CS9150_B

The UNIVERSITY OF WARWICK

Advanced Computer Security

Standard Examination: Summer 2022

Time Allowed: 2 hours

Calculators are not required and not allowed.

Answer ALL FOUR questions.

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

Question 1: Classical cryptography [25 marks]

1.1 A substitution cipher works by randomly substituting letters based on using a permutation vector as the key. What is the key size of a substitution cipher? Elaborate how a substitution cipher can be broken without knowing the key. [5 Marks]

1.2 Vigenère cipher was designed to address the weakness of the substitution cipher, but it remains insecure. The following is a segment of the ciphertext generated by using a Vigenère cipher (the unknown key is a string of multiple letters).

...KIOVIEEIGKIOVNURNVJNUVKHVMGZIA...

Apply the Kasiski test to guess the likely key lengths and explain why. [5 Marks]

1.3 An alternative way to find out the key length is by calculating the index of coincidence. Briefly explain what the index of coincidence is and how to apply the index of coincidence to determine the key length. Note that the index of coincidence for random letters is 0.038 while for English text is 0.065. [10 Marks]

1.4 Assume you have obtained the correct key length by using the index of coincidence method. Explain how you can subsequently derive the key. [5 Marks]

Question 2: Public Key Cryptography [25 marks]

2.1 Bob, a software developer, is tasked to implement a public key encryption system for all employees of a company. He decides to adopt RSA for public key encryption and use HSM for key management. He first generates an RSA modulus $n = p \times q$ on a host computer, and then saves the prime factors p and q in secure memory of HSM. Next, he generates a random public and private key pair (e, d) on a computer for every employee and distributes the private keys to all employees through the company's internal network behind a firewall.

There are several security weaknesses in the above design. List four weaknesses and for each weakness briefly explain how an attacker may exploit it. [8 Marks]

2.2 In case an employee loses their private key, Bob plans to define the following HSM API to recover the private key.

Private key recovery API

Host -> HSM: e
HSM -> Host: d

Is this possible? Explain your answer. [7 Marks]

2.3 Later, Bob is asked to add a digital signing function for every employee. To avoid creating another key pair, he decides to use the same RSA key pair for both encryption and digital signature. He provides every employee with a program that performs basic (or textbook) RSA encryption/decryption and digital signature without using any padding. Is it secure to use the same key pair for both RSA encryption and digital signature? Elaborate your answer. (Hint: show how RSA encryption/decryption and digital signing/verification work and discuss if the same key can be used for both schemes.) [10 Marks]

Question 3: Network Security [25 marks]

3.1 Briefly describe how the DNS cache poisoning attack works. Explain the difference between a remote DNS cache poisoning attack and a local DNS cache poisoning attack. [5 Marks]

3.2 A remote DNS cache poisoning attack is more challenging than a local DNS cache poisoning attack. Highlight two challenges and explain how the Kaminsky attack overcomes these challenges. [10 Marks]

3.3 What is the fundamental problem of the DNS protocol that makes DNS vulnerable to DNS cache poisoning attacks? How does DNSSEC address this problem? [5 Marks]

3.4 An attacker tries to launch a DNS cache poisoning attack against a local DNS server, and provides the following spoofed DNS reply.

```
;; QUESTION SECTION:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 259200 IN A 129.211.32.34

;; AUTHORITY SECTION:
example.net. 259200 IN NS ns.tklp-server.net
example.com. 259200 IN NS ns.gltd-server.net

;; ADDITIONAL SECTION:
ns.gltd-server.net 259200 IN A 132.2.10.9
ns.tklp-server.net 259200 IN A 130.3.11.39
ns.atfz-server.com 259200 IN A 128.0.31.66
```

Describe which parts of the answer will not be cached by the DNS server, and explain why. [5 Marks]

Question 4: Hardware API security [25 marks]

The following example illustrates how an IBM 3624 Hardware Security Module (HSM) computes a PIN for a bank card based on the customer's Primary Account Number (PAN).

PAN	4556 2385 7753 2239
Encrypted PAN	3F7C 2201 00CA 8AB3
Shortened Encrypted PAN	3F7C
Decimalisation table	0123456789ABCDEF
	0123456789012345
Decimalised PIN	35**
Public Offset	4344
Final PIN	7816

4.1 Explain how the decimalisation table is used to compute the decimalised PIN, and compute the last two digits of the decimalised PIN. [5 Marks]

4.2 One bank wishes to restructure the customer account numbers. However, changing the account number would cause all PINs to be changed, and customers would not accept new PINs. So, the bank requested the HSM manufacturer to add the following API to compute a new offset so that the customer's final PIN will remain unchanged:

Host -> HSM: old_PAN, new_PAN, old_offset

HSM -> Host: new_offset

Explain how an insider attacker (e.g., a bank employee) can learn the PIN of an arbitrary customer by abusing this API. [20 Marks]

-END-