INSTITUTO FEDERAL
DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
Ceará

Gestão de Segurança da Informação

Attack and Defense

Vaux Gomes [1]

[1]Instituto Federal de Educação, Ciência e Tecnologia do Ceará
Campus Jaguaribe

25 de março de 2025

Sumário

Attacks

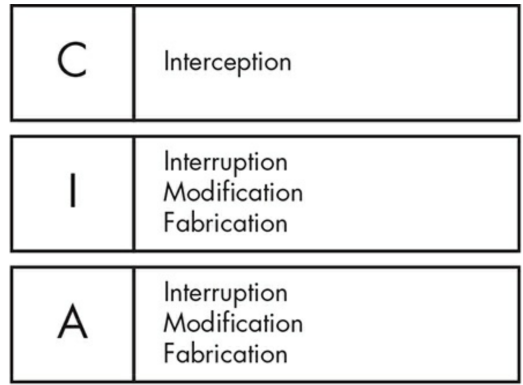
Types of Attacks

- You may **face attacks from a wide variety of approaches and angles**.
- You can break these down according to:
  - The **type** of attack
  - The **risk** the attack represents
  - The **controls you might use to mitigate it**.

Attacks

Types of Attacks

- You can generally **place attacks into one of four categories**:
  - Interception
  - Interruption
  - Modification
  - Fabrication
- Each of the categories **can affect one or more of the principles** of the CIA triad



Interception

Interception attacks **allow unauthorized users to access your data**, applications, or environments and are primarily **attacks against confidentiality**

- Examples:
  - Unauthorized file viewing or copying
  - Eavesdropping on phone conversations
  - Reading someone else's email

Note

When they're properly executed, interception attacks can be difficult to detect

Interruption

Interruption attacks **make your assets unusable or unavailable** to you on a temporary or permanent basis. These attacks **often affect availability but can affect integrity**, as well

- Examples:
  - DoS attack on an mail server
  - Intentional power break

Modification

Modification attacks involve **tampering with an asset**. Such attacks might primarily be **considered attacks on integrity** but **could also represent attacks on availability**.

Example

If you **access a file in an unauthorized manner and alter the data** it contains, you've **affected the integrity** of the file's data. However:

- If the file in question is a configuration file that manages how a service behaves, changing the contents of the file might affect the **availability** of that service
- If the configuration you altered in the file for your web server changes how the server deals with encrypted connections, you could even call this a **confidentiality** attack

Fabrication

Fabrication attacks **involve generating data**, processes, communications, or other similar material with a system. Fabrication attacks **primarily affect integrity but could affect availability**, as well.

- Examples:
  - Generating fake information in a database
  - Generate email (a common method for propagating malware)
  - If you generated enough additional processes, network traffic, email, web traffic, or nearly anything else that consumes resources, **you might be conducting an availability attack** by rendering the service that handles such traffic unavailable to legitimate users

Attacks

Threats, Vulnerabilities, and Risk

- When you look at how an attack might affect you, you can speak of it in terms of **threats, vulnerabilities, and the associated risk**

Threats

Ultimately, a threat is something that has the **potential to cause harm**

- Threats **tend to be specific to certain environments**, particularly in the world of information security

Example

Although a virus might be problematic on a Windows operating system, the same virus will be unlikely to have any effect on a Linux operating system

Vulnerabilities

Vulnerabilities are weaknesses, or holes, that threats can exploit to cause you harm

- A vulnerability might involve:
  - A **specific operating system** or application that you're running
  - The **physical location** of your office building,
  - A data center that is overpopulated with servers and **producing more heat than its air-conditioning system can handle**
  - A **lack of backup** generators
  - etc

Risk

Risk is the **likelihood** that something bad will happen. For you to have a risk in an environment, **you need to have both a threat and a vulnerability** that the threat could exploit

Example

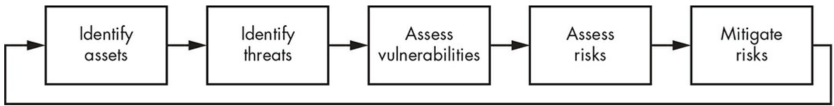
- If you have a structure that is made from wood and you light a fire nearby, you have both a threat and a matching vulnerability. In this case, you most definitely have a risk.
- Likewise, if you have the same threat of fire but your structure is made of concrete, you no longer have a credible risk because your threat doesn't have a vulnerability to exploit.

Impact

Impact **takes into account the value of the asset** being threatened and uses it **to calculate risk**

- Some organizations, such as the US National Security Agency (NSA), add the factor *impact* to the threat/vulnerability/risk equation
- In the backup tape example, if you consider that the unencrypted **tapes contain only your collection of chocolate chip cookie recipes**, you may **not actually have a risk** because the data exposed contains nothing sensitive

- Risk management processes **compensate for risks** in your environment
- The following figure shows a typical risk management process at a high level



Risk Management

Identify Assets

- The **most important parts** of the risk management process is **identifying the assets** you're protecting
- After that you need to **decide which of them are critical business assets**
- It may be a complicated task. Large enterprises might have:
  - Various generations of hardware
  - Assets from acquisitions of other companies
  - Many virtual hosts in use
  - etc

Failing to identify important assets

If you can't enumerate your assets and evaluate the importance of each, protecting them can become a difficult task indeed.

- After enumerating your critical assets, you can then begin to identify the threats that might affect them
- It's **often useful to have a framework** for discussing the nature of a given threat (like the Parkerian hexad)
- **You need to be concerned with losing control of data, maintaining accurate data, and keeping the system up and running**

Risk Management

Identify Threats

Confidentiality	If you **expose data inappropriately**, you could potentially have a breach
Integrity	If **data becomes corrupt**, you may incorrectly process payments
Availability	If the system or **application goes down**, you won't be able to process payments
Possession	If you **lose backup media**, you could potentially have a breach
Authenticity	If you **don't have authentic customer information**, you may process a fraudulent transaction
Utility	If you **collect invalid or incorrect data**, that data will have limited utility

Tabela 1: Example of threats for an application that processes credit card payments

- When assessing vulnerabilities, you need to do so **in the context of potential threats**
- Any given asset may have thousands or millions of threats that could impact it, but **only a small fraction of these will be relevant**

Let's have a look

1. **Confidentiality** If you expose data inappropriately, you could have a breach.
   - Your sensitive **data is encrypted** at rest and in motion. Your **systems are regularly tested** by an external penetration testing company. *This is not a risk*
2. **Integrity** If data becomes corrupt, you may incorrectly process payments
   - You carefully **validate that payment data is correct** as part of the processing workflow. **Invalid data results in a rejected transaction**. *This is not a risk*
3. **Availability** If the system or application goes down, you can't process payments.
   - **You do not have redundancy** for the database on the back end of the payment processing system. If the database goes down, you can't process payments. *This is not a risk*

4. **Possession** If you lose backup media, you could have a breach.
   - Your **backup media is encrypted** and hand-carried by a courier. *This is not a risk*
5. **Authenticity** If you don't have authentic customer information, you may process a fraudulent transaction.
   - Ensuring that valid payment and customer information belongs to the individual conducting the transaction is difficult. **You do not have a good way of doing this**. *This is a risk*
6. **Utility** If you collect invalid or incorrect data, that data will have limited utility.
   - To protect the utility of your data, you checksum credit card numbers, make sure that the billing address and email address are valid, and perform other measures to **ensure that your data is correct**. *This is not a risk*

Risk Management

Assess Risks

- *Risk is the conjunction of a threat and a vulnerability*
- A vulnerability with no matching threat or a threat with no matching vulnerability does not constitute a risk
- In the availability example from before (3): you have both a threat and a corresponding vulnerability
  - You risk losing ability to process credit card payments because of a single point of failure on your database back end

- To mitigate risks, **you can put measures in place to account for each threat**
- These measures are called **controls**. Controls are divided into three categories:
  1. **Physical controls** protect the physical environment in which your systems sit, or where your data is stored.
     - Such controls also **control access in and out of such environments**.
     - Physical controls include fences, gates, locks, bollards, guards, and cameras, but also systems that maintain the physical environment, such as heating and air-conditioning systems, fire suppression systems, and backup power generators.
     - If attackers can physically access your systems, **they can steal or destroy them**, rendering them unavailable for your use—in the best case.
     - In the worst case, attackers will be able to access your applications and data directly and **steal your information and resources or subvert them for their own use**

2. **Logical controls** (or technical controls) protect the systems, networks, and environments that process, transmit, and store your data.
   - Logical controls can include items such as passwords, encryption, access controls, firewalls, and intrusion detection systems
   - Logical controls **enable you to prevent unauthorized activities**
   - If your logical controls are implemented properly and are successful, **an attacker or unauthorized user can't access your applications and data without subverting the controls**

3. **Administrative controls** are based on rules, laws, policies, procedures, guidelines, and other items that are "paper" in nature.
   - Administrative controls **dictate how the users of your environment should behave**
   - You may have an administrative control, such as one that requires you to change your password every 90 days

When enforcing a rule

If you don't have the authority or the ability to ensure that people comply with your controls, they are worse than useless because **they create a false sense of security**. For example, if you create a policy that says employees can't use business resources for personal use, you'll need to be able to enforce this.

- If your risk management efforts are not as thorough as you hoped you can react with incident response
- You **should direct your incident response** at the items that you feel are **most likely to cause your organization pain**[1]
- As much as possible, **you should base your reaction to such incidents on documented incident response plans**, which should be **regularly reviewed, tested, and practiced** by those who will be expected to enact them in the case of an actual incident

- The incident response process, at a high level, consists of the following:
  - Preparation
  - Detection and analysis
  - Containment
  - Eradication
  - Recovery
  - Post-incident activity

[1] You should have already identified these as part of your risk management efforts

Preparation

The preparation phase of incident response consists of **all the activities you can perform ahead of time** to better handle an incident.

- Involves creating policies and procedures that govern incident response and handling, conducting training and education

Detection and analysis

In this phase, you detect an issue, **decide whether it's actually an incident, and respond to it appropriately**

1. Most often, you'll detect the issue with a security tool or service, like an intrusion detection system (IDS), antivirus (AV) software, firewall logs, proxy logs
2. The analysis portion of this phase is often a combination of automation from a tool or service, usually a SIEM (Security Information and Event Management) tool, and human judgment

Containment

Containment involves taking steps to **ensure that the situation doesn't cause any more damage** than it already has.

- If the problem involves a malware-infected server actively being controlled by a remote attacker, you must disconnect the server from the network and put firewall rules in place to block the attacker, for example

Eradication

During eradication, you'll attempt **to remove the effects of the issue from your environment**

- In the case of your malware-infected server, you've already isolated the system and cut it off from its command-and-control network
- Now you'll need to clean the malware from the server and ensure that it doesn't exist elsewhere in your environment

Recovery

Recovery might involve **restoring** devices or data from backup media, rebuilding systems, or reloading applications

- This can be a more painful task than it initially seems because your knowledge of the situation might be incomplete or unclear

Post-Incident Activity

In the post-incident activity phase you attempt to determine specifically what happened, why it happened, and what you can do to keep it from happening again

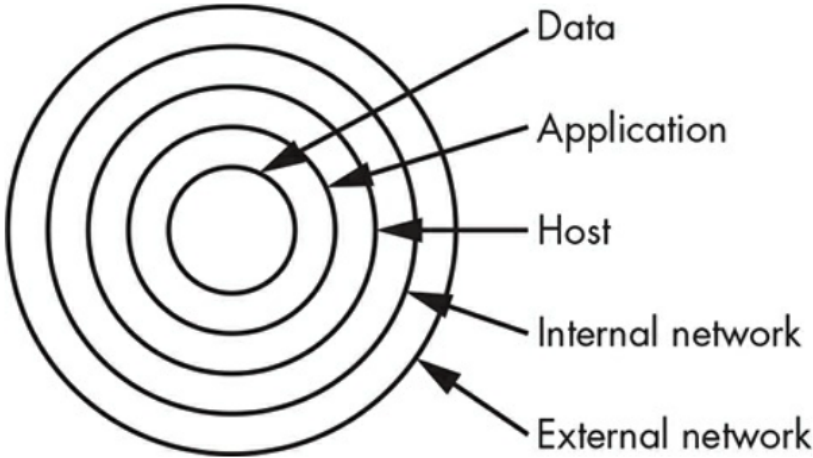
- The purpose of this phase is to ultimately prevent or lessen the impact of future such incidents

Defense in Depth

Defense in depth

Defense in depth is a strategy common to both military maneuvers and information security. The basic concept is to **formulate a multilayered defense that will allow you to still mount a successful resistance should one or more of your defensive measures fail**

Defense in Depth



Defense in Depth

- Well-implemented defenses at each layer make it difficult to successfully penetrate your network and attack your assets directly
- No matter how many layers you put in place or how many defensive measures you place at each layer, you won't be able to keep every attacker out for an indefinite period.
- The goal is to place enough defensive measures between your truly important assets and the attacker so that you'll notice that an attack is in progress and have enough time to prevent it

Defense in Depth

Defense by Layer

1. **External network** DMZ, VPN, Logging, Auditing, Penetration testing, Vulnerability analysis
2. **Network perimeter** Firewalls, Proxy, Logging, Stateful packet inspection, Auditing, Penetration testing, Vulnerability analysis
3. **Internal network** IDS, IPS, Logging, Auditing, Penetration testing, Vulnerability analysis **Host** Authentication, Antivirus, Firewalls, IDS, IPS, Passwords, Hashing, Logging, Auditing, Penetration testing, Vulnerability analysis
4. **Application** SSO, Content filtering, Data validation, Auditing, Penetration testing, Vulnerability analysis
5. **Data** Encryption, Access controls, Backups, Penetration testing, Vulnerability analysis

Exercises (Chapter 1)

1. Explain the difference between a vulnerability and a threat.
2. What are six items that might be considered logical controls?
3. Which category of attack is an attack against confidentiality?
4. How do you know at what point you can consider your environment to be secure?
5. Using the concept of defense in depth, what layers might you use to secure yourself against someone removing confidential data from your environment on a USB flash drive?

Exercises (Chapter 1)

6. Based on the Parkerian hexad, what principles are affected if you lose a shipment of encrypted backup tapes that contain personal and payment information for your customers?
7. If the web servers in your environment are based on Microsoft's Internet Information Services (IIS) and a new worm is discovered that attacks Apache web servers, what do you not have?
8. Considering the CIA triad and the Parkerian hexad, what are the advantages and disadvantages of each model?

References

J. Andress. *Foundations of information security: a straightforward introduction*. No Starch Press, 2019.