CSCD27

09/10

Big Definitions

Safety is defined as reasonable input for reasonable output, or correctness, or the program does what is intended.
Security is defined as unreasonable inputs get reasonable outputs.
Threat – Possibility of damage, can be tangible, possible, whatever. A threat can be accepted or not accepted. Rejected threats are ones that are not cost-effective or low possibility.
Vulnerability – A weakness in the system, but not necessarily something that can be exploited or no exploit has been discovered yet.
A vulnerability enables a threat, and an attack/exploit takes advantage of a vulnerability. There is a clear differentiation between an attack and a vulnerability. An attack realizes a threat.
Countermeasure – something done to disable an attack, limit the possibility or consequences of damage. So this can be like a patch or workaround. It mitigates a thread or removes/reduces a vulnerability
CIA – An acronym for the three pillars of security, confidentiality, integrity and availability. For example, confidentiality means only the student can see their own grade, integrity is only the professor can enter a grade, availability just refers to keeping important systems online like 2FA. There are sub properties, see slides for Venn diagram.
Anonymity vs Pseudonymity – Pseudonymity is like hiding behind a username or pseudoname, like a Reddit account. But as you make posts, people can begin tracing stuff back to you. True anonymity eliminates this.
The properties of CIA can be conflicting or even undesirable.
An example of where properties are conflicting, voting is an example.

Classical Cryptography

Two kinds of cryptography fields, one is the pure mathematical side building the individual tools. Then there is a technical side that utilizes these tools to build crypto protocols.
Caesar Cipher – Oldest cryptosystem. It is a **shift cipher** where you shift the alphabet by a fixed offset.
Interception – Attacker obtains and reads the message. (Confidentiality)
Modification – Attacker changes the message (Integrity)
Fabrication – Attacker injects a message (Integrity)
Interruption – Attacker disrupts communications (Availability)
Cryptography only addresses confidentiality. Secure messages/channel over an insecure medium.
Plaintext – Original message intended for author and recipient.
Ciphertext – Encrypted message.
Encryption – Turning plaintext into ciphertext.
Decryption – Turning cipertext into plaintext.
Cryptographic algorithm – Method to do encryption and decryption.
Cryptographic key – Input used by algorithm to perform the actions. For example case of Caesar cipher the key is the shift offset.
N-Bit security entropy – The measure in which we measure the strength of the algorithm. It is the number of bits to encode the number of possible keys. So for example in the Caesar cipher, with 25 possible rotations (not counting a full rotation which is dumb) you need 5 bits.
100 bits is the minimum threshold to not be considered a weak key.
In the example big picture, an integrity attack can be where Mallory takes the message and sends it to someone else other than Bob, or resends it to Bob later.