Issa Odeh

Module 8 assignment

November 1st,2021

1. Let's say F is an error-detection function, and C is a MAC function. The message M will be split into small data package (i.e., M_1 ~ M_n) and sent from Alice to Bob, through external error control scheme or MAC scheme, respectively, as shown in the figures below. The red arrows mean the public network, which is considered as vulnerable. Other parts are private, under fully control of either Alice or Bob.

a) in error control scheme, which part/data (i.e. M_1 ~ M_n, E, K, E(K,M), F, F(E(K,M_i)) – i: 1~n, D) should be considered as accessible by attackers? (note: shall we assume the attack can obtain some M_i and F(E(K,M_i)) ?) (1pts) **In a error control scheme, a hacker can make a new message with a valid error-control codes. E(K,M) is accessible by hackers.**

b) in MAC scheme, which part/data (i.e. M_1 ~ M_n, E, K_1, K_2, E(K_2,M), C, MAC(K_1, E(K_2,M_i)) – i: 1~n, D) should be considered as accessible by attackers? (note: shall we assume the attack can obtain some or all of M_i, MAC(K_1, E(K_2,M_i)) ?) (1pts) **MAC(k1,E(K2,M)) is most accessible by attackers**.

c) in terms of confidentiality and authenticity, does error detection function provide any of them? Why? Does MAC scheme provide any of them? Why? (2pts) **Error detection provides just authentication because an attacker would have a hard time generating a ciphertext that when it is decrypted, it would have valid error control bits. MAC provides authentication and confidentiality. This is because it is a symmetric key. The sender and the receiver share a symmetric key. MAC is used to authenticate the message.**

d) for the MAC scheme, can we use RSA-based public-private key scheme as an alternative? If yes, is there any trade-off to use RSA-based public-private key scheme? If no, why? (2pts) **yes, it is possible to use RSA since it uses confidentiality and authenticity like a mac scheme. The downside is that it is slow and it uses more computing power. It takes a longer time to do its encryption/decryption.**

2. the brute force collision attack has two lines of attack:

-First is to attack the key space. If the attacker can figure out the mac key, then it is very possible to generate a new valid mac value for any input that is x.

-Second is to attack the mac value. This is done by generating a valid tag for a message that can be used or try to find a message that matches a given tag.

3.

A). WEP Is used for IEEE 802.11 wireless networks, and it is the security algorithm. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. A standard 64-bit WEP uses a 40-bit key, that is put together with a 24-bit initialization vector to form what's known as a RC4 key. A 64-

bit WEP key is entered as a string consisting of 10 hexadecimals. Each character is 4 bits. A 128-bti WEP key is entered as a string consisting of 26 hexadecimals. WPA uses the full availability of IEEE 802.11. WPA is implanted through firmware upgrades on a wireless network interface cards that was designed for WEP. The WPA protocol implants a protocol called Temporal Key Integrity Protocol (TKIP). As said above, WEP uses a 64- or 128-bit key that must be entered by a user. TKIP is totally different. It employs a per-packet key. This means that is generates a new key for each packet. With TKIP, it prevents attacks. WPA2 was made to replace WPA, then WPA3 was made to replace WPA2. The WPA3 key uses a 192-bit length.

B). As mentioned above, when using WEP, the user must manually enter the numbers using a 64-bit key. This feature in the WEP makes the security weak as one only key sends out information, and eventually a hacker will crack that key. At first it wasn't a problem, but as time went on, hackers broke the code behind the keys. WPA is more secure as it uses multiple security protocols to secure those wireless networks. WEP isn't used very much anymore but it is better to have it then no security at all. WPA is a little more secure, but it is vulnerable to intrusion. WPA is more efficient then WEP and more users/companies use WEP more as it generates its own random numbers instead of a user doing it. The main purpose for a WEP is to protect wireless communication from eavesdropping, it prevents unauthorized access to a network. The main purpose for the WPA is provide more complex data encryption and it is better then WEP at authentications.