Security Requirements

Introduction

A system can fail due to various reasons:

- Operator mistakes
- Hardware failures
- Poor implementation
- Deliberate human actions designed to cause failure

Cyber security is concerned with such **intentional failures**. We are concerned with the following:

Assets

- Hardware
- Software
- Data and information
- Reputation, which is intangible

Threat

- A set of circumstances that has the potential to cause loss or harm

Vulnerability

- A weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm

Control

- A control, countermeasure, security mechanism is a mean to counter threats
- It is an action, device, procedure, or technique that removes or reduces a vulnerability

A *threat* is blocked by *control* of a *vulnerability*

There are a few other terminologies, but it sums up to:
*There is a **threat agent** that gives rise to a **threat** that exploits a **vulnerability** that leads to a **risk** that can damage an **asset** and cause an **exposure**, all of which can be counter measured by a **safeguard** that directly affects the **threat agent**.*

Within **control**, there are a few kinds.

- Level 3: Physical Controls
  - Facility protection
  - Security guards
  - Locks
  - Monitoring
  - Environmental control
  - Intrusion detection
- Level 2: Technical Controls
  - Logical access controls
  - Encryption
  - Security devices
  - Identification and authentication
- Level 1: Administrative Controls
  - Policies
  - Standards
  - Procedures

    - Guidelines
    - Screening personnel
    - Security awareness training
- Level 0: Company data and assets

Administrative controls are often the hardest and the weakest link, since they involve people.

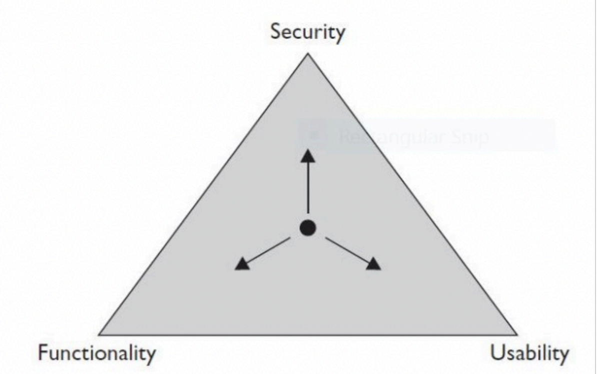
It can be difficult to achieve security due to:

- Not considering security during early design stage of a system
- Difficult to formulate security requirements
- Various design constraints
- Difficult to verify that a design achieves the intended security requirements
- Even if the design is secure, the implementation may be wrong
- There will always be a weakest point
- The humans involved in operating the system can be exploited
    - Configuration errors
    - Mismanagement of credentials/patches/etc.

There is always a **trade-off** between security and:

- Ease-of-use: Security mechanisms interfere with working patterns users are originally familiar with
- Performance: Security mechanisms consume more computing resources
- Cost: Security mechanisms are difficult to develop

Security, Functionality and Ease-Of-Use Triangle:
The more secure something is, the less usable and functional it becomes:



We can consider potential harm to assets in two ways.

- What bad things can happen to assets
- Who or what can cause or allow those bad things to happen

CIA

Confidentiality

- The ability to ensure that an asset is viewed only by authorized parties
- Prevention of unauthorized disclosure of information

Integrity

- The ability to ensure that an asset is modified only by authorized parties
- Prevention of unauthorized modification of information or processes

Availability

- The ability to ensure that an asset can be used by any authorized parties
- Prevention of unauthorized withholding of information or resources

The above are the C-I-A triad or security triad.

Others

ISO 7498-2 [ISO89] adds to them two more properties that are desirable, particularly in communication networks:

Authenticity/Authentication

- The ability of a system to confirm the identity of a sender

Non-repudiation/Accountability

- The ability of a system to confirm that a sender cannot convincingly deny having sent something

The US Department of Defense adds:

Auditability

- The ability of a system to trace all actions related to a given asset.

Looking at the CIA-triad At Another Angle

We can view it in terms of the nature of harm caused to assets, characterized by four acts:

- Interception
  - Confidentiality suffers if someone intercepts the data
- Interruption
  - Availability is lost is someone or something interrupts a flow of data or access to a computer
- Modification and Fabrication
  - Integrity can fail

Breaches in Recent Security News

Examples of Advanced Persistent Threats, which are often by an organized, well-financed and patient assailants:

- In 2012 and 2013, a series of attacks, apparently organized and supported by the Chinese government, was used to obtain product designs from aerospace companies in the United States. The stub of the attack code was loaded into the victim machines long in advance of the attack. The more complex code was then installed and helped to extract the data.
- In 2014, a series of attacks against J.P. Morgan Chase bank and up to a dozen similar financial institutions allowed the assailants access to 76 million names, phone numbers and email addresses. The attackers – and even their country of origin – remain unknown, as does the motive.