Cybersecurity Fundamentals

Intern Documentation Project

Prepared: February 2026

This document covers the key cybersecurity concepts I learned during my internship, including the CIA Triad, different types of attackers, common vulnerabilities, and how attacks happen across different stages of data flow. I've tried to document everything in a clear way with real-world examples.

ADHITHYAN MP

GITHUB ID :Kmcadhix1-creator

Contents

1. CIA Triad - The Foundation of Security

The CIA Triad is basically the core framework for thinking about cybersecurity. It stands for Confidentiality, Integrity, and Availability - three principles that need to be balanced to keep systems secure.

Confidentiality

This is about keeping information secret from people who shouldn't see it. Only authorized users should be able to access sensitive data.

How it's protected:

- Encryption (making data unreadable without a key)
- Access controls and authentication (passwords, biometrics, etc.)
- Data classification systems
- VPNs and secure communication channels

Common breaches:

- Database leaks where hackers dump customer data online
- Phishing attacks that steal login credentials
- Employees accidentally sharing confidential files
- Intercepting unencrypted communications

Integrity

Integrity means data stays accurate and hasn't been tampered with. You need to trust that the information you're looking at is legitimate and hasn't been modified by unauthorized people.

How it's protected:

- Hash functions (like checksums to verify files haven't changed)
- Digital signatures
- Audit logs to track who changed what and when
- Input validation to prevent malicious data entry

Common breaches:

- SQL injection attacks that modify database records
- Ransomware corrupting files

- Man-in-the-middle attacks changing messages in transit
- Hackers altering financial transaction amounts

Availability

Systems and data need to be accessible when users need them. If a system is down, it doesn't matter how secure it is - it's not doing its job.

How it's protected:

- Redundant systems and backups
- DDoS protection and load balancing
- Disaster recovery plans
- Regular maintenance and updates

Common breaches:

- DDoS attacks overwhelming servers with traffic
- Ransomware locking users out of their systems
- Power failures without backup generators
- Hardware failures without redundancy

2. Who Are the Attackers? (Types and Motivations)

Not all hackers are the same. Understanding who might attack you and why helps you prioritize your defenses. Here's a breakdown of the main types:

Type	What Drives Them	Skill Level	What They Target
Script Kiddies	Curiosity, wanting to look cool, boredom	Low - use tools made by others	Easy targets, personal websites
Hacktivists	Political beliefs, social causes	Medium - organized groups like Anonymous	Government sites, corporations they oppose
Cybercriminals	Money - selling data, ransomware, fraud	Medium-High - it's their job	Banks, businesses, anyone with money
Insider Threats	Revenge, greed, being blackmailed	High - they already have access	Their own company's data
Nation-State Actors	Espionage, political power, warfare	Very High - government resources	Other governments, critical infrastructure
APTs	Long-term spying, stealing IP	Very High - sophisticated and patient	Large companies, defense contractors

A Few Examples:

Script Kiddies

These are beginners who download hacking tools from the internet and use them without really understanding how they work. Think of them like people using a pre-made cake mix instead of baking from scratch. They're not super dangerous individually, but there are a lot of them.

Cybercriminals

This is organized crime on the internet. They're in it for the money - running ransomware attacks, stealing credit cards, identity theft, etc. They treat hacking like a business with customer service, affiliate programs, and everything.

Nation-State Actors

Government-backed hackers with massive budgets. They're looking for state secrets, trying to sabotage critical infrastructure, or gathering intelligence. These are the most sophisticated attackers with basically unlimited resources.

Insider Threats

Sometimes the threat comes from inside the organization - disgruntled employees, people being bribed or blackmailed, or just careless workers. They're dangerous because they already have legitimate access, so they can bypass a lot of security controls.

3. Attack Surfaces - Where Systems Are Vulnerable

An 'attack surface' is basically all the different ways an attacker could try to get into your system. The bigger your attack surface, the more opportunities hackers have. Here are the main ones:

Network Attack Surface

What it includes:

- Routers, switches, firewalls
- Any ports that are open to the internet
- Wi-Fi networks
- VPN connections

Common attacks:

- Port scanning to find vulnerabilities
- Man-in-the-middle attacks on public Wi-Fi
- DNS spoofing (redirecting you to fake websites)

Application Attack Surface

What it includes:

- Websites and web apps
- Mobile apps
- APIs (how different software talks to each other)
- Third-party code libraries

Common attacks:

- SQL injection (injecting malicious database commands)
- Cross-Site Scripting or XSS (injecting malicious scripts)
- Using known vulnerabilities in outdated libraries
- API abuse to extract data

Human Attack Surface

Honestly, humans are often the weakest link in security. Social engineering attacks target people instead of technology because it's often easier to trick someone than to hack a system.

Common attacks:

- Phishing emails pretending to be from your bank or boss
- Phone calls from fake 'IT support' asking for passwords
- USB drives left in parking lots that install malware when plugged in
- Pretending to be someone important to get access to buildings

Physical Attack Surface

What it includes:

- Servers and data centers
- Computers and laptops
- Mobile devices
- USB ports and other physical connections

Common attacks:

- Stealing laptops or phones
- Installing keyloggers on unattended computers
- Plugging in malicious USB devices
- Dumpster diving for sensitive documents

Cloud/Third-Party Attack Surface

More and more companies use cloud services and third-party tools, which adds new attack vectors. You're not just securing your own systems anymore - you're relying on others' security too.

Common attacks:

- Misconfigured cloud storage (leaving databases publicly accessible)
- Compromised API keys giving access to cloud services
- Supply chain attacks (hacking a vendor to get to their customers)
- Exploiting vulnerabilities in third-party software

4. Real-World Application Security Risks

Different types of applications face different security challenges. Here's what I learned about how security risks vary depending on what kind of system you're protecting:

Application	Main Risks	What Needs Protection	How to Protect It
Online Shopping Sites	Stolen credit cards, fake accounts, inventory manipulation	Payment info, customer data, product prices	PCI compliance, SSL encryption, input validation
Banking Apps	Account takeover, fraud, unauthorized transfers	Account credentials, transactions, balances	2FA, encryption, transaction monitoring
Healthcare Systems	Patient data theft, ransomware, privacy violations	Medical records, personal health info	HIPAA compliance, strict access controls, backups
Social Media	Account hacking, data scraping, fake news	User profiles, private messages, photos	Strong passwords, OAuth, rate limiting
IoT Devices	Device hijacking, privacy invasion, botnets	Sensor data, camera feeds, control systems	Secure firmware, network isolation, updates
Cloud Storage	Data leaks, unauthorized access, account compromise	User files, sharing permissions, metadata	Encryption, access controls, audit logs

Some Real Examples:

E-Commerce Sites

Shopping sites are huge targets because they handle payment information. Attackers use SQL injection to dump customer databases, install credit card skimmers on checkout pages, or create fake accounts for fraud. That's why they need PCI-DSS compliance (a security standard for handling card data) and why you should always check for the lock icon in your browser.

Healthcare Portals

Medical data is super valuable on the black market. Ransomware gangs love targeting hospitals because they can't afford downtime when people's lives are at stake. Plus, medical records contain everything needed for identity theft. That's why healthcare has strict HIPAA regulations.

IoT/Smart Devices

Smart cameras, thermostats, and other IoT devices are notoriously insecure. Hackers can turn them into botnets for DDoS attacks, spy on people through their own cameras, or even manipulate industrial control systems. The scary part is many of these devices never get security updates.

5. How Attacks Happen During Data Flow

Data doesn't just sit in one place - it moves through different stages from when it's created until it's deleted. Attackers can target any of these stages. Here's how it works:

Stage 1: Data Collection (User Input)

Attack vectors:

- SQL injection through web forms
- XSS by injecting scripts into input fields
- Uploading malicious files disguised as images or documents
- Bypassing client-side validation

Example scenario:

You have a login form that doesn't properly validate input. An attacker types something like "admin' OR '1'='1" into the username field. If the code isn't protected, this can bypass the login and give them admin access.

Stage 2: Data Transmission (Over the Network)

Attack vectors:

- Man-in-the-middle attacks intercepting data
- SSL stripping (forcing connections back to unencrypted HTTP)
- Packet sniffing on public Wi-Fi
- Session hijacking by stealing cookies

Example scenario:

Someone connects to a coffee shop's Wi-Fi and logs into their email. An attacker on the same network is running packet-sniffing software. If the connection isn't encrypted, they can see the email password in plain text as it travels across the network.

Stage 3: Data Processing (Server-Side)

Attack vectors:

- Buffer overflow attacks corrupting memory
- Race conditions exploiting timing issues
- Insecure deserialization executing malicious code

- Server-Side Request Forgery (SSRF)

Example scenario:

An application deserializes data from users without validation. An attacker sends a specially crafted serialized object that, when the server processes it, runs arbitrary code and gives the attacker control of the server.

Stage 4: Data Storage (Databases/Files)

Attack vectors:

- Direct database access through SQL injection
- Weak access controls allowing unauthorized reads
- Storing sensitive data without encryption
- Misconfigured cloud storage buckets left public

Example scenario:

A company stores customer data in an Amazon S3 bucket but accidentally leaves it publicly accessible. Automated scanners find it within hours, and thousands of customer records get downloaded before anyone notices.

Stage 5: Data Retrieval (Sending Back to Users)

Attack vectors:

- Broken authentication allowing unauthorized access
- Missing authorization checks (accessing other users' data)
- IDOR - Insecure Direct Object References
- APIs returning more data than necessary

Example scenario:

A web app displays user profiles at URLs like '/profile?id=123'. An attacker just changes the number to '124', '125', etc., and can view everyone's private profiles because the app doesn't check if they're authorized to see that data.

The Complete Picture - Data Flow with Attack Points

Stage	What Happens	How It Can Be Attacked	How to Defend
Collection	User enters data in forms	SQL injection, XSS, file uploads	Input validation, sanitization
Transmission	Data travels over network	MITM, packet sniffing, SSL stripping	HTTPS/TLS, certificate validation
Processing	Server runs application logic	Code injection, buffer overflow	Secure coding, memory protection
Storage	Data saved in databases/files	Unauthorized access, leaks	Encryption, access controls
Retrieval	Data sent back to users	Auth bypass, IDOR, excessive data	Proper authorization, minimal data
Disposal	Data deleted/archived	Incomplete deletion, data remnants	Secure deletion, retention policies

Defense in Depth

The key takeaway is you can't just protect one stage and call it good. You need multiple layers of security - that's called 'defense in depth'. If attackers get past one layer, there should be another one to stop them.

The layers:

- **Prevent:** Firewalls, encryption, input validation, access controls
- **Detect:** Monitoring, logging, intrusion detection systems
- **Respond:** Incident response plans, isolate compromised systems
- **Recover:** Backups, disaster recovery, business continuity plans

6. Key Takeaways and Best Practices

After going through all this material, here are the main things I think are most important to remember:

Main Takeaways:

- **Security is about balance:** CIA Triad shows you need confidentiality, integrity, AND availability - not just one
- **Know your enemy:** Different attackers have different goals, so you need to think about who's most likely to target you
- **Reduce your attack surface:** The fewer entry points you have, the easier it is to defend
- **One size doesn't fit all:** An e-commerce site needs different security than a hospital system
- **Protect data everywhere:** Every stage of the data lifecycle has vulnerabilities
- **Humans are important:** Technical controls don't matter if someone falls for a phishing email

Practical Best Practices I Learned:

If you're building/coding:

- Always validate user input on the server side, not just the client
- Use prepared statements for database queries (prevents SQL injection)
- Never store passwords in plain text - use proper hashing (bcrypt, Argon2)
- Keep all libraries and dependencies updated
- Use HTTPS everywhere, not just on login pages
- Follow OWASP Top 10 guidelines
- Implement proper error handling (don't leak system info in errors)

If you're managing systems:

- Enable multi-factor authentication on everything you can
- Use the principle of least privilege (only give people the access they need)
- Keep backups and test them regularly
- Monitor logs for suspicious activity

- Have an incident response plan and practice it
- Regular security audits and penetration testing
- Train employees on security awareness

General advice:

- Use a password manager with unique passwords for everything
- Be skeptical of emails asking for sensitive information
- Keep your devices and software updated
- Use a VPN on public Wi-Fi
- Think before you click - most attacks rely on human error

Final Thoughts

Security is constantly evolving - new vulnerabilities are discovered every day, and attackers are always coming up with new techniques. The fundamentals in this document are a good starting point, but staying current is really important. Some good resources to keep learning:

- OWASP (owasp.org) - especially the Top 10 list
- NIST Cybersecurity Framework
- CVE database for tracking vulnerabilities
- Security subreddits and communities
- Capture The Flag (CTF) competitions for hands-on practice

The most important thing I learned is that security isn't just a technical problem - it's about people, processes, and technology all working together. You can have the best firewalls and encryption in the world, but if someone's password is '123456', none of that matters.

This concludes my documentation on cybersecurity fundamentals. I hope this is useful for understanding the core concepts!