Khai Phan Thanh (100901164)

BTN710 – Information Security

1. Briefly explain Kerckhoffs' principle and its importance in security.

* Kerckhoff’s principle is that quoted from Wikipedia, “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.” What it means is that, even if the cryptosystem revealed, without a key, nobody could mess up with the data. Therefore, the security isn’t really about the system, but it’s about the key to access to the system. Based on what we did on Lab 4, a stranger who has my key can easily decrypt the encrypted data using that key. However, data that was encrypted using a key that only the system and the encrypter know will never be decrypted by somebody else.
  + In a longer explanation, Kerckhoff came up in 1883 while designing security cipher, which is extreme and become standard in IT security. The system must not be able to translate or read in any form (1) or by anyone if they have control on the system (2) and the key to access the system must be able to “remember,” unable to retrieve but must be able to change, modify or delete by an authorized user (3). It must be able to communicate in telegraph (4), portable in any form and require as least people as possible to operate to avoid the risk of leaking (5) and it must be easy and take less time to use by those who are authorized and trained (6). As an IT security, whenever implementing the security, they must assume and take a position as an attacker to think if it is possible to break in? Why and How to fix it? One important rule that is still matters in nowadays security environment is that the fewer people know about the system, the safer the key. Most of the system encrypted keys to access into the system are usually stored into the hard drive that contains the system. In some scenarios, they can be stored in a different hard drive to avoid the risk of attack (you can either lose one, not both). When the risk arises, the people responsible for the system should be able to change the key (to another hard drive or change the method) without any hassle.

1. Search the Internet for three examples of Botnets. For each one, explain:
2. Propagation method
3. Payload
4. Control method
5. Victim type
6. One more point you find interesting about that botnet

All of the attack lists below are controlled by a script developed by the attacker or the attacker re-use from someone else. As script-based, it can be scale and monitor easily on a large scale with a target victim that ranges from a few thousand users to million users.

* **Distributed Denial-of-Service (DDoS):** use an infected machine as one of the botnets to continuously send a large amount of traffic to a target website to “eat up” its bandwidth and overloading their resources. Once the system and database couldn’t handle all of the traffic coming, the site will be “shut down,” It will take days for IT personnel to fix and bring it up again. This method can easily get user out-of-control because it will use a large amount of bandwidth and resources available to attack the other system. The real victim in this will be the user and the attacked website.
* **Cryptocurrency Mining:** unlike DDoS, where the attack could be suspicious, Cryptocurrency mining will secretly use the bandwidth and resources available in your system and help the attacker “mine the gold.” Cryptocurrency is harder to detect since the attacker could adjust the usage of resources and bandwidth so that the user will unlikely to notice the difference. The real victim in this will be the user.
* **Browser Add-On Installtion:** this is another interesting botnet attack that not many people realize. This kind of botnet is usually hidden in most popular software, and the user will be less likely to notice. For a non-tech person, when installing software, they will choose the express option which will install the software by its defaults and also install many other "trash" software that comes with it. Interestingly, the list of additional install software is not the same every time you install the main software). With a high-tech person, they can easily spot out and cancel the action right away. The add-on will change the user's default web browser to the attack based-built (with the almost exact layout with some of the popular search engines in the market). For every search, a pop-up with an advertisement will appear and count as a paid click for the botnet owner. Sometimes, the botnet can change banner from the website you visit with one of their advertisement to generate more money.

1. National Institute of Standards and Technology (NIST) provides helpful guidelines and standards for security measures in different systems. For this question, you are asked to read parts of a document that contains policies about password security.
2. Please read section 5.1.1 of the document available here: <https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret>
3. You are encouraged to read the other sections as it is very informative, but it is not necessary for this question.
4. After reading the section, name 12 different points suggested with respect to password security, e.g., regarding length, complexity, duration, changing, etc.
   * The password must be at least in 8 characters in length if chosen by the user, where numeric, ASCII, Unicode and space should be accepted as one character and doesn’t require a combination of those. Multiple spaces may be combined into one space to avoid accidents hit. The user should approve of them before the system is doing so. Truncation is strictly avoided.
   * If a Unicode entered, the system must apply the Normalization Process for Stabilized Strings before hashing the byte to store it into the endpoint. Users must be advised that using Unicode character could affect their authentication later on (mismatch string or character).
   * The password must be at least in 6 characters in length if generated by the system. The password should generate randomly using a bit generator (method usually use if the user wants to access the account in a different platform using 2-factor authentication).
   * The system should allow users to select a hint for their password. Still, it cannot be obvious that someone who has access can guess the password by looking at the hint (ex. A question where the password is related to the answer). The hint and password shouldn’t related to each other or it shouldn’t completely not helping the user.
   * When making a change to the password, the system must taken account that user could use password that is the same/similar to previous breach corpuses, dictionary words, repeated word/number or name that is easy to guess. System must reject users to do so to avoid any unwanted breach.
   * Guidance to a strong password is recommended and encourage so the user can step out of the zone and think of something more complex to get an approval. An implemented meter or list of password requirements should be available so the user can follow.
   * The system must implement a standard fail-rate for each user. It can limit the failed-authentication from the user before block the user out.
   * The system should not require the user to have a combination of their password. However, it is strongly encouraged to increase security. The system also shouldn’t make the user change their password frequently unless required if there is a compromise of authenticator.
   * User will likely type their password elsewhere before entering into the system so they can remember the password better. Using “●” can easily make users make mistakes somewhere and can’t figure out. Therefore “paste” functionality should be allowed.
   * The system should allow users to display what they type in the password field by using some checkmarks such as “show my password.” In addition to that, it must show the user the last character the user types in and wait for a few seconds before turn it into “●”
   * When accepting the password, the system must store the password to avoid any attack, offline or online. The password and the salt will be passed to Key derivation functions to generate a password hash and store it into the database. This step will take the attacker more time and resources to solve the hash function.
   * Salt must be at least 32-bits in length to avoid any duplication that might occur in the future with other passwords and randomly assigned to the password. Salt value and Hash value will be store together for each user for authentication purpose.