Homework 2_3

111061610 謝崇志

1. Consider the following hash function. Messages are in the form of a sequence of numbers in Z_n , $M = (a_1, a_2, \ldots, a_t)$. The hash value h is calculated as $(\sum_{i=1}^{t} a_i^2)$ mod n for some predefined value n.

   (a) Does this hash function satisfy any of the requirements for a hash function listed bellow? Explain your answer for each case.

   - It can be applied to a block of data of any size. (5 points)

     Ans:

     Yes. When we've got a fixed 'n' and we're adding up all the stuff in 'x', you can use the Hash function (H) on a bunch of data, no matter how big. Just add up everything and throw in that modulo function.

   - It produces a fixed-length output. (5 points)

     Ans:

     Yes, it satisfies this requirement. The output is calculated as $\left(\sum_{i=1}^{t} a_i^2\right)$ mod n, which is a fixed-length value since it involves a modulo operation with n.

   - It is relatively easy to compute for any given input. (5 points)

     Ans:

     Yes, it satisfies this requirement. The computation involves squaring each element of the sequence and then taking the product, followed by a modulo operation. These are computationally straightforward operations.

   - Preimage resistance. (10 points)

     Ans:

     No, it does not satisfy this requirement. Preimage resistance implies that it should be computationally infeasible to determine the original input from its hash value. In this case, since the function involves squaring elements, it may be possible to find different inputs that result in the same hash value.

   - Secondary preimage resistance. (10 points)

     Ans:

     No, it does not satisfy this requirement either. Secondary preimage resistance implies that it should be computationally infeasible to find a different input that produces the same hash value as a given input. However, since the function only involves squaring elements and taking the product, it might be susceptible to finding secondary preimages.

   - Collision resistance. (10 points)

Ans:

No, it does not satisfy collision resistance. Collision resistance means that it should be computationally infeasible to find two different inputs that produce the same hash value. In this case, due to the squaring and modulo operations, there might be cases where different inputs result in the same hash value, violating collision resistance.

(b) Compute the hash for M = (120, 145, 224, 657) for n = 981. (5 points)

Ans:

$$\boldsymbol{h = \left(\sum_{i=1}^{t} a_i^2\right) mod\; n,\;\; M = (120, 145, 224, 657), n = 981}$$

$$\textbf{So, } \boldsymbol{(120^2 + 145^2 + 224^2 + 657^2)\; mod\;\; 981 = 263}$$

2. The chart below shows an authentication protocol, followed by data exchange, followed by disconnection. Only an initial part of the authentication protocol is shown; here, pw is A's password, J is a key derived from pw, and L is a high-quality key. Assume an attacker that can (1) eavesdrop messages and (2) intercept and spoof messages sent by A (but not those sent by B). Complete the authentication protocol (i.e., Supply the part indicated by the "** .... * *") so that in spite of this attacker

   - B authenticates A,
   - this authentication is not vulnerable to off-line password guessing, and
   - A and B establish a session key S (for encrypting data) such that after A and B disconnect and forget S, even if the attacker learns pw, the attacker cannot decrypt the data exchanged. (15 points)

Ans:

Here's an authentication protocol and key establishment process:

$A \rightarrow B: A\ and\ NonceA$

A sends its identity (A) and a nonce (NonceA) to B.

$B \rightarrow A: B, NonceB\ and\ (J, NonceA)K_b$

B sends its identity (B), a nonce (NonceB), and an encrypted message containing J, and NonceA encrypted with B's key (K_b) to A.

$A \rightarrow B: (NonceB)J$

A decrypts the message using J and responds with NonceB encrypted with J.

$B \rightarrow A: B, (\ NonceA, NonceB, S)K_b$

B decrypts the message using K_b, and both parties confirm their identities by exchanging nonces. B generates a session key (S) and sends it along with the exchanged nonces encrypted with K_b.

A and B share the established session key S for subsequent data exchange.

3. Suppose that the current replay window spans from 111 to 430. (15 points)

   (a) If the next incoming authenticated packet has sequence number 99, what will the receiver do with the packet, and what will be the parameters of the window after that?

Ans:

The receiver will consider this packet out of the current replay window (111 to 430). As 99 is less than the lower bound of the window (111), it is considered too old and potentially part of a replay attack. Therefore, the receiver will discard the packet.

So, the parameters of the window remain the same: [111, 430].

(b) If instead the next incoming authenticated packet has sequence number 420, what will the receiver do with the packet, and what will be the parameters of the window after that?

Ans:

The receiver will accept this packet, as its sequence number falls within the current replay window (111 to 430).

After accepting the packet, the replay window parameters will be updated. Since the packet with sequence number 420 is at the upper bound of the current window, the new window will likely shift to cover subsequent sequence numbers. The new replay window may be something like [112, 431] or another appropriate size.

(c) If instead the next incoming authenticated packet has sequence number 566, what will the receiver do with the packet, and what will be the parameters of the window after that?

Ans:

The receiver will consider this packet out of the current replay window (111 to 430). As 566 is greater than the upper bound of the window (430), it is considered too new and might be a delayed or reordered packet. Therefore, the receiver will discard the packet.

The parameters of the window remain the same: [111, 430].

4. An attacker is intent on disrupting the communication by inserting bogus packets into the communications. Discuss whether such an attack would succeed in systems protected by IPsec. Discuss whether such an attack would succeed in systems protected by SSL. (10 points)

Ans:

IPsec:

Likelihood of Success: Low

Encryption and Authentication: IPsec provides both encryption and authentication of IP packets. This means that even if an attacker manages to

insert bogus packets, they would need to be encrypted to be of any use. Without knowledge of the encryption key, the attacker would not be able to create valid encrypted packets.

Integrity Protection: IPsec ensures the integrity of the transmitted data through hashing. Any modification of the packet content would result in a mismatched hash value, causing the recipient to discard the packet.

Anti-Replay Mechanism: IPsec includes an anti-replay mechanism, which means that even if an attacker manages to insert previously captured packets, they would be detected as duplicates and discarded.

SSL :

Likelihood of Success: Low to Moderate

Encryption and Authentication: SSL provides encryption and authentication for data in transit. If an attacker tries to insert bogus packets, they would need to be encrypted using the appropriate keys. The encryption and authentication mechanisms in SSL make it difficult for an attacker to create valid packets without the proper credentials.

Certificate-based Security: SSL relies on certificates to verify the identity of the communicating parties. Without a valid certificate, it is challenging for an attacker to successfully impersonate a legitimate participant in the communication.

Server Authentication: SSL ensures server authentication, making it difficult for an attacker to insert bogus packets and pretend to be a legitimate server.

However, the success of such attacks might increase under certain conditions, such as weak or compromised keys, implementation vulnerabilities, or misconfigurations. It's crucial to keep both IPsec and SSL implementations up-to-date, use strong key management practices, and follow security best practices to minimize the risk of successful attacks.

5. Can a packet filter block all incoming email containing the phrase ”Homework 2 is out”? If yes, show a packet filtering ruleset that provides this functionality; if no, explain it. (10 points)

   Ans:

   No, a packet filter alone cannot reliably block all incoming email containing the phrase "Homework 2 is out." Packet filters typically operate at the network or transport layer based on criteria such as source and destination IP addresses, ports, and protocols. They are not designed to inspect the content of the data payload, such as the actual text within an email.