note 2: Add screenshots of relevant in your report in order to prove that the capture trace used for analysis is indeed of your own!!

PS: What's Wireshark++? Wireshark + Key log file!

Deliverables in GC as a tar ball:

- A readable PDF Report with name "TLSAsg-<RollNo>.PDF"
- Deliverables 1-3 (refer page-1 of the assignment)
- SSL Key Log File
- Shell scripts written for openssl based decrypting of TLS and HTTPS session (optional)

References:

1. **Article: K50557518 - Decrypt SSL traffic with the SSLKEYLOGFILE environment variable on Firefox or Google Chrome using Wireshark (f5.com)**
2. **Wireshark Tutorial: Decrypting HTTPS Traffic (Includes SSL and TLS) (paloaltonetworks.com)**
3. **Decrypting TLS Streams With Wireshark: Part 1 | Didier Stevens**
4. **http://www.motobit.com/util/base64-decoder-encoder.asp**
5. **SSL Server Test (Powered by Qualys SSL Labs)**

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.

Name:
Date:
Signature: <keep your initials here>

Late Policy:

10% cut in marks for each late day