

## CS2107 Tutorial 3 (Encryption & Password)

School of Computing, NUS

7–11 September 2020

1. Discuss the following security questions:

- (a) “When did you graduate from college?”
- (b) “Which college did you graduate from?”
- (c) “What is the name of your first pet?”
- (d) “What is your favorite food?”
- (e) “What are your birthday and your spouse’s birthday in MMDDYYMMDDYY? format”

Suggest a good security question.

### Solution

The listed security questions are not good because:

- (a) It is not safe as it can be guessed based on social-media information; is not universal (i.e. some people don’t go to college).
- (b) It is not safe as it can be guessed based on social-media information; is not universal.
- (c) It is not universal.
- (d) It is inconsistent (may change) over time.
- (e) It is not safe as it can be guessed based on social-media information; is not universal.

An open-ended question can make a good question. Also highlight that the user doesn’t have to faithfully give the actual/right answer.

(*Note:* Nowadays, a second factor (e.g. SMS) or secondary email address is preferred over security questions for resetting password. You can additionally read: <https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/>.)

2. You have intercepted two ciphertexts  $C_1$  and  $C_2$ , which were generated by a stream cipher using the same secret key:

$$C_1 = 0111\ 11011011$$

$$C_2 = 0111\ 00101011$$

The first 4 bits of each ciphertext form the used IV. You know that the plaintext must be among the following 4 sequences:

$$P_1 = 00000000, P_2 = 11111111, P_3 = 00001111, P_4 = 11000011.$$

What are the possible plaintexts of the captured ciphertexts  $C_1$  and  $C_2$ ?

#### Solution

This is an example of the ciphertext xor-ing attack described in Lecture 1:

$$C_1 \oplus C_2 \text{ (by omitting the IV)} = P_2 \oplus P_3 = 11110000.$$

Notice that the attack is applicable because: (a) a stream cipher is employed;  
(b) the same secret key and IV are used in generating the two ciphertexts.

3. Consider two password authentication systems S-I and S-II:

S-I: After a user has entered his/her userid, the system sleeps for 0.5 second, and then checks whether the userid is in the database. If it is not in, the system sleeps for another 0.5 second, displays an error message, and then prompts for the new userid; Otherwise, the system prompts for the password. If the password is wrong, the system sleeps for another 0.5 second, and then prompts for the new userid again.

S-II: After a user has entered his/her userid and password, the system sleeps for 0.5 second, and then checks whether the entered credential information is correct. If it is wrong, the system sleeps for another 0.5 second, displays an error message, and then prompts for the new userid and password again.

What are the security implications of the two different checking mechanisms adopted by S-I and S-II?

#### Solution

Suppose, in order to log in as a valid user, an attacker requires  $x$  guesses for the userid, and  $y$  guesses for the password. The attacker will thus need  $x + y$  guesses on S-I, whereas he will need  $x \cdot y$  guesses on S-II.

(Note: Notice that, in practice, userid is not a secret. But for a layered defense, it is good to hide it as much as possible. Ultimately, the security still relies on the password.)

4. A university library provides a Web-based service for the students to renew their books. To get authenticated, a student must key in: (a) student ID, (b) date of birth in DDMMYYYY format, and (c) family name. After authenticated, the list of books borrowed by the student is displayed, and then the student can choose which book(s) to be renewed. No other action can be performed through this service.

(a) What are the advantages of the authentication mechanism above compared to the typical password-based authentication?

- (b) What are the weaknesses of the system above? Are there any concerns on the students' privacy?  
(*Hint:* Besides the information of students' borrowed books, there may be another subtle leakage of personal information in the system.)
- (c) Do you prefer the above authentication, or the typical password-based authentication to be used by the university?

#### Solution

- (a) There is no bootstrap process needed to set up user passwords. Additionally, the pieces of information needed are easy to remember.
- (b) There is a potential privacy breach:
  - i. If an adversary knows a student's social information, then he can log in to see the books being borrowed by the student;
  - ii. If the adversary knows only a student's ID and family name, then he can still probe the login screen to find out the birthday, and subsequently find out the books being borrowed the student.

(Notice that the National Library Board used to have such a system for many years. Now, a password-based system is used.)
- (c) Ultimately, it is a trade-off between usability and security.

5. A bank's IT team is planning to enhance the password+SMS 2FA of its online banking service. To use the service, a user first logs-in using the password (without the SMS) using his/her PC. After the user has logged in, the user's account number would be displayed on the PC, together with a few transaction options. If the user wants to transfer money to another account, the following steps will be carried out:
- (1) The user enters the required transaction information (account number and amount) to the PC, which in turns sends the information to the server.
  - (2) The server sends a OTP to the user via SMS. The SMS will be delivered to the user's mobile phone by the telecommunications service provider (e.g. Singtel, M1 or Starhub).
  - (3) The user enters the OTP to the PC, which in turn sends the OTP to the server.
  - (4) The server checks the sent OTP and, upon receiving a valid OTP, sends a confirmation to the user's PC.
  - (5) After receiving the confirmation from the server, the PC finally displays a message "transaction completed".

Now, the IT team has to decide what information to be included in the SMS in step (2). Below are examples of two considered choices:

M-I: "Enter OTP 132373 to complete your transaction."

M-II: “You have requested to transfer \$10,000 from account no 1388293-43-23 to account no 12398-234-A2. Enter OTP 132373 to complete your transaction.”.

- (a) Give a situation where M-I is preferred.
- (b) Give another situation where M-II is preferred.
- (c) If you were in the IT team, which message format would you choose?

(*Hint:* You can consider the fact that a SMS is not encrypted in an “end-to-end” fashion, and there could be multiple telco entities handling the SMS. You can also consider the scenario where the PC is in an Internet cafe, and the cafe owner could be malicious, or honest but curious.)

#### Solution

Before answering the questions, notice that arguing “*a system  $M_1$  is more secure than  $M_2$* ” requires us to find attacks that do not apply to  $M_1$ , but apply to  $M_2$ .

Also pay attention to the meaning of “end-to-end encryption”, i.e. only Alice & Bob can know the original message.

- (a) *M-I is more secure:* If the mobile phone is lost or somehow an adversary can access to it, and the previous messages are not deleted, then the adversary will be able to see the undeleted transaction details. This information leakage represents a privacy breach. Alternatively, if the adversary can tap into the SMS communication channel, then he will be able to capture the transaction history.
- (b) *M-II is more secure:* If a piece of malware resides, or is purposely planted on the PC, then the message displayed on the user’s PC can be different from the actual transfer being made with the server. M-II can help the user verify that his/her transfer details are correct.
- (c) You can decide on the message format. How about showing partial account information?

6. (From [Gollmann], page 64:)

You are shipping WLAN access points. Access to these devices is protected by password.

- (a) What are the implications of shipping all access points with the same default password?
- (b) What are the implications of shipping each access point with its individual password?

(*Hint:* Argue from the viewpoint of usability vs security.)

#### Solution

- (a) An attacker can access a device if the common default password is left unchanged.
- (b)
  - i. For you (device manufacturer): Cost will increase since now there is a need to: print the individual default password on each equipment/manual/case; record the passwords in a password database; and have a customer service line or web site to help users retrieve their device's password.
  - ii. For device users: Usability will decrease if a user is unable to find or retrieve the individual default password. This may lead to a bad product review, and subsequently may affect the manufacturer's sales.

7. A company has installed fingerprint-based door access systems at their server room and gym. The two systems are exactly the same, but the company can set different thresholds to adjust the FNMR and FMR (see Lecture 2). Suppose the threshold set for the server room is 0.5, what would be a reasonable threshold for the gym: larger, smaller, or equal to 0.5?

#### Solution

Smaller than 0.5 in order to be more accepting than the server room.  
Recall again that when threshold is 0, the system accepts everyone;  
whereas when it is 1, the system accepts no one, i.e. rejects all.

8. Find out more about these security terms:  
*Graphical passwords, covert channel, side channel attack, end-to-end encryption.*

#### Solution

Please google/wiki the terms.

Notice that a covert channel is a channel *intentionally* created by an attacker to leak information out of the target system; whereas a side channel is an *unintentional* channel taken advantage by an attacker to obtain more information about the target system. A side channel attack exploits a side channel.

— End of Tutorial —