14-741/18-631: Midterm exam
Thursday October 17, 2019, 80 minutes

Name:

Andrew ID:

Scores

Problem 1 (26 pts max):

Problem 2 (30 pts max):

Problem 3 (12 pts max):

Problem 4 (20 pts max):

Problem 5 (12 pts max):

Total (100 pts max):

Guidelines

- This exam contains 5 problems and is 16 pages long. Check you have all pages.
- If you need more space than what's given on the page for a question, please use the extra page and add a note stating that "more on the extra page".
- Be neat and concise in your explanations. Limit your answers to the space provided. You won't be penalized for using incorrect grammar, but you will get penalized if we can't understand what you are writing.
- Show your work clearly. If your reasoning (in other words, steps) is correct, but your final answer is wrong, you will receive most of the credit. On the other hand, answers without proof, explanation, or argumentation get no credit, *even if they are correct*.
- This exam is open-book. All reference books, class notes, dictionaries are allowed. No electronic devices are allowed.
- Open-book does not mean open neighbor. Cheating on the exam (including accessing the Internet) automatically results in failure of the class and will be reported to the University administration. We do enforce the INI plagiarism policies strictly.
- It is advantageous to partially answer a question than not attempt it at all.
- Problems are independent of each other, and **all questions in each problem are independent of each other**. If you get stuck, just skip the question that you can't solve and come back to it later.
- Good luck!

1 Short answers (26 pts)

Each of the following questions can be answered in a couple of sentences. Be concise.

1. (4 pts) Give one reason why the government wants backdoors in cryptography.

2. (4 pts) Give one reason why allowing government-controlled backdoors in cryptography is a bad idea.

3. (4 pts) Alice and Bob are communicating with each other over an insecure connection. Describe an attack of the confidentiality of the message exchange, if Alice did not adequately validate Bob's public key.

4. (4 pts) Alice and Bob are communicating with each other over an insecure connection. Describe an attack of message authentication of the message exchange, if Alice did not adequately validate Bob's public key.

5. (4 pts) Explain why ECB is not recommended for encrypting sensitive data.

6. (6 pts) Name one principle that Saltzer and Schroeder advocates in designing an access control system. Explain what it is and give an example.

2 Automatic meter reading (30 pts)

Electricity meters measure the amount of electricity usage in a household. With traditional meters, every month or so, an employee of the power company had to come and do a visual read of the meter, and report it back to the power company, so that the power company could invoice each customer properly.

Because having a bunch of employees going house to house to read every single meter is not very effective, the power company has decided to replace all of the existing meters by fancier meters that are able to communicate with the power company over a network. The system works as follows:

- The meter is a monotonically increasing counter $C(t)$ that represents the meter reading at time t. The counter is implemented as a 64-bit integer.
- At the top of every hour the system sends the current value $C(t)$ back to the company. The company has a log and checks to make sure that a reading is received every hour (if not, an employee is sent to check and fix the meter).
- Every month the company sends an invoice to the customer based on their prior month usage.
- Meters are read-only and can be considered as trusted. Users cannot tamper with the physical meter.
- The communication network used for communication between the meter and the company is a wireless (radio) network.

1. (8 pts) Your threat model should account for protecting both customers and the power company. (The power company is deemed honest, and the meter itself is trusted.) Answer the following questions.

   (a) (4 pts) Does the system need to enforce confidentiality of each $C(t)$ sent from the meter to the company? Explain why or why not.

   (b) (4 pts) Does the system need to enforce integrity of each $C(t)$ sent from the meter to the company? Explain why or why not.

2. (12 pts) Engineer Alice proposes the following protocol: Every hour, the meter sends $C(t)$, t, and $\mathsf{HMAC}(H(C(t)), K)$ to the company where H is the SHA-256 function. t is "Unix time", that is, encoded on 32 bits ($t = 0$ corresponds to January 1, 1970, 0:00 UTC, and the base unit is a second). K is a symmetric key shared between all the meters and the server of the power company.

   (a) (4 pts) Does this protocol enforce the confidentiality of the meter reading $C(t)$? Explain why or why not. If the protocol does not provide a property, explain why not via a simple attack.

   (b) (4 pts) Does this protocol enforce the integrity of the meter reading $C(t)$? Explain why or why not. If the protocol does not provide a property, explain why not via a simple attack.

(c) (4 pts) Does this protocol enforce the message authentication of the meter reading $C(t)$? Explain why or why not. If the protocol does not provide a property, explain why not via a simple attack.

3. (10 pts) Problem and fixes

   (a) (4 pts) The power company realized that after deploying Alice's protocol, the company started to lose a lot of money. Explain how can this happen.

   (b) (6 pts) Propose your own protocol, so the power company collect the right amount of charges from the customers. Briefly explain why your protocol is able to achieve this.

3 Password (12 points)

Company A has a large number of online customers. Each user has a username and a password. A's server saves only the hash of those passwords. Currently, A uses SHA-256, which outputs a 256-bit digest (i.e., a bit-string of 256 bit). When a user wants to log in via A's website, the hash of the user inputted password will be compared to the stored password hash for that customer. Login is only successful if the two hash values are the same.

1. (6 pts) Company A had a data breach and the password hash file of A's customers is posted online. Bob decides to try his luck in recovering the plain text of A's customers' passwords. How many passwords does Bob have to try to have 75% chance of recovering one of A's customer's password? Please write out the formula and briefly explain the formula. No need to use approximations. No need to produce a concrete number.

2. (6 pts) After the breach, A decides to upgrade to SHA-512, which outputs a 512-bit digest. What is the least number of customers that A has to have to have 90% chance of the following happening: there exists a customer (let's call him or her X), who can loggin as another customer (who is not X), using X's own password? Here the customers are trusted and do not attempt to crack passwords. Please write out the formula and briefly explain the formula. No need to use approximations. No need to produce a concrete number.

4 A Role-Based Access Control System (20 points)

Instead of assigning access rights to each individual principals directly, role-based access control assigns each principal one or multiple roles and assigns access rights to objects based on the roles. Alice is in charge of implementing access control for medical records using role-based access control for hospital H.

- The write permission (W) of a directory allows the creation and deletion of files within the directory. The read permission (R) of a directory allows listing the files within the directory. The execute permission (X) of a directory allows entering the directory, and accessing files and directories inside that directory.
- Roles of employees in hospital H include doctors, pharmacists, and receptionists.
- A patient's files include doctors' notes, prescriptions, and upcoming appointments. Each appointment file includes the appointment date/time, the reason for the visit (e.g., getting a sprained ankle checked out etc.), and the name of the doctor.
- The access-control policy that Alice needs to implement is as follows:

  P1. Only the doctors that are assigned to treat the patient can read/write/create doctors' notes.

  P2. Only the doctors that are assigned to treat the patient can write/create the prescription files.

  P3. Doctors and pharmacists can read all of the prescription files of patients.

  P4. Everyone, including the receptionists, can read/write/create patients' appointment files, so receptionists can remind patients of their upcoming appointments.
- Alice decided that the file system is organized into subdirectories, one for each patient. Under each patient's directory, there is a sub-directory for each of the following: notes, prescriptions, and appointments.

1. Basic implementation (10 points) Help Alice draw an access control matrix to implement the above policy. The rows of the matrix are roles and the columns are directories for patient 1 and patient 2. Fill the R/W/X bits for each role. Note that you are allowed to add your own roles if necessary. Keep in mind that the matrix should not allow unauthorized accesses and should not denied allowed accesses.

2. Plugging holes (10 points) Upon learning the risks of privacy breaches, Alice's boss decides that H needs to implement the following policy as well:

   P5. Employees other than doctors who treat that patient are not allowed to learn anything about that patients personal health information such as diagnosis, prescriptions, and the patients medical conditions.

   Alice realizes that the current system design does not implement the above policy.

   (a) (5 pts) Explain in 1-2 sentences why P5 is violated.

   (b) (5 pts) Propose fixes to enforce P5. Explain your proposal in detail.

5 A defense against buffer overflows (12 points)

We propose a defense mechanism that works as follows: a shadow copy of the return address is stored in a designated area on the heap when a function's activation record is created. Upon return, the shadowed return address on the heap is used as the return address.

1. (6 pts) Explain why common buffer overflows can be prevented by this defense. You can use the following simple program to help you explain.

```
void function(){
    char buf[4];
    // mangles saved return address to 0x44434241
    strcpy(buf, "AAAAAAAAABCD");
}
```

2. (6 pts) Explain why this mechanism cannot protect against all buffer overflow attacks. Please be as concrete as possible.

Extra Page