Question 1 (10 points)

Describe how the feature of gratuitous ARP can pose a security threat in local area networks and how from a network perspective this might be detected.

Feature of Gratuitous ARP (Address Resolution Protocol): One of the optimizations to the ARP protocol is that nodes can broadcast an ARP reply to the network *proactively* that is, a reply is sent without having received an inquiry first. This feature is called gratuitous ARP.

Threat in local area networks due to feature of gratuitous ARP: The threat is imposing as someone else - ARP spoofing and CAM table flooding.

Threat detected from network perspective: Gratuitous ARP are easy to detect: the source and destination MAC address of the Ethernet frame is set to the broadcast MAC address ff:ff:ff:ff:ff:ff so that it is flooded through the entire network. By disabling gratuitous ARP, nodes would only update their ARP caches after an existing entry has expired and is re-queried again. This is however also an imperfect solution, as gratuitous ARP does serve important purposes as discussed above; disabling them completely might break other things, such as high availability solutions that rely on gratuitous ARP for intermediate failover.

Question 2 (10 points)

Stream ciphers contain certain advantages of block ciphers when used over wireless links. Summarize the advantages and risks for stream ciphers and explain how wireless protocol would need to be setup to reap the benefits while avoiding their weaknesses.

Stream ciphers contains the advantages of block ciphers when used over wireless links and Setup of wireless protocol to reap benefits while avoiding the weakness:

The stream ciphers split the key into two parts – a long term secret key and a public key that is unique per key stream. This has the advantage that the shared secret can remain in place for an extended period, while the second component can be cycled too often.

1. Stream ciphers encrypt every bit individually, they are more resilient to transmission errors. Wireless channels are prone to flipping random bits, a message over such link encrypts with a stream cipher would suffer only from one corrupted bit. *Block ciphers* on the other hand encrypt and decrypt a predefined chunk of information (AES-128 works on blocks of 16 bytes). Here, one corrupted bit would influence many others or may lead to the entire block not being decipherable anymore.
2. The WEP designers address the issue of wireless channels prone to frequent packet loss, due to collisions, interference or fading by creating new stream for every packet. If one packet is lost, all subsequent packets would still be decipherable. Loosing a packet in a synchronous stream cipher is disastrous as it unsynchronises the 2 key streams of sender and receiver.

Risk of Stream Ciphers:

1. Knowing the plaintext to a corresponding ciphertext lets an attacker retrieve the key stream bytes the plaintext attack.
2. Obtaining two cipher texts for which one of the two plaintexts is known lets an attacker also determine the unknown plaintext
3. Possessing a valid key stream lets an attacker construct a correctly encrypted message even without possession of key or seed.
4. Authentication Spoofing: Reusing the same seed by a sender creates a significant danger.
5. The commutative property allows an adversary to gain access to a WEP-encrypted network without the knowledge of the PSK.
6. The use of CRC (cyclic redundancy check) introduces vulnerabilities.

7. Authentication spoofing, Reuse and Decryption tables, Message injection and Message tampering, Retrieving the WEP key

290 292 294

Question 3 (10 points)

Summarize why a link layer security mechanism should not only protect the confidentiality of the content but also the integrity of the meta-data. Explain which vectors was avoided by computing the AAD in WPA2.

A link layer security mechanism should not only protect the confidentiality of the content but also the integrity of the meta-data –

1. WiFi protected access 2 -WPA2 introduces the new default method for encrypting and validating the WiFi traffic: CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
2. CCMP employs AES (Advanced encryption standard) in counter mode(CTR) for data encryption and to provide confidentiality, in cipher block chaining mode (CBC-MAC) for creating a message integrity code to authenticate the source of transmission and ensure the integrity of the frame. This dual usage lends CCMP its name. Although AES is a block cipher, utilizing it in CCM mode (Counter with CBC-MAC) effectively turns it into stream cipher, utilizing it in CCM mode effectively turns it into stream cipher and the same precautions of stream cipher can be considered.

Vectors avoided by computing AAD in WPA2-

The selected fields such as the *duration or retry flags* are deliberately excluded from the AAD (Additional Authentication Data), as in case of collision and retransmit the MIC would need to be computed. The parts of the "message" which are verified by the CBC-MAC is hence the plaintext and selected metadata to prevent repurposing or replaying a frame, while still allowing minor modifications that would occur during normal protocol operation.

324 326

Question 4 (10 points)

You can accomplish the segmentation of networks into individual compartments by user group either logically through techniques such as 802.1Q Virtual LANs, or physically by deploying different hardware for each compartment. Discuss the advantages and disadvantages of each solution.

Advantages and disadvantages of 802.1Q Virtual LAN:

When VLAN segments are logically segmented and traffic is only forwarded to select nodes, the logical compartments still physically share the same infrastructure and remain partially entangles; traffic in one compartment hence can have a f=direct performance impact on communication taking place in another disjunct segment. If no other mitigation schemes are in place, an attacker may launch a Denial of service attack against another VLAN by consuming the entire bandwidth capacity of the underlying shared physical medium, or through specifically crafted packet trains bursts degrade the performance of real time applications in other compartments.

Advantages and disadvantages of deploying different hardware for each compartment: 269

Connecting different hardware with different cables makes it both costly and highly impractical: different cables and switches would need to be deployed for every different level of access, shared resources like a server would need one network port per

user group and every organizational change would require an error-prone network redesign and reconfiguration. While physically separating devices is clearly not a viable option, such partitioning may be efficiently implemented logically on a protocol level. IEEE 802.1Q, more commonly referred to as VLAN, is one of these techniques. VLAN capable hardware separates a physical network into logical partitions by inserting and interpreting an additional field into the Ethernet header.

269,270