Network Security

Network Security Introduction

- **Network security** consists of the **policies, processes, and practices adopted** to **prevent, detect, and monitor unathorized access, misuse, modification, or denial of service**.
- **Confidentiality** refers to the **state of keeping secret or private**. Only the **sender** and **intended reciever** of a **message** should be able to **understand the message**.
  - This is done with **encryption**. The sender encrypts the message, and the inteneded receiver decrypts the message.
- **Authentication** is the **process or action** of **verifying the identity** of a **user or process**.
  - In **network security**, we want to **confirm the identity** of the **sender and receiver of messags**.
- **Message integrity** means that a **message has not been tampered with or altered without detection**.
- **Access and availability of services** means tat services must be accessable and available to users.

Types of Actions a malicious Actors can Perform

- **Malicious actors** can do the following (and other stuff that is not included):
  1. **Eavesdrop / intercept messages**.
  2. **Actively insert messages** into a **connection**.
  3. **Impersonation via spoofing**.
  4. **Hijacking ongoing connections**.
  5. **Denial of service attacks**.

Cryptography

- To **encrypt a message**, the sender uses an **encryption key** to create a **ciphertext**, that can only be **decrypted by the intedned receiver's decryption key**.
- This way, **malicious actors** can view the **ciphertext**, but have to way to **know what it means**.
- There are **type classes of cryptographic algorithms**:
  1. **Symmetric algorithms** use the **same key to encrypt and decrypt the message**.
  2. **Asymmetric algorithms** use **two different keys, one to encrypt and the other to decrypt the message**.
- To attempt to **decrypt ciphertext's**, **malicious actors** can use a **brute force search through all of the keys, or a statistical analysis**.
- If a **malicious actor** has **the plain text, and the ciphertext**, they can **determine the key**.

Cryptographic Algorithms

- The **Data Encryption Standard (DES)** is an older encryption standard that uses a **56-bit symmetric key, with 64-bit input**.
  - DES is not a good encryption algorithms as it can be brute forced in a day.
  - One solution to improve the security, is to encrypt the input three times with three different keys (know as 3DES).
- The **Advanced Encryption Standard (AES)** is a **symmetric encryption algorithm** created to **replace DES**. Keys can be **128-bit, 192-bit, or 256-bit**. The **encryped data** is **processes in 128-bit blocks**.
  - Brute force decryption takes 149 trillion years for AES (whereas it takes 1 second with DES).
- The **Rivest, Shamir, Adelson (RSA) algorithm** is an **asymmetric, public-private key encryption algorithm**.

Authentication

-