WARWICK
THE UNIVERSITY OF WARWICK

UNIVERSITY OF WARWICK

Paper Details

Paper Code: CS9150_B

Paper Title: Advanced Computer Security

Exam Period: Summer 2023

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.

WARWICK
THE UNIVERSITY OF WARWICK

Question 1: Symmetric cryptography [25 marks]

a) For many years, One-Time Pad (OTP) was believed to provide "perfect secrecy", but there was no proof. In 1949, Claude Shannon provided a definition for "perfect secrecy". According to Shannon, a cryptosystem has perfect secrecy if $P(m \mid c) = P(m)$ for all $m \in M$ and $c \in C$ where M and C represent the spaces for the plaintext message and ciphertext respectively.

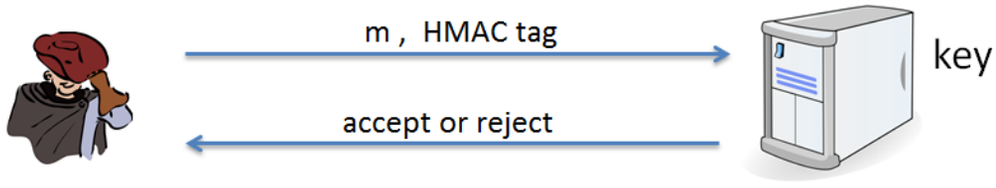
i) Define how OTP works. [2]

ii) Prove that OTP satisfies perfect secrecy. [6]

iii) Even though OTP has perfect secrecy, this cipher is almost never used in practice. Explain why. [2]

iv) A software developer uses the same secret pad to encrypt two different messages m_1 and m_2. Describe two negative consequences of doing this. [2]

b) In the following web application, a user sends a message together with a Hash-based Message Authentication Code (HMAC) tag to the web server. The web server will only accept the message if the verification of the HMAC tag is successful.



The web server uses the following HMAC verification function. The "==" operator is implemented as a byte-by-byte comparison.

```
def Verify(key, msg, sig_bytes):
    return HMAC(key, msg) == sig_bytes
```

i) Define a secure HMAC in terms of existential forgery. [3]

ii) Explain how an attacker can forge a valid HMAC tag for any given message. How many times on average does the attacker need to send the message/tag requests to the server? Assume the HMAC tag is 20 bytes long. [6]

iii) Suggest one countermeasure and explain its possible limitation. [4]

---

continued

WARWICK
THE UNIVERSITY OF WARWICK

Question 2: Public-key cryptography [25 marks]

a) Alice and Bob want to use the Diffie-Hellman Key Exchange protocol to generate a shared secret key k for secure communication. They have agreed to use p = 13 with g = 2. (Note: this is a toy example. In practice, p is a large prime number)

i) Demonstrate how $2^{11}\ mod\ 13$ can be computed based on a square-and-multiply algorithm. How many modular multiplications do you need? Show all your working. [5]

ii) Alice chooses her secret key $a = 3$ and Bob chooses his secret key $b = 4$. What is the value of the shared secret key k computed by Alice and Bob respectively? Show all your working. (Note: k may be further hashed to generate a session key, but you do not need to consider the hash function here). [6]

iii) Explain how Mallory, a man-in-the-middle attacker, could corrupt the Diffie-Hellman Key Exchange protocol. Compute the shared secrets obtained by Alice, Bob and Mallory. Assume Mallory chooses a secret key $c = 2$. [7]

b) A digital signature signing operation is normally applied on a one-way hash of the message, instead of on the message directly. One of the reasons is the cost because signing a short hash value is more efficient than signing a message that can be very long. Bob says that his message is always short, so he decides to directly sign the message, rather than signing its hash. Assume that Bob uses a textbook RSA digital signature scheme. His private key is d and his public key is e. The modulus is $n = p \times q$, where p and q are secret prime factors.

i) Define a secure digital signature scheme in terms of existential forgery. [2]

ii) Without knowing Bob's private key, can you generate a pair (m, s), where s is Bob's signature on m, and m can be anything? Explain your answer. [5]

---

continued

WARWICK
THE UNIVERSITY OF WARWICK

Question 3 Software Security [25 marks]

a) Consider the following C program.

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int foo(char *str)
{
        char buffer[100];
        strcpy(buffer, str);
        return 0;
}

int main(int argc, char **argv)
{
        char str[400];
        FILE *myfile;
        badfile = fopen("myfile", "r");
        fread(str, sizeof(char), 300, myfile);
        foo(str);
        printf("Returned Properly\n");
        return 0;
}
```

i) Identify the line of code which is vulnerable to a buffer overflow attack and briefly explain why it is vulnerable. [2]

ii) Draw a memory layout on the stack for foo() to briefly describe the buffer overflow attack. [6]

iii) The myfile contains malicious code, which is loaded to the stack through a buffer overflow. The attacker needs to know the memory address for the malicious code, but he can only guess an approximate address. Explain what the attacker can do to increase the chance of success in the attack. [2]

iv) Draw a revised memory layout to explain how StackGuard works and why it can prevent the buffer overflow attack. (Hint: in the revised layout, show where you insert the Guard on the stack, relative to positions of the Return Address, and the buffer array). [5]

---

continued

b) The following is a Set-UID program that is owned by root, but can be run by a user called Bob.

```
#include <unistd.h>
#include <stdio.h>
#include <string.h>
int main()
{
        char * fn = "/tmp/XYZ";
        char buffer[60];
        FILE *fp; /* get user input */
        scanf("%50s", buffer);

        if(!access(fn, W_OK))
        {
                fp = fopen(fn, "a+");
                fwrite("\n", sizeof(char), 1, fp);
                fwrite(buffer, sizeof(char), strlen(buffer), fp);
                fclose(fp);
        } else printf("No permission \n");

        return 0;
}
```

i) What are the Real UID and the Effective UID for running this program? [2]

ii) Does this program have a race condition problem? Explain your answer. [6]

iii) Suggest two countermeasures to prevent the race condition attack. [2]

continued

WARWICK
THE UNIVERSITY OF WARWICK

Question 4 Web Security [25 marks]

a) During a security audit of a company's website, it is found that some of its web pages are vulnerable to Cross-Site Request Forgery (CSRF) attacks.

i) Use an example to illustrate what a CSRF attack is. [2]

ii) Using the same-site cookie is suggested as a countermeasure. Please explain why it may prevent CSRF attacks. Also, explain the limitation of this method. [4]

iii) It's noticed that some web pages still use HTTP. Someone argues that once they are changed to use HTTPS, the CSRF attack will go away. Please comment if this is true. [4]

iv) Someone proposes the following solution to address CSRF attacks. When a web page sends a request to its server, the session ID is always attached in the cookie section of the HTTP header. The suggested solution is to require all the requests sent from its own pages to also attach the session ID in its data part (of either GET or POST request). This sounds redundant because the session ID is already included in the request. However, by checking whether a request has the session ID in its data part, the web server can tell whether a request is a cross-site request or not. Please explain why the web server can tell apart the two different types of requests. [5]

b) In the same security audit, it is found that some of the company's web pages are also vulnerable to cross-site scripting (XSS) attacks.

i) To defeat XSS attacks, someone proposes to implement filtering on the browser side. His proposal is to add JavaScript code on each vulnerable page, and the JavaScript code checks the user's data input and removes any JavaScript code contained inside the data. Can this approach prevent XSS attacks? List two limitations of this solution. [4]

ii) Can the same-site cookie countermeasure that is used to prevent CSRF attacks be used to defeat XSS attacks? Explain your answer. [3]

iii) Can the secret token countermeasure that is used to prevent CSRF attacks be used to defeat XSS attacks? Explain your answer. [3]

End