Xi'an Jiaotong-Liverpool University

西交利物浦大學

Paper code	Examiner	Department	Tel
CSE316		Computer Science	

Spring Semester 2019 Resit Examination

Computer Systems Security

Time allowed: 2 hours

Instructions to candidates

- **Total marks available are 100**
- **There are 4 questions**
- **Answer all questions**
- **Points for each question are clearly indicated**
- **Write your answers in the answer book provided**
- **All answers must be in English**
- **All materials must be returned to the invigilator upon completion of the exam. Failure to do so will be deemed as academic misconduct and will be dealt with according to the University's policy.**

Short Answer Section

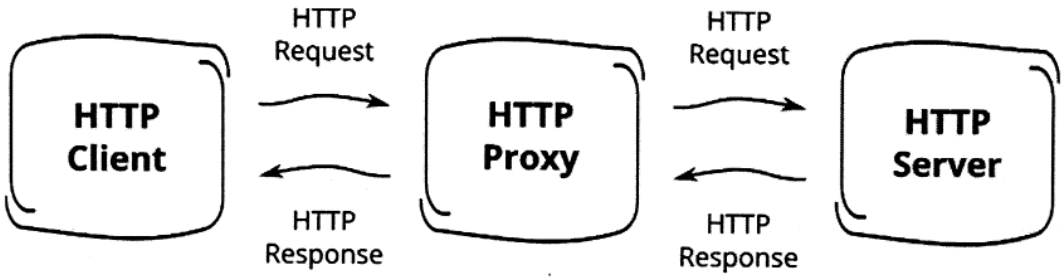
1. On June 7th, LinkedOut confirmed that it had experienced a data breach that likely compromised the e-mail addresses and passwords of 6.5 million of its users. This confirmation followed the posting of the password hashes for these users in a public forum.

   Assume that each stolen password record had three fields in it: [`user_email, SHA666(password + salt), salt`] where the salt is 32 bits long and that a user login would be verified by looking up the appropriate record based on user_email, and then checking if the corresponding hashed password field matched the SHA666 hash of the password inputted by the user trying to log in plus the salt. The SHA666 algorithm was written by LinkedOut because "other hashing algorithms were too slow", so they wrote one that was 10x faster than any existing hash algorithm.

   It was further discovered that the widely used random number generator used to generate the salt was poorly written and only generated 4 possible salts. Given this:

   a) **(7 points)** What effect does the flaw in the random number generator used have on the security of the LinkedOut scheme?
   b) **(7 points)** Is the selection of the SHA666 algorithm a good thing or a bad thing? In 1-2 sentences explain why.
   c) **(6 points)** It turns out that 20% of LinkedOut users with Yahoo Mail e-mail addresses used the same password at LinkedOut as at Yahoo. You learn that, unlike LinkedIn, Yahoo correctly salts its passwords. Should Yahoo be concerned about the LinkedIn breach or not? Explain why.

2. An http proxy server is a server which sits in between a user's browser and a web server and forwards http requests and responses.



Http proxies can be used for several reasons, such as speeding up web access by keeping a local cache of popular web pages, or bypassing blocking or filtering software by encrypting requests.

a) **(15 points)** Briefly explain how a malicious proxy server could perform a man-in-the-middle attack on site protected by SSL/TLS.

b) **(5 points)** Do browsers have any existing protection against this, and if so what? If not, suggest a protection mechanism.

Long Answer Section

The following questions should be answered in 1-2 pages of your answer booklet. You will be graded on the completeness and technical accuracy of your answers, but not the grammar or writing style.

3. **(30 points)** You are an engineer for the DingDong shopping network (dd.com). Your core system consists of a database which contains customer data, product data, etc, and a web server (which is connected to your database) that customers use to access your website. Discuss how you would use six different protection mechanisms to protect both the data while it is stored in the database as well as while it is in transit to and from the customer. Feel free to draw a small diagram if it helps you explain.

4. **(30 points)** You are employed as an engineer for the defense contracting company, Boing. Evil Country X has offered you a large sum of money to give them information about your company's projects. Describe at least 5 ways you could exploit your insider position to gain access to information you would not normally have access to. You do not need to include technical details, but you need to clearly explain how you would perform each attack (meaning this should not be just a list of short answers).

END OF EXAM