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, and Access Control and Privacy Policies
Examination Period	January 2018 (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

TURN OVER WHEN INSTRUCTED

© 2018 King's College London

1.

a. When storing passwords, the passwords should always be hashed and salted. (1) How do the salts help with preventing dictionary attacks? Give two facts. (2) In the context of passwords, should salts be kept secret or not?

[3 marks total]

b. 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]

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

[2 marks total]

d. Why is making bank customers liable for financial fraud a bad design choice for credit card payments?

[2 marks total]

e. (1) Give the five main requirements in voting systems. [5 marks]
(2) In the Estonian general election, votes can be cast via Internet 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 requirement for voting systems does this procedure address in Estonia (give one requirement)? [2 marks]

[7 marks total]

f. Explain the main disadvantage of the following protocol that establishes a mutual key between two parties A and B with the help of a mutually trusted third party S:

$$A \to S: \ A, B$$
$$S \to A: \ \{K_{AB}\}_{K_{AS}} \text{ and } \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$$
$$A \to B: \ \{K_{AB}\}_{K_{BS}}$$
$$A \to B: \ \{m\}_{K_{AB}}$$

[4 marks total]

g. (1) Explain briefly how an attacker can use chain voting in order to influence the outcome of a poll that uses paper ballots. [6 marks]
(2) Explain briefly how to defend against such chain voting without compromising ballot secrecy. [2 marks]

QUESTION 1 CONTINUES ON NEXT PAGE

SEE NEXT PAGE

[8 marks total]

h. If the 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]

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. Why does randomising the addresses from where programs are run help with defending against buffer-overflow attacks?

[2 marks total]

k. In case a buffer-overflow attack includes a payload (for example for starting a shell), what is the purpose of padding the string at the beginning with NOP-instructions?

[2 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.

[10 marks total]

2.

a. In the context of privacy, what is meant by a *re-identification attack*?

[2 marks total]

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

[2 marks total]

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

[2 marks total]

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

[2 marks total]

e. 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]

f. 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]

g. Write down (1) the read rule and (2) the write rule of the Biba access policy. [2 marks each]. (3) In terms of information flow, what does this access policy ensure? [1 mark]

[5 marks total]

h. 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]

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

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

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

[6 marks total]

j. Explain briefly:
(1) What is spear phishing? [2 marks]
(2) Why is it so effective? [4 marks]

[6 marks total]

k. 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?)

[8 marks total]

l. What information about the employees of a target organisation is important when it comes to a penetration test? Name at least 2 types of information and why they are important/useful?

[8 marks total]