C2107 Tutorial 3 (Password, 2FA, a bit of PKC)

Chang E.-C., School of Computing, NUS

September 1, 2025

1. This is a paragraph from RFC4086 mentioned in Lecture 2 on password strength.

   ```
   Assume that user passwords change once a year and that it is desired that the
   probability that an adversary could guess the password for a particular account be less
   than one in a thousand....

   To have a one-in-a-thousand chance of guessing the password in  500,000 tries implies
   a universe of at least 500,000,000 passwords, or about 2^29.  Thus, 29 bits of
   randomness are needed.  This can probably be achieved by using the US DoD-
   recommended inputs for password generation, as it has 8 inputs that probably average
   over 5 bits of randomness each (see section 7.1).  Using a list of 1,000 words, the
   password could be expressed as a three-word phrase (1,000,000,000 possibilities).  By
   using case-insensitive letters and digits, six characters would suffice
   ((26+10)^6 = 2,176,782,336 possibilities).

   For a higher-security password,...To go to a one-in-10^9 chance, 49 bits of randomness
   are needed, implying a five-word phrase or a ten-letter/digit password.''
   ```

   The above mentions three methods to generate passwords. Let's consider the second method (i.e. choosing 3 words from a dictionary of 1000 words). Suppose we want to have 50 bits of randomness and using the same 1000-word dictionary, how many words are required in a password[1]?

   Guideline on entropy required. RFC4086 doesn't explicitly state how much entropy is sufficient to prevent online dictionary attack. Implicitly, it suggests 29 bits or 49 bits for "higher-security". The RFC also doesn't state requirement of offline dictionary attack. For the purpose of discussion and assessment in this course, let us fix the requirement as follow:

   (a) To prevent online dictionary attack, entropy is at least 50 bits.

   (b) To prevent offline dictionary attack, entropy is at least 128 bits.

   Tthe above requirement is not commonly practiced in the industry. It is for the purpose of this course.

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

[1] The above question does not precisely state whether the selection is done with or without replacement. The two different settings will lead to different answers, but with very small difference. In this question, the easier setting to handle is "with replacement".

3. (*Security Analysis: comparing two systems*)

   An IT team is planning to deploy 2FA for an online-banking service. They are consider password + SMS, or password + hardware token. In both options, the user first log-in using the password (without the second factor) via a PC. After the user has logged in, the user's account number would be displayed on the PC, together with a few options[2].

   If the user wants to transfer money to another account, the second factor is to be used.

   (SMS)

   S1. The user enters transaction (e.g. account number and amount) to the PC, which in turns sends the information to the server.

   S2. The server sends a OTP to the user via sms. The sms will be delivered to the user's phone by the telecommunications service provider (eg. Singtel). The sms contains full detail of the transaction, e.g. *"You have requested to transfer $50,000 from account 1388293-43-23 to the account 12398-234-A2, enter OTP: 132373".*

   S3. The user enters the OTP to the PC. The PC sends the OTP to the server.

   S4. The server checks the OTP. If correct, the server sends a confirmation to the PC. PC displayed the confirmation.

   (Token)

   T1. The PC displays the full detail of the transaction, follows by *"To confirm, press * in your OTP token and enter the displayed 6-digit here ".*

   T2. The user presses the token and enters the OTP to the PC. The PC sends the OTP to the server.

   T3. The server checks the OTP. If correct, the server sends a confirmation to the PC. PC displayed the confirmation.

   (a) Consider this attack scenario.

   - The user is using a PC in a Internet cafe. The PC is already compromised and is controlled by the attacker. Hence, the attacker can modify the user's input, and can modify information displayed for the user. In other words, the user is interacting with the bank through a malicious middle man.
     With respect to this scenario, which option is more secure?

[2]We assume the connection from the PC to server is through HTTPS. We would study HTTPS later. Under HTTPS, even if the the attacker is an entity in-between the PC and the server, e.g. an insider in the Internet Service Provider, what the attacker can get is ciphertext encrypted/protected by HTTPS. However, if the attacker is a malware in the PC, the attacker might able to get everything.

(b) Consider this scenario.

- Alice is a billionaire. She attended a conference in a nice pacific island. During the conference, she concluded some business deal and carry out the online transaction. There are many participants in the conference including her competitors who want to spy on Alice's business plan. She used her own laptop and we can assume that it was free from malware. We assume that SMS can be spoofed and sniffed by anyone in the conference[3].
  Now, with respect to this scenario, which option is more secure?

(c) Let's suppose that the IT team has decided to use sms. The IT team has choose one among two sms formats. Let us compare these two formats:

M1 *"Enter OTP: 132373".*

M2 *"You have requested to transfer $50,000 from account 1388293-43-23 to the account 12398-234-A2, enter OTP: 132373".*

- Give a attack scenario that M2 can prevent but not M1.
- M1 and M2 have their own limitation. How to get a tradeoff between the two choices?

4. (*Confidentiality does not implies Authenticity*). The plaintext

   "`U00013 gives U12345 $1000 dollars`"

   was encoded as ASCII and encrypted using AES CTR mode. Let c be the ciphertext (including IV). Mallory sniffed c. Mallory knew the plaintext was of the form

   "`U`x `gives U`y `$1000 dollars`",

   and the user name x, y were each 5 characters long. However, Mallory didn't know the actual value of the string x and y. Can Mallory generate a c' that would be decrypted to

   "`U`x `gives U`y `$9999 dollars`"?

   Remark: the term "malleability" refer a property of an encryption scheme whereby it is possible to transform (without knowledge of the secret key) a ciphertext to another ciphertext of a related plaintext. Stream cipher is malleable.

5. (Open-ended question. No "standard" answer) We often receive SMS or email with OTP for password reset, or confirmation of transaction. For security, is it advisable to *securely delete*[4] them after usage? Under what situation could an attacker gains something useful if those are not deleted.

[3] It is extremely easy for anyone to spoof an SMS. To sniff, although possible, requires other capability, for e.g. to have access to the base station.

[4] Note that a deleted email is still temporarily stored in the "recycle bin"

6. (*"see-with-you-own-eyes" a public key*)
   Visit `https://www.nus.edu.sg`. Find the padlock in the address bar and click to find details about the item "certificate" (different browsers have different interface). The certificate should contain some public key info. NUS's public key is RSA-based. What is NUS's public key? Recap that RSA encryption and decryption are done by exponentiation with modulo n. What is the n? What is the exponent? (Answer: the exponent is $2^{16} + 1$=65537). What is the advantage of having small exponent? Not all public key is RSA-based. Try to find a website that use DSA-based, which should be appeared as "Elliptic Curve". We will study certificate and revisit this question.

7. Find out more about these:
   Single Sign-On (SSO), retinal vs iris scan.