CECS: 478 Week 2
Group: Super Secure Bros
“Security is not an afterthought it begins at design”
“There is no security in obscurity”

Tuesday 9/11/2018

Quiz Answer

- After the solution has been developed you must perform analysis on the solution. Make sure the cost of implementing the solution does not outweigh the cost of a successful attack.

Zero day attacks:

- Attacks that have yet to occur on a public system/publicly undiscovered exploits.
    - Part of maintaining your solutions after release. Must be aware of new exploits or vulnerabilities that have been released
    - Best defence is to keep your system updated with the latest security patches

Steps in securing a deployed system

Maintain: Maintain the deployed system with latest, proven security patches
Identify: Identify your assets and adversaries
Protect: Design, analyze, maintain
Detect: Detect attacks that are taking place against your solution, monitor

- Timely detection is key, find the attack as early as possible
- Identify the right communication or data stream to monitor

Respond - If an attack is successful mitigate the incident as quickly as possible

- Have a response protocol. Disaster Recovery Plan (DRP), need to specify the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) and required escalation per the situation

Recover - Assess damages, Isolate infected systems, forensics/take images of system, recover infected systems, fix problem. Type of recovery depends on the scale, type and priority of the attack.

- **False Positive:** Alarm is not raised when it should have been
- **False Negative:** Alarm is raised when it should not have been

Thursday 9/13/2018

- Tesla car example. Tesla cars are updated over the air. A malicious update has been pushed out to your cars what is your response after detection.
    - First action is mitigation, contain the damages the attack has caused from spreading to more vehicles. Then push a secure fix/update out to all vehicles removing the damage.

Cryptography

- Practice of securing communications in the presence of an adversary
- Encoding and encryption are different
    - Encryption requires the use of a key so that communications between the communicating parties are secured even with knowledge of the encryption method

Encryption & Decryption

Plaintext -> Key & Encryption Algorithm -> Ciphertext

Ciphertext -> Key & Decryption Algorithm -> Plaintext

Kerckhoff's Principle

- There is no security in obscurity (The adversary should be able to know your algorithm and still be unable to break your encryption)

Knowledge of Attacks

- Ciphertext only
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext
- Oracle Padding attack

Caesar Cipher: Key space value 0-25
Key space: All possible values of your keys
Brute Force: Try all values in your key space