CS742 MidSem, Nov 20, 2017 (2.00pm to 5.00pm) **[40 Marks]**

Your Name: _____ Your Roll Number: _____

Code of Honour: I hereby declare that I will not cheat (or have not cheated) in this examination. _____ (signature)

Q1	Q2	Q3	Q4	Q5	Q6	Total

General Instructions:

- Handwritten notes (only) are allowed.
- State any assumptions clearly (they should make sense). Draw neatly. Please be crisp and to the point in your answers.
- **No marks for answers without explanation**

Overview: Question 1 [13 Marks]

These are short-answer questions. Please answer in 2-4 lines and not in paragraphs. ***Explain your reasoning behind the answer.*** *Yes/no answers will not fetch you marks.*

1. Why are the public key (pk) and secret key (sk) in the RSA encyrption scheme inverses in group mod $\varphi(n)$ and not inverses in group mod n, where n is the product of two distinct large prime numbers?

   Since n is public, if they were inverses modulo n, then knowing the public key, one can determine the private key. It is difficult to figure out totient of n, without being able to determine the factors of n.

2. Consider a k-bit (output) hash function. If an attacker is trying to find a collision of h i.e. find any two x1 and x2 such that h(x1)=h(x2). How does the expected number of tries before the attacker succeeds grow with respect to k?

   $O(2^{\wedge k/2})$ due to birthday paradox.

3. Name two best practices to follow when designing authentication protocols.

   Use sequence numbers to order messages (prevents insertion)
   Use integrity check that encompasses previous messages (ensures both sides are on same page)

4. Name one similarity and one difference between KDC and CA.

   Similarity: Both help in key distribution

Difference: KDC has to be online for two parties to communicate, not the case with CA.

5. Name two challenges faced by an attacker when perform DNS cache poisoning.

Race against time (the real authoritative server replying before the attacker) and determining the query id when not on path.

6. During the handshake phase of the SSL, what data is exchanged in what manner (open or encrypted, if so how?) to compute a shared secret master key?

Nonce (two, one in each direction); sent in open
A pre-master key sent encrypted by the client using the server's public key

7. Is http://www.coolvids.com:3000/index.html the same origin as http://coolvids.com:3000/index.html ?

No. The host names are different www.coolvids.com, not the same as coolvids.com

8. Name one differences between virus and worms.

Viruses need human intervention to propagate, while worms can propagate without any user intervension.

9. An IP packet is secured using IPSec. In which mode (AH vs ESP and transport vs tunnel) does the original IP header of the packet get encrypted?

ESP in tunnel mode (ESP supports encryption, in the tunnel mode a new Ip header is generated and the original one is part of the payload to be encrypted)

10. Many people lock valuables in a safe in their house in addition to locking the doors of the house. Which among the following practices best describe this approach?
Ensure Complete Mediation
Defense in Depth
Don't rely on security
Privilege Separation

Defense in depth: multiple redundant techniques to make it harder to break

11. Alice knows that she will want to send a single 128-bit message to Bob at some point in the future. To prepare, Alice and Bob first select a 128-bit key $k \in \{0,1\}^{128}$ uniformly at random. When the time comes to send a message $x \in \{0,1\}^{128}$ to Bob,

Alice considers two ways of doing so. She can use the key as a one time pad, sending Bob $k \oplus x$. Alternatively, she can use AES to encrypt x. Recall that AES is a 128-bit block cipher which can use a 128-bit key, so in this case she would encrypt x as a single block and send Bob $AES_k(x)$. Assume Eve will see either $k \oplus x$ or $AES_k(x)$ and that Eve knows an initial portion of x (a standard header), and that she wishes to recover the remaining portion of x. If Eve is an all powerful adversary and has time to try out every possible key key $k \in \{0,1\}^{128}$ which scheme is more secure and why? [2 Marks]

Both are equally secure. With one time pad as we covered in class that it is unconditionally secure, even after trying every possible key (including the actual one), Eve will have no way of recognizing the correct plaintext or even narrowing down the possibilities in any way.

Coming to AES, it is a distinct permutation on $\{0, 1\}^{128}$ under each possible key, and the key was selected uniformly at random, given any plaintext, each possible ciphertext is equally likely. So when AES is used for a single block with a random key of the same length, the effect is exactly the same as using a one time pad: the ciphertext reveals no information about the plaintext.

12. In a stream cipher, if an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. This is a vulnerability, WEP is based on RC4 stream cipher, does it suffer from this vulnerability?

    This vulnerability is handled in WEP through integrity check based on CRC. This check is not very secure but can catch such alterations.

Question 2: CIA investigation of Wireless [6 Marks]

You walk into a coffeeshop with free WiFi. You learn that the network sends all packets unencrypted. And then you see your arch rival Hacker Hari (a very powerful hacker) sitting at a table next to yours using a laptop connected to the same WiFi.

Consider the basic security properties of **confidentiality**, **integrity**, and **availability**. For each of the following scenarios, if you were to start a web session, specify whether Hari can undermine the CIA properties, or not (specific questions which you should answer are listed below). Justify your answer and specify clearly assumptions made (should make sense).

Scenarios:

- DNSSEC-only: your laptop looks up all of the domain names for your web session using DNSSEC but your actual web traffic, however, uses HTTP.
- HTTPS-only means that for a given web site, your laptop looks up all of the domain names for your web session using ordinary DNS but your actual web traffic, however, uses HTTPS.

- DNSSEC+HTTPS means that both your domain name lookups use DNSSEC and your actual web traffic uses HTTPS.

a) Can Hari break confidentiality of your web connection content? Answer for each of the three scenarios.

YES for DNSSEC-only: the web traffic uses ordinary HTTP, which does not provide any confidentiality of its contents.
NO for HTTPS-only and DNSSEC+HTTPS, as HTTPS provides confidentiality.
Note: if you have thought of some MIM attacks, since HTTPS is based on SSL , the browser will check server certificate and caution in case of any issue there. Hari can succeed only if you are careless to ignore such warnings.

b) Can Hari break Confidentiality of keeping private what sites you communicate with? Answer for each of the three scenarios.

YES for all three schemes. DNSSEC does not hide the names you look up nor the replies for those names. HTTPS does not mask your IP address nor that of the servers you visit.

c) Can Hari break integrity of your web connections (i.e. inject data into your connection)? Answer for each of the three scenarios.

YES for *DNSSEC-only*, because HTTP does not provide integrity.
NO for *HTTPS-only* and *DNSSEC+HTTPS*, as HTTPS provides integrity.

d) Can Hari break "Availability" of your web connections? Availability here refers to you being able to access data and services as and when you wish. Answer for each of the three scenarios.

YES for all three schemes. Hari can use TCP RST injection to terminate your connections before you are able to receive any web content. HTTPS protects above *layer 4, but not layer 4 itself.*

Question 3: Web Security Potpurri [6 Marks]

Part-A : Which of the following attacks can <u>web servers</u> protect against by sanitizing user input? For each case, justify your answer.

a) Persistent/Stored XSS

Helps. Atackers often upload scripts using web forms that cause these attacks. If server sanitizes input, this can be prevented.

b) Non-persistent/Reflected XSS

Helps. Atackers uses some script as input to search function. If server sanitizes input, this can be prevented.

c) CSRF

Does not help. A CSRF attack looks identical to a legitimate request; thus, sanitization can't help with blocking them

d) SQL Injection

Helps. Attacker often passes some SQL commands as input (say username or password) to the server for processing.

e) Phishing

Does not help. This targets web browsers, servers have no role

f) Clickjacking

Does not help. In Clickjacking attacks, target web servers receive requests that look identical to legitimate requests.

Question 4: Format String [3 Marks]

Consider the below code which has a format string vulnerability. What argument should the attacker give to change the value of x to 50 (from 1)? Assume that the address of user_input is 0x1111EC11. State all other assumptions made. Draw the stack when explaining your answer.

```
int main(int argc, char *argv[])
{
char user_input[100];
int x=1;
scanf("%s", user_input); /* getting a string from user */
printf(user_input); /* Vulnerable place */
……..
return 0;
}
```

Assuming x occupies 4 bytes and is stored on stack below user_input towards the lower address. The address of X is thus 4 bytes below i.e. at 0x1111EC11 – 4 = 0x1111EC0D.

The attacker should give as argument "\x11\x11\xEC\x0D%46d%n"

Printf prints 4 characters (1 for each of \x) and then it will print the value of x but with 46 space-padding. So overall it prints 50 characters. The next %n will take the value of 100 write to the address 0x1111EC0D since the stack pointer would go past x (which it accessed with %d) and point to the beginning of user_inpu which holds this address.

Question 5: Memory Safety [6 Marks]

Memory safety is the state of being protected from various software bugs and security vulnerabilities when dealing with memory access. Buffer overflow, arithmetic overflow, format string etc are examples of memory safety problems.

For the following code, assume an attacker can control the values of **item** *and* **n** *passed into* **print_report()**.

```
1  /* Returns in "plural" the plural of the given string "str". */
2  void plural(char* str, char* plural)
3  {
4      char* buf;
5      size_t n;
6
7      plural[0] = '\0';
8
9      if ( str == 0 ) return;
10
11     n = strlen(str);
12     if ( n == 0 ) return;
13
14     buf = malloc(n+1);
15     if ( buf == 0 ) return;
16
17     char last = str[n-1];
18     if ( last == 's' )
19         /* Assume it's already plural. */
20         strcpy(buf, str);
21     else if ( last == 'h' )
22         /* fancy plural, like church -> churches */
23         sprintf(buf, "%ses", str);
24     else /* regular plural */
25         sprintf(buf, "%ss", str);
26
27     strcpy(plural, buf);
28     free(buf);
29 }
30
31 void print_report(char *item, int n)
32 {
33     char item_plural[256];
34     plural(item, item_plural);
35     printf("We sold %d %s\n", n, item_plural);
36 }
```

Note: *strlen(s)* calculates the length of the string s, not including the terminating *'\0'* character. *strcpy(dst, src)* copies the string pointed to by *src* to *dst*, including the terminating *'\0'* character. *sprintf* works exactly like *printf*, but instead writes to the string pointed to by the first argument. It terminates the characters written with a *'\0'*.

a) Are there any memory safety problems at lines 23 and 25? Note these need not relate to buffer overflow. Justify your answer.

Yes. *These will write past the end of the heap memory allocated for* **buf**, *since it only has room for the characters in* **str** *plus a terminating* **'\0'** *(due to using* **n+1** *in the call to* **malloc()***).*

b) How about at line 20 and line 27? Justify your answer.

The ***strcpy()*** call at line ***20*** does not present a memory safety problem because there is (just barely) enough room in ***buf*** to hold a copy of ***str***, including the terminating character.

There is a problem at line **27** *because at line* **33** *the code declares* **item_plural** *to have enough storage to hold 256 characters. Therefore if the attacker supplies a value of* **item** *whose plural (including the terminator) exceeds 256 bytes in size, a stack overflow will result when line* **27** *executes the call to* **strcpy()**.

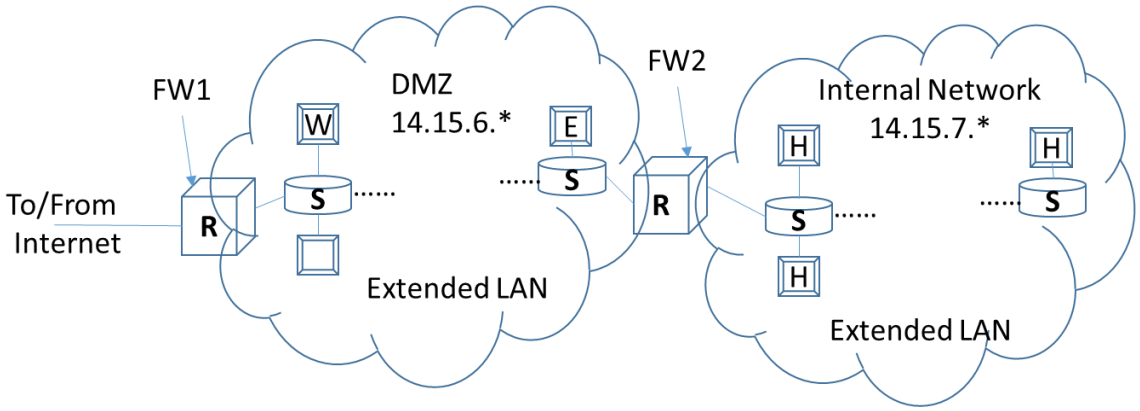
c) Does the code have any format string vulnerabilities? If so, explain how it can be exploited.
The code does not have a format-string vulnerability. Such vulnerabilities only arise when the ***format*** *argument in a call to a function such as* **printf()** *or* **sprintf()** *comes from a value controlled by the attacker. In this code, the calls at lines* **23**, **25**, *and* **35** *all instead use fixed formats.*

Question 6: Firewall [6 Marks]

Consider a network as shown below (IITB follows similar topology). All external facing servers (i.e. servers that need to interface with the outside world) like the web server (W), email server (E) are hosted in a demilitarized zone (DMZ). This DMZ is nothing but an extended LAN served by the network prefix 14.15.6.*. All internal hosts (like your machine and mine) are in the internal network, another extended LAN served by the network prefix 14.15.7.*. A router (R) connects the organization to the Internet and another router (R) interconnects the two LANs. These routers also implement firewall functionality (FW1 and FW2 as shown). Create minimum possible stateless firewall rules for the two firewalls FW1 and FW2 satisfying the below policies. Justify the purpose of each rule.

a) Use a default deny policy.

b) All hosts (including hosts in Internal network) except those belonging to domain 12.16.*.* (organization of suspected hackers), should be able to communicate with the web server 14.15.6.2 over http (port 80).
c) Hosts in a sister organization belonging to 11.14.*.* should be able to speak with any DMZ host over ssh (port 22)
d) Any host in the internal network should be allowed to talk to the DMZ SMTP email server (port 25).
e) Any DMZ host should be allowed to talk to any internal network host via ftp (port 21)
f) Any DMZ system should be able to talk to the DMZ SMTP server 128.168.11.5 (port 25).



FW1					
Src Addr	**Src Port**	**Dest Addr**	**Dest Port**	**Accept/Deny**	**TCP Flags**
12.16.*.*	*	**14.15.6.2**	**80**	**Deny**	**Any**
..*.*	*	**14.15.6.2**	**80**	**Accept**	**Any**
14.15.6.2	**80**	*	*	**Accept**	**Any**
11.14.*.*	*	**14.15.6.***	**22**	**Accept**	**Any**
14.15.6.*	**22**	**11.14.*.***	*	**Accept**	**Any**
..*.*	*	*.*.*.*	*	**Deny**	**Any**

The above handle parts b and c with default deny policy. Note that we need to enable two way communication that is why there are two entries , except for the first rule. For the first rule, if you drop the first syn packet, no more packets will wise from the web server to that domain.

FW2					
Src Addr	**Src Port**	**Dest Addr**	**Dest Port**	**Accept/Deny**	**TCP Flags**
14.15.7.*	*****	**14.15.6.2**	**80**	**Accept**	**Any**
14.15.6.2	**80**	**14.15.7.***	*****	**Accept**	**Any**
14.15.7.*	*****	**14.15.6.5**	**25**	**Accept**	**Any**
14.15.6.5	**25**	**14.15.7.***	*****	**Accept**	**Any**
14.15.6.*	*****	**14.15.7.***	**21**	**Accept**	**Any**
14.15.7.*	**21**	**14.15.6.***	*****	**Accept**	**Any**
.*.*.	*****	***.*.*.***	*****	**Deny**	**Any**

The above handle parts b, d and e with default deny policy. Note that we need to enable two way communication that is why there are two entries.

The policy "f" does not need a firewall rule since they can talk directly in the extended Lan, this traffic will not hot the routers.

TimePass:

1. Topic you liked best in the course:

   A teacher is not supposed to have favourites ;-)

2. Topic you liked least in the course

   Malware material could use some excitement.

3. How would you introduce yourself when you are 30? ☺

   Haha, I am past that age ☺

(Rough)