**Chapter 5 – Availability**

Availability refers to a property of software that is there and ready to carry out its task when you need it to be. It is a broad perspective, and it subsumes concepts of reliability, confidentially, and integrity, Fundamentally, availability is about minimizing service outage time by mitigating faults. One of the most demanding tasks in building a high-availability, fault-tolerant system is to understand the nature of the failures that can arise during operation. (Planning for failure) Once those are understood, mitigation strategies can be designed into the software.

A failure’s cause is called a fault. A fault can be either internal or external to the system under consideration. Intermediate states between the occurrence of a fault and the occurrence of a failure are called errors. Faults can be prevented, tolerated, removed, or forecast. In this way a system becomes “resilient” to faults.

*Planning for failure*

The first step is to understand what kinds of failures your system is prone to, and

what the consequences of each will be.

The well-known techniques for getting a handle on this are

*Hazard analysis*

It is a technique that attempts to catalog the hazards that can occur during the operation of a system. It categorizes each hazard according to its severity. Catastrophic, hazardous, major, minor, no effect.

**Fault tree analysis**

Fault tree analysis is an analysis technique that specifies a state of system that negatively impacts the safety, reliability, and then analyzes the system’s context and operation to find all the ways that the undesired state could occur. The technique uses a graphic construct (the fault tree) that helps identify all sequential and parallel sequences of contributing faults that will result in the occurrence of the undesired state, which is listed at the top of the tree (the “top event”).

The symbols that connect the events in a fault tree are called gate symbols and are taken from Boolean logic diagrams.

**Availability General Scenario**

*Portions and their explanation*

Source of Stimulus – We differentiate between internal and external origin of faults or failure because the desired system response may be different.

Stimulus – A fault of one of the following classes occur -> Omission, Crash, Timing, Response

Artifact – This specifies the source that is required to be highly available.

Environment – The state of the system when the fault or failure occurs.

Response – There are a number of possible reactions to a system fault.

Response Measure – It can specify an availability percentage, time to detect the fault, time to repair the fault etc.

**Portion of Scenario – Possible Values**

Source – Internal/external; people, hardware, software, physical infrastructure, physical environment

Stimulus – Fault: omission, crash, incorrect timing, incorrect response

Artifact – Processors, communication channels, persistent storage, processes

Environment – Normal operation, startup, shutdown, repair mode, degraded operation, overloaded operation

Response – Prevent the fault from becoming a failure

* Detect the fault
* Recover from the fault

Response Measure – Time or time interval when the system must be available.

**Sample Concrete Availability Scenario**

The heartbeat monitor determines that the server is nonresponsive during normal operations. The system informs the operator and continues to operate with no downtime.

Source: Heartbeat Monitor

Stimulus: Unresponsive

Artifact: Process

Environment: Normal Operation

Response: Inform Operator and Continue to Operate

Response Measure: No Downtime

**Summary**

Availability refers to the ability of the system to be available for use, especially after a fault occurs. The fault must be recognized (or prevented) and then the system must respond in some fashion. The response desired will depend on the criticality of the application and the type of fault and can range from “ignore it” to “keep on going as if it didn’t occur.”

**Chapter 9 – Security**

Security is a measure of the system’s ability to protect data and information from unauthorized access while still providing access to people and systems that are authorized. An action taken against a computer system with the intention of doing harm is called an attack and can take a number of forms. It may be an unauthorized attempt to access data or services or to modify data, or it may be intended to deny services to legitimate users.

The simplest approach to characterizing security has three characteristics:

Confidentiality, Integrity, and Availability (CIA)

1. Confidentiality is the property that data or services are protected from unauthorized access. For example, a hacker cannot access your income tax returns on a government computer.
2. Integrity is the property that data or services are not subject to unauthorized manipulation. For example, your grade has not been changed since your instructor assigned it.
3. Availability is the property that the system will be available for legitimate use. For example, a denial-of-service attack won’t prevent you from ordering book from an online bookstore.

Other characteristics that are used to support CIA are these: Authentication, Nonrepudiation, Authorization

We will use these characteristics in our general scenarios for security.

Approaches to achieving security can be characterized as:

* those that detect attacks
* those that resist attacks
* those that react to attacks
* those that recover from successful attacks

**Security General Scenario**

Our technique that is used in the security domain is threat modeling. An “attack tree”, similar to a fault tree in discussed in Chapter Availability, is used by security engineers to determine possible threats. The root is a successful attack, and the nodes are possible direct causes of that successful attack. Children odes decompose the direct cause, and so forth. An attempt is made to break CIA (Confidentially, Integrity, Availability), and the leaves of attack trees would be the stimulus in the scenario. The response to attack is to preserve CIA or deter attackers through monitoring of their activities.

**Portion of Scenario – Possible Values**

Source – Human or another system which may have been previously identified (either correctly or incorrectly) or may be currently unknown. A human attacker may be from outside the organization or from inside the organization.

Stimulus – Unauthorized attempt is made to display data, change, or delete data, access system services, change the system’s behavior, or reduce availability.

Artifact – System services, data within the system, a component or resources of the system, data produced or consumed by the system

Environment – The system is either online or offline, either connected to or disconnected from a network, either behind a firewall or open to a network, fully operational, partially operational, or not operational.

Response – Transactions are carried out in a fashion such that

* Data or services are protected from unauthorized access
* Data or services are not being manipulated without authorization
* Parties to a transaction are identified with assurance
* The parties to the transaction cannot repudiate their involvements.
* The data, resources, and system services will be available for legitimate use.

Response Measure – One or more of the following

* How much of a system is compromised when a particular component or data value is compromised
* How much time passed before an attack was detected
* How many attacks were resisted
* How long does it take to recover from a successful attack
* How much data is vulnerable to a particular attack

**Sample Concrete Security Scenario**

A disgruntled employee from a remote location attempts to modify the pay rate table during normal operations. The system maintains an audit trail, and the correct data is restored within a day.

Source: Disgruntled Employee from Remote Location

Stimulus: Attempts to Modify Pay Rate

Artifact: Data within the System

Environment: Normal Operations

Response: System Maintains Audit Trail

Response Measure: Correct Data is Restored within a Day and Source of Tampering Identified

**Security Tactics**

Attack -> Detect Attacks, Resist Attacks, React to Attacks, Recover from Attacks -> System detects, resists, reacts, or recovers

**Summary**

Attacks against a system can be characterized as attacks against the confidentially, integrity, or availability of a system or its data.

* Confidentiality means keeping data away from those who should not have access while granting access to those who should have.
* Integrity means that there are no unauthorized modifications to or deletion of data.
* Availability means that the system is accessible to those who are entitled to use it.

The emphasis of distinguishing various classes of actors in the characterization leads to many of the tactics used to achieve security. Identifying, authenticating, and authorizing actors are tactics intended to determine which users or systems are entitled to what kind of access to a system.

An assumption is made that no security tactic is foolproof and that systems will be compromised. Hence, tactics exist to detect an attack, limit the spread of any attack, and to react and recover from an attack.