Cybersecurity from Beginner to Paid Professional

Part 1

Protecting Systems, Data and Networks

Written By

Bolakale Aremu

Cybersecurity From Beginner to Paid Professional, Part 1

Protecting Systems, Data and Networks

Published in the United States

Table of Contents

1. Introduction to Cybersecurity & CIA Triad

Every day, headlines are filled with reports of the latest cyberattacks, showing us the pervasive and evolving threat of cybercrime. These attacks disrupt governments, businesses, and individuals alike, but what exactly are these attacks, and how are they made possible? Cybercrime doesn't occur in isolation—it is facilitated by vulnerabilities in our technology, the limitations of our laws, and even certain social norms. This book aims to explore the major drivers behind cybercrime and the cybersecurity measures that are designed to detect, respond to, and ultimately prevent these incidents from happening in the first place.

In recent years, cyberattacks have grown in both frequency and complexity. Between 2021 and 2024, cybercrime reached alarming new levels, with several high-profile attacks highlighting the growing sophistication of hackers.

One notable case occurred in 2024 when the **MOVEit** file transfer software breach made headlines globally. Hackers exploited a vulnerability in the software to steal sensitive data from thousands of organizations, including government agencies and corporations. This attack underscored the rising threat of software supply chain attacks, where vulnerabilities in widely used tools are exploited to compromise large numbers of users. These cases reflect the growing scale and impact of cybercrime on both personal privacy and national security.

Another notable case occurred in 2023 when hackers targeted **Optus**, one of Australia's largest telecommunications companies. The attack exposed the personal information of nearly 10 million customers, including passport numbers, driver's licenses, and contact details. Investigations revealed that the breach was due to a vulnerability in Optus's API (Application Programming Interface), highlighting the increasing threat posed by insecure APIs in modern digital systems.

Another significant case in 2023 involved the **Medibank** ransomware attack, where hackers breached Australia's largest health insurer, stealing sensitive medical records. The attackers demanded a ransom, threatening to release patients' private medical histories online. Medibank refused to pay the ransom, leading to the public release of some records, which caused widespread concern about the privacy of healthcare data.

In 2021, the Colonial Pipeline ransomware attack brought a major US fuel supplier to a halt, causing widespread panic and fuel shortages along the East Coast. The attack was carried out by the DarkSide ransomware group, which exploited vulnerabilities in the company's IT infrastructure, encrypting critical data and demanding ransom. Colonial Pipeline eventually paid the attackers millions of dollars to restore their systems. This attack underscores how cybercriminals can paralyze essential infrastructure, disrupting daily life for millions of people.

These examples highlight the critical need for robust cybersecurity. However, they also raise essential questions: How do these attacks happen, and what makes them so hard to prevent? In many cases, cybercriminals exploit weaknesses in software, poor security practices, and human error. In the case of SolarWinds, the hackers used a supply chain attack—a method where malicious code is introduced during a software update, spreading through systems unnoticed. Similarly, in the Colonial Pipeline attack, weak security protocols allowed hackers to gain access and hold the company's systems hostage. Both cases demonstrate the delicate balance between technological advancement and security preparedness.

As technology becomes more integrated into every aspect of our lives, the opportunities for cybercriminals increase. From state-sponsored espionage to criminal organizations seeking

profit, the motivations behind cybercrime are diverse and growing. Laws and regulations struggle to keep up with these fast-moving threats, creating gaps that attackers readily exploit. While businesses and governments are investing heavily in cybersecurity, they often find themselves reacting to attacks rather than proactively preventing them. Understanding the root causes of these attacks is crucial for developing better defenses and improving global cybersecurity practices.

This book will delve into these challenges, examining the interplay between technology, legislation, and social dynamics that make cybercrime possible. By understanding both the technical aspects of cybersecurity and the broader context in which these crimes occur, we can begin to develop strategies to mitigate the risk of future attacks. Ultimately, the goal is not just to respond to cybercrime but to build a more secure digital world where these threats are minimized from the outset.

1.1. The CIA Triad

In cybersecurity, a key framework for protecting information and systems is known as the **CIA triad**, which stands for **Confidentiality, Integrity, and Availability**. These three concepts form the foundation of effective security practices, ensuring that sensitive data is protected and remains trustworthy and accessible.

Let’s break it down:

Confidentiality is all about keeping information private. Only authorized people should be able to access sensitive data, whether it's personal, financial, or business-related. Think of it like having a lock on your mailbox—only you and anyone you trust with the key should be able to see what's inside. When confidentiality is breached, it can lead to identity theft, financial loss, or even harm a company’s reputation.

Integrity focuses on keeping data accurate and unchanged. Imagine if someone tampered with a company’s financial records or altered medical data—those changes could lead to serious consequences. Integrity ensures that information remains exactly as it should be, without unauthorized modifications. Maintaining data integrity is critical for trust and decision-making because inaccurate or corrupted data can cause major disruptions or financial losses.

Availability means that information and systems are accessible whenever they’re needed. If your organization relies on an online platform or database, but that system suddenly goes offline, it can bring operations to a halt. Ensuring availability helps businesses and users access the data they need, especially in times of crisis.

Therefore, the **CIA triad** helps guide cybersecurity measures to ensure data is protected, trusted, and always accessible, which is vital for both personal and business security.

1.2. Computer and Network Security in the Context of CIA

Computer security and **network security** are both key components of protecting digital systems and data, and they both rely on the **CIA triad** as guiding principles. However, their focus and methods differ.

Computer Security

Computer security focuses on securing individual systems, such as computers, servers, or devices, by ensuring they meet the required levels of confidentiality, integrity, and availability.

For example, if a computer is used to store sensitive data (like financial records or personal information), confidentiality is crucial. This can be achieved through encryption, secure passwords, and access controls, ensuring that only authorized users can view or alter sensitive files.

Integrity is protected by measures like antivirus software, firewalls, and file integrity checks, which prevent unauthorized changes to data or software. Availability ensures that the system and its data are accessible when needed, through backup systems, redundancy, or hardware maintenance, reducing the impact of hardware failures or cyberattacks.

Each computer system might prioritize these elements differently based on its use. For example, a hospital's computer systems may place a higher value on availability to ensure continuous access to patient data in emergencies, whereas a financial institution might focus on confidentiality and integrity to protect against fraud.

Network Security

Network security extends the protection to the transmission of data across multiple systems, ensuring that the CIA triad is applied to data as it moves between devices, servers, and external systems. Confidentiality in network security involves using tools like VPNs (Virtual Private Networks) or encryption protocols to ensure that data remains private and unreadable by unauthorized users during transmission.

Integrity is maintained through measures such as firewalls and intrusion detection systems, which prevent malicious activities like man-in-the-middle attacks, where data could be altered during transmission. Availability is supported by tools such as load balancers, redundancy mechanisms, and DDoS (Distributed Denial of Service) protection to keep the network accessible and operational even under attack.

In short, while computer security focuses on protecting individual systems, network security ensures that the data flowing between those systems remains secure and accessible. Both work together, using the CIA triad as a framework to minimize risks and protect digital assets effectively.

Computer and network security are both critical in safeguarding data and systems, but they operate in different ways. Let's look at some examples to highlight the distinction between the two, including the difference between HTTP and HTTPS.

1.2.1. Examples of Computer Security

1. **Antivirus Software**: Programs like Norton or McAfee scan for malware and viruses on a computer, protecting its integrity by preventing unauthorized changes to the system.

2. **Encryption**: On a personal computer, files containing sensitive information can be encrypted so only authorized users can access them. This enhances confidentiality.

3. **User Access Controls**: A computer system can restrict access by using usernames and passwords, or multi-factor authentication, ensuring that only authorized users can access critical data or functions.

4. **Operating System Patches**: Keeping operating systems like Windows or macOS up to date is vital for fixing vulnerabilities that could compromise availability or integrity.

1.2.2. Examples of Network Security

1. **Firewalls**: Firewalls, either hardware or software, act as barriers between a trusted internal network and untrusted external networks, such as the internet. They control incoming and outgoing traffic based on security rules, protecting the network's confidentiality.

2. **Virtual Private Networks (VPNs)**: A VPN encrypts data sent over a public network, ensuring that sensitive information, like credit card details or corporate secrets, is kept confidential during transmission.

3. **Intrusion Detection Systems (IDS)**: These monitor network traffic for suspicious activities, helping to maintain the integrity of data by preventing unauthorized access or attacks.

4. **DDoS Protection**: Tools that defend against Distributed Denial of Service (DDoS) attacks, which overwhelm a network and can bring down critical services, help maintain availability.

Distinction Between HTTP vs. HTTPS (Network Security)

The distinction between HTTP and HTTPS is a classic example of network security in action.

- **HTTP (Hypertext Transfer Protocol)** is the basic protocol for transferring data over the web. However, it does not encrypt the data being transferred between the user's browser and the website. This makes it vulnerable to eavesdropping, where an attacker could intercept and read the data, violating confidentiality.

- **HTTPS (Hypertext Transfer Protocol Secure)**, on the other hand, adds a layer of security through encryption using **SSL (Secure Sockets Layer)** or **TLS (Transport Layer Security)** protocols. With HTTPS, the data transferred between the user and the website is encrypted, ensuring that sensitive information like login credentials, credit card numbers, or personal details are protected from unauthorized access during transmission. This ensures confidentiality and integrity by preventing interception and tampering.

Therefore, computer security focuses on protecting individual systems, while network security involves protecting data and systems as they communicate over a network, with HTTPS being a key example of securing data transmission on the web.

The shift from HTTP to HTTPS for all web traffic comes down to the need for improved security in the modern digital landscape. Although encrypting and decrypting data via HTTPS requires more processing power and resources than HTTP, the risks associated with unencrypted web traffic are simply too high to ignore.

With HTTP, data is sent in plain text, making it vulnerable to interception by attackers. This could lead to the exposure of sensitive information like passwords, financial details, or personal data, increasing the likelihood of identity theft or data breaches. In contrast, HTTPS uses encryption to secure this data, ensuring confidentiality and protecting users from these risks.

While encryption adds extra processing demands on both servers and clients, the benefits far outweigh the cost. Given the rise in cyberattacks, it is now seen as necessary to protect even the simplest web interactions, such as browsing or submitting forms. The management of

cryptographic keys does add complexity, but for most organizations, the security and trust provided by HTTPS—especially in e-commerce and data-sensitive industries—justifies these costs. Today, securing web traffic with HTTPS is the standard, ensuring data integrity, privacy, and a secure user experience across the internet.