IoT Security and Privacy

Assignment 3 - Introduction to Security and Privacy (20 points)
Rajib Dey
PID: 4166566

R1. What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer. (3 points)

Answer:
Message Confidentiality makes sure that no one else can read the message except the sender and the receiver. If the intruder gets an encrypted plaintext, which is also called ciphertext, he/she will not be able to read the message. Thus, confidentiality of the message would be ensured.

Message Integrity lets the user know if the message was altered or not in transit to the receiver.

We can have either of them without having the other one. For example, We can have confidentiality without having integrity. The intruder can not get the plaintext from a ciphertext, which would ensure confidentiality. But the intruder can alter the ciphertext itself, without knowing the content of the plaintext. On the receiving side, the receiver will receive an edited ciphertext(which will get decrypted into a different plaintext) which he/she would have no idea that it was edited in transit, as integrity was not provided.

The same way, We can have integrity without providing confidentiality. If the sender sends a message without encryption then the intruder can easily read the plaintext thus violating privacy of the message. But by implementing integrity checks the receiver can know if the message was changed or not in transit.

R7. Suppose n = 10,000, a = 10,023, and b = 10,004. Use an identity of modular arithmetic to calculate in your head (a • b) mod n . (2 points)

Answer:

We know, [(a mod n) • (b mod n)] mod n = (a • b) mod n

a mod n = 10023 mod 10000 = 23

b mod n = 10004 mod 10000 = 4

So, [(a mod n) • (b mod n)] mod n= [23 * 4] mod 10000 = 92

The calculated value of (a • b) mod n is 92.

R9. In what way does a hash provide a better message integrity check than a checksum (such as the Internet checksum)? (2 points)

Answer:

Hash function is very difficult to fake. In other words, if one message M1 has a hash function of H1 then another altered message M2 would have a hash function of H2. It would be very tough for the intruder to edit the second hash function H2 to make it exactly like H1.

On the other hand, checksum or internet checksums can be easily faked by changing the order of the message. So, you can have the same checksum for two different message. The intruder can take the original message, edit it, and then generate the same checksum as the original message. When the receiver receives it, he/she would have no idea if the message was altered in transit or not.

R15. Suppose Alice has a message that she is ready to send to anyone who asks. Thousands of people want to obtain Alice's message, but each wants to be sure of the integrity of the message. In this context, do you think a MAC-based or a digital-signature-based integrity scheme is more suitable? Why? (4 points)

Answer:

Digital signature based integrity scheme would more suitable in this context.

Mainly because, in Digital signature based integrity scheme she could just create her own digital signature by signing the hash of the message with her private key, which can be used for all the recipients. Any recipient can verify her digital signature by getting the public key from the Certification Authority.

In MAC-based integrity scheme, She needs to share a secret shared key to each receiver. Which can result in her sharing thousands of shared key, and each receiver needs to know the secret key to check the integrity of the message. Which will slow down the communication and bring extra unwanted burden to the network.

R20. In the SSL record, there is a field for SSL sequence numbers. True or False? (2 points)

Answer:

False.

Implicit sequence numbers are used in SSL. Which is why there is no need for a SSL sequence numbers.

P8. Consider RSA with $p = 5$ and $q = 11$.
a. What are n and z ? (2 points)
b. Let e be 3. Why is this an acceptable choice for e ? (1 point)
c. Find d such that $de = 1 \pmod z$ and $d < 160$. (1 point)
d. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding ciphertext. Show all work. (3 points)

Hint: To simplify the calculations, use the fact:

$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

Answer:

a) n=pq=5*11=55 and z= (p-1)(q-1)=4*10=40

b) e=3 should be acceptable because it is less than n and has no common factors with z (except 1).

c) de = 1 (mod z), so de mod z =1
so, d*3 mod 40 = 1
d=27

d) Here,
For Encryption:
m = 8, key= (n , e)=(55,3)

ciphertext, $c = m^e \bmod n = 8^3 \bmod 55 = 512 \bmod 55 = 17$