Raluca Ada Popa
Spring 2018

CS 161
Computer Security

Midterm 1

PRINT your name: _____, _____
(last) (first)

I am aware of the Berkeley Campus Code of Student Conduct and acknowledge that academic misconduct will be reported to the Center for Student Conduct.

SIGN your name: _____

PRINT your class account login: `cs161-`_____ and SID: _____

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

You may consult one sheet of paper of notes. You may not consult other notes, textbooks, etc. Calculators, computers, and other electronic devices are not permitted.

If you think a question is ambiguous, please come up to the front of the exam room to the staff. If we agree that the question is ambiguous we will add clarifying assumptions to the central document projected in the exam rooms. Write your student ID on the top of every page.

You have 80 minutes. There are 8 questions, of varying credit (155 points total). The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until your instructor tells you to do so.

SID _____

Problem 1 ***True or False*** **(20 points)**

Bubble in True or False for each of the questions below. You do not need to explain your answers.

(a) If WˆX is enabled and an attacker induces a buffer overflow that overwrites a local variable with attacker code, if afterwards the original program writes to the local variable, an error will occur flagging this situation.

O True O False

(b) If ASLR is enabled and we leak the address of a local variable, then we know the address of all local variables since ASLR does not randomize their relative offsets.

O True O False

(c) If we have a stack canary and the attacker does not know its value, it is impossible (except with small probability) for an attacker to overwrite the return address of a function and cause the execution of other code.

O True O False

(d) A larger TCB is more secure because it means that more components of the system must be broken in order to compromise the system.

O True O False

(e) In the Diffie-Hellman protocol, one way to calculate $g^x \bmod p$ in polynomial-time is to multiply g by itself $x - 1$ times, reducing modulo p at every iteration.

O True O False

(f) It is OK if the attacker knows the IV which will be used for AES-CTR in advance.

O True O False

(g) If one bit of a plaintext block is flipped in AES-CTR mode, that changes roughly half of the bits of that ciphertext block.

O True O False

(h) If one bit of a plaintext block is flipped in AES-CBC mode, that changes roughly half of the bits of that ciphertext block.

O True O False

(i) Say that Alice and Bob have two pre-shared keys k and k'. Alice can guarantee the integrity and confidentiality of a message M if she sends AES-CBC$_k(M)$ and the tag MAC$_{k'}(M)$.

O True O False

(j) Say we have two similar messages M and M'. We encrypt both messages in CBC mode, but accidentally reuse the same IV. Then we encrypt both messages in CTR mode, but accidentally reuse the same IV (but different from the one we used for CBC mode). CBC mode will compromise lesser or equal amounts of information compared to CTR mode.

O True O False

SID _____

Problem 2 ***Short Answer*** **(15 points)**

Give **concise** answers to the following questions. Do not provide multiple answers to a question; you will not receive credit even if your answers contain a correct answer.

(a) Give one way an attacker could exploit a buffer overflow without executing their own shellcode.

(b) On some Linux systems, the least significant byte of a stack canary is always NUL (`0x00`). However, this decreases the entropy of the canary making it easier for an attacker to guess the canary randomly. Identify one **advantage** of having this NUL byte in stopping buffer overflow exploits.

(c) Alice and Bob are thinking of using asymmetric encryption with a **single** public & private key that they both share. Explain one advantage of symmetric encryption over this asymmetric encryption model.

(d) What is the computationally difficult problem that RSA digital signatures rely on?

(e) In all the confidentiality cryptography games we have discussed, the adversary gets to send a pair of messages (m_0, m_1) to the challenger. The challenger only reveals the encryption of one of these messages. Explain why m_0 and m_1 need to be the same length.

SID _____

Problem 3 ***Student Linked List*** **(20 points)**

Lord Dirks writes the following code below to manage the students of Leland Junior University:

```
1  struct student_node {
2      char name[8];
3      struct student_node *next;
4  };
5
6  typedef struct student_node student_node;
7
8  void add_student(student_node *head, char *student_name) {
9      student_node *new_student = calloc(1, sizeof(student_node));
10     while (head->next) head = head->next;
11     head->next = new_student;
12     strcpy(head->name, student_name);
13 }
14
15 student_node first;
16
17 int main() {
18     char *name_to_add;
19     first.next = NULL;
20     while (has_input()) {
21         name_to_add = safely_read_input();
22         /* esp = 0xbfff'f09c */
23         add_student(&first, name_to_add);
24     }
25 }
```

(a) Identify the line which causes the vulnerability. What vulnerability is this?

(b) Raluca needs your help to PwN Lord Dirks. To help you, she added some shellcode at the memory address `0xdeadbeef`. What names would you need to enter into the program in order to cause the execution of the shellcode? Note that the value of `esp` at line 21 is `0xbffff09c`. Assume that the compiler does not reorder any local variables or pad stack frames. Furthermore assume that the call to `strcpy` is inlined.

SID _____

Problem 4 ***New Operating Systems*** **(20 points)**

Answer the following questions about security principles as presented in class as **concisely** as you can.

(a) Alice is writing a new operating system TuxOS. She notices that the following lines of code appear many times:

```
1 FILE *fp;
2 if (!access_ok(filename)) exit(1);
3 fp = open_file(filename, "r");
```

i. Alice is scared that eventually she will forget to add an `access_ok` check. Which security principle is most relevant to this situation?

ii. How would you fix the security issue above?

iii. What other security issue is relevant to this code?

(b) Bob is frustrated with TuxOS and decides to develop a new open source OS, Noobuntu. The main feature of Noobuntu is that the user needs to specify the permissions with which each program runs. This means that if a user wants a video chat application to work properly, they would grant the application access to: a temporary directory to store temporary files, the internet, the camera, the microphone, and the speakers. Bob argues that this will secure users against malware from the internet.

i. What security principle does Bob have in mind with this feature?

ii. Alice asks Bob how Noobuntu handles programs running other programs. He didn't think about that and runs home to patch Noobuntu before anyone notices. He specifies that programs run other programs with the same set of permissions that were granted to the first program. Is this design secure? Why or why not?

iii. Bob, frustrated with all the people trying to attack his system, decides to rewrite his code in Penguin++, a new programming language he wrote up overnight. Bob, proud of his knowledge of cryptography implements cryptographic primitives in his language to add extra security. He reasons that because nobody knows Penguin++ they won't be able to understand what he is doing, and definitely won't be able to attack his system. What are two reasons why Bob's new system may be insecure?

SID _____

Problem 5 ***Selection*** **(20 points)**

Evelyn is working on some code to sort the prefix of an array. Here is her code so far:

```
1  /** Sort the first n integers of the array a */
2  void sort(int a[], size_t n) {
3      for (size_t i = 0; i < n; i++) {
4          size_t idx = i;
5          for (size_t j = i; j < n; j++)
6              if (a[j] > a[idx])
7                  idx = j;
8
9          /* part (b) */
10
11         int tmp = a[idx];
12         a[idx] = a[i];
13         a[i] = tmp;
14     }
15 }
```

(a) What are the preconditions needed for memory safety of the above code?

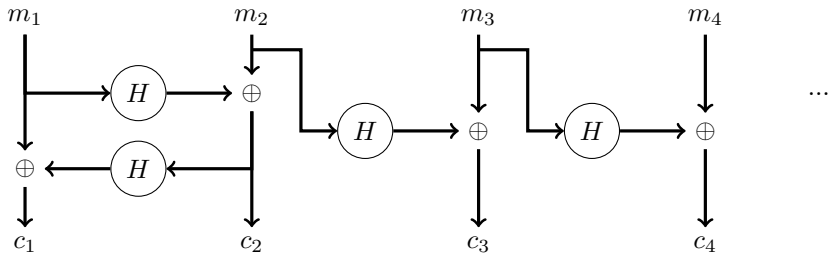
(b) What are the invariants which hold at the line denoted part (b)? Express your answer mathematically or in very precise English.

(c) What are the postconditions ensured by this function? Express your answer mathematically or in very precise English.

SID _____

Problem 6 ***Hashing a Scheme Out*** **(15 points)**

Alice doesn't trust block ciphers because she feels that rectangular shapes can't be trusted, so she has created her own encryption scheme using hashing. She's enlisted your help in analyzing the security of her scheme; just don't tell her that this is a "block" diagram.



(a) Now Alice needs to choose the hashing function H. Assume that key is a 128-bit key (generated randomly once) and IV is a 128-bit initialization vector (generated randomly for every encryption). Furthermore we define $a||b$ as the concatenation of a and b. For example if $a =$ "Hello" and $b =$ "World", then $a||b =$ "HelloWorld".

If H was defined as

$$H(x) = \text{SHA256}(\text{IV}||\text{SHA256}(x||\text{key}))$$

would this make scheme IND-CPA? Explain your reasoning.

○ Yes ○ No

Explain:

(b) What would decryption look like in this scheme? Listing decryption for m_1 and m_i where $i > 1$ is sufficient.

SID _____

Problem 7 ***Protocols*** **(25 points)**

Alice wants to send a message to her friend Bob. Evaluate each of the cryptographic protocols below on confidentiality, integrity, and authenticity by marking all that apply. **Confidentiality** means that an eavesdropper cannot learn any information about the contents of the message. **Integrity** means that a man-in-the-middle cannot modify any messages sent without Bob eventually detecting it. **Authenticity** means that Bob can tell that the message came from Alice. (Assume that everyone knows Alice and Bob's public keys.)

Mark **Broken** if it is impossible for Bob to decrypt the message, or if it is impossible to perform the protocol. If a protocol is **Broken**, you do not need to determine its other properties.

(a)
1. Alice sends Bob a key k, encrypted with Bob's public key.
2. Alice sends Bob AES-CBC$_k(M)$.

☐ Confidentiality ☐ Authenticity

☐ Integrity ☐ Broken

(b)
1. Alice sends Bob two keys k and k', both encrypted with Bob's public key.
2. Alice sends Bob AES-CBC$_k(M)$, MAC$_{k'}$(AES-CBC$_k(M)$).

☐ Confidentiality ☐ Authenticity

☐ Integrity ☐ Broken

(c)
1. Alice sends Bob a key k, encrypted with Bob's public key.
2. Alice sends Bob a signature on k using her RSA key.
3. Alice sends AES-CBC$_k(M)$ to Bob.

☐ Confidentiality ☐ Authenticity

☐ Integrity ☐ Broken

(d)
1. Alice sends Bob a key k, encrypted with Bob's public key.
2. Alice sends Bob a signature on k using her RSA key.
3. Alice sends $M, \text{MAC}_k(M)$ to Bob.

☐ Confidentiality ☐ Authenticity

☐ Integrity ☐ Broken

(e)
1. Alice breaks her message up into small blocks $B_1, B_2, \ldots, B_n$. These blocks are small enough to be encrypted and signed asymmetrically (say 1024 bits).
2. Alice encrypts each block B_i with Bob's public key to produce a ciphertext C_i. Then, Alice signs C_i to produce a signature s_i.
3. Alice sends $(C_1, s_1), \ldots, (C_n, s_n)$ to Bob.

☐ Confidentiality ☐ Authenticity

☐ Integrity ☐ Broken

SID _____

Problem 8 ***Food!*** **(20 points)**

Suppose there is a database where each entry is a name of a person and the person's favorite food, all encrypted. Mallory is an "honest but curious" employee at the company who knows the names of every person in the database but wants to know about their favorite food. However, she does not have the private keys to any encryption scheme the database uses.

Note that in this particular database, the names do not repeat, but the foods may repeat. Also assume that when encrypting, padding is used so the length is the same.

(a) Suppose there is a request made to the database to fetch all the names. Each name is encrypted and sent out, and Mallory can see all of these encrypted names. More concretely, she sees $E_k(\text{name}_1), E_k(\text{name}_2), \ldots$ If the encryption scheme was deterministic could Mallory learn anything new? Why or why not?

(b) Could Mallory learn anything new if the encryption scheme was IND-CPA? Why or why not?

(c) Suppose a new request is made to obtain all the foods. As previous, Mallory can see all of these encrypted values: $E_k(\text{food}_1), E_k(\text{food}_2), \ldots$ If the encryption scheme was deterministic, could Mallory learn anything new? Why or why not?

(d) Could Mallory learn anything new if the encryption scheme was IND-CPA? Why or why not?

SID _____