University of Strathclyde Glasgow

Department of Computer and Information Sciences

CS808 Computer Security Fundamentals

Monday 5th December 2022 **10am – 12pm**

Duration: 2 hours

Attempt all Questions

Q.1

You have been employed by Help4You, a small business which provides mental health counselling services for individuals. Help4You currently has a website which was created by a friend of the company owner. However, the website has been attacked and now the owner, Alex, realises the website was very insecure. You have been tasked with exploring the aspects of the website which are insecure and assisting in improving the robustness of the website, whilst educating the owner so they do not make the same mistakes in the future.

The first thing area to examine is authentication and access control. There are three main user groups for the website; the counsellors, the administrators and the clients. The counsellors should be able to perform functions such as accepting counselling session requests, creating and accessing counselling notes, and viewing a calendar of their appointments. Clients can view their own details such as name and address and request a counselling session. Administrators can edit client and counsellor details and assign counsellors to clients.

Alex has reviewed the functionality and proposes the following applies the principle of least privilege.

-view counselling requests can be done by administrators and counsellors
-assign counsellor to client can be done by administrators and counsellors
-view counselling notes can be done by administrators and counsellors
-request counselling session can be done by clients and administrators
-edit client details can be done by administrators, counsellors, and clients

a) Evaluate whether the above aligns with the principle of least privilege, making sure you justify your argument. State any assumptions.

(3 marks)

The owner is concerned that a client could potentially use a counsellor's account to get access to highly sensitive information on other clients.

b) Identify what type of attack the owner is describing and justify why it is this type of attack.

(3 marks)

c) From the perspective of a legitimate client, detail two approaches to completing the attack type described in part b.

(6 marks)

d) Alex, the owner of help4you, wants to ensure users of the system select sufficiently strong passwords. Alex heard that one way of measuring password security is through entropy. One example of a password Alex has used in the past is alexSecret3. Using this example password, explain how entropy works, what it represents, and how it would be applied to the old password. You can assume an alphabet of lower-case a-z, upper case A-Z, and numbers 0-9. You are not expected to perform the calculation, but should highlight how this is applied to the example provided. The equation is $\log_2 n^l$

(8 marks)

Q.2

You have been employed by a company who wishes to test the security of their systems and processes. Firstly, you must get access to their local network. The company works in a building which houses several organisations. There is a coffee shop on the entry floor which has its own network to allow customers to access the internet. Several employees use this network to access their work email over the web client. The coffee shop network has a password which is written on a blackboard in plain sight.

a) Describe a series of steps which you could take in an attempt to capture a legitimate user's company e-mail address and password. Identify any conditions which must be met for such an attack to be successful.

(5 marks)

b) The next step is to access the floor of the building in which the company resides. In order to do this, you must get past the reception desk where a member of staff permits or denies entry. Describe a social engineering attack which you could attempt to gain access. In particular, identify the manipulation techniques which you aim to exploit and how you plan to execute these.

(5 marks)

c) You have now been able to connect to the organisation's network. You are using a packet sniffing tool and notice that there are unencrypted messages which are frequently sent between client and a server. You deduce that it would be possible to complete a man in the middle attack, where you spoof the server to the client. What security mechanism would mitigate such an attack? Provide justification for your choice.

(5 marks)

d) You have now deployed malware on the server which provides the functionality of a game. When the user runs the game, it then emails all their e-mail contacts with a link to the game for them to download and run, what type of malware is this likely to be and why?

(5 marks)

Q.3

A small accountancy firm based in Glasgow provides services to clients such as sending invoices for services rendered on a client's behalf, responding to client queries, and completing the annual accounts and tax returns for clients. Kris is a client of the accountancy firm, but has moved to the highlands. Each client has an accountant assigned to them.

a) Kris wishes to securely communicate with the accountancy firm and has to overcome the key exchange problem. Identify two approaches to solve this which do not involve meeting to share a key, highlighting how these approaches solve the key sharing problem.

(5 marks)

Kris wants to send their accountant a message that includes an invoice for Sam who owes Kris £250. Kris and the accountant have a shared secret X. Kris initiates a communication with the accountant by sending: KR + AC + n (Kris's identity, the accountant's identity, and a random number n) encrypted using the accountant's public key. This message can be represented as PubK_AC(KR+ AC + n) The accountant maintains a list of the random numbers sent by Kris.

Propose cryptographic messages (similar to the example above) which should be sent to meet the security requirements detailed below. Assume that Kris and the accountant do not currently share a symmetric key (K), but both have distributed their public keys PubK_KR (Kris's public key) and PubK_AC (Accountant's public key).

b) Propose a message which the accountant could send to Kris which would provide assurance the message was from the accountant and ensures confidentiality.

(2 marks)

c) Kris is now assured they are communicating with the accountant, Kris and the accountant need to agree a symmetric session key K. Propose a message exchange between Kris and the accountant which would achieve this whilst ensuring confidentiality, authenticity, and integrity and confirmation of the agreed symmetric key.

(4 marks)

d) Propose two checks the accountant could use to mitigate a replay attack, explaining why they would help mitigate a replay attack.

(4 marks)

e) As a software developer, the accountancy firm have contacted you to discuss threat modelling. The firm wish to develop software which clients can use to collate and send invoices and receipts. They are keen to ensure it is designed and built with security in mind. Propose and describe a form of threat modelling which might suit this context, justifying your choice.

(5 marks)

END OF PAPER

Dr Rosanne English