Alan Palayil
A20447935

ECE 543

# Homework #1

Due Date: 1/29/23

Chapter 2

2) Appending a hash of a message is known as message authentication code (MAC), it is a commonly used technique in cryptographic protocols to prevent unauthorized modification of messages. However, this technique alone is not sufficient to fully solve the problem of message modification by an intruder as it has several vulnerabilities such as the ability to recalculate the hash to match a modified message, pre-computed table attacks, and the possibility of the authentication key being compromised. To fully solve the problem of message modification by an intruder, we can use a secure encryption technique such as public-key encryption in addition to the MAC to ensure the confidentiality and integrity of the message.

3) Having each person use their own unique secret key is not more secure than having them all use the same secret key. I think, its less secure as each person has to use their own key, it creates a key management problem as each person needs to have different keys for different people they communicate with. This means that Alice needs to know Carols secret key (KC) in order to verify Carol's answer to Alice's challenge. However, this also means Carol needs to have a different key for Bob, and Bob needs to have a different key for Alice. This creates a lot of complexity and overhead in managing the keys.
∴ It's not more secure than having the same secret key used by all of them.

4) Digital signatures provide authenticity and data integrity. Instead of encrypting the message, a hash of the message is created and encrypted using private key and sent with the data. This way, any alteration of the message or hash can be detected by the receiver. It is also common to sign the hash of the message for performance reasons. Hash functions

are used to create a fixed-length output, known as a message digest, from an input of any length, making it difficult to find two messages with the same digest. This way, integrity checks and sender verification can be performed using a cryptographic checksum or digital signature. If two messages have the same digest, the method is not valid and easily vulnerable to attackers.

5) A reflection attack is a way to exploit a challenge-response authentication system that uses the same protocol in both directions, by opening two simultaneous connections. As per the hint, Alice can use the second connection to solve for Bob's challenge in the first connection, thus undermining the security of the system.

6) The advancement in computer speeds works in favor of the good guys, as their performance increases linearly with the length of the key. This means that doubling the computer speed allows for doubling the length of the key without any performance penalty. However, for the bad guys, the number of keys that must be checked grows exponentially with the length of the key. eg. If the original key was 8 bits, the bad guys would have to check 256 keys. With faster computers, the good guys can use a 16-bit key, while the bad guys would have to check 512 keys. However, since the number of keys grow exponentially, the bad guys would now have to check 65536 keys, taking 128 times longer than the original 8-bit key.

Chapter 9

2) The given protocol is a password-based authentication system that does not utilize public key cryptography. As a result, it doesn't provide complete protection against eavesdropping and server-side disclosure. The main benefit of this system is that the password is only known to the user,

Alice. However, there are several security challenges that need to be addressed. One such challenge is eavesdropping, which can be mitigated by regularly changing passwords and using complex and difficult passwords. The scheme is also vulnerable to online and offline dictionary attacks, which can be addressed by using a table of password hashes or by encrypting the password using a high-quality key. Additionally, it should be noted that Bob is not authenticated in this scheme. To address this issue, one can use Lamport's Hash signature scheme, which utilizes a secure one-way function to secure the password. It is important to consider these potential security challenges when using this password-based authentication scheme to ensure its effectiveness.