King's College London

This paper is part of an examination of the College counting towards the award of a degree. Examinations are governed by the College Regulations under the authority of the Academic Board.

Degree Programmes	MSc, MSci
Module Code	7CCSMSEN
Module Title	Security Engineering
Examination Period	January 2017 (Period 1)
Time Allowed	Two hours
Rubric	ANSWER ALL QUESTIONS
Calculators	Calculators are not permitted
Notes	Books, notes or other written material may not be brought into this examination

PLEASE COMPLETE YOUR ANSWERS IN THIS BOOKLET AND PROVIDE YOUR CANDIDATE NUMBER BELOW	
CANDIDATE NUMBER	

PLEASE DO NOT REMOVE THIS PAPER FROM THE EXAMINATION ROOM

1. a. Before starting a TCP connection, clients and servers perform the following three-way handshake:

$A \rightarrow S$: SYN
$S \rightarrow A$: SYN-ACK
$A \rightarrow S$: ACK

Describe briefly how this handshake protocol can be abused by an attacker.

[5 marks total]

b. In terms of security, what is the main difference between online banking and e-voting?

[3 marks total]

QUESTION 1 CONTINUES ON NEXT PAGE

c. In which situations does it make sense to install on a computer an invalid (that is, self-signed) certificate? Give 2 example situations.

[2 marks total]

d. Explain briefly what is meant by a certification authority becoming "too big to fail" when it has issued a large number of certificates. (Hint: Consider the incentives of the browser vendors.)

[2 marks total]

QUESTION 1 CONTINUES ON NEXT PAGE

e. What does *Kerckhoffs' principle* say?

[2 marks total]

f. Nonces are unpredictable random numbers used in protocols. Consider the following protocol using a secret shared key K_{AB} and a nonce N:

$$A \to B: \quad N$$
$$B \to A: \quad \{N+1\}_{K_{AB}}$$

Write down 3 facts that A can infer after this protocol has been successfully completed.

[6 marks total]

QUESTION 1 CONTINUES ON NEXT PAGE

g. How can an attacker exploit the fact that every night root has a cron job that deletes the files in `/tmp`? (Hint: what is a cron-attack?)

[6 marks total]

h. If an attacker uses a buffer-overflow attack in order to inject code, why can this code not contain any zero bytes (that is $\backslash 0x00$)?

[2 marks total]

QUESTION 1 CONTINUES ON NEXT PAGE

i. Why is it crucial that the stack grows from higher addresses to lower ones for a buffer-overflow attack to work? (Hint: Explain carefully what is stored on the stack and how it influences the control flow of the program.)

[6 marks total]

j. A few years ago, a Google executive tried to dispel worries about Google reading and storing all your emails on Gmail. He argued: "Worrying about a computer reading your email is like worrying about your dog seeing you naked". What is wrong with this argument? Give 2 counter arguments.

[2 marks total]

QUESTION 1 CONTINUES ON NEXT PAGE

k. Consider buffer-overflow attacks: When filling the buffer with a payload (for example for starting a shell), what is the purpose of padding the string at the beginning with NOP-instructions?

[4 marks total]

l. Consider the following simple mutual authentication protocol:

$$\begin{aligned} A \to B&: \quad N_A \\ B \to A&: \quad \{N_A, N_B\}_{K_{AB}} \\ A \to B&: \quad N_B \end{aligned}$$

Explain how an attacker E can launch an impersonation attack by intercepting all messages for B and make A decrypt her own challenges.

QUESTION 1 CONTINUES ON NEXT PAGE

[10 marks total]

2. a. In the context of privacy, what is meant by the term *forward privacy*?

[2 marks total]

b. In the Estonian general election, votes can be cast via Internet for some time before the election day. These votes can be changed an unlimited amount of times; the last vote is tabulated. You can even change your vote on the polling day in person. Which security requirements for voting systems does this procedure address?

[3 marks total]

QUESTION 2 CONTINUES ON NEXT PAGE

c. Is it possible that Bitcoins can become lost (that is, become irretrievable)? Explain briefly your reasoning.

[2 marks total]

d. The department has a number of labs full of computers that are mostly idle over night. Why is it a bad idea to let these computers mine for Bitcoins?

[2 marks total]

QUESTION 2 CONTINUES ON NEXT PAGE

e. In the context of security validation, what is the main difference between hacking and penetration testing?

[2 marks total]

f. (1) What are the differences between a penetration test and a vulnerability scan? Give 2 facts and explain your answers. (2) What are the similarities between a penetration test and a vulnerability scan? Give 2 facts and explain your answers.

[8 marks total]

QUESTION 2 CONTINUES ON NEXT PAGE

g. Write down the (1) read rule and the (2) write rule of the Bell-LaPadula access policy. (3) In terms of information flow, what does this access policy ensure?

[3 marks total]

h. What can an attacker who controls the network do to a communication between a client and a server? Write down 4 attacks and classify them as passive or active. (Hint: Think about the messages a server and client exchange.)

[4 marks total]

QUESTION 2 CONTINUES ON NEXT PAGE

i. Consider the following protocol between a car C and a key transponder T:

1. C generates a random number N
2. C calculates $(F, G) = \{N\}_K$
3. $C \rightarrow T$: N, F
4. T calculates $(F', G') = \{N\}_K$
5. T checks that $F = F'$
6. $T \rightarrow C$: N, G'
7. C checks that $G = G'$

(1) Assume the key K is shared only between the car and the transponder. Does the protocol achieve that the transponder authenticates itself to the car? If yes, briefly explain why. If not, briefly describe an attack. (2) Does the car authenticate itself to the transponder? Again, explain briefly your reasoning. (3) Why must the random number N be unpredictable and from a large pool of possibilities for this protocol to be secure?

[9 marks total]

QUESTION 2 CONTINUES ON NEXT PAGE

j. A Unix directory might look as follows:

```
$ ls -ld . * */*
drwxr-xr-x 1 alex staff  32768 Apr  2 2010 .
-rw----r-- 1 alex gurus  31359 Jul 24 2011 manual.txt
-r--rw--w- 1 marc gurus   4359 Jul 24 2011 report.txt
-rwsr--r-x 1 marc gurus 141359 Jun  1 2013 microedit
dr--r-xr-x 1 marc staff  32768 Jul 23 2011 src
-rw-r--r-- 1 marc staff  81359 Feb 28 2012 src/code.c
-r--rw---- 1 lisa gurus    959 Jan 23 2012 src/code.h
```

with group memberships assigned as follows:

Members of group staff: alex, marc, lisa
Members of group gurus: lisa

The file microedit is a text editor, which allows its users to open, edit and save files. Note carefully that microedit has set its setuid flag, indicated by the lower-case `s`. Fill in the access control matrix below that shows for each of the above five files, whether alex, marc, or lisa are able to obtain the right to read (R) or replace (W) its contents using the editor microedit.

	manual.txt	report.txt	microedit	src/code.c	src/code.h
alex					
marc					
lisa					

[15 marks total]