UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR10058 COMPUTER SECURITY

Tuesday 10th May 2016

09:30 to 11:30

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

CALCULATORS MAY NOT BE USED IN THIS EXAMINATION

Year 3 Courses

Convener: C. Stirling
External Examiners: A. Cohn, T. Field

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. **Passwords** [*25 marks*]

The University of Edinburgh has been requiring staff members and students to pick 8-character-long passwords made up only of letters (lower and upper case) and digits. Each character can appear at most once in each password. If a user enters a wrong password they are prompted to try a different one.

The University is now reconsidering its password policy as it fears that the current one is not secure enough as passwords are too short. It now requires that password be 12 characters long, and can contain any of the 95 possible characters. It further allows for passwords to contain repeated characters. To make the longer passwords more usable in the new system, if a user enters a wrong password during login he is told how many of the initial characters match the correct password. For example if Alice's password is 123456789ABC, and she types in 1234567alice, the server replies that the 7 first characters are correct.

Determine which of these two policies is more secure against brute force attacks by answering the following questions:

(a) What is the maximum number of guesses an attacker needs to make to find a user's password chosen under the first policy? Provide the mathematical expression for computing this number. [*4 marks*]

(b) What is the maximum number of guesses an attacker needs to make to find a user's password chosen under the second policy? Provide the mathematical expression for computing this number. [*4 marks*]

The social networking website LinkedIn was hacked on 5 June 2012, and usernames and passwords for nearly 6.5 million user accounts were stolen by cybercriminals. The stolen passwords, which were only hashed, were cracked and posted on a forum later on that day. Internet security experts said that the passwords were easy to unscramble because of LinkedIn's failure to use a salt when hashing them.

(c) Suppose an attacker wants to find the password for a specific user via a dictionary attack. Does the absence of salting in LinkedIn's scheme make the attack computationally less expensive for the attacker than if it were salted? [*4 marks*]

(d) Suppose the attacker wants to find at least half of the passwords via a dictionary attack. Does the absence of salting in LinkedIn's scheme make things computationally more expensive for the attacker? [*4 marks*]

QUESTION CONTINUES ON NEXT PAGE

(e) 20% of the LinkedIn users that have a Yahoo account use the same password both for their LinkedIn and Yahoo accounts. However, unlike LinkedIn, Yahoo salts the stored passwords. Does that mean that these users do not need to change the passwords of their Yahoo accounts? [*4 marks*]

(f) How does salt slow down an offline dictionary attack? Explain why a random salt protects against a rainbow attack. [*5 marks*]

2. **Web security** *[25 marks]*

TheBookShop allows clients to order books online visiting a URL of the form

`https://www.thebookshop.com/order?title=OliverTwist`

```
def order_handler(cookie, param):
    print "Content-type: text/html\r\n\r\n",

    user = check_cookie(cookie)
    if user is None:
       print "You first need to log in"
       return

    book = param['title']
    if in_stock(book):
       ship_book(book, user)
       print "Order succeeded"
    else:
       print "Book", book, "is currently not in stock"
```

The `param` argument contains the query parameters in the HTTP request (*i.e.*, the part of the URL after the question mark). The function `check_cookie` checks the cookie and returns the username of the authenticated user.

(a) Briefly define cross-site scripting (XSS) attacks. Explain the difference between reflected and stored XSS attacks. *[5 marks]*

(b) Is this website vulnerable to an XSS attack? If your answer is yes, explain how an attacker could exploit it, and explain how TheBookShop could fix it. If your answer is no, explain why such an attack is not possible. *[5 marks]*

(c) Briefly define cross-site request forgery (CSRF) attacks. *[4 marks]*

(d) Is this website vulnerable to a CSRF attack? If your answer is yes, explain how an attacker could exploit it, and explain how TheBookShop could fix it. If your answer is no, explain why such an attack is not possible. *[5 marks]*

(e) Suppose a user uses two browsers: one for visiting low-security websites, and a different one for visiting "sensitive" websites. For example, the user could use Chrome to read blogs and Firefox for banking. You will assume that each browser stores temporary files and cookies in a different directory.

i. Would using two browsers in such a way prevent reflected XSS attacks? *[2 marks]*

ii. Would using two browsers in such a way prevent stored XSS attacks? *[2 marks]*

iii. Would using two browsers in such a way prevent CSRF attacks? *[2 marks]*

3. **Network/System Security** *[25 marks]*

An online marketing company ZoomMarket recently learned that an attacker named Eve hacked into their systems and stole their valuable customer data. ZoomMarket hired a security forensic analyst to determine how Eve accomplished the attack. ZoomMarket would like to implement some of the analyst's recommendations, but they are suspicious that the advice might not work for them. They have hired you to provide additional advice on how to prevent future attacks like Eve's.

Below are three attacks Eve used on ZoomMarket and the recommendations of the security analyst. Answer the questions for each attack. Marks will be awarded to succinct answers that address the points being asked, providing relevant specific details.

Attack: Eve sent phishing emails to ZoomMarket employees asking them to log into a fake website she controlled. One employee fell for the attack and logged into the fake site using his ZoomMarket username and password. ZoomMarket uses one-factor password authentication, so Eve was able to use the compromised credentials to log in as a legitimate employee.

Analyst Recommends: Use two-factor authentication for all logins.

(a) Would two-factor authentication have protected ZoomMarket against the above attack? Explain your answer. *[2 marks]*

(b) Suggest a way two-factor authentication could be practically implemented on ZoomMarket's website without buying special equipment for each employee. Be specific and include the factors you would use. *[3 marks]*

(c) Describe an additional non-technical approach ZoomMarket could use to help their employees avoid falling for Phishing attacks. Give an example of how this approach might work. *[2 marks]*

(d) ZoomMarket's board is concerned about spearphishing attacks containing malicious attachments. They want you to install a firewall that will protect employee email by removing all .zip and .doc attachments. Where would you recommend such a firewall be installed (router, email server, or the client computer), and why would you recommend that it be located there? *[4 marks]*

(e) Would the firewall the CEO is asking for in (d) have prevented Eve's phishing attack? Explain your answer. *[2 marks]*

QUESTION CONTINUES ON NEXT PAGE

Attack: Eve discovered that ZoomMarket had an internal web server visible from other computers on ZoomMarket's network. She used the well known Shell Shock vulnerability to trick the web server into running shell commands using the authority of the web server user. She uses the attack to disable the database logging process.

Analyst Recommends: Update the server in accordance with Cyber Essentials requirements.

(f) Would updating all the software on the server have protected ZoomMarket against the above attack? Explain your answer. [*2 marks*]

(g) The programmer who wrote the code on the web server no longer works for ZoomMarket and updating the server is impossible. Name two other requirements of Cyber Essentials and describe how you might use each to protect ZoomMarket's vulnerable web server. [*4 marks*]

(h) There are five common security properties. What security property was violated by disabling logging? (Only answer in regards to the logging, not what might happen after.) [*1 mark*]

Attack: Eve uses a SYN flood attack sent from a single computer she controls to create a large amount of traffic that takes down ZoomMarket's main external web server.

Analyst Recommends: Install an Intrusion Detection System (IDS) and monitor it regularly for attacks.

(i) Would an Intrusion Detection System have prevented the above attack on ZoomMarket's external web server? Explain your answer. [*2 marks*]

(j) What is the general terminology for the type of attack Eve is using against the external website? [*1 mark*]

(k) Describe one problem with SYN Flooding that makes it less than ideal for attackers and provide an alternative attack Eve could have used that would not have the problem. [*2 marks*]