The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2020-2021

Computer Security

Time allowed: ONE HOUR (60 MINUTES)

Candidates may complete the front cover of their answer book and sign their desk card but must NOT write anything else until the start of the examination period is announced

Answer ALL questions

This exam is worth a total of 60 marks

No calculators are permitted in this examination.

Dictionaries are not allowed with one exception. Those whose first language is not English may use a standard translation dictionary to translate between that language and English provided that neither language is the subject of this examination. Subject specific translation dictionaries are not permitted.

No electronic devices capable of storing and retrieving text, including electronic dictionaries, may be used.

DO NOT turn your examination paper over until instructed to do so

Collect examination question papers at the end of the examination.

1. As an expert in computer security, many people approach you with basic questions about the topic. Please (briefly) answer all of the following:

(a) What do the letters stand for in the CIA model of computer security? [1 mark]

(b) After a GNU/Linux user types "`chmod 377 test.sh`" in a directory containing his file `test.sh`, can this user then read the contents of this file? [1 mark]

(c) If a firewall policy blocks/drops access by default, but allows some specific listed services / ports: would this policy most accurately be called a Blacklisting or Whitelisting policy? [1 mark]

(d) In software quality assurance, is testing without access to the actual source code more accurately called Black Box or White Box testing? [1 mark]

(e) Would a hacker who uses his/her skills to cause damage, commit crime, and hurt people more accurately be called a Black Hat or White Hat hacker? [1 mark]

(f) Define "Security Engineering." [2 marks]

(g) Define Kerckhoffs's Principle. [2 marks]

(h) Tigress is a freely available (but not open source) C obfuscator, developed at the University of Arizona: What does a code obfuscator do? [2 marks]

(i) Two benefits of public key cryptography are encryption and signing (authenticating): briefly explain how these both of work using public key cryptography. [3 marks]

(j) What is the value of 11^{29} (MOD 12)? [3 marks]

(k) Consider a program that reads in a series of integers and calculates their sum. One Metamorphic Relation for this program would be that any permutation of the series should not impact the output value (`sum(a,b,c,d) == sum(d,c,b,a)`). Very briefly outline a different possible Metamorphic Relation for this program. [3 marks]

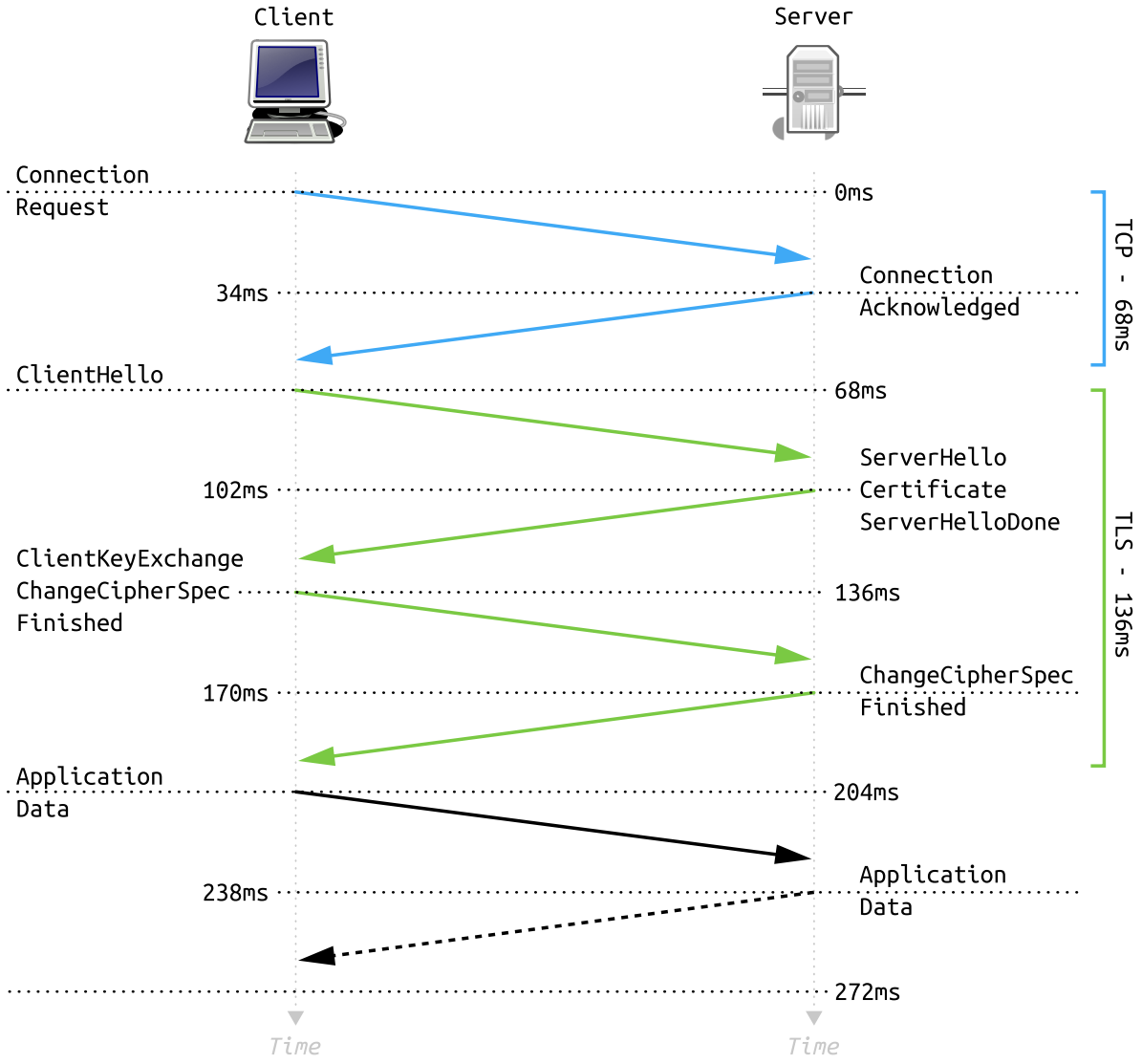
[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

<<Turn over>>

2. You are a professor of Security Engineering, and you enjoy teaching your students about all aspects of Security. You especially like telling stories about how many security mistakes in the past were caused by simple human error. While talking about SSL and TLS, you decide to discuss the Heartbleed incident.

(a) What do the letters SSL and TLS stand for? [2 marks]

The following diagram shows a simplified presentation of the full TLS 1.2 handshake, between a Client and Server:



As part of the [**ClientHello**] message, the client indicates that it supports (and requests) use of TLS version 1.1. In response, the server, in the [**ServerHello**] message, will specify which TLS version to use.

(b) If the server supports versions 1.1, 1.2, and 1.3 (the latest version), which version will/should it specify in the [**ServerHello**] message?

[2 marks]

Heartbleed refers to a security bug introduced into some very widely-used software in 2012, and publicly disclosed in 2014.

(c) What was the name of the software that the Heartbleed bug was introduced into? [1 mark]

(d) Explain (in detail) what the Heartbleed bug is, and how it could be exploited. [8 marks]

(e) Explain how Metamorphic Testing might have been expected to identify what became the Heartbleed bug. [4 marks]

Although publicly disclosed in 2014, it has been suggested (by Bloomberg News) that the USA's NSA knew about the flaw/vulnerability much earlier. However, instead of reporting it, they kept it secret, along with other unreported zero-day vulnerabilities.

(f) What do the letters NSA stand for? [1 mark]

(g) What is a zero-day vulnerability or zero-day attack? [2 marks]

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

<<Turn over>>

3. You prefer to use Microsoft products, including as your main operating system, your DBMS, and other things. People often ask you questions related to the security issues associated with Microsoft.

(a) Many systems include databases that support queries written in SQL. Briefly explain the concept of an SQL injection attack.

[2 marks]

(b) Attackers may use "Database Fingerprinting" as a step in their attack on a system. Very briefly outline the principles behind this.

[2 marks]

An attacker uses the following input to explore the system under attack, where `waitfor` is an instruction that only works on Microsoft SQL Server, causing such systems to wait for the specified duration:

```
http://shop.com/items.php?id=2; waitfor delay '0:0:10'--
```

(c) If the target system is running MySQL, how many seconds delay will the attacker experience?

[1 mark]

(d) What do the letters TOCTTOU stand for? [1 mark]

(e) Is a cryptographic system where the same key is used do both encrypt and decrypt more accurately described as symmetric or asymmetric?

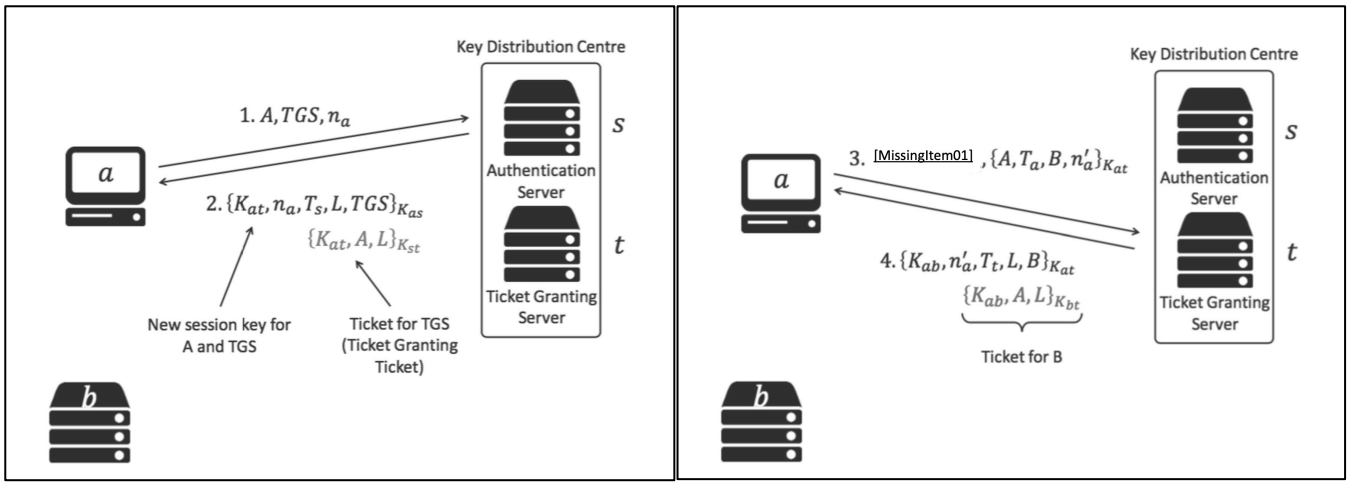
[1 mark]

The Kerberos system is a popular network authentication protocol that uses a concept of *tickets* to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It is used as a default in Windows OS.

(f) Is a cryptographic system that Kerberos uses more accurately described as symmetric or asymmetric?

[1 mark]

The following diagrams outline part of a typical exchange with Kerbros. In this example, Node 'a' wants to communicate with Node 'b'. As part of this, Node 'a' asks the Authentication Server to enable Node 'a' to communicate with the Ticket Granting Server. Node 'a' then asks the Ticket Granting Server to give it a "ticket" to enable it to communicate directly with Node 'b'. (The notation $\{SomeContent\}_{K_{xy}}$ means that "SomeContent" is encrypted with a key that only x and y have.)



(g) In the picture on the right-hand side, beside Step 3, what is the actual content of "[MissingItem01]"?

[2 marks]

In the picture on the right-hand side, in Step 4, the "Ticket for B" is essential for Node 'a' to next communicate with Node 'b'.

(h) Can Node 'a' read the content of "Ticket for B"?

[1 mark]

(i) Explain/justify your answer to the previous question ('h').

[3 marks]

(j) The next step (after Step 4 in the right-hand picture) will involve Node 'a' sending "Ticket for B" to Node 'b'. Explain in detail what Node 'b' will do when receiving it.

[6 marks]

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam

<<End>>