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)?

- Ethernet
- SYN packet
- UDP
- Fiber optics
- BitTorrent
- TTL field
- 127.0.0.1
- 802.11n WiFi

(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?

**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?

**Question 3** ***TLS*** **(10 min)**

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

(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?

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