Assignment 1 – Network security protocols

Assignment reports must be submitted by ***Thursday, August 12, 2021****.*

Assignment Description

In this assignment you will carry out exercises related to the CryptoWorks21 lectures on network security protocols. You will send a secure email, and investigate different network security protocols.

Assignment Requirements and Setup

You will need to use the Kali and SEED Linux virtual machines in this assignment. If you have not downloaded and installed it yet, please check the "Lab 0" document available on Avenue to Learn. These virtual machines will need to be configured to communicate with each other via the "NAT Network" configuration in VirtualBox. Please see the Lab 0 instructions to achieve this.

To Hand In

Answer the questions labelled "1-1", "1-2", etc. For some questions, you will be asked to include a screenshot so that we can check your answers.

1 Secure email – PGP

PGP is one tool for sending digitally signed and/or encrypted email. In this section, you will install GPG (an open source version of PGP) and use it to send a signed/encrypted email.

You will need to use a desktop mail program, as opposed to webmail. If you do not already have a desktop mail program set up, one popular open-source cross-platform program is Mozilla Thunderbird (https://www.mozilla.org/en-US/thunderbird/). You can set it up to connect to your UWaterloo email account using the IMAP protocol using the instructions here: https://uwaterloo.ca/information-systems-technology/services/student-email/mailservices/set-up.

PGP is not built into any mail programs, so you will need to install an add-on in order to be able to use it. There are add-ons available for most major email programs:

- Mozilla Thunderbird: https://addons.mozilla.org/en-US/thunderbird/addon/enigmail/

- Microsoft Outlook: https://www.gpg4win.org/
- Apple Mail: https://gpgtools.org/gpgmail/

Your task is to (i) install PGP, (ii) generate a public key / private key pair for yourself, and (iii) send me a signed and encrypted email. You can find instructions for doing most of this in Thunderbird here: https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages If you use a different mail program, it should be possible to adapt most of those instructions to the interface of your program.

In order to be able to encrypt a message for me, you will need to use my PGP public key, a copy of which can be found on my website: https://www.douglas.stebila.ca/about/contact/

1-1. **[1 mark]** Send me a signed and encrypted email at dstebila@uwaterloo.ca. Please put "CryptoWorks21 encrypted email LASTNAME, FIRSTNAME" in the subject line. I will reply confirming that I received it.

1-2. **[1 mark]** If I receive your signed email, do I really have any assurance that it's coming from you? Why or why not?

1-3. **[1 mark]** Are you assured that only I can read your email? Why or why not?

After completing this assignment, you may or may not want to continue using PGP in your email. Personally, I do not send signed emails very often, unless I know the person I'm communicating with also uses PGP. (People who don't use PGP will see extra junk when they look at a PGP-signed message; see for example the difference when you look at the message in the Gmail interface.) Note as well that in some jurisdictions, a digital signature on an email can be considered a legal signature (https://en.wikipedia.org/wiki/Electronic_signatures_and_law).

2 Inspect certificate in your web browser.

In this section, you will examine the operation of the Transport Layer Security (TLS) protocol as well as configure public key authentication in SSH.

Visit an encrypted webpage using the Firefox web browser[1], for example, https://www.uwaterloo.ca/. Click on the security icon in your web browser's location bar.

1-4. **[2 marks]** What TLS ciphersuite was used? Which encryption algorithm was used to provide confidentiality of application data? Include a screenshot.

[1]Different browsers show different information. Firefox and Opera often show the most detailed information, including information on the server's certificate and the encryption mode used. (Google Chrome has, for some reason, reduced the amount of information they show.)

Take a look at the certificate.

1-5. **[2 marks]** Who is the certificate authority that issued the certificate? What type of validation did the certificate authority use? Include a screenshot.

3 Use Wireshark to examine an HTTPS connection.

The Wireshark packet capture software is installed in your Kali Linux virtual machine. Launch Wireshark by going to Applications → Sniffing & Spoofing. Initiate a packet capture on your main outgoing network interface, which is probably `en0` or `eth0`.

Visit an unencrypted webpage in your web browser, then visit an encrypted web page. Switch back to Wireshark and stop the packet capture.

You can now filter the Wireshark packet capture to see what the network traffic looks like. If you filter for `http`, you should see the various connections that were made to the unencrypted website. If you filter for `ssl`, you should see the various connections that were made to the encrypted website. You will see the various TLS messages sent (`ClientHello`, `ServerHello`, etc.) and you can drill down to the see the contents of those messages in the bottom half of the Wireshark window.

1-6. **[2 marks]** Which TLS message do you look in to see which ciphersuite was negotiated? For your connection, which ciphersuite was negotiated? Include a screenshot.

Notice as well that you cannot read the body of the requests that were sent to the encrypted website. They only appear as `Application data` in the TLS filter. This is all that an eavesdropper on the Internet would see.

4 Choosing network security protocols

Suppose that you are responsible for designing a secure Internet banking application. You have been asked to consider basing security on one of three security protocols: (i) HTTP with "basic access authentication"[2]; (ii) TLS; (iii) IPSec.

Consider each of these protocols in turn to answer the following questions:

1-7. **[1 mark]** Does HTTP basic access authentication provide the required security services? Explain your answer.
1-8. **[1 mark]** Does TLS provide the required security services? Explain your answer.
1-9. **[2 marks]** Does IPsec provide the required security services? What IPsec architecture would be suitable? Why is this choice not widely used in practice?

[2] https://en.wikipedia.org/wiki/Basic_access_authentication