CECS 378
SPRING SEMESTER 2018

INSTRUCTOR: DR. MERHDAD ALIASGARI

06 February 2018

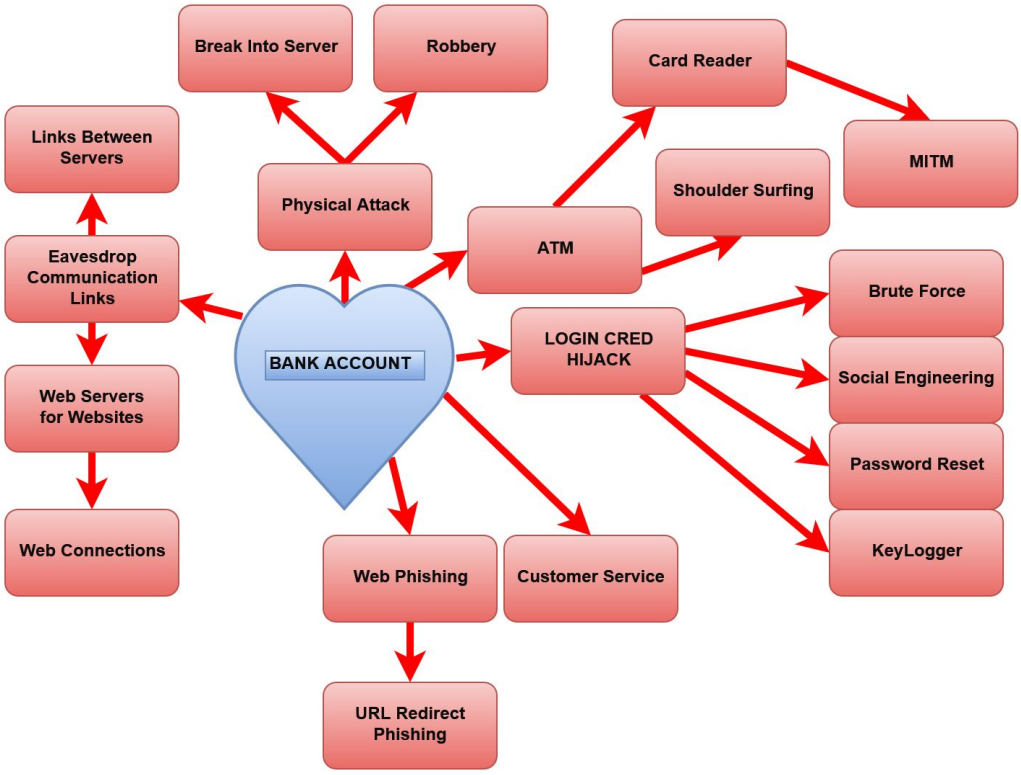
Security is not an afterthought. Security begins at the design process.

Defensive layering

- Defensive layering is multiple solutions that work in parallel that do not depend on each other but all want to achieve the same goal.
    - This is extremely beneficial in security because in the real world one solution is usually not enough to protect your assets/stakeholders from attackers.
    - Multiple layers requires attackers to penetrate through multiple solutions before they can even get a chance to change/manipulate or steal your assets/data.
- With availability, you have to constantly monitor your server/services from attackers and problems. Constantly monitoring a network is a difficult task.
    - Chevron has a 24/7 staff on hand all over the world to monitor, detect problems/attacks, and instantly respond.
    - Some solutions are not applicable to certain areas because of international laws or policies that may not allow your solution to be implemented without breaking a law.
    - Chevron has on average around 10-30 machines that have been fully compromised. They are a large company worth billions and are a juicy target to attack.
    - When Chevron is attacked, they have certain policies in regards to how to handle incidents. The tech guys follow these policies and respond to these incidents.

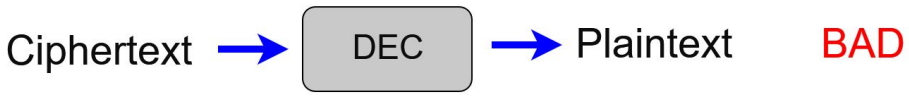
- There are different policies for different types of incidents. Policies are important to make sure that there are specific steps that employees know to take to solve a problem from beginning to end.
    - Sometimes there are whole bunch of employees hired to handle only one type of incident such as verifying identity.
    - Credit card companies have to deal with this very often. Their users may fall for a scam that manages to obtain critical information that can be used to steal money from the victim.
    - An example of bad policy is when a scammer managed to steal another person's gmail, icloud, and other accounts by calling Apple and masquerading as the owner to pretend to have forgotten their password so that Apple would reset or give them the password.
- Never made an assumption on your adversary's strategy.
    - No matter how nasty, pathetic, or ridiculous your attacker's strategy, if the attacker is eventually successful, you are the loser.

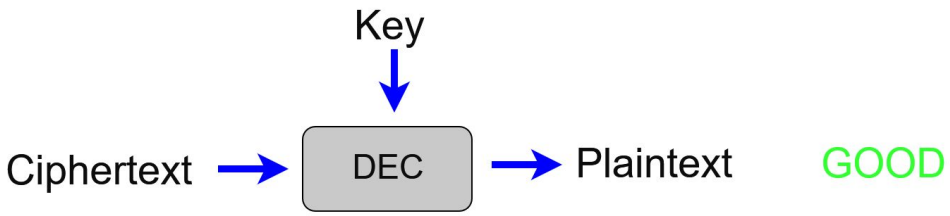
ATTACK TREE



Encryption

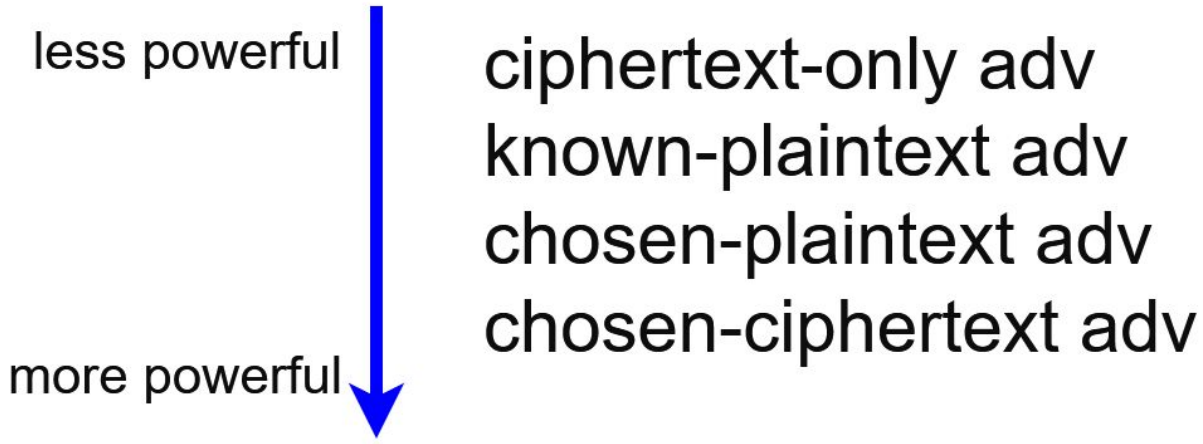
- Encryption is when you mask your message so that your message will appear to be gibberish to anyone that the message is not intended for. Encryption was designed for confidentiality.
    - You start out with plain text that goes through an encryption and is transformed into “ciphertext”.
- It is very important that you are able to always 100% get the same plaintext from your encrypted ciphertext.
    - The only person that needs to have the decryptor is the person who receives the message.
    - You also need to hide the encryptor because they may be able to reverse engineer the encryptor to figure out to how to decrypt the message.
- A better model for protecting your encryption device/decryption device is to introduce a third factor called a key which is needed to use the device.





    - A key would provide another layer of protection from adversaries from reaching the precious software/understanding of how you are encrypting your messages.
    - In the case that your device was stolen or compromised, the device would be useless without the key and adversaries would be unable to access the software/inner workings of your encryption device.
- **OBSCURITY IS NOT SECURITY (Kerchoff’s principle)**

    - Thou shall not rely on your algorithms to protect your data. Just because people can not see your algorithms or software
    - Only secret inputs can protect you from adversaries.
        - The secret inputs should be easily changeable incase you are compromised.
        - Authorized users should be able to change the secret input.
    - **NEVER HARDCODE YOUR SECRET INPUTS/KEYS IN YOUR SOFTWARE**
        - Aliasgari will come and hunt you down.
- Different types of adversaries in encryption
    - An adversary that only knows about the ciphertext is called a ciphertext-only adversary.
    - An adversary that knows a little bit about the translation between ciphertext and plaintext than he/she is known as a “known-plain-text” adversary.
        - This type of adversary is much more powerful than a ciphertext-only adversary.
    - A “chosen-plain-text” adversary is when the adversary somehow gets the person with the encryption to encrypt a known plain text message into ciphertext. Since the adversary already knows what the message actually is then they can work backwards and find out how to decrypt other messages.
    - A “chosen-ciphertext” adversary is when and adversary sends a known ciphertext message to a person who has a decryption key to revert the message back into plaintext.



- Ways to break encryption
    - Brute force is the dumbest adversary but brute force can be very inexpensive for the adversary.
    - Brute force costs is the number of attempts and the costs of verifying that the key is valid/correct.
        - The Egyptians would have slaves who spoke their enemies' languages and ask them if the ciphertext that they brute forced into a plaintext makes any sense.