Threats and Attacks

Madiba Hudson-Quansah

Contents

Chapter 1

Threat Categories

There are 12 categories of threats:

- Compromises to Intellectual Property
- Deviations in quality of service
- Espionage / Trespass
- Forces of Nature
- Human error / Failure
- Information Extortion
- Sabotage / Vandalism
- Software Attacks
- Technical Hardware failures / Errors
- Technical Software failures / Errors
- Technological Obsolescence
- Theft

1.1 Compromises to Intellectual Property

Definition 1.1.1: Intellectual Property

Creation, ownership, and control of original ideas, information, and creative works.

IP breaches compromise the **Confidentiality** of information, some examples are piracy, and copyright infringement.

1.1.1 Technical Controls

- Watermarking
- Embedded Code
- Registration Keys
- Intentional Corruption
- Obfuscation

1.1.2 Administrative/Legal Controls

- End User License Agreements (EULA)
- Copyrights
- Licenses

1.2 Deviations in Quality of Service

Deviations in quality of service occur when products or services are not delivered as expected, this compromises the **Availability** of a system. This is commonly cause by:

- Failure of interdependent support systems
- Supply Chain failures
- Failure of critical infrastructure (e.g power grid)

1.2.1 Technical Controls

- Redundancy
- Failover Systems / Redundant Systems (e.g. Redundant Array of Independent Disks (RAID))
- Backup Internet Service Providers (ISPs)
- Load Balancing
- Cloud Geographic Distribution

1.2.2 Administrative Controls

- Service Level Agreements (SLAs) - Contract between service provider and customer that specifies the level of service expected during its term.
- Policies and Procedures to deal with QoS issues

1.3 Espionage / Trespass

Definition 1.3.1: Espionage / Spying

Gaining unauthorized access to the information of an organization. The practice of obtaining information about an organization without the permission of the holder of the information.

Definition 1.3.2: Trespass

The act of entering someone's land or property without permission.

Espionage and Trespass primarily compromise the **Confidentiality**. Some examples include:

- Shoulder Surfing - Observing a person's private information over their shoulder.
- Industrial Espionage
- Hacking
- Governmental Espionage
- Social Engineering

1.3.1 Technical Controls

- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)
- Firewalls
- Encryption

1.3.2 Administrative Controls

- Access Control Policies
- Background checks
- Non-Disclosure Agreements (NDAs)

1.3.3 Physical Controls

- Security Guards
- CCTV Surveillance
- Privacy Screens

1.4 Forces of Nature

Disrupts not only individual loves but also the storage, transmission and use of information. Natural disasters primarily compromises **Availability** and **Integrity**. Some examples include:

- Fires
- Floods
- Earthquakes

1.4.1 Technical Controls

- Offsite Backups
- System Redundancy and Failover
- Uninterruptible Power Supplies (UPS)

1.4.2 Administrative Controls

- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Risk Assessments

1.4.3 Physical Controls

- Secure Facility design
- Geographic Diversity

1.5 Human Error / Failure

Occurs when users or administrators make mistakes that compromise information systems. This primarily compromises **Confidentiality**, **Integrity**, and **Availability**. Some examples include:

Social Engineering - The use of social skills for the purpose of gaining unauthorized access to information or systems.

Other

- Phishing
- Spearpshising
- Whaling
- Watering Hole Attacks
- Pretexting
- Vishing

1.5.1 Technical Controls

- Email Filtering
- Anti-Phishing software
- Multifactor Authentication

1.5.2 Administrative Controls

- Regular Security Awareness Training
- Phishing Simulations
- Clear Reporting Procedures

1.5.3 Operational Controls

- Incident Response Plans
- Monitoring Unusaal Account Activity
- Regular Software Updates and Patch Management

1.6 Information Extortion / Cyberextortion

An attacker steals information from a computer system and demands compensation for it's return or non-disclosure. Cyberextortion primarily compromises **Availability**, then **Integrity** and **Confidentiality** if data is exfiltrated. There are two types of ransomware attacks:

- Lock screen - Prevents access to the device
- Encryption - Encryptions sensitive files

1.6.1 Technical Controls

- Anti-Malware Software
- Email and Web Filtering
- Data Backups

1.6.2 Administrative Controls

- User Training
- Incident Response Plan
- Regular Software Updates and Patch Management

1.7 Sabotage / Vandalism

Definition 1.7.1: Sabotage

The obstruction of a system's operations or intended functions. Sabotage is often directed with an explicit reason / goal.

Definition 1.7.2: Vandalism

The intentional destruction or defacement of property. The main intention of vandalism is destruction.

Involves the deliberate sabotage of a computer system or business, or acts of vandalism to destroy and asset or damage the image of an organization. This primarily compromises **Integrity** and **Availability**. Some examples include:

- Website defacing - Erodes consumer confidence
- Hacktivism / Cyberactivism
- Cyberterrorism / Cyberwarfare.

1.7.1 Technological Controls

- Web Application Firewalls (WAF)
- Distributed Denial of Service (DDoS) protection
- Website defacement monitoring
- Backups

1.7.2 Administrative Controls

- Policies and Procedures
- Legal Enforcement
- Awareness Training

1.7.3 Operational Controls

- Physical security of equipment.
- Host Redundancy
- Incident Response
- Monitoring

1.8 Software Attacks

Definition 1.8.1: Malware

Malicious software designed to infiltrate or damage a computer system without the owner's informed consent.

Involve designing and deploying malware to compromise a system. Software attacks may overwhelm the processing capabilities of online systems or allow access to protected systems by hidden means. Software attacks primarily compromise **Confidentiality**, **Integrity**, and **Availability** to varying severities. Some examples include:

Traditinoal Malware Viruses, Worms, Trojans, Spyware, Adware, Ransomware, Rootkits, Keyloggers

Access/Control Malware Backdoors, Botnets, Remote Access Trojans (RATs)

Disruption Attacks Denial of Service (DoS), Distributed Denial of Service (DDoS)

Interception Attacks Spoofing, Man-In-the-Middle (MitM), Session Hijacking, Packet sniffing, pharming

Definition 1.8.2: Viruses

A type of malware that attaches itself to a legitimate program or file and spreads to other programs and files when executed.

Definition 1.8.3: Worm

A type of malware that can replicate itself and spread independently without needing to attach to a host program.

Definition 1.8.4: Trojan

A type of malware that disguises itself as a legitimate program or file to trick users into installing it, often creating a backdoor for unauthorized access.

Definition 1.8.5: Logic Bomb

A type of malware that is triggered by a specific event or condition, such as a date or the deletion of a file.

Definition 1.8.6: Zero-Day Attack

An attack that exploits a previously unknown vulnerability in a computer application, meaning there is no existing patch or fix for the vulnerability.

Definition 1.8.7: Pharming

A cyberattack that redirects a website's traffic to a fraudulent website, often through DNS cache poisoning or modifying the hosts file on a victim's computer.

Definition 1.8.8: Phising

A cyberattack that uses fraudulent emails or websites to trick individuals into revealing sensitive information, such as passwords or credit card numbers.

1.8.1 Technical Controls

- Anti-Virus / Anti-Malware Software
- Firewalls
- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)
- Patch Management
- Secure Software Development Practices

1.8.2 Administrative Controls

- Security Policies on patching
- User Training
- Software Inventory Management

1.8.3 Operational Controls

- Incident Response Planning and Policies

- Malware Analysis Teams
- Threat Intelligence Sharing
- Backups

1.9 Technical Hardware Failures / Errors

Occurs when a manufacturer distributes equipment containing a known or unknown flaw. This primarily compromises **Availability** and **Integrity**. Some examples include:

- Pentium II Floating Point Division Bug
- Spectre and Meltdown CPU Vulnerabilities
- Hardware crashes
- RAM failures

1.9.1 Technical Controls

- Redundancy (e.g RAID)
- Error Checking RAM
- Uninterruptible Power Supplies (UPS)

1.9.2 Administrative Controls

- Vendor Risk Assessment
- Procurement Policies
- Warranty and Maintenance Agreements

1.9.3 Operational Controls

- Preventative Maintenance Schedules
- Hardware Monitoring Tools
- Asset Lifecycle Management

1.10 Technical Software Failures / Errors

Occurs when software contains undetected bugs or flaws that lead to vulnerabilities. Some of these common vulnerabilities include:

Input and Validation Issues - Can compromise **Confidentiality**, **Integrity**.

- Buffer overrun
- Command injection
- Cross-site scripting (XSS)
- SQL injection

Cryptographic and Authentication Failures - Can compromise **Confidentiality**

- Failure to use cryptographically strong random numbers
- Improper use of SSL
- Unauthenticated key exchange

Logic and Control Issues - Can compromise **Integrity** and **Availability**

- Catching exceptions
- Failure to handle errors
- Race Conditions

Data Protection Failures - Compromises **Confidentiality**

- Failure to protect network traffic
- Failure to store and protect data securely
- Information leakage

1.10.1 Technical Controls

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Runtime Application Self-Protection (RASP)
- Web Application Firewalls (WAF)

1.10.2 Administrative Controls

- Secure Coding Practices

1.10.3 Operational Controls

- Code reviews
- Peer Audits
- Penetration Testing

1.11 Technological Obsolescence

Old and outdated technology that is no longer supported or maintained primarily compromises **Availability** and **Integrity**.

1.11.1 Technical Controls

- Regular Patching
- System Upgrades
- Migration to Supported Platforms
- Virtualisation

1.11.2 Administrative Controls

- IT governance frameworks
- Lifecycle Management Policies
- Vendor Risk Management

1.11.3 Operational Controls

- Asset Inventory and Monitoring
- End of Life (EOL) Planning
- Scheduled decommissioning of obsolete systems

1.12 Theft

Illegally taking physical, electronic, or intellectual property, compromises **Confidentially**.

1.12.1 Technical Controls

- Encryption of sensitive data
- Access Control
- Data Loss Prevention (DLP) solutions

1.12.2 Administrative Controls

- Security Policies
- Employee Background Checks
- IP protection agreements

1.12.3 Operational Controls

- CCTV Surveillance
- Security Guards
- Asset Tracking

Chapter 2

Threat Modelling

2.1 Introduction

Definition 2.1.1: Threat Modelling

A systematic listing of different ways a threat may be realized. In this process potential threats are identified, categorized and analysed, to identify the potential harm, the probability of occurrence (risk), the priority of concern, and security controls, or countermeasures to mitigate the threats.

Threat modelling is useful as it helps to:

- Identify ways to improve software development processes
- Improves the system's configuration management and security controls
- Identify vulnerabilities in software
- Increase user awareness, incident detection and response.

2.2 Threat Modelling Methodologies

Threat modelling commonly involves the following tasks:

Determining Vulnerabilities - Identify potential vulnerabilities in the systems that could lead to compromise of the CIA triad.

Determine Adversaries - Identify potential adversaries, their motivations, and capabilities

Determine Potential Attack Vectors - Identify whether a given threat source has the means to exploit the vulnerability.

Definition 2.2.1: Risk Assessment

The overall process of identifying, evaluating, and estimating the levels of risk involved in a situation, to determine an acceptable level of risk and the appropriate ways to eliminate or control the risk.

Threat modelling can be performed either as a **proactive** measure during design and development or a **reactive** measure once a product has been deployed.

2.2.1 Defensive / Proactive Approach

Proactive threat modelling takes place during the early stages of systems development, and involves predicting threats and designing defences before deployment. This is more cost-effective and successful as security solutions are integrated in the development process. Some examples of proactive threat modelling methodologies include:

Security Development Lifecycle (SDL) - Aims to reduce the number of security-related design and coding defects, and to reduce the severity of any remaining defects.

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) - A model for identifying computer security threats.

PASTA (Process for Attack Simulation and Threat Analysis) - A seven-step, risk-centric methodology that aims to align business objectives and technical requirements.

2.2.1.1 STRIDE

STRIDE is a mnemonic for a set of threats

Spoofing - An attack with the goal of gaining access to a target system using a falsified identity. Compromises **Authentication**

Tampering - Any action resulting in unauthorized changes or manipulation of data, whether in transit or in storage. Compromises **Integrity**

Repudiation - The ability of a user or attacker to deny having performed an action or activity by maintaining plausible deniability. Compromises **Non-repudiation**

Information Disclosure - The exposure of private, confidential, or controlled information to external or unauthorized entities. Compromises **Confidentiality**

Denial of Service - An attack that attempts to prevent authorized use of a resource. Compromises **Availability**

Elevation of Privilege - An attack where a limited user account is transformed into a full privileged user account with greater powers and access. Compromises **Authorization**

2.2.1.2 PASTA

Involves simulating attacks to IT applications analysing the threats their origin, the risks they pose to an organization, and how to mitigate them. Organizations can determine the most appropriate countermeasures that must deployed to mitigate risk. It is a risk-centric approach that aims at selecting / developing countermeasures in relation to the value of the assets being protected.

2.2.1.3 STRIDE vs PASTA

- PASTA is risk-centric, STRIDE is threat-centric.
- PASTA is a seven-step process, STRIDE is a categorization model.
- PASTA focuses on simulating attacks, STRIDE focuses on identifying threats.
- PASTA is an end-to-end methodology, STRIDE is a component of threat modelling.

2.2.2 Adversarial / Reactive Approach

Reactive threat modelling takes place after a product has been created / deployed. It is the core concept behind ethical hacking penetration testing, source code review, and fuzz testing.

Definition 2.2.2: Fuzzing

An automated software testing method that injects invalid, malformed or unexpected inputs into a system to reveal software defects and vulnerabilities.

2.3 Threat Intelligence

Definition 2.3.1: Threat Intelligence

Knowledge that allows the prevention or mitigation of cyber-attacks by studying the threat data and providing information on adversaries.

Threat intelligence is useful as it helps to:

- Identify, prepare and prevent attacks by providing information on attackers, their motives and capabilities.
- Prepares organizations to be proactive with predictive capabilities
- Identify, classify and prioritize threats to ensure effective documentation and reporting.

2.4 Reduction Analysis / Decomposition

Definition 2.4.1: Reduction Analysis / Decomposition

A method of breaking down a complex system into smaller, more manageable components to gain a greater understanding of the logic of the product, its internal components and its interactions with external elements.

Reduction Analysis focuses on

Software - Subroutines, models, or objects

System - Computers and Operating Systems

Network - Protocols

Business infrastructure - Departments, tasks and networks.

Reduction must identify five key concepts:

Trust Boundaries - Points in a system where data or control flows from one component to another, and where the level of trust changes.

Data Flows - The movement of data between components in a system.

Inputs - The data or control signals that enter a system or component.

Privileged Functions - Operations or actions that require elevated permissions or access rights to perform.

Security Approach

2.5 Prioritization and Response

Once threats have been identified, they must be prioritized based on a specified technique. Some techniques include:

- Probability / Damage matrix
- High / Medium / Low (H/M/L) rating
- DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)

2.5.1 Probability / Damage Matrix

Produces a risk severity number on a scale from 1 to 100 by multiplying the probability of occurrence (1-10) by the potential damage (1-10).

2.5.2 H/M/L Rating

Classifies threats into three categories:

High - Threats that are likely to occur and could cause significant damage.

Medium - Threats that have a moderate likelihood of occurring and could cause moderate damage.

Low - Threats that are unlikely to occur and would cause minimal damage.

2.5.3 DREAD

DREAD stands for:

Damage Potential - How severe is the damage likely yo be if the threat is realized?

Reproducibility - How complicated is it for attackers to reproduce the attack?

Exploitability - How hard is it to launch the attack?

Affected Users - How many users are likely to be affected by the attack?

Discoverability - How easy is it for an attacker to discover the vulnerability?

Chapter 3

Risk Management

Definition 3.0.1: Risk

The probability of an unwanted occurrence such as an adverse event or loss.

Definition 3.0.2: Risk Management

The process of identifying, assessing, and controlling risks facing an organization.

3.1 Components of Risk Management

Risk management involves the following components:

Risk Identification - The process of examining an organization's current IT security situation to recognize enumerate and document the risks to its IT assets.

Risk Assessment - Determination of the extent to which an organization's IT assets are exposed to risk.

Risk Control - Application of controls that reduce the risks to an organization's ID assets to an acceptable level.

Definition 3.1.1: Risk Appetite / Tolerance

The quantity and nature of risk that an organization is willing to accept as they evaluate the trade-offs between risk and cost. The general rule is to never spend more to protect an asset than the asset is worth.

Definition 3.1.2: Residual Risk

Risk that is left over after the risk management process has concluded. The reaming risk that has not been removed, shifted or planned for when vulnerabilities have been controlled as much as possible.

Residual risk is a combined function of:

- A threat minus the effect of threat-reducing controls
- A vulnerability minus the effect of vulnerability-reducing controls
- An asset minus the effect of asset value-protecting controls

The goal of risk management is to reduce the residual risk to a level within an organization's risk appetite, I.e less than or equal to the risk tolerance.

3.1.1 Risk Identification

Risk identification involves the following steps:

Plan and Organize -

Identify, inventory and categorize assets

Classify, value and prioritize assets

Identify and prioritize threats

Specify asset vulnerabilities