Xi'an Jiaotong-Liverpool University

西交利物浦大學

Paper code	Examiner	Department	Tel
CSE316		Computer Science	

Spring Semester 2019 Final 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.**

1. On June 7th, LinkedIn 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. One criticism of LinkedIn is that they used *unsalted* password hashes. In this question we'll explore this criticism.
   Assume that each stolen password record had two fields in it: `[user_email, SHA1(password)]` 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 SHA1 hash of the password inputted by the user trying to log in. By contrast, if LinkedIn had used a salted scheme, then each record would have had three fields: `[user_email, salt, SHA1(password+salt)]` and login verification would similarly require looking up the salt and using it when matching hashes. Given this:

   a) **(7 points)** Suppose the attacker's goal is to break *your* password via a dictionary attack. Does the lack of salting in LinkedIn's scheme make this goal substantially easier? Explain why.
   b) **(7 points)** Suppose the attacker's goal is to break at least half the passwords via a dictionary attack. Does the lack of salting in this scheme make this goal substantially easier? Explain why.
   c) **(6 points)** It turns out that 20% of LinkedIn users with Yahoo Mail e-mail addresses used the same password at LinkedIn as at Yahoo. You learn that, unlike LinkedIn, Yahoo salts its passwords. Should Yahoo be concerned about the LinkedIn breach or not? Explain why.

2. A consortium of printer vendors have come up with a great new protocol to help users automatically discover the set of printers on their local network. In this protocol, when the user wants to print something, the user's computer automatically broadcasts a Printer Discovery packet. A Printer Discovery packet is a UDP packet whose destination address is the broadcast address, and whose source and destination port is 56184. Because this is a broadcast packet, every host on the local network will receive it. Printers constantly listen for Printer Discovery packets. Any time that they receive one, they immediately respond with a Printer Announcement packet. A Printer Announcement packet is a UDP packet whose destination address is the broadcast address, and whose source and destination port is 56185; its payload identifies the name of the printer, the printer's IP address, and any special options supported by the printer (e.g., 2-sided printing, color printing, 3D printing, etc). The Printer Announcement packet is broadcast to the entire network, so that other hosts on the local network can also learn about this printer. Whenever a machine receives a Printer Announcement packet, it checks that the source address of the packet matches the printer's IP address found in the payload. In case of a mismatch, it ignores the packet. Otherwise, it accepts the packet and adds this printer to its list of known printers. To accommodate changes in address assignment, if the machine's list of known printers already contains a printer with the same name, the machine overwrites the previous entry in its list with the information found in the newly received packet.

   Victor the Victim is about to connect his laptop to a local switched Ethernet network. His laptop will use this printer discovery protocol to look for a printer, and then Victor will connect to one of the printers found in this way and send it a sensitive corporate document to be printed. Meanwhile, Hermione the Hacker is attached to this same network. Hermione has the ability to inject packets onto this network and to receive all broadcast packets, but she cannot eavesdrop on other traffic. The printers are in locked rooms that Hermione does not have access to, and Hermione has not been able to hack or access any of the machines or printers attached to this network, so her only hope is to attack the printer discovery protocol.

   a) **(10 points)** Can Hermione arrange to learn the contents of Victor's document, without physically accessing any of the printers? If yes, describe the attack, if no explain why the attack isn't possible.
   b) **(10 points)** Can Hermione modify what is printed on the printer? In other words, Hermione wants to replace Victor's chosen document with something else Hermione has chosen, hopefully without Victor noticing. It's not acceptable if Victor's original document gets printed in addition to Hermione's replacement, because then Victor might notice and get suspicious. Can Hermione mount such an attack without physically accessing any printers? If yes, describe the attack, if not explain why the attack isn't possible.

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)** The Micro$soft company runs a collection of websites, all with single sign on. All of their websites use TLS, but because certificates are expensive, they decide to self-sign all their TLS certificates. Supposed you have a neighbor who uses unencrypted wifi to access some of these websites, and you'd like to steal his user name and password. Describe at least 5 attacks that you could use to accomplish this, clearly outlining how the attack would work, and what level of control of or access to the network you would need. (This could be anything from no special access to that you would need to work for a major government agency.) **Assume that the cryptography itself is unbreakable.**

4. **(30 points)** In your spare time, you've decided to set up a botnet, so you can make a little extra cash sending spam. Describe how you'd do this. Include how you'd get the software on the victims' computers, how you'd hide it from them, how you'd control your botnet, and how you'd hide what you were doing when the police came looking for you.

END OF EXAM