Chapter – Introduction to Security

* **Security – Protection From harm (The State of being free from danger or threats)**
* **Computer Security – Protection of Computer Systems from harm on hardware, software and Data**
* **3 Main Categories of Harm –**

1. **Theft of Info – (Corporate Secrets, personal info, military intelligence), prevent stealing sensitive info that can be used for identity theft**
2. **Alteration of Info –** (Break in and deface a website, alter DB records to coverup fraud), Alter data, system config
3. **Denial of Service (DoS) –** (System busy responding attackers, doesn’t provide service to legitimate users)

* **Counter to these harms – Confidential data, Data not changed by unauthorized user, System remains operational, reachable, functional and available to users.**
* **Real-World Security –** Protecting valuable things – Physical stuff (jewelry, phones), People, Access to somewhere (Secure means no one can take it, harm it or use it without permission)
* **Core Goals of Computer Security (CIA Triad)- The NIST Standards for security Categorization of Federal Information and Information Systems (FIPS 199) lists confidentiality, integrity, and availability, as three security objectives.**

1. **Confidentiality – Preserving authorized restrictions on access and disclosure, (means to protect personal privacy and proprietary info. A loss of confidentiality is the unauthorized disclosure of info**
2. **Integrity -** Guarding against improper info modification or destruction, including ensuring info non-repudiation and authenticity. A loss of integrity is unauthorized modification or destruction of info
3. **Availability – Ensuring timely and reliable access and use of info. A loss of availability is the disruption to access to or use of info or an info system.**

* **Attack Scenario compromising Availability- Denial of Service – Possible to overwhelm an online service, unavailable**
* **How to Achieve Security Goals**

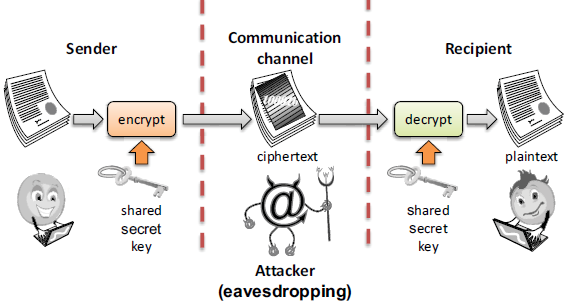
1. **Understand the Adversary – What resources are available, what is the goal of attack?**
2. **Understand Modes of Attack –** In what ways attack can be launched, what are the vulnerabilities?
3. **Understand the Security/usability tradeoff (tradeoff-** giving up something in return for getting something else)

* **About Adversary – The Adversary can be either Active or Passive (Adversary – opponent in contest)**

1. **Active – Takes active part in scenario, corrupts transmitted message, prevents ongoing communication, injects virus into a system**
2. **Passive –** Silent and Stealthy, He Eavesdrops the radio communications (Eavesdrops- Secretly listen to comms), He logs transmitted messages transmitted in local network

**Confidentiality:**

* **Encryption – Encrypt data using an encryption key**

****

* **Authentication – Determination of identity or role that someone has. Fingerprint, password, smart card**

**Tools for Integrity:**

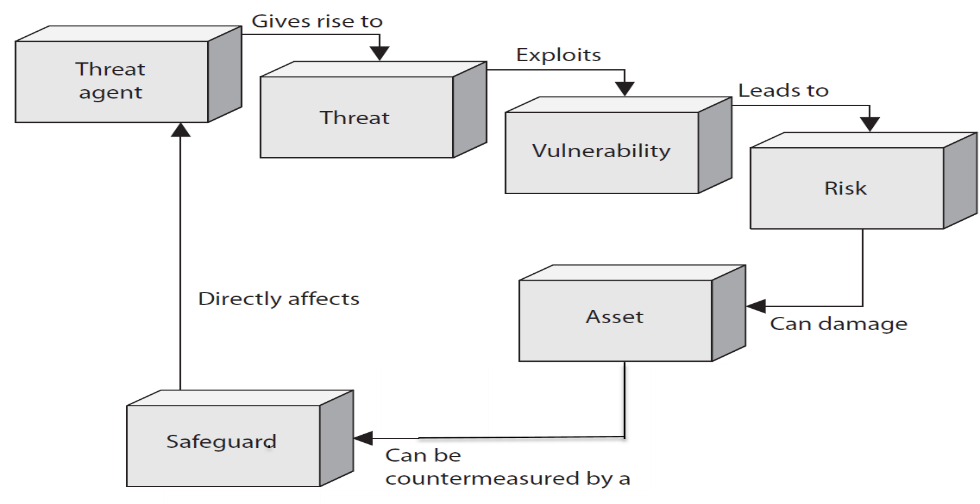
* **Prevention Measures: Authentication, Access Control, Message signing**

**(Message Signing-Cryptographic technique to detect whether bits have been modified)**

* **Detective Mechanisms – Intrusion Detection and Prevention: try, understand normal behavior and detect anomalous**
* **Monitors Characteristic of single host for suspicious activity**
* **Monitors Network Traffic and analyzes network, transport, and application protocols to identify suspicious activity**
  + **Deep Packet Inspection – Look at packet contents (check character strings in packet against DB of known virus, attack strings)**
* **Physical Barriers: Secure building**
* **Construction of building incorporating copper mesh (Faraday cages) so electromagnetic cannot enter/exit enclosure**
* **Data Correcting Codes: the ability to restore the original data if a transient error took place**
* **Message Authentication Code: Cryptographic technique to detect whether bits have been modified**
* **Access Control - Fundamental component of Data security, checks who’s allowed to access and use company info/resource**
* **Tools for Availability**
* **Redundancies: Backup, Multiple mail/DNS/DHCP servers, multiple network paths to ISP**
* **Firewall: Isolates organization’s internal net from larger internet, allowing some packets to pass, blocking others**
* **Intrusion Prevention**
* **Fail-safe defaults: access decisions should be based on permission rather than exclusion**
* **Complete Mediation: every access must be checked against the access control mechanism**
* **Open Design: the design of a security mechanism should be open rather than secret.**
* **Separation of privilege: a practice in which multiple privilege attributes are required to achieve access to a restricted resource**
* **Least Privilege: Every process and user should operate using the least set of privileges to do necessary tasks**
* **Isolation:**

1. **Public Access systems should be isolated from critical resources, to prevent disclosure or tampering**
2. **The processes and files of individual users should be isolated from one another except where it is desired**
3. **Security mechanisms should be isolated in the sense of preventing access to those mechanisms**

* **Encapsulation: a specific form of isolation based on object-oriented functionality**
* **Modularity: refers to both development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation**
* **Layering: The use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.**
* **Least Astonishment- means that a program or user interface should always respond in the way that is least likely to astonish the user**

****

* **Virus: Propagates by infecting other programs, usually inserted into host code**
* **Worms: Propagates automatically by copying itself to target systems.**

**Vulnerability:**

* **Asset: entity you want to protect. Data Exposure: instance of being exposed to losses**
* **A vulnerability is a weakness in system that allows a threat to be realized, compromising CIA**
* **Identify: How is system affected by a threat, what weaknesses are present inside a system to enable a threat to work**
* **Controls: Safeguard implemented to close vulnerabilities, controls can be physical (locking the door denies access), procedural (2 employees must be present) or technical in nature (System Policies such as require data to be encrypted)**
* **Threat: anything that can exploit a vulnerability. Can be malicious and accidental, maybe external or internal**
* **Control: A control, countermeasure or safeguard, that can be implemented to close vulnerabilities and mitigate the potential risk in order to protect CIA of the system**

**Introduction to cryptography:**

**Classification of Cryptography**:

Modern applications of Cryptography: GNU PG, TrueCrypt, Secure Shell, VPN, etc.

Cryptography- Symmetric algorithm, asymmetric Algorithm, protocol

* Set-up for symmetric cryptography: (simple) problem: communication over insecure channel.

Channel examples: internet, airwaves GSM, wifi, etc.

In practice, never use an untested crypto algorithm

A picture containing text, blackboard

Description automatically generated

Kerchkhoff’s Principle: cryptosystem should be secure even if attacker knows all the details about the system, except for the secret key

* Substitution Cipher (historical cipher – operated on letters)

Idea: replace every plaintext letter by a fixed cipher text letter.

1) Attack: Brute-force attack/ exhaustive key search: 26.25.24…1=26! = 2^88 = 2^56 x 2^32 (keyspace is too large to workout)

2) Attack: Letter frequency Analysis works because identical plaintext mapped to identical ciphertext symbols

* Classification of Attacks

Many Possible attack approaches (“attack vectors”)

A person writing on a chalkboard

Description automatically generated

Modular Arithmetic: Goal: computation in finite sets

Example: for a finite set in everyday life: clock: meet after 32 hours= 32%24=tomorrow 12

A green chalkboard with white writing

Description automatically generated with medium confidence

A green chalkboard with white writing

Description automatically generated with low confidence

Investigate:

1. Computation of the remainder

A picture containing text, blackboard, device, meter

Description automatically generated

A picture containing text, blackboard

Description automatically generated

A picture containing text, blackboard

Description automatically generated

A picture containing text, blackboard, night sky

Description automatically generated

The Remainder is not unique

1. Equivalence Classes

A green chalkboard with equations

Description automatically generated with low confidence

A person writing on a chalkboard

Description automatically generated

Text

Description automatically generated 81 x 81 (81=77+4)

2)Definition of integer ring: consists of

A green chalkboard with white writing

Description automatically generated with low confidence

A person writing on a chalkboard

Description automatically generated with medium confidence 3=! 1 => inverse does not exist

3)Shift or Caesar cipher-

Shift letters in alphabetical order

A picture containing text

Description automatically generated

Two attacks possible: Brute force attack, frequency analysis

4)Affine Cipher

Text

Description automatically generated

A picture containing text, blackboard

Description automatically generated

Two attacks possible: Brute force attack, frequency analysis

* Stream Ciphers: encrypts bits individually

A picture containing text, blackboard

Description automatically generated

Why encryption and decryption the same operation: (Proof)

A picture containing text, blackboard

Description automatically generated

Mod2 addition and subtraction are the same operation

A picture containing text, blackboard

Description automatically generated mod 2 is same as xor

If si is 0=> no need to flip. If Si is 1=>you flip

A picture containing diagram

Description automatically generated

How do we generate the key Stream bits Si: Somehow related to randomness

* Random Number Generators (RNG) :

A green board with white writing

Description automatically generated with medium confidence

A green board with white writing

Description automatically generated with medium confidence

A picture containing text, blackboard

Description automatically generatedA blackboard with white writing

Description automatically generated with low confidence

Text, letter

Description automatically generated

* One Time Pad: Goal: to build a ‘perfect’ cipher

A cipher is “unconditionally secure” or information theoretically secure if it cannot be broken even with infinite computing resources

Text

Description automatically generated

BIG drawback: key is as long as the message.

Text

Description automatically generated

A picture containing text, blackboard, sign

Description automatically generated

A hand writing on a chalkboard

Description automatically generated with medium confidence

Text

Description automatically generated

* Introduction to Linear Feedback Shift registers (LFSRs)

Goal: Stream cipher that is small (=low power) in hardware

Atomic Element: Flip-flop: stores 1 bit

A picture containing text, blackboard

Description automatically generated

Clock cycles the shift registers will push the o/p to the next

A green chalkboard with white writing

Description automatically generated with medium confidence

* General LSFRs

A picture containing text, blackboard

Description automatically generated

A chalkboard with equations

Description automatically generated with low confidence

Multiplayer

A picture containing text, blackboard

Description automatically generated1. Close switch, 2nd is open switch

A picture containing text, blackboard

Description automatically generated