CS5285: Information Security for eCommerce Autumn, 2024
Tutorial 9, Week 11 (November 19)

Questions:

1. **Password Security (1)**

   (a) Suppose a 10-character password is chosen where each character can be one of the letters 'A' to 'Z', 'a' to 'z' or '0' to '9'. Determine the size of this password space.

   (b) What is the strength of such a password in bits?

   (c) Compared to the suggested strength for symmetric key encryption, is this strong?

   (d) In the real world, if you asked people to create and use passwords as described above, would those passwords actually be as strong as you calculated?

   (e) So how big a dictionary will an attacker need to build? How much effort is needed?

   (f) How big would the dictionary be if we add a salt value (16-bit integer)

   (g) Sometimes terminology differs a bit - what are the possible differences between dictionary, rainbow table and brute force attacks on passwords?

2. **Password Security (2)** Normally we will of store a password record as (y, s) where $y = h(\text{password}, s)$ and s is a salt. Determine which of the following two alternative methods for calculating y is insecure.

   1 $y = E(\text{password}, s)$ where E is a block cipher and y is the encryption of password, s using the password as the key.

   2 $y = E(s, \text{password})$ where E is a block cipher and y is the encryption of password, s using s as the key.

3. **Authentication** Authentication can be based on (1) something you *know*, (2) something you *have* or (3) something you *are*. In the following situations, which one(s) of the three categories are used?

   (a) You enter CityU by putting your student card on the turnstyle reader.

   (b) You log into online banking using your username, a password and a hardware token which generates a number when you press a button.

   (c) You travel to another country and go through immigration. First you hand your passport to the officer, then the officer asks you to place your hand on a fingerprint reader.

   (d) You enter going through immigration using an automated system. First you insert your ID card or passport and enter a PIN, then place your thumb on a fingerprint reader.

4. **Phishing** Phishing has some technical complexity but can be argued to be an attack based more on social engineering. Educated users as to the risks of phishing is important but can we also implement technical authentication measure to mitigate the impact of phishing compromise?