CECS 478: Week 2

Tues: 9/4/18 & Thurs: 9/6/18

“Security is not an afterthought it begins at design”

Tuesday: 9/4/18

Objectives of Security

- **Confidentiality:** Information is masked and only accessible to those who are authorized to access it.
- **Integrity:** The data or service is genuine
- **Availability:** A service or data is always available to be used/accessed
- **Accountability:** Users are held accountable for their actions, and their actions are always monitored
- **Authentication:** Ensuring the user is he/she says they are
- **Anonymity:** Being able to deny all actions

Security At Design

Identify your Assets:

- Data
- Stakeholders
- Hardware
- Software

Adversary Model:

- Think about if the **value of their goal** is less than her cost of resources
- Think about their **capability**; how powerful is our adversary
    - Asset access level
    - Resources
        - Computational Power
        - Communication Links
            - Bandwidth / Comm
        - Power Consumption
    - Knowledge of the system
        - Insider/Outsider
    - Passive
        - Monitoring or collecting information (observer)
        - Not intervening with the system
    - Active
        - Manipulates the functionality of the system or compromises the data
        - Actively trying to interrupt or gain access to a system
- **“Man in the Middle”** (**MITM**) - Active adversary
    - “Inevitable” adversary.
    - Two communication link A to B, and a malicious user intercepts communication and does something with that communication
- **Eavesdropper -** Passive Adversary would be (packet sniffing)

End to End

Typical method of data transfer:

Client -> Server -> Client

Client -> Server: Encrypted in transfer so server cannot see any information from client

No web app for the project. Do not use java to use your client app.

Thursday 9/6/18

Attack Surfaces:

- Once you know all the surfaces then you just have to block all those surfaces, eliminate all attack paths

Analysis:

- See if your solution works against the attacks your attempting to protect against
- Place it in a sandbox environment
- If analysis fails your restart

END OF DESIGN PHASE OF ADVERSARY MODEL