National University of Computer and Emerging Sciences

Lahore Campus

Information Security (CS3002)

Date: November 2nd, 2024

Course Instructor(s)

AK, AIS, MZH, SMI, AH, RAR

Sessional-II Exam

Total Time (Hrs): 1

Total Marks: 40

Total Questions: 4

_____ _____ _____

Roll No Section Student Signature

Do not write below this line

Note: Students will also write the formula used in each calculation, no direct answer will be accepted. If you think some information is missing then make an assumption and write it clearly. Write all the answers including MCQs on the given answer sheet.

CLO-1	Explain key concepts of information security such as design principles, cryptography, risk management
CLO-2	Discuss legal, ethical, and professional issues in information security
CLO-3	Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy
CLO-4	Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security
CLO-5	Describe issues related to ethics in the field of information security

CLO #: 1

Question No. 1: Choose the correct options(s). [5 marks]

1. What is NOT an advantage of password salting?
   a) Attacker cannot see which users had same passwords.
   b) Users can not choose weak passwords.
   c) Attacker needs a lot more work for dictionary attacks.
   d) All the above are advantages of salting.

2. Kerberos ticket granting tickets are issued by the _____.
   a) application server
   b) ticket granting server
   c) authentication server
   d) none of the above

3. What is the primary purpose of a Certificate Revocation List (CRL)?

a) To issue new digital certificates
b) To list certificates that have been revoked before their expiration date
c) To encrypt data in transit
d) To authenticate users

4. In the Prefix-Postfix MAC, the sender _____ and ____ the key to the original message, then applies a hash function on the ____ message. The ____ is then appended to the original message as the ____, and then transmitted to the receiver.

a) prepends; appends; modified; digest; MAC
b) prepends; appends; modified; key; digest
c) prepends; appends; original; digest; MAC
d) prepends; inserts; original; digest; key

5. Collision Resistance can be explained as:

a) Given a specific message and its digest, it must be extremely difficult to create another message with the same digest
b) Given a hash function h and a digest y, it must be extremely difficult for Adam (attacker) to find any message, M', such that y = h(M')
c) Given a hash function h and a digest y, it must be extremely difficult for Adam (attacker) to find a different hash function h'. such that y = h'(M)
d) Adam (attacker) cannot find two messages (from scratch) that hash to the same digest

CLO #: 3

Question No. 2 [6+3 marks]

A. In a Kerberos setup, there are three application services that need user authentication. The user needs to access each of these services at least five times a day. How many times per day, will the user need to interact with **(a)** the authentication server and **(b)** the ticket-granting server? Elaborate your response. (6)

User needs to interact with authentication server **only once** for initial login. The auth server will issue the TGT.
Afterwards, user needs to request service tickets from TGS by supplying their TGT. Since a service ticket is unique for one application server, user needs to interact with TGS **three times**.

B. What problem is solved by challenge-response authentication? (3)

When user credentials need to be transmitted over a network, there is a possibility of attacker eavesdropping all traffic. So, passwords and other secrets can't be sent in clear.
Challenge response strategy helps in such scenarios, it allows remote authentication without the overhead of establishing an encrypted channel.

CLO #: 4

Question No. 3: [5+10 marks]

A. A retail company experienced a breach in which an attacker injected malicious SQL queries through a vulnerable web form, gaining access to the company's customer database. The attacker exploited the SQL injection vulnerability to retrieve sensitive information, including credit card numbers, by modifying the query logic.
Describe the steps involved in a typical SQL injection attack. What measures can be implemented to prevent SQL injection vulnerabilities in web applications? (5)

Steps
Hacker finds a vulnerability in a web application and sends malicious requests that contain SQL commands involving tautology, piggybacked query, union queries etc. Web server forwards the sql command to database server for execution.
Attacker may need to collect more information first using blind injection and/or incorrect queries.

Prevention
Parametrized queries, sanitization and validation of inputs

B. Answer the given questions according to the following code. Note that scanf() is used in C to get string/integer input from user. It takes two parameters: input_format and dest_address. (10)

```
int getMarks(int rollNumber);
Boolean checkName (int rollNumber, int obtainedMarks);

int main (int argc, char **argv)
{
    Boolean valid = False;
    int rollNumber = 0;
    int marks = 0;
    char firstname[15] = "";

    printf("Enter your roll  number: ");
    scanf("%d", &rollNumber);

    // function to get marks from the database
    marks = getMarks(rollNumber);

    printf("Enter your first name: ");
    scanf("%s", firstname);

    // function “checkName” validates the name of the user against
```

```
    // the rollNumber and returns a Boolean value.
    valid = checkName(rollNumber, firstname);

    if (valid == False)
        return 0;

    printf("%s ", firstname);
    printf("your marks are  %d\n", marks);

    return 0;
}
```

1. Depict how stack will grow? (2)
2. Identify the problem in the above code? (3)
3. How can you exploit firstname input to display **98** as your marks? (5)

1.

top

firstName (15 bytes)
marks (int)
rollNo (int)
valid (bool)
old frame pointer
main() return address
argc
argv address

2.

For first name, user input is directly saved in memory without bounds-checking. It will result in buffer overflow. Adjacent memory cells will be overwritten (other local variables, then the return address).

For roll number input, user can provide a really large number, but only lower 4 bytes will be stored, causing an integer overflow.

One more minor error is incorrect data type being passed in the 2nd param of checkName

3.

Provide as input a string of exactly 16 characters. First 15 characters can be anything, but the last character should have ascii code 98 (that's letter "b").

Last character will overflow into marks variable, which will be treated as an integer with value 98.

CLO #: 4

Question No. 4: [6+5 marks]

A. Identify the type of malware in the following scenarios. State your reasons.

1. You visited a friend's house and connected your laptop to their Wi-Fi network. Without any further action on your part, the PC crashed due to malware attack. (2)
2. You obtained a cracked copy of Photoshop from an unknown website. It apparently works fine, but you notice that the computer has got very slow and laggy ever since. (2)
3. While browsing the Internet, following message suddenly pops up: ALERT. You location is Lahore, Pakistan, and your activities are being tracked. To protect your privacy, get this VPN service. (2)

1. Worm, auto spreading over the network devices by exploiting vulnerabilities in OS/apps.
2. Trojan, hidden functionality
3. Scareware + trojan, tempting user to install it.

B. Following code exists on the website of an ecommerce store.

```
<form action="http://shopping.pk/order.php">
  <input name="item" value="(item's id number)">
  <input name="quantity" value="1">
  <button>Buy Now</button>
</form>
```

1. An attacker clones the above form on their website. What extra code or steps will they need to launch a forged CSRF request? (3)

<script> document.forms[0].submit(); </script>

above code line causes the form to auto submit. Alternatively, they can also submit the form in response to a user action (e.g. click on a different button)

2. How can the website alter the above form so that CSRF requests can be identified? Show the extra code that needs to be added. (2)

add a hidden field containing STP token
<input type="hidden" name="token" value="(STP token)" />