CE708-7-AU

UNIVERSITY OF ESSEX

Postgraduate Examinations 2022

COMPUTER SECURITY

Time allowed: **TWO** hours (exam time) + **ONE** hour to allow for submission time (total **THREE** hours)
(Please see your exam timetable or check on FASER for the deadline to upload your answers)

The times shown on your timetable are in British Summer Time (BST) (GMT+1). Please check online for a conversion to your local time if you will be undertaking your assessment outside the United Kingdom

Candidates are permitted to use:
Calculator – Casio FX-83GT Plus/X or Casio FX-85GT Plus/X ONLY

The paper consists of **FOUR** questions.

Candidates must answer **ALL** the questions.

The questions are **NOT** of equal weight.

The percentages shown in brackets provide an indication of the proportion of the total marks for the **PAPER** which will be allocated.

If you have a query with the content of this exam paper please use the revision FAQ Forum on the module's Moodle page. Your academic will be available to answer any queries in real-time.

If you have a technical problem with FASER, or any other query, please go to Exams Website to find contact details of the teams that can help you.

Please note that the time allocated for this assessment includes time for you to download this question and answer paper and to upload your answers to FASER.

You should complete the Answer Sheet supplied using a word-processed file format or PDF. If you need to handwrite/draw any or all of your answers, you should take a photo or scan these to be included **WITHIN** one answer sheet. (i.e. ALL YOUR ANSWERS SHOULD BE UPLOADED TO FASER IN ONE DOCUMENT – THE EXTRA HOUR ON THE EXAM LENGTH IS TO ALLOW YOU TIME TO DO THIS AND DEAL WITH ANY TECHNICAL ISSUES).

Please allow at least 30 minutes at the end of your exam time to upload your work. Once you have completed the assessment do not leave it to the last minute to upload.

Please save your work throughout the examination to avoid losing your work. Please do not communicate with any other candidate in any way during this assessment. Your response must be your own work. Procedures are in place to detect plagiarism and collusion.

Question 1

You are required to develop a message authentication system for a healthcare company to deal with the messages sent from doctors to patients. This system requires the use of keys, a hash function and a substitution cypher.

a) Draw a schematic of a message authentication system using all the three components discussed above (Keys, hash function and substitution cypher). Comment on your design creating a justification for the method you created. [10%]

b) Describe two choices of different hash functions and substitution cyphers that can be used by your message authentication system. [10%]

c) Describe a set of vulnerabilities with the hashed message authentication and suggest modifications to have a more secure system. [10%]

Question 2

A technology company is asked to develop a bespoke software system which will allow doctors to access the health records of patients from any personal computer, including laptops, connected to the internet. A bespoke client-side application will be deployed on each personal computer. A centralized server will hold the entire dataset for all patients.

The security of the system is very important; in particular, the patients' data must be kept strictly confidential.

Comment on each of the three proposed design decisions below. For each design: discuss the strengths and weaknesses of each proposal with respect to security, identify specific attacks and discuss how the design could be improved.

a) Users will be authenticated using passwords over a securely-encrypted connection. Each user will be allowed to choose their own password, provided that it contains at least 128 bits of entropy. A hash of the user's password will be retained on the authentication server, but not the password itself. A user's account will be temporarily locked if more than twenty consecutive unsuccessful login-attempts originate from the same IP address. [10%]

b) Users will be authenticated using RSA (RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977). A national public-health body acts as a Certificate Authority (CA) for users' public keys. Keys will be chosen such that the exponent can be represented as a 256-bit integer. The private-key will be stored on the user's hard disk. [10%]

c) In order to keep data secure while it is transferred from the server to the client, it will be encrypted using the Data Encryption Standard (DES). The DES key will be negotiated on a per-session basis using a Diffie-Hellman (DH) protocol. The DH protocol uses 2048-bit keys. [10%]

Question 3

Alice sends a message, x, to Bob where the message is protected using encrypt(x) where encrypt(x) is generated using either: An AES cypher created using a shared secret key; or an RSA using Alice's private key and Bob's public key.

An attacker, Oscar, is able to observe the message x sent from Alice to Bob and Oscar knows Alice's public key, but does not know the shared secret key used for the AES or Alice's private key. Three potential attacks include:

- Bruteforce attack with a differential cryptoanalysis;
- Replay of the message;
- Man in the middle attack;

For each of the scenarios below, answer the questions and state whether, and how, either AES or RSA provide protection against the stated attack.

a) Bob claims that he received an encrypted message encrypt(x) from Alice (e.g., the decoded message reads "Transfer $1000 from Alice to Bob") but Alice claims she has never sent it. Can Alice clear this question in either case? Explain why. [7%]

b) Alice sends a message x = "Transfer $1000 to Mark" using encryption(x) to Bob. Oscar intercepts the message using bruteforce with a differential cryptoanalysis and replaces "Mark" with "Oscar." Will Bob detect this? [7%]

c) Alice sends a message x = "Transfer $1000 to Oscar" using encryption(x) to Bob. Oscar observes the message and sends it 100 times to Bob. What can Alice and Bob do to overcome this attack? [7%]

Question 4

Assume you receive an e-mail that appears to come from a senior manager of your company, with a subject indicating that it concerns a project that you are currently working on. The email asks you to review the attached revised press released, supplied as a PDF document, to check that all details are correct before management releases it. When you attempt to open the PDF, the viewer pops up a dialog labelled "Launch File," indicating that "the file and its viewer application are set to be launched by this PDF file." In the section of the dialog labelled "File" there are a number of blank lines and finally the text "Click to 'open' button to view this document." You also note that there is a vertical scroll-bar visible for this region.

a) What type of threat might this pose to your computer system should you indeed select the "Open" button? [5%]

b) How could you check your suspicions without threatening your system? [5%]

c) What type of attack is this type of message associated with? [5%]

d) How many people are likely to have received this particular e-mail? [4%]

END OF PAPER CE708-7-AU

Once you have completed your answers, please upload them to FASER
http://faser.essex.ac.uk

Remember to add your REGISTRATION NUMBER onto ALL documents that you upload.