(4)

(*Knowledge for Development*)

KIBABII UNIVERSITY

UNIVERSITY EXAMINATIONS
2021/2022 ACADEMIC YEAR

END OF SEMESTER EXAMINATIONS
YEAR ONE SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF
MASTER OF SCIENCE IN DIGITAL FORENSICS

COURSE CODE : MDF 810

COURSE TITLE : PRINCIPLES OF SECURITY ENGINEERING

DATE: 30/09/2022 TIME: 09:00 A.M – 12:00 A.M.

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTIONS ONE AND ANY OTHER TWO.

QUESTION ONE [20 MARKS]

Many critical industries, such as electricity, water, oil and gas, have plant controlled by complex digital systems. These "Supervisory Control and Data Acquisition" (SCADA) systems connect sensors, such as temperature and pressure gauges, with actuators, such as valves and switches, and control rooms. They were originally standalone systems and were thus designed without security mechanisms. However, over the last ten years, they have increasingly acquired Internet connectivity, and now there is serious concern about "cyberterrorism" in the form of online sabotage.

As a result, the North American Electric Reliability Corporation (NERC) has ordered critical electricity utilities to protect their networks from 2022 or face substantial fines.

You have been hired by a utility that has several thousand devices on its central sites and several hundred at remote locations (the exact numbers are not known).

These devices will disclose data to, or act on data from, anyone who communicates with them using the appropriate protocol.

a) Discuss the advantages and disadvantages of the following protective strategies.

   i. Implementing fault-tolerant logic in the control system to identify and isolate faulty sensors. [4 marks]

   ii. Using a firewall to isolate the control system network from the corporate network and the Internet. [4 marks]

   iii. Authenticating traffic on the control system network by replacing sensors and actuators by, or supplementing them with, devices that can generate and verify message authentication codes. [4 marks]

b) Your customer opts for strategy (ii) in respect of central sites and strategy (iii) for remote devices. Sketch an overall system design and discuss any residual risk. [8 marks]

QUESTION TWO [20 MARKS]

a) Formally state the two rules of the Bell-LaPadula (BLP) security policy model and then re-state them informally in terms of a single rule about the direction of information flow.

[2 marks]

b) Consider a distributed system in which A is a TOP SECRET process running on machine Alice and B is a CONFIDENTIAL object residing on machine Bob.

i. Explain and justify whether A is allowed to read and/or write from B according to the BLP policy. [2 marks]

ii. Discuss the claim made by some researchers that this scenario highlights a fundamental problem with the BLP policy. [4 marks]

c) Explain the difference between discretionary and mandatory access control.

[3 marks]

d) Discuss how one might implement a system enforcing the Bell–LaPadula model.

[5 marks]

e) Explain what covert channels are, and how they can limit the usefulness of multilevel secure systems. [4 marks]

QUESTION THREE [20 MARKS]

a) Explain the concept of a Trusted Computing Base and outline its meaning in the context of the access control provided by a typical Unix workstation. [5 marks]

b) An automatic teller machine (ATM) communicates with a central bank computer for PIN verification. A 32-bit CRC code is added to each packet to detect transmission errors and then the link is encrypted using a block cipher in counter mode. Describe an attack that is possible in this setup. [5 marks]

c) (i) Describe a cryptographic protocol for a prepaid telephone chip card that uses a secure 64-bit hash function H implemented in the card. In this scheme, the public telephone needs to verify not only that the card is one of the genuine cards issued by the phone company, but also that its value counter V has been decremented by the cost C of the phone call. Assume both the card and the phone know in advance a shared secret K.

[5 marks]

(ii) Explain the disadvantage of using the same secret key K in all issued phone cards and suggest a way around this. [5 marks]

QUESTION FOUR [20 MARKS]

a) Social networking sites are becoming ever more popular, and many other sites now let users add each other as friends. Discuss the effect that social context has on

i. Phishing [2 marks]

ii. Inference control [2 marks]

iii. Market for privacy [2 marks]

iv. Community detection [2 marks]

b) Threat modeling can help make your product more secure and trustworthy. Discuss the following methods of threat modelling as used within an Agile environment.

i. STRIDE [3 marks]

ii. PASTA [3 marks]

iii. OCTAVE [3 marks]

c) In what ways might social context be used to protect against harm online? [3 marks]

QUESTION FIVE [20 MARKS]

The lifecycle of an exam question in a fictitious university includes at least the following stages, which take place over several months:

i. Lecturer sets the question.

ii. Chief examiner sanity-checks it.

iii. Lecturer amends it if necessary.

iv. External examiner sanity-checks it.

v. Lecturer amends it again if necessary.

vi. Chief examiner approves final version.

vii. Examination coordinator prints question in required number of copies.

Following a scandal whereby some dishonest candidates got hold of questions ahead of time, thus forcing the whole exam to be invalidated and repeated to the dismay of the honest participants, the university has put pressure on its departments to ensure this will not happen again.

a) The Head of Department A, where the leak occurred, is now paranoid about computer networks and insists that no exam question shall ever reside on any networked computer system until after the corresponding exam takes place.

   i. Describe four ways that a determined undergraduate might nonetheless get hold of exam questions before the exam even if those requirements were observed. [4 marks]

   ii. Describe a security policy suitable for department A, taking into account the head-of-department's requirements and the staff workflow. Discuss it thoroughly, including requirements analysis, incentives and technical mechanisms. [4 marks]

b) The Head of Department B finds that A's requirement would impose an excessive penalty on the productivity of her staff. At the same time, she certainly does not want to be blamed for the next leak.

   i. Describe a security policy suitable for department B, taking into account the head of department's requirements and the staff workflow. Discuss it thoroughly, including requirements analysis, incentives and technical mechanisms. [6 marks]

   ii. Describe three trade-offs between security and usability that you considered in devising the policy in (b)(i) and justify the choices you made. [6 marks]