Jawale & Dutra
Summer 2019

CS 161
Computer Security

Discussion 6

Network Security I

Question 1 ***Internet layering*** **(10 min)**

(a) Complete the diagram showing the five layers of the internet protocol stack.

7	_____
4	_____
3	_____
2	_____
1	_____

(b) Write the number of the layer that corresponds to each protocol.

- ARP _____
- HTTP _____
- TCP/UDP _____
- Voltage levels _____
- IP _____

Question 2 ***DHCP*** **(10 min)**

Rafael gets home after a tiring day of lecturing CS 161. He opens up his laptop and goes on Twitter. From a networking and web perspective, what are the steps involved in loading the Twitter homepage?

Rafael's computer needs to connect to the wifi. What messages are exchanged in the 4 part handshake in order to achieve this?

Rafael's computer sends: _____.

This message is *broadcasted / unicasted*. Choose one and explain:

A DHCP server replies with a DHCP Offer. What does this message contain? What can a malicious attacker do at this step? Keep in mind that an attacker on the same subnet can hear the discovery message.

Rafael's computer sends: _____.

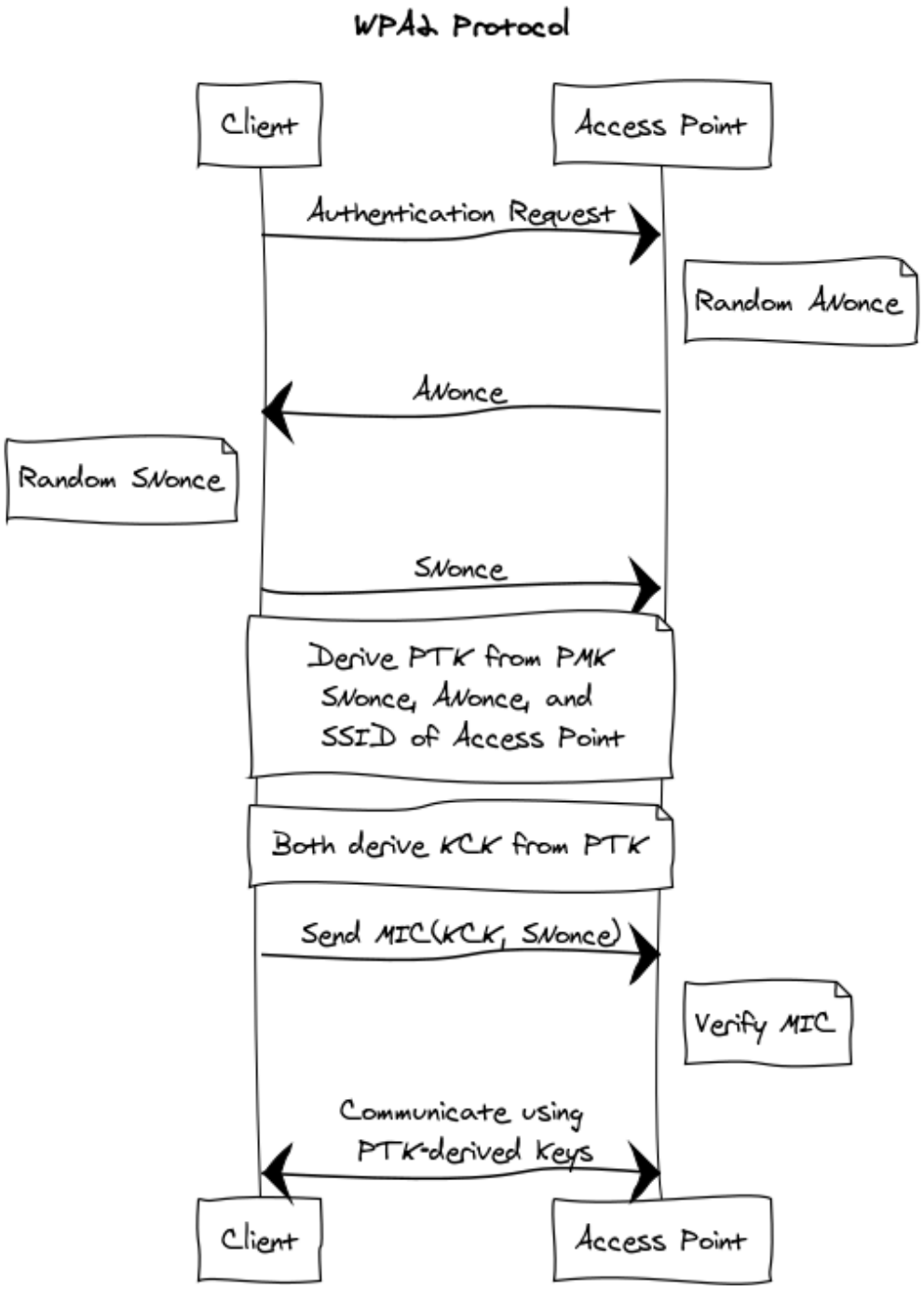
This message is *broadcasted / unicasted*. Choose one and explain:

The server then responds with: _____.

Question 3 ***WPA2*** **(20 min)**

Let's review WPA2. You might find some of the definitions below helpful.

- PMK is the *premaster key*, also known as "the WiFi password".
- PTK is the *pairwise transient key*, which is used to derive symmetric keys.
- KCK is the *key confirmation key*, which helps the client and the access point confirm they've agreed on the same keys.



(a) Louis Reasoner proposes that we don't generate ANonce or SNonce, and instead derive the PTK directly from the SSID and PMK. What sort of attack does this fail to prevent?

(b) WPA2 has an interesting pattern which is common in cryptographic protocols. Both parties agree on a shared secret, which they use to derive keys. Which other protocol have we seen which follows this motif?

(c) Alyssa P. Hacker wants to compromise a WPA2 WiFi network. In order to do so, she performs the handshake many times. She bruteforces possible PMK against the Access Point many times, until the access point eventually accepts it. If the password has 28 bits of entropy[1] and the attacker can make 10 guesses a second, how long will it take to bruteforce the password?

(d) Ben Bitdiddle has an alternate idea. Ben waits until Louis attempts to connect to the network. While this happens, he records all of the messages that Louis sends over the network. How can Ben use this to bruteforce possible PMKs? Why do we expect this to be faster than Alyssa's method?

[1] As per this XKCD comic, a password which looks like `Tr0ub4dor&3` has roughly 28 bits of entropy.