University of Waterloo
Midterm Examination

Term: Fall Year: 2014

Student Name _____

UW Student ID Number _____ **ANSWER KEY** _____

Course Abbreviation and Number	CS 458/658
Course Title	Computer Security and Privacy
Section(s)	001, 002 and 003
Instructor	Douglas Stinson and Tariq Elahi
Date of Exam	October 16, 2014
Time Period	Start time: 7:00 pm End time: 8:20 pm
Duration	80 minutes
Number of Exam Pages (including this cover sheet)	11 pages
Exam Type	Closed Book
Additional Material Allowed	NO ADDITIONAL MATERIALS ALLOWED

Answer all questions in the space provided. If you need extra space, use the backs of pages or the extra page at the end of the exam. Answers will be marked for clarity as well as correctness.

Marking Scheme (for graders' use only):

Question	Max	Score	Marker
1	20		
2	11		
3	9		
4	6		
5	9		
6	9		

Maximum Total Score: 64

Total Score:

1. (20 points) True or false with explanation/justification.

For each of following statements, give both a TRUE/FALSE answer (1 mark) **and** a brief explanation or justification of your answer, which should include a definition, example, or explanation of the relevant technical concept (1 additional mark).

Statement	True or False?
The Heartbleed bug allows the attacker to send malformed messages to the server causing the server to reveal private information. The attacker can request a large chunk of the server's memory as a heartbeat response due to a missing length check.	T
To exploit a buffer overflow bug, the aim is to hijack the flow of the program by overwriting the frame pointer. The **return address** is overwritten.	F
The Morris worm is named after the popular 1970's dance of the same name. The Morris worm was named after its inventor.	F
A rootkit allows the administrator to remove infections from hosts on their network. A rootkit is malware that enables privileged access to a computer and which employs stealth capabilities to avoid detection.	F
The "control-alt-delete" used in Windows operating systems is a defence against interface illusions. This key sequence takes the user to a real "login" screen, bypassing a fake login screen created by an attacker.	T

Statement	True or False?
The "chroot" attack allows a malicious user to gain root access on a remote machine. The chroot attack allows a malicious program to break out of a sandbox.	F
Requiring a password in addition to four-digit PIN is an example of two-factor authentication. Passwords and PINS are both "something you know".	F
Biometric identification is usually a search problem. A characteristic (e.g. an unknown fingerprint) must be matched to one in a database, which requires a search.	T
Even if two users choose the same password, they are unlikely to have the same fingerprints if salt is used. The fingerprint is created by hashing the password and user-specific salt.	T
The setuid bit in Unix is used to create a new user id. The setuid bit in Unix specifies that an executable should be run with the permissions of its owner.	F

2. (11 points) Buffer overflows.

Consider the following program which runs with elevated privileges on a 32-bit x86 architecture, but accepts command-line input from an untrusted user.

```
int main(int argc, char *argv[])
{
    int x = 0;
    int n = atoi(argv[1]);
    int *p = &global_storage;
    int y = 0;
    char buf[32];

    strncpy(buf, argv[2], 48);
    *p = n;
    return 0;
}
```

(The `int atoi(char *s)` function converts a string to a number; for example, `atoi("157")` returns the number `157`.)

(a) The program was compiled using the same compiler and options you used in the UML environment in Assignment 1. What does the stack look like for `main`? Draw the stack, indicating the direction of increasing memory addresses. Label the contents of each four bytes. (You can use a compressed notation for the large buffer.)

32 byte buf, 4 byte y, 4 byte p, 4 byte n, 4 byte x, 4 byte saved frame pointer, 4 byte retaddr, 4 byte argc, 4 byte argv (in increasing order of memory address). [4 points]

(this question continued on the next page)

(this question continued from the previous page)

(b) What memory can an attacker overwrite? How can the attacker overwrite the return address in order to execute shellcode of his choosing?

The attacker can overwrite buf, y, p, n, and x. The attacker could insert a nop slide and shell code into the beginning of buffer, then overwrite p to point to the return address, and overwrite n to point to somewhere in the nop slide. When the line *p=n executes, the program will overwrite the return address with the desired execution location. [3 points]

(c) To protect against buffer overflow attacks the compiler adds a canary to the stack. The value of the canary is 0xffbe00cc. Does this remove the possibilities of a buffer overflow attack? Give details of why or why not.

It does not. Since the attack above overwrites the return address specifically it can avoid overwriting the canary and thus not cause any alarms.[2 points]

(d) A solution that has been suggested to address the basic buffer overflow problem on a stack is to have the stack grow in the opposite direction (i.e., the stack pointer would increase when the stack grows). Explain how this suggestion could prevent a basic buffer overflow.

Overflowing a buffer will no longer overwrite the return address; instead it will overflow the unused portion of the stack.[2 points]

3. (9 points) CIA

(a) What are the CIA goals of computer security?

Confidentiality, integrity, availability. [3 points]

(b) For each of the following attacks, briefly describe the attack or give an example of the attack, say which CIA goal is being defeated by the attack and give a brief explanation as to how the attack defeats the goal. You should only provide *one* goal (i.e., the primary goal) for each attack. The three attacks are meant to illustrate all three CIA goals.

Timing attack on a smart card that is doing encryption operations

Confidentiality. By monitoring operational characteristics of a smart card such as timing, it may be possible to determine confidential information such as a cryptographic key. [2 points]

A virus infects an executable program

Integrity. The payload of a virus infects a file or program, that is, the program is modified from its original form. [2 points]

A logic bomb encrypts a users hard drive and issues a ransom demand

Availability. The data on the hard drive is not available until the ransom has been paid. [2 points]

4. (6 points) Malware and Software Flaws

(a) How does a worm spread from one computer to another?

The worm infects vulnerable network daemons and other already running background processes on hosts. [2 points]

(b) Some backdoors in software are non-malicious intentional flaws. Give an example of how this could occur, justifying why the flaw is non-malicious and intentional.

A backdoor may be inserted intentionally for (non-malicious) debugging purposes by the programmer, who later forgets to remove it when the software goes into production. (Other answers are also acceptable.) [2 points]

(c) Web bugs allow advertisers to track users' visits to websites. In the following HTTP request for a LinkedIn ad, describe how the identity of a user could potentially be revealed and to whom.

```
GET [path of ad]
HOST: ad.doubleclick.net
Referer:  https://www.linkedin.com/
profile.php?id=123456789&ref=name
Cookie:  id=2015bdfb9ec
```

doubleclick learns from the referrer field that the user has come from LinkedIn as well as the LinkedIn profile accountID. The LinkedIn accountID leads to a user page which could include name, education, and other personally identifiable information. This way doubleclick can relate the cookie (which so far did not tell doubleclick who the person they are tracking is in real life) to a particular identity extracted from the LinkedIn profile page. [2 points]

5. (9 points) Bell-La Padula

Suppose that objects have classification levels

"top secret" $\geq$ "secret" $\geq$ "confidential" $\geq$ "unclassified"

and are assigned to compartments from the set {Asia, Middle East, Africa, South America}. Secret Agent 86 has clearance "secret" and is assigned to compartments {Asia, Africa}. Read-write access is governed by the Bell-La Padula confidentiality model.

(a) Can Agent 86 read a document with classification "confidential" and compartments {Asia, South America}?

No; the documents's compartments are not a subset of 86's compartments [2 points]

(b) Can Agent 86 read a document with classification "top secret" and compartments {Asia}?

No; the document's classification level is higher than 86's clearance level [2 points]

(c) Can Agent 86 write to a document with classification "top secret" and compartments {Asia, Africa, South America}?

Yes; the document's classification level is higher than 86's clearance level, *and* the document's compartments are a superset of 86's compartments [2 points]

(d) Suppose now we are considering the **dynamic** version of Bell-Lapuda, where any read-write access is allowed, but subjects and/or objects may subsequently be reclassified using "low watermark" rules. Suppose Agent 86 writes to a document with classification "top secret" and compartments {Asia, South America}? After this "write" operation, which subjects/object(s) will be reclassified and what will be their new classification?

The **document** must be reclassified to GLB((TS,{Asia, South America}), (S, {Asia, Africa})) = (S, {Asia}). [3 points]

6. (9 points) Miscellaneous

(a) Describe a polymorphism technique that a virus might use to try to fool signature-based virus scanners. How might this technique still be detected by a signature-based virus scanner?

A copy of the virus consists of a random key, decryption code, and the encrypted virus code. The decryption code is the same in all copies of the virus, so this can potentially be recognized by a signature-based scanner. [3 points]

(b) On Android phones, applications ask the users to approve permissions at install time. Sometimes applications request more permissions than the application actually requires, e.g., access to location information for a news feed. Give two possible reasons why the developer might ask for unnecessary permissions. Which one of the Saltzer-Schroeder design principles is being violated by this practice? Explain.

Advertising purposes, or just carelessness on the part of the developer (the developer can't be bothered to think about which permissions are actually required, so he requests all of them). Least privilege is being violated. [3 points]

(c) Why is an access control matrix rarely implemented as a matrix? Name and describe the two common ways in which access control matrices *are* implemented.

It is very sparse. Implementations: *access control lists (ACLs)*, the column-wise representation of the matrix, in which each object is associated with a list of subjects and their access rights or as *capabilites*, the row-wise representation, in which each subject is given a set of unforgeable tokens that convey access rights. [3 points]

(Extra space for any question, if needed)