Song
Spring 2015

CS 161
Computer Security

Discussion 11

April 14 & April 15, 2015

Question 1 ***Networking*** **(12 min)**

(a) **Protocol Layers.** At which network layer does each of the following operate (physical, link, network, transport, or application)?

Solution:

- Ethernet – **Physical (1), Link (2)**
- SYN packet – **Transport (4)**
- UDP – **Transport (4)**
- Fiber optics – **Physical (1)**
- BitTorrent – **Application (7)**
- TTL field – **Network (3)**
- 127.0.0.1 – **Network (3)**
- 802.11n WiFi – **Physical, Link (1, 2)**

(b) **TCP and UDP.** The transmission control protocol (TCP) and user datagram protocol (UDP) are two of the primary protocols of the Internet protocol suite.

i. How do TCP and UDP relate to IP (Internet protocol)? Which of these protocols are encapsulated within (or layered atop) one another? Could all three be used simultaneously?

ii. What are the differences between TCP and UDP? Which is considered "best effort"? What does that mean?

Solution:

i. TCP and UDP both exist within the transport layer, which is one layer above IP (network layer). Either can be encapsulated in IP, referred to as TCP/IP and UDP/IP. TCP and UDP are alternatives; neither would normally be encapsulated within the other.

ii. TCP provides a *connection-oriented*, *reliable*, *bytestream* service. It includes sophisticated rate-control enabling it to achieve high performance but also respond to changes in network capacity. UDP provides a *datagram-oriented*, *unreliable* service. (Datagrams are essentially individual packets.) The main benefit of UDP is that it is lightweight.

"Best effort" refers to a delivery service that simply makes a single attempt to deliver a packet, but with no guarantees. IP provides such a service, and because UDP simply encapsulates its datagrams directly into IP packets with very little additional delivery properties, it too, provides "best effort" service.

Question 2 *IP Spoofing* (15 min)

You are the network administrator for a large company.

(a) Your company will be held liable for any spoofing attacks that originate from within your network (i.e., packets leaving your network with spoofed IP header information). What can you do to prevent spoofing attacks by your own employees?

You now want to evaluate the risk your employees face from spoofed IP packets originating from outside the network.

(b) Assess the likelihood and dangers of spoofed IP packets that use TCP as the transport layer protocol. What applications might be vulnerable to such an attack? How does this change with UDP?

(c) What can be done to prevent parties outside your network from sending your employees spoofed traffic that impersonates your own employees.

(d) *(Optional)* Now consider that your network has multiple links to the internet. Is there anything you can do to reduce the possibility of outsiders successfully sending your employees spoofed packets?

Solution:

(a) Inspect the source IP address of all outgoing packets. If a packet has an address from outside the range assigned to your network, block the packet. This is called *egress filtering.*

(b) Recall that TCP uses a 3-way handshake to establish a connection. As part of that handshake each side must agree upon a pair of valid sequence numbers. In order to successfully spoof a new connection, or to inject a spoofed packet into an existing connection, the attacker must either know or correctly guess the valid sequence numbers.

For a *blind* spoofing attack, without the use of any other attack techniques, the likelihood of correctly guessing the sequence numbers is quite small. (You'll work out this math in a later assignment.)

However, if the attacker is on-path (can eavesdrop) then spoofing TCP connections is quite easy.

An example of an application that would be vulnerable to such an attack would be HTTP. Later in the semester we will discuss TLS (SSL) and how that could help mitigate this attack.

Contrasting to TCP, UDP does not require a 3-way handshake. The attacker must only know the right source port from which the victim has started an outgoing connection. Thus, spoofing UDP packets requires much less effort. If application layer protocols wish to defend against this kind of attack they must develop their own defenses.

An example of an application that would be vulnerable to such an attack is DNS. We will explore DNS attacks in more depth in the next question.

(c) Packets originating from outside your network should never have a source IP address from inside your network. Using this fact you can filter (block) incoming packets that contains source IP that belongs to your own network. This is called *ingress filtering*.

(d) It is highly dependent on how your system is setup. If you know what IP addresses are associated with the networks behind the different links, and a packet comes in on a link that does not match with the IP addresses associated with that network, you can filter out those packets. This is again *ingress filtering*. It is not always possible to associate a set of IP addresses with a link connection. ISPs can do this for traffic coming from their edge customers (on separate autonomous systems).

Question 3 *TLS* (10 min)

(a) In TLS, what security properties are achieved, and what components of the TLS protocol enable these properties?

Solution: Confidentiality - communication is encrypted using session keys. Integrity - TLS uses MACs to prevent message tampering. One-way authentication - Signed certificates provide a means of authenticating the server.

(b) Recall that in practice, TLS as used on the web typically only provides one-way authentication – that is, when communicating securely over the web, only the server is required to authenticate themselves, and not the client. Why is TLS usually used this way?

Solution: One reason is that it is rather inconvenient for the average user to have to set up their own client certificate. Websites would not want to block users who haven't set up a client certificate. Another reason is that in many cases, the server doesn't care who is connecting to it, since it's providing a service over the web that anyone can use. A user certainly cares that they are connecting to the correct server; a server likely expects connections from many clients, so it may not need or want to authenticate them all.

(c) How else might a web server authenticate a user? (if the user is not authenticated by TLS)

Solution: Servers often authenticate the user by requiring them to establish a username and password with the site. That way, once a secure TLS connection has been established, the server knows which of its users it is communicating with.

A final note: do not hesitate to ask for help! Our office hours exist to help you. Please visit us if you have any questions or doubts about the material.