Lecture 1: Core Concepts and Terminology in Information Security

Theme: Information Security Fundamentals

Technical University of Moldova

Lecturer: Maxim Masiutin, Associate Professor

Introduction

Hello, everyone. Welcome to our first lecture in the Information Security Technologies course. Over the next three months, we will explore the fascinating and critically important world of information security. Today, we begin with the foundational concepts that everything else builds upon.

Before we dive into specific technologies, attacks, or defenses, we need to establish a common vocabulary. Information security has its own language, and understanding these terms precisely is essential. A single misunderstood concept can lead to a misconfigured system, and a misconfigured system can lead to a breach affecting millions of people.

Let me start with a question: How many of you have heard about a data breach in the news this year? I suspect everyone raised their hand. Data breaches are now so common that we almost expect them. Cybersecurity Ventures, a cybersecurity research publisher, reported that global cybercrime costs reached **10.5 trillion dollars annually by 2025**, and projections indicate this will continue to rise to **13 trillion by 2028**. That number is larger than the GDP of most countries. This is why we are here today.

Part 1: Information Security vs. Cybersecurity

Let us begin by clarifying two terms that are often used interchangeably but have distinct meanings: information security and cybersecurity.

Information security, sometimes called InfoSec, is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. Notice that this definition does not specify how the information is stored. Information security covers paper documents in a filing cabinet just as much as it

covers data in a cloud server. If you have ever seen a notice saying "Authorized Personnel Only" on a door, that is information security in action.

Cybersecurity is a subset of information security that specifically deals with protecting electronic systems, networks, and data from digital attacks. When we talk about firewalls, intrusion detection systems, or malware, we are in the realm of cybersecurity.

Here is a practical way to think about the difference: If someone breaks into an office and steals printed customer records from a desk, that is an information security incident but not a cybersecurity incident. If someone hacks into a database remotely and downloads those same records, that is both an information security incident and a cybersecurity incident.

Throughout this course, we will focus primarily on cybersecurity, but always remember that it exists within the broader context of information security. The most sophisticated firewall in the world cannot protect you if an employee leaves confidential documents on a train.

Part 2: The CIA Triad

Now we come to the most fundamental model in information security: the CIA Triad. No, this has nothing to do with the Central Intelligence Agency. In our context, CIA stands for **Confidentiality**, **Integrity**, and **Availability**. These three properties form the foundation of every security decision we make.

Let me draw this on the board as a triangle. Each corner represents one of these properties, and a secure system must maintain all three in balance.

Confidentiality

Confidentiality means ensuring that information is accessible only to those who are authorized to access it. When we protect confidentiality, we are preventing unauthorized disclosure of information.

Think about your bank account. Only you and authorized bank employees should be able to see your account balance. If a random stranger could view your financial information, that would be a confidentiality breach.

Confidentiality is threatened by various attacks:

- **Eavesdropping**: Someone intercepts your network traffic to read your emails
- **Shoulder surfing**: Someone watches you type your password
- **Social engineering**: Someone tricks you into revealing confidential information
- **Data breaches**: Attackers steal databases containing personal information

We protect confidentiality through:

- **Encryption**: Converting data into an unreadable format without the proper key
- **Access controls**: Ensuring only authorized users can access specific resources
- **Authentication**: Verifying the identity of users before granting access
- **Physical security**: Locks, guards, and secure facilities

Let me give you a real-world example. In 2017, the Equifax breach (Equifax is a consumer credit reporting agency) exposed the personal information of 147 million Americans. More recently, the **23andMe breach (2023)** (23andMe is a consumer genetics company) exposed sensitive genetic data of nearly 7 million users via credential stuffing. The lesson here is that confidentiality requires constant vigilance over both systems and user access.

Integrity

Integrity means ensuring that information remains accurate, complete, and unaltered except by authorized parties. When we protect integrity, we are preventing unauthorized modification of data.

Consider a medical records system. If a patient is allergic to penicillin, that information must remain accurate in their medical record. If an attacker or a software bug changed that record, the consequences could be fatal. That is why integrity matters.

Integrity is threatened by:

- **Man-in-the-middle attacks**: An attacker intercepts and modifies data in transit
- **Malware**: Viruses or worms that corrupt or modify files
- **Insider threats**: Employees who intentionally alter records
- **Hardware failures**: Disk errors that cause data corruption
- **Software bugs**: Programming errors that unintentionally modify data

We protect integrity through:

- **Hashing**: Creating a digital fingerprint of data to detect changes
- **Digital signatures**: Cryptographically verifying the source and integrity of data
- **Version control**: Tracking all changes to detect unauthorized modifications
- **Access controls**: Limiting who can modify data
- **Checksums**: Mathematical verification that data has not been altered

Here is an example to illustrate the importance of integrity. In 2010, the Stuxnet worm targeted Iranian nuclear facilities. It did not steal data; instead, it modified the instructions sent to centrifuges, causing them to spin at incorrect speeds while displaying normal readings to operators. This was an integrity attack with physical consequences. The centrifuges destroyed themselves, setting back Iran's nuclear program by years.

Availability

Availability means ensuring that information and systems are accessible to authorized users when needed. When we protect availability, we are preventing disruption of service.

Imagine you need to withdraw money from an ATM, but the bank's systems are down. Or consider a hospital where doctors cannot access patient records during an emergency. Availability is about ensuring systems work when you need them.

Availability is threatened by:

- **Denial of Service (DoS) attacks**: Overwhelming systems with traffic to make them unavailable
- **Distributed Denial of Service (DDoS) attacks**: DoS attacks from many sources simultaneously
- **Ransomware**: Malware that encrypts data, making it unavailable until ransom is paid
- **Hardware failures**: Server crashes, disk failures, network outages
- **Natural disasters**: Floods, fires, earthquakes that damage infrastructure
- **Power outages**: Electricity failures that shut down systems

We protect availability through:

- **Redundancy**: Having backup systems ready to take over if primary systems fail
- **Backups**: Regular copies of data stored separately. **Recovery Time Objective (RTO)** is critical here; backups are useless if restoration takes weeks (as seen in recent ransomware attacks like MGM Resorts, a major hotel and casino operator).
- **Disaster recovery planning**: Procedures for restoring operations after a major incident
- **Load balancing**: Distributing traffic across multiple servers
- **DDoS mitigation**: Systems designed to absorb or deflect massive traffic attacks

Let me share an availability example. In 2016, the Mirai botnet took down major internet services via DDoS. More dramatically, the **CrowdStrike Outage (2024)** (CrowdStrike is an endpoint security vendor) showed how a single faulty software update could crash millions of Windows systems globally, grounding flights and halting hospitals. This demonstrated that availability threats can come from trusted vendors, not just attackers.

Balancing the Triad

Here is something important to understand: these three properties often conflict with each other. Improving one can sometimes harm another.

For example, to maximize confidentiality, you might encrypt all data and require multiple forms of authentication. But this could harm availability because authorized users might find it difficult to access the data they need quickly.

To maximize availability, you might remove all access controls and store data on many servers. But this would destroy confidentiality because anyone could access anything.

Security professionals must constantly balance these competing demands based on the specific context and risk tolerance of their organization. There is no universal right answer.

Part 3: Beyond the CIA Triad - Additional Security Properties

While the CIA Triad has served us well for decades, modern security requirements have expanded. Let us discuss three additional properties that are now considered essential.

Authentication

Authentication is the process of verifying that someone or something is who or what they claim to be. Before you can enforce any access controls, you must first know who is making the request.

Authentication typically relies on three primary factors:

- **Something you know**: A password or PIN
- **Something you have**: A smart card, phone, or security token
- **Something you are**: Biometrics like fingerprints or facial recognition

Modern systems also use **contextual attributes** (sometimes called "Something you do" or "Somewhere you are") to enhance security without requiring explicit user action:

- **Location**: GPS coordinates or IP address geolocation
- **Behavior**: Typing rhythm, mouse movement patterns, or time of day

Multi-factor authentication (MFA) combines two or more of the primary factors. When you log into your bank and receive a text message with a code, you are using two factors: something you know (your password) and something you have (your phone). Contextual attributes are often used for **Risk-Based Authentication (RBA)** to decide if additional challenges are needed.

Non-repudiation

Non-repudiation ensures that a Subject cannot deny a previous action or inaction. It provides **proof of origin** (the sender cannot deny sending) and **proof of delivery** (the receiver cannot deny receiving), going beyond simple legal contracts.

In the digital world, non-repudiation is achieved through digital signatures and comprehensive logging. When an executive approves a financial transaction with their digital signature, they cannot later deny having approved it because the cryptographic evidence proves their involvement.

Non-repudiation is crucial for:

- Legal evidence in court
- Audit trails for compliance
- Accountability in financial transactions
- Preventing fraud

Accountability

Accountability means being able to trace actions to the entity that performed them. Every action in a system should be attributable to a specific user or process.

Accountability requires:

- Strong authentication to identify users
- Comprehensive logging to record actions
- Secure log storage to prevent tampering
- Regular log review to detect anomalies

Without accountability, it is impossible to investigate incidents, enforce policies, or hold individuals responsible for their actions.

Part 4: Assets, Threats, Vulnerabilities, and Risks

Now let us discuss four interconnected concepts that are fundamental to security analysis: assets, threats, vulnerabilities, and risks.

Assets

An **asset** is anything of value that an organization wants to protect. Assets can be tangible or intangible.

Tangible assets include:

- Servers and computers

- Network equipment
- Buildings and facilities
- Physical documents

Intangible assets include:

- Data and databases
- Software and applications
- Intellectual property
- Brand reputation
- Customer trust

When performing security analysis, we must first identify what we are trying to protect. You cannot secure what you do not know you have.

Threats

A **threat** is any potential cause of an unwanted incident that could harm an asset or the organization. Threats can be intentional or accidental, internal or external.

Intentional external threats:

- Hackers seeking financial gain
- Nation-state actors conducting espionage
- Hacktivists making political statements
- Competitors stealing trade secrets

Intentional internal threats:

- Disgruntled employees sabotaging systems
- Insiders stealing data for sale
- Contractors exceeding their authorized access

Accidental threats:

- Employees clicking phishing links
- Administrators misconfiguring systems
- Developers introducing bugs

Environmental threats:

- Natural disasters
- Power failures
- Hardware malfunctions

Vulnerabilities

A **vulnerability** is a weakness that can be exploited by a threat to gain unauthorized access or cause harm. Vulnerabilities exist in systems, processes, and people.

Technical vulnerabilities:

- Unpatched software with known security flaws
- Misconfigured firewalls allowing unauthorized traffic
- Weak encryption algorithms that can be broken
- Default passwords that were never changed

Process vulnerabilities:

- Lack of security policies
- Insufficient employee training
- Inadequate incident response procedures
- Missing access reviews

Human vulnerabilities:

- Susceptibility to social engineering
- Tendency to use weak passwords
- Failure to report suspicious activities
- Negligence in following procedures

Risks

Risk is the potential for loss or damage when a threat exploits a vulnerability. Risk is typically calculated as:

Risk = Threat × Vulnerability × Impact

Or sometimes simplified as:

Risk = Likelihood × Impact

Where likelihood is the probability that a threat will exploit a vulnerability, and impact is the consequence if it does.

Let me illustrate with an example. Suppose your organization uses a web server running old software with a known vulnerability. The threat is hackers who could exploit this vulnerability. The vulnerability is the unpatched software. The risk depends on how likely attackers are to find and exploit this vulnerability and what damage they could cause.

If the server is on the public internet containing customer credit card data, the risk is very high. If the server is on an isolated network containing only public marketing materials, the risk is much lower.

Understanding risk allows us to prioritize our security efforts. We cannot protect everything equally, so we must focus on the highest risks first.

Part 5: Security Incidents vs. Security Breaches

Students often confuse these terms, so let us clarify them.

A **security incident** is any event that potentially compromises the confidentiality, integrity, or availability of an information asset. Incidents include:

- Attempted attacks, even if unsuccessful
- Policy violations
- System malfunctions
- Suspicious activities

A **security breach** is a security incident that results in confirmed unauthorized access to data, applications, services, networks, or devices. All breaches are incidents, but not all incidents are breaches.

Here is an example: If someone tries to log into your account with an incorrect password, that is an incident. If they succeed in logging in without authorization, that is a breach.

Organizations must detect, respond to, and learn from both incidents and breaches. Incident response procedures, which we will cover later in this course, define how to handle these situations.

Defense in depth is a security strategy that uses multiple layers of protection. If one layer fails, others remain to provide security. This concept comes from military strategy, where castles had moats, walls, towers, and armed guards, each layer making penetration more difficult.

In information security, defense in depth includes:

Physical layer: Guards, locks, fences, surveillance cameras

Perimeter layer: Firewalls, intrusion detection systems, demilitarized zones

Network layer: Network segmentation, VPNs (Virtual Private Networks), access control lists

Host layer: Antivirus software, host-based firewalls, patch management

Application layer: Input validation, secure coding practices, web application firewalls

Data layer: Encryption, access controls, data loss prevention

Human layer: Security awareness training, policies, background checks

Each layer addresses different threats and provides additional protection. An attacker must penetrate multiple layers to reach valuable assets, making successful attacks

much more difficult.

Zero Trust Architecture: While traditional defense in depth relies on a strong perimeter, **Zero Trust** assumes that the network is already compromised. It operates on the principle of "never trust, always verify." Every access request is fully authenticated, authorized, and encrypted before granting access, regardless of where it originates.

Part 7: Security by Design and Security by Default

Two principles guide how we should build secure systems from the beginning.

Security by design means considering security throughout the entire development lifecycle, not as an afterthought. When architects design a building, they include fire exits and sprinkler systems from the start. They do not add them after construction is complete. The same principle applies to information systems.

Security by design includes:

- **Threat modeling**: A structured approach (using frameworks like **STRIDE** (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege)) to identify threats during requirements gathering
- **Secure architecture decisions**: Choosing secure patterns and technologies
- **Security testing**: Regular code analysis and penetration testing throughout development
- Security reviews before deployment

Security by default means that systems should be secure in their default configuration. Users should not need to enable security features; they should need to explicitly disable them if desired.

Examples of security by default:

- Passwords required immediately after installation
- Network services disabled unless explicitly enabled
- Encryption enabled by default
- Minimal privileges granted by default

The opposite approach, where systems ship insecure and users must configure security, leads to countless vulnerabilities because many users never change defaults.

Part 8: Practical Applications

Let me conclude with some practical applications of what we have learned today.

Scenario 1: Designing a new application

When your organization develops a new customer portal, you should:

1. Identify assets: Customer data, login credentials, transaction records
2. Identify threats: Hackers, malicious insiders, accidental exposure
3. Identify vulnerabilities: Potential SQL injection, weak authentication, insufficient logging
4. Calculate risks: High risk for customer data theft
5. Apply controls: Encrypt data (confidentiality), validate inputs (integrity), deploy redundant servers (availability)
6. Implement defense in depth: Firewall, WAF (Web Application Firewall), secure coding, encryption, monitoring

Scenario 2: Evaluating a vendor

When selecting a cloud provider, ask:

- How do they protect confidentiality? (Encryption, access controls)
- How do they ensure integrity? (Checksums, version control)
- What is their availability SLA? (Uptime guarantees, redundancy)
- How do they handle incidents? (Response procedures, notification)
- What certifications do they have? (ISO 27001, SOC 2 (Service Organization Control Type 2))

Scenario 3: Responding to a phishing attempt

If an employee receives a suspicious email:

1. Do not click links or download attachments
2. Report to security team (this is an incident)
3. Security team analyzes the threat
4. If credentials were compromised, it becomes a breach
5. Implement additional controls (training, email filtering)
6. Document lessons learned

Part 9: Modern Risk Management Tools (EASM & GRC)

1. External Attack Surface Management (EASM)

EASM tools are designed to discover "unknown" risks. They scan the internet from the outside (like an attacker would) to find every digital asset an organization owns—including forgotten servers, cloud buckets, or shadow IT.

- **Primary Goal:** Discovery and vulnerability mapping from an external perspective.
- **Key Examples:**
- **IONIX**, an attack surface management vendor: Focuses on mapping the "real" attack surface, including complex digital supply chains and cloud dependencies.
- **UpGuard**, a cyber risk management vendor, / **SecurityScorecard**, a security ratings provider: Provides a "security rating" (like a credit score) for your organization and your third-party vendors.
- **Target Audience:** Security Engineers, Threat Intelligence Teams.
- **Analogy: The Building Inspector.** They walk around the exterior of the building looking for cracks, open windows, and broken locks that you didn't know were there.

2. Governance, Risk, and Compliance (GRC)

GRC tools are the internal "ledgers" of security. They track policies, audits, and known risks. They help ensure the organization is following laws (like the GDPR (General Data Protection Regulation)) or standards (like ISO 27001).

- **Primary Goal:** Tracking compliance, documenting internal risks, and managing audits.
- **Key Examples:**
- **RSA Archer**, an enterprise risk management platform: A traditional, enterprise-grade solution for managing corporate risk and compliance.
- **OneTrust**, a privacy and data governance vendor: Heavily focused on privacy risk and data governance.
- **Target Audience:** CISOs, Risk Officers, Compliance Managers.
- **Analogy: The Filing Cabinet.** It stores the blueprints, the inspection reports, and the certificates proving the building is legally up to code.

Pros and Cons

Category	Pros	Cons
EASM	Finds immediate technical threats; requires almost no manual setup to start scanning.	Can generate "noise" (false positives); doesn't tell you how to fix the policy behind the risk.
GRC	Centralizes all risk data; essential for passing audits and legal requirements.	Heavy administrative burden; relies on manual data entry ("garbage in, garbage out").

Conclusion

1. **Information security vs. cybersecurity**: InfoSec protects all information; cybersecurity focuses on electronic systems
2. **The CIA Triad**: Confidentiality, Integrity, and Availability are the three pillars of security
3. **Additional properties**: Authentication, non-repudiation, and accountability extend the basic model
4. **Assets, threats, vulnerabilities, and risks**: Understanding these relationships enables effective security planning
5. **Incidents vs. breaches**: Incidents are potential compromises; breaches are confirmed unauthorized access
6. **Defense in depth**: Multiple layers of protection provide resilience
7. **Security by design and default**: Build security in from the start

In our next lecture, we will explore the threat landscape in detail, examining who attacks us, why they do it, and what methods they use. We will also discuss frameworks like MITRE ATT&CK that help us understand and categorize threats.

Are there any questions before we conclude?

Discussion Questions

1. In what scenarios might the CIA triad properties conflict with each other, and how should organizations resolve such conflicts?
2. What are the biggest challenges organizations face when implementing defense in depth, and how can they be addressed?

Thank you for your attention. I will see you in our next session.

Review Questions

1. Explain the difference between information security and cybersecurity. How do their scopes overlap and differ?
2. How do authentication, non-repudiation, and accountability extend the basic CIA model?
3. Describe the relationship between assets, threats, vulnerabilities, and risks. How does understanding this chain help in security planning?
4. What is the difference between a security incident and a security breach? Why does this distinction matter?
5. Explain the defense-in-depth strategy and provide examples of controls at three different layers.
6. What does "security by design" mean, and how does it differ from adding security after deployment?
7. Give an example of a scenario where two elements of the CIA triad conflict with each other.

Key Terms

- **Accountability**: The property ensuring that actions of an entity can be traced uniquely to that entity
- **Asset**: Anything of value to an organization, including data, hardware, software, and personnel
- **Authentication**: The process of verifying a claimed identity
- **Availability**: Ensuring that authorized users have timely and reliable access to information and resources
- **Breach**: A confirmed incident in which data is accessed or disclosed without authorization
- **CIA Triad**: The three fundamental security objectives: Confidentiality, Integrity, and Availability
- **Confidentiality**: Preventing unauthorized disclosure of information
- **Cybersecurity**: Protection of electronic systems, networks, and data from attacks
- **Defense in Depth**: A security strategy using multiple layers of controls
- **Incident**: A potential or attempted compromise of security policies or practices
- **Information Security**: Protection of information in all forms from unauthorized access, use, disclosure, or destruction

- **Integrity**: Ensuring that data has not been modified in an unauthorized manner
- **Non-repudiation**: The assurance that someone cannot deny having performed an action
- **Risk**: The potential for loss resulting from a threat exploiting a vulnerability
- **Security by Default**: Systems shipped with the most secure configuration as the default
- **Security by Design**: Building security into systems from the earliest design stages
- **Threat**: A potential cause of an unwanted incident that may result in harm
- **Vulnerability**: A weakness in a system that can be exploited by a threat

References and Further Reading

For those interested in deeper exploration:

- ISO/IEC 27000:2022 for formal definitions of security terms
- NIST Glossary of Key Information Security Terms