UNIVERSITY OF WARWICK

Paper Details

Paper Code: CS9150

Paper Title: Advanced Computer Security

Exam Period: Summer 2024

Exam Rubric

Time Allowed: 2 hours

Exam Type: Standard Examination

Approved Calculators: Not Permitted

Additional Stationery

N/A

Instructions

Answer **ALL FOUR** questions.

Read carefully the instructions on the answer booklet and make sure that the particulars required are entered on each answer booklet.

The exam question paper **MUST NOT** be removed from the examination venue.

Calculators are not required and not allowed.

Question 1 Symmetric cryptography [25 marks]

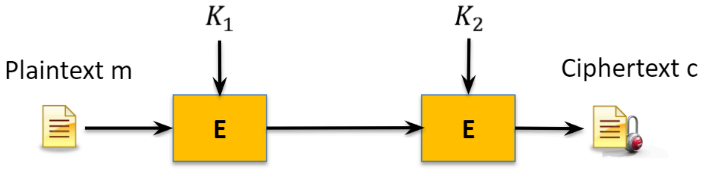
A Feistel network is one primitive used for constructing many block ciphers including DES. Answer the following questions.

a) Draw one round of the Feistel network. Clearly label the input, the output, the randomization function and the secret key in this drawing. Use L_i and R_i to denote the left and right halves of the input. Use L_{i+1} and R_{i+1} to denote the left and right halves of the output. Use $F(K_i)$ to denote the randomization function where K_i is the secret key for this round. [5]

b) The Feistel network is known for being invertible. Explain what it means by being invertible. Use mathematical equations and the diagram in a) to explain why it is invertible. [10]

c) DES includes 16 rounds of the Feistel network. All rounds are the same except the last round. Draw a diagram to explain the difference and why. [5]

d) Given a block cipher with a short key size, say 56-bit, one way to increase the key size is by concatenating the two ciphers with two different keys together as below. The key size becomes 112-bit. However, the security level of the concatenated cipher is only 57-bit. Explain why this is the case with the example of an attack. [5]



continued

Question 2 Public key cryptography [25 marks]

a) To generate a pair of RSA keys, Alice first generates two large primes p and q, and computes $N = p \times q$. She then computes $\phi(N) = (p - 1)(q - 1)$. To define the public key, Alice chooses a random integer e such that $\gcd(e, \phi(N)) = 1$. Explain how to obtain the private key d. Why do we require $\gcd(e, \phi(N)) = 1$? [5]

b) In one implementation, Alice applies RSA to encrypt and decrypt a message m as follows.

Encryption: $c = m^{e}\, mod$ N
Decryption: $m = c^{d}\, mod$ N

Semantic security is often used to define the security of a public-key encryption system. Explain what semantic security means. There are several attacks on the above RSA system. As an example, you may use this RSA system to encrypt a bid in a sealed-bid auction under an auctioneer's public key (e, N). Suppose your bid price is $m = 1,000$. However, your bid is intercepted by an attacker. Explain how this attacker may modify your ciphertext so that the decrypted bid will be three times the value of your original bid. [10]

c) Alice has learned that in practice, people often choose the RSA public key e to be a small value, e.g., $e = 3$. What's the likely reason for choosing a small value for e? When e is small, the decryption becomes much more expensive than the encryption. Explain why. [5]

d) Besides the RSA encryption, Alice implements a RSA digital signature scheme as follows.

Signing: $\sigma = m^{d}\, mod\, N$
Verification: Check if $m = \sigma^{e}\, mod\, N$

For simplicity, Alice decides to use a single pair of RSA keys for both RSA encryption and digital signature. Is this secure? Explain your answer. [5]

continued

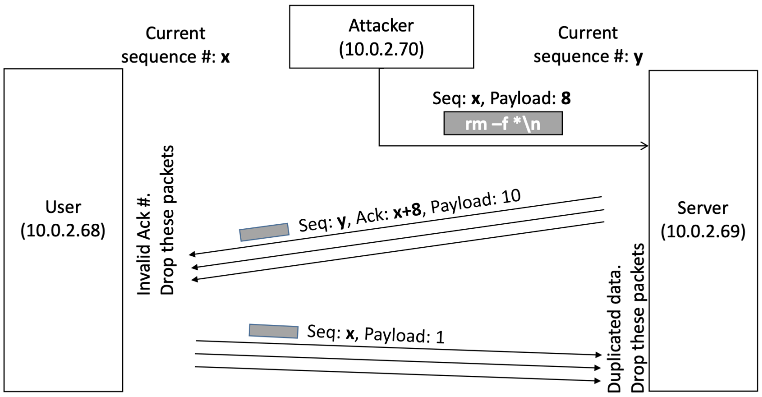
Question 3 Network security [25 marks]

a) The SYN flooding attack is launched from a computer, where the attacker has the root privilege, and the source of the IP address is randomized. Explain why the root privilege is required, and why the attacker must randomize the source IP address. What will happen if the spoofed source IP address belongs to a machine that is currently running? [5]

b) An integer 0xAABBCCDD is stored in a memory address starting from 0x1000. If the machine is a Big-Endian machine, what is the value stored in addresses 0x1000, 0x1001, 0x1002, and 0x1003, respectively? If the machine is a Little-Endian machine, how is this integer stored? [5]

c) A network protocol contains a four-byte integer, specifying the length of the payload in the packet. The implementation of this protocol has a mistake in it. When a packet is received, the protocol implementation needs to copy the payload to a buffer. It first copies the length field from the packet header to a variable, but the program forgets to convert the number into the host order. Assume the value of this variable is X. The program then allocates X bytes of memory to hold a copy of the payload. On a Little-Endian machine, if the payload of a received packet is 255 bytes, how much memory will be allocated? What is a likely consequence of this mistake? [5]

d) In a TCP session hijacking attack, an attacker (10.0.2.70) sends a crafted TCP packet to successfully hijack a telnet session as shown in the diagram below. The attacker then injects a command “rm -f *\n” to the telnet session. After this, the user (10.0.2.68) tries to type something in the local telnet terminal, but the program does not respond; it freezes. Wireshark shows that there are many retransmission packets between the user (10.0.2.68) and the server (10.02.69). Draw a TCP three-way handshake diagram (clearly label SYN and ACK sequences to highlight their relations in the three-way handshake). Explain why there are many retransmissions of packets between the user and the server occurring in both directions. [10]


Current sequence #: **x**
Attacker (10.0.2.70)
Current sequence #: **y**
Seq: **x**, Payload: **8**
rm –f *\n
User (10.0.2.68)
Invalid Ack #. Drop these packets
Seq: **y**, Ack: **x+8**, Payload: 10
Server (10.0.2.69)
Seq: **x**, Payload: 1
Duplicated data. Drop these packets

continued

Question 4 Hardware Security [25 marks]

a) Hardware Security Modules (HSMs) are widely used by banks, government agencies and enterprises to manage cryptographic keys and perform cryptographic operations. However, they are costly. Some people claim that HSMs are essentially computers. Therefore, it should be possible to use a laptop to do the same thing: i.e., saving cryptographic keys in a secure memory, and invoking a computer program to perform cryptography. Explain how HSMs crucially differ from a personal computer. [5]

b) Before the Chip-and-PIN cards were deployed, bank cards only had a magnetic stripe where the user's account number was stored. To support local PIN verification, one bank wrote the encrypted PIN to the card stripe using a symmetric key shared with the ATM machine. Alice and Bob are both customers of this bank. One day Alice discovered that money had been withdrawn from her account but she didn't do it. Later, it was found that it was actually Bob who withdrew the money, but Bob didn't know Alice's PIN. Draw a diagram to show the data stored on the bank card and explain how Bob managed to withdraw money from Alice's account without knowing Alice's PIN. Suggest a countermeasure to prevent this attack while still supporting local PIN verification. [10]

c) The following shows an example of how banks use an HSM to generate a customer PIN from their primary account number (PAN).

Account Number	4556 2385 7753 2239
Encrypted Accno	3F7C 2201 00CA 8AB3
Shortened Enc Accno	3F7C
Decimalization table	0123456789ABCDEF
	0123456789012345
Decimalised PIN	3572
Public Offset	4344
Final PIN	7816

One bank wishes to restructure the customer's account numbers but wants to keep the PINs unchanged. Therefore, they ask the HSM manufacturer to add the following API.

Host -> HSM: old_PAN, new_PAN, old_offset
HSM -> Host: new_offset

When the new_offset is used to replace the Public Offset, the Final PIN remains unchanged. Therefore, there is no need for customers to update PINs. Explain how an insider attacker who has access to the HSM may abuse this API to calculate the PIN for any customer. [10]

End