CHAPTER 32

Lab Assignments for Chapter 32

We have created three lab assignments for this chapter: Lab32-1, Lab32-2, and Lab32-3. We have also included three lab-report sheets, which means that each lab should be reported in a separate sheet. It is assumed that you have done the lab assignment for Chapter 1, which told you how to install the Wireshark software and how to use it.

The first two assignments use security at the transport layer to secure an application-layer communication; the third shows how we can use security at the network layer.

32.1 LAB32-1: IPSEC

IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security at the network level. IPSec setting and configuration is overwhelming because rather than defining specific implementation, it provides a framework with many possible negotiated choices:

- IPSec can be set up to work under Transport Mode or Tunnel Mode. Tunnel mode is often used between two gateways (such as routers) to provide Private Virtual Network (PVN), while the transport mode is more suitable for host-to-host communication.
- IPSec can provide authentication alone by using Authentication Header (AH) algorithm or it can provide encryption with authentication option by using Encapsulating Security Payload (ESP) algorithm.
- Two host can exchange the key manually or they can do it online using the Internet Key Exchange (IKE) mechanism.
- IPSec can use many different hash functions such as SHA-1 and MD5.
- IPSec can use many different encryption algorithms such as DES, 3DES, and AES.

To use IPSec, we must first set and configure it on both host. The set-up and configuration procedure is slightly different for different operating systems. You should check the internet to see how it is down for your operating system. Two possible way to set up IPSec policies in Windows are:

1. Select Run from the Start menu; type *mmc* and click OK. This will take you to the Microsoft Management Console (MMC) which is a component of Windows oper-

ating systems. This console provides users with an interface through which they may configure and monitor the system. On the File menu, click Add/Remove Snap-in. Click Add, and then double-click IP Security Policy Management and follow the instructions on the screen.

2. Select Programs from the Start menu, select Administrative Tools, and select Local Security Policy.

32.1.1 Assignment

- Open Wireshark and start capturing.
- Using one of the hosts, run one of the C server program or one of the Java program in Chapter 25
- Using the other host, run the C client program or the Java client program corresponding to the server program you are running in the previous step.
- Let wireshark capture some packets.
- After enough packets have been captured or one of the running program has been terminated, stop Wireshark and save the captured file.

Part I: ESP or AH packets

Depending on whether, you set the IPSec to provide authentication alone (using AH algorithm) or encryption with authentication option (using ESP) you may capture AH or ESP packets.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. AH or ESP packets are encapsulated in what protocol?
2. What is the protocol number for AH or ESP?
3. What information can an attacker sniff if she intercepts a communication protected by IPSec? Can she get the IP addresses of the two hosts? Can she guess about the type of packet carries by the ESP (for example, can she tells if the ESP contains VOIP?)
4. Open an AH or an ESP packet. What information is inside the packet?

Part II: ISAKMP packets

If the hosts are using Internet Key Exchange (IKE) mechanism, you notice several ISAKMP packets.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. How many different ISAKMP exchange type are in the trace?
2. Does an ISAKMP use the service of UDP or TCP?
3. In which exchange type do you find the Security Association (SA)?

4. What encryption method is used?
5. What authentication method is used?

32.1.2 Documents to Turn in

1. A copy of the Lab32-1 report sheet that contains answered questions.
2. A printout of the supporting captured information.

32.2 LAB32-2: SSL

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide security over the Internet above the transport layer. In this lab we capture packets while we are doing a secure transaction such as on-line banking, checking our credit card statement over the Internet, or purchasing something on-line.

32.2.3 Assignment

- Start the Wireshark and start capturing packets.
- Open your browser and make a secure connection to your bank, to your credit card company, or to purchase something on line. So some transaction and terminate the connection.
- Go to Wireshark, stop packet capturing, and save the file.
- Type **ssl** (lower case) in the filter field and press enter. You will see many SSL packets as well as TCP packets.

Part I: General

In this part, we explore the general issues related to the SSL protocol.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. What is the SSL version?
2. Can SSL uses the service of UDP? Explain.
3. What is the server port number?
4. Does an SSL packet carry HTTP or HTTPS packet?
5. Can we open an HTTPS payload? Can we open its headers?
6. Can we identify SSL source and destination addresses?
7. Are the SSL payload and the message authentication code (MAC) encrypted together or separately?
8. Is the user name and password encrypted? What can you say about security of SSL?
9. Select **Analyze** from the drop-down menu and then click **Follow TCP stream**. What do you see?

Part II: SSL Client Hello

The first step in establishing an SSL connection is an SSL handshake. SSL handshake enables the SSL client and server to agree on cryptographic algorithms, authenticate each other, and use asymmetric encryption techniques to generate a shared secret key. SSL then uses the shared key for the symmetric encryption of messages. The SSL handshake starts with the SSL Client Hello message that contains information such as the SSL version, the Cipher Suites (combination of key exchange, hash, and encryption algorithms) supported by the client, a session ID and a random byte string that is used in subsequent computations, and data compression methods.

In the packet list pane, select an SSL Client Hello message. In the packet detail pane, click the box to the left of Secure Socket Layer to reveal the detail of the packet (the plus sign will be changed to minus sign). Similarly, click on all the subsequent boxes to open them all the way.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. What is random byte string generated by the client?
2. Can you tell what information the client is using to create this random byte string?
3. What is the hexadecimal value of the session ID?
4. How many different Cipher Suites (combination of key exchange, hash, and encryption algorithms) supported by the client?
5. Is any compression method supported by the client?

Part III: SSL Server Hello

The handshake is followed by the SSL Server Hello message that contains the Cipher Suite chosen by the server from the list provided by the client, the session ID, another random byte string, and the SSL server digital certificate. It may also includes request for client certificate.

In the packet list pane, select an SSL Server Hello message; In the packet detail pane, select the Secure Socket Layer and expand it all the way.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. What is random byte string? Is it the same as the client's one?
2. What is the hexadecimal value of the session ID? Is it the same as the client's session ID?
3. Which Cipher Suite is chosen by the server?
4. Does the server request for client certificate?

Part IV: Rest of SSL handshake

After verifying the digital signature of the server's digital certificate, the client sends a random byte string encrypted with the server's public key. Client and server use this random number to compute the secret key for encrypting subsequent message data. Cli-

ent also sends a random byte string encrypted by the client's private key together with the client's digital certificate if it is requested by the server.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. Locate messages that are labeled Change Cipher Spec and Encrypted Handshake Message. Are these sent by the server, by the client or by both?
2. What is the purpose of Change Cipher Spec?
3. Locate and open a message labeled Certificate. What does the packet contain?
4. Locate and open a message that are labeled Client Key Exchange. What does the packet contain?
5. Is there any Encrypted Alert message in your trace? What is the purpose of an Encrypted Alert message?

Part V: Application Data

When handshaking is complete, the client and server exchange data encrypted symmetrically with the shared secrete key for the duration of the session.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. What is the Application-Data content type
2. Open any Application-Data packet and describe it.

32.2.4 Documents to Turn in

1. A copy of the Lab32-2 report sheet that contains answered questions.
2. A printout of the supporting captured information.

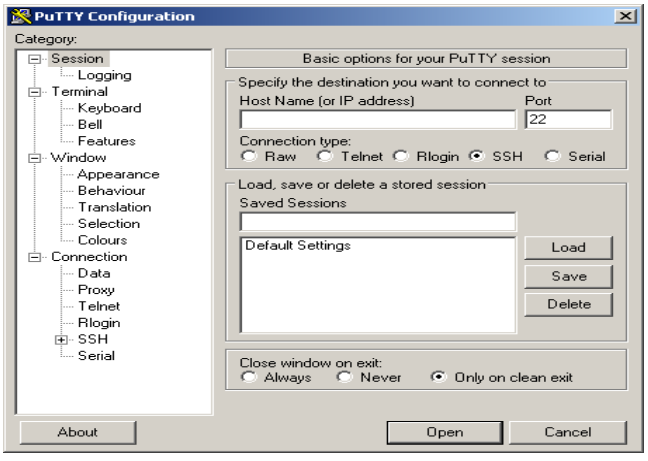
32.3 LAB32-3: SSH

In Lab2-3, we observe TELNET packets. TELNET protocol provides remote logging over the Transmission Control Protocol (TCP). TELNET requires user name and password for login, Nevertheless, the user name and the password, as well as the content of TELNET session, are not encrypted and can be easily hacked by any intruder. SSH, on the other hand, provides a secure tunnel for remote login. As in the case of TELNET, we can use PuTTY to open a SSH session, but we need to select the SSH radio button instead of the Telnet button (See Figure 32.1).

32.3.5 Assignment

- Start PuTTY and configure it to use SSH, but do not access any site.
- Open Wireshark and start capturing.

Figure 32.1 *PuTTY utility used for SSH*



- Go back to PuTTY and log into a PuTTY server that you have an account and permission to do so (such as a server in the lab of your college or university. Wireshark starts capturing packets.
- Use a few Unix commands. You can find the list of Unix commands in the lab assignment for Chapter 26.
- After executing some PuTTY commands, close the session, go back to the Wireshark, stop capturing, and save the captured file.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. Identify the three TCP packets that are used to establish the SSH connection?
2. Can SSH packets use the service of UDP? Explain.
3. What are purpose of the first two SSH packets?
4. Examine a client Key Exchange packet. What is the content of this packet?
5. Examine a server Key Exchange packet. What is the content of this packet?
6. Does your trace contains Diffie–Hellman key exchange packets? What are the purpose of these packets?
7. Are the payload and the message authentication code (MAC) encrypted together or separately?
8. Is the user name and password encrypted? What can you say about security of SSH?
9. Can you identify any command you used in any of the SSH session?
10. Click **Analyze** from the drop-down menu and then click **Follow TCP stream**. What do you see in the Follow TCP stream window?

32.3.6 Documents to Turn in

1. A copy of the Lab32-3 report sheet that contains answered questions.
2. A printout of the supporting captured information.