Information Security Fundamentals

Understanding How We Protect Digital Information

Prepared by Security Team

February 17, 2025

Introduction to CIA: The Foundation of Security

What is Information Security?

Just like we protect valuable things in the physical world with locks and safes, we need ways to protect our digital information.

- Information security protects everything from your personal photos to your banking information from people who shouldn't have access to it.
- The **CIA triad** is like a three-part checklist that helps us make sure our information is properly protected.
- Every time you use a password, encryption, or verify a website's security, you're using CIA principles.
- We'll explore how these principles work together to keep our digital world safe.

Confidentiality: Keeping Secrets Safe

- **Confidentiality** is about keeping secrets secret - making sure only the right people can see sensitive information.
- Think about how we protect private information:
  - **Passwords**: Like having a key to your digital house
  - **Encryption**: Like putting a message in a special code
  - **Access controls**: Like having an ID card to enter restricted areas
  - **Private mode browsing**: Like leaving no footprints behind
- When you send a private message, confidentiality ensures only the intended recipient can read it.
- Banks use confidentiality to protect your account information from unauthorized viewers.

Integrity: Keeping Information Trustworthy

Why Integrity Matters

Imagine if someone could change your grades or bank balance without permission - integrity prevents this!

- **Integrity** means making sure information hasn't been tampered with or accidentally changed.
- When you download a file, your computer checks if it downloaded correctly and completely.
- Digital signatures are like a wax seal on a letter - they show if something has been changed.
- Social media platforms use integrity checks to ensure your posts aren't altered by others.

Availability: Making Sure Information is There When You Need It

Availability Impact

Even brief system outages can have severe consequences - from lost sales to life-threatening situations

Availability ensures systems work when legitimate users need them:

- Systems must respond quickly and reliably
- Backup systems provide redundancy when primary systems fail
- Load balancing prevents system overload
- Disaster recovery plans ensure business continuity

Putting CIA Together: Real World Examples

Here's how CIA principles protect common services:

- **Mobile Banking**:
  - Confidentiality: Encryption of transactions
  - Integrity: Transaction verification codes
  - Availability: Multiple server locations
- **Email Services**:
  - Confidentiality: Message encryption
  - Integrity: Digital signatures
  - Availability: Redundant storage

Non-repudiation: Taking Responsibility

Non-repudiation prevents users from denying their actions on a system.

- Key components of non-repudiation:
  - Digital signatures on documents
  - Secure timestamp services
  - Audit log maintenance
  - Access tracking systems
- Common applications:
  - Email communication records
  - Financial transaction logs
  - Document modification history
  - System access records

Introduction to AAA: Authentication, Authorization, and Accounting

The Three Steps of Access Control

Think of AAA like a secure building: checking ID (Authentication), determining where you can go (Authorization), and keeping records (Accounting)

AAA provides a framework for controlling system access:

- Authentication verifies identity claims
- Authorization determines access rights
- Accounting tracks user actions
- Together they create:
  - Complete access control
  - Audit capabilities
  - Security compliance
  - Incident investigation tools

Authentication: Proving Who You Are

Authentication Factors

Something you know, something you have, something you are

- **Authentication** is how you prove you are who you say you are in the digital world.
- Passwords and PINs are like digital keys that only you should know.
- Two-factor authentication is like needing both a key and an ID to enter.
- Using multiple factors makes it much harder for someone to pretend to be you.

Authenticating People: Methods We Use

- Common ways people prove their identity:
  - **Knowledge-based**:
    - Passwords you remember
    - Security questions
    - PIN numbers
  - **Possession-based**:
    - Phone for SMS codes
    - Security keys
    - ID cards
  - **Biometric**:
    - Fingerprint scans
    - Face recognition
    - Voice patterns

Authenticating Systems: Machine Identity

- **Machine authentication** ensures computers and devices can trust each other.
- When you visit a website, your browser checks its digital certificate - like checking a store's business license.
- Secure websites use HTTPS to prove they are legitimate, showing a padlock icon in your browser.
- Digital certificates are like ID cards for websites and servers, issued by trusted authorities.

Authentication in Action: Real-World Examples

Common Authentication Scenarios

Let's look at how authentication protects you every day

- When you unlock your phone with a fingerprint, you're using biometric authentication.
- School computers might require both your student ID and password to log in.
- Online banking often uses multiple steps: password, security questions, and text message codes.
- Gaming consoles authenticate both you and your games to prevent unauthorized access.

Authorization: Determining What You Can Do

Authentication vs. Authorization

Authentication proves who you are, authorization determines what you're allowed to do

- **Authorization** is like having different access cards for different areas of a building.
- Just because you can log into a system doesn't mean you can access everything in it.
- Your student ID might let you into the library but not the teacher's lounge.
- Different permission levels help protect sensitive information and resources.

Authorization Models: Different Ways to Control Access

- Common authorization models include:
  - **Role-Based Access Control (RBAC)**:
    - Like how students, teachers, and administrators have different permissions
    - Access based on your role, not who you are
    - Easier to manage for large organizations
  - **Discretionary Access Control (DAC)**:
    - Like when you choose who can see your social media posts
    - Owner decides who gets access
    - Common in personal computing

Access Control Lists (ACLs)

- **Access Control Lists** are like guest lists that specify exactly who can do what.
- They work similarly to file permissions on your computer, controlling who can read, write, or modify.
- In social media, your friends list acts like an ACL for your private posts.
- ACLs can be very specific - like allowing someone to view a document but not edit it.

Principle of Least Privilege

A Fundamental Security Rule

Give users only the access they need to do their job - nothing more!

- **Least privilege** is like giving a housesitter only the front door key, not keys to everything.
- This principle helps prevent accidental changes and limits what attackers can do if they break in.
- Apps on your phone ask permission only for what they need - they shouldn't get more access than necessary.
- Even administrators should use regular accounts for daily tasks, using admin access only when needed.

Accounting: Keeping Track of What Happens

- **Accounting** in security means creating detailed records of who did what and when.
- System logs track important events like failed login attempts, file changes, and permission changes.
- This information helps investigate security incidents and prove what happened - like a security camera's footage.
- Logs must be protected from tampering and backed up regularly to maintain their integrity.
- Good accounting practices help organizations comply with legal requirements and industry standards.

Security Logs: What We Track

- Important events we need to monitor:
  - **Authentication Events**:
    - Successful and failed login attempts
    - Password changes
    - Account lockouts
  - **System Events**:
    - File access and modifications
    - Software installations
    - System reboots
  - **Security Events**:
    - Firewall alerts
    - Antivirus detections
    - Permission changes

Gap Analysis: Finding Security Weaknesses

What is a Security Gap?

A security gap is the difference between where your security is and where it needs to be

- **Gap analysis** helps identify weaknesses in security systems, like finding holes in a fence.
- Organizations compare their current security measures against industry best practices and requirements.
- Regular assessments help catch problems before they can be exploited by attackers.
- Gap analysis leads to concrete recommendations for improving security.
- Think of it like a security health check-up that shows what needs improvement.

Conducting a Basic Gap Analysis

- Steps in performing a basic gap analysis:
  - **Assessment**:
    - Document current security measures
    - Review existing policies
    - Test security controls
  - **Comparison**:
    - Check against security standards
    - Review industry best practices
    - Consider legal requirements
  - **Planning**:
    - Prioritize identified gaps
    - Develop improvement plans
    - Set realistic timelines

Zero Trust: A Modern Security Approach

Trust Nothing, Verify Everything

Traditional security trusted everything inside the network - Zero Trust trusts nothing by default

- **Zero Trust** is like a security guard who checks everyone's ID, even if they work there.
- Traditional security was like a castle with strong walls but trust once inside.
- Modern networks need security everywhere because there is no clear "inside" anymore.
- Every access request is treated as potentially dangerous and must be verified.
- Working from home and cloud computing make Zero Trust especially important.

Traditional vs. Zero Trust Security

Traditional Security	**Zero Trust**
Trust inside network	Trust nothing by default
Verify once at entry	Verify every request
Like castle walls	Like security checkpoints everywhere
Focus on perimeter	Security throughout system
Location-based trust	Identity-based trust
Static access rules	Dynamic access decisions

Components of Zero Trust: Control Plane

Understanding the Control Plane

The **Control Plane** is the brain of Zero Trust, making smart decisions about who gets access.

- Key elements that manage Zero Trust security:
  - **Adaptive Identity**:
    - Continuously evaluates user behavior
    - Adjusts access based on risk
    - Considers context like location and device
  - **Policy Engine**:
    - Makes real-time access decisions
    - Applies security rules consistently
    - Updates policies automatically
- The control plane acts like a smart security system that's always watching and adjusting.

Zero Trust in Action

Even with the right password, you might be denied access if:

- Your location suddenly changes (like logging in from another country).
- You're trying to access resources at unusual times.
- Your behavior patterns don't match your normal activity.
- The device you're using isn't recognized or secure.
- The system detects potential security risks in real-time.
- This dynamic approach helps catch potential security breaches early.

Policy-Driven Access Control

Automated Security Decisions

Policies are like a rulebook that automatically determines who gets access to what

- **Policy-driven access** means using clear rules to make security decisions automatically.
- These policies consider multiple factors like user role, device security, and risk level.
- Rules can change automatically based on security threats or unusual activity.
- Think of it like a smart doorman who knows all the building's rules and applies them consistently.
- Policies must be detailed enough to be secure but flexible enough to allow legitimate work.

The Policy Administrator

- Components of policy administration:
  - **Policy Creation**:
    - Writing clear security rules
    - Defining access conditions
    - Setting up authentication requirements
  - **Policy Management**:
    - Updating rules as needed
    - Monitoring policy effectiveness
    - Responding to security incidents
  - **Policy Enforcement**:
    - Ensuring rules are followed
    - Logging policy violations
    - Taking action on violations

Understanding the Data Plane

The Data Plane

The **Data Plane** is where the real security checks happen, like a security checkpoint at an airport. It implements the rules set by the Control Plane.

- Every time you try to access something, the Data Plane:
  - Checks your identity and permissions
  - Verifies your device's security status
  - Ensures the connection is secure
  - Monitors for suspicious behavior
- This happens continuously, not just when you first connect.
- Even a brief security issue can cause access to be revoked immediately.
- The Data Plane works with the Control Plane to keep systems secure.

Threat Scope Reduction

Making the Target Smaller

The less attackers can see or access, the harder it is for them to cause harm

- **Threat scope reduction** is like keeping valuables in separate safes rather than one big vault.
- Systems are divided into smaller, isolated segments to limit potential damage.
- Users can only see and access what they absolutely need for their work.
- Even if attackers break in somewhere, they can't easily reach other parts of the system.
- Regular access reviews help remove unnecessary permissions that could be exploited.

Understanding Implicit Trust Zones

What is an Implicit Trust Zone?

Areas where traditional security assumes everything is safe - a dangerous assumption!

- An **implicit trust zone** is like assuming everyone in a school building is supposed to be there.
- Traditional networks trusted everything inside the company network.
- This old approach is risky because:
  - One breach gives access to everything
  - Insider threats go unnoticed
  - Compromised devices spread problems
- Zero Trust eliminates these assumed-safe zones entirely.

Problems with Implicit Trust

- Real-world examples of implicit trust problems:
  - **Building Security**:
    - Tailgating through doors
    - Borrowed access cards
    - Unauthorized visitors
  - **Network Security**:
    - Infected company laptops
    - Compromised user accounts
    - Malicious insiders
  - **Application Security**:
    - Stolen login credentials
    - Session hijacking
    - Excessive permissions

Subject and System Interactions

- In Zero Trust, every interaction between users (**subjects**) and resources (**systems**) must be verified.
- Examples of subject/system interactions:
- Opening a document requires checking:
  - User identity and permissions
  - Device security status
  - File sensitivity level
  - Location and time of access
- These checks happen automatically and continuously.
- Even small changes in any factor can trigger a security response.
- The system maintains detailed logs of all interactions.

Policy Enforcement Point (PEP)

The Security Checkpoint

Like a guard checking IDs, the PEP verifies every request before allowing access

- The **Policy Enforcement Point** acts as the security guard of the Zero Trust system.
- Every request must pass through the PEP, with no exceptions.
- The PEP communicates with the Policy Engine to make access decisions.
- It can immediately block access if security requirements aren't met.
- Modern PEPs are smart enough to consider context and adapt to changing conditions.
- They maintain detailed records of all access attempts, approved or denied.

Introduction to Physical Security

Critical Reminder

Physical security failures can completely bypass even the strongest digital protections

- **Physical security** protects tangible assets and critical infrastructure
- Protection requires multiple elements:
  - Deterrence measures
  - Access control systems
  - Detection mechanisms
  - Response procedures
- Every measure needs:
  - Regular testing
  - Backup systems
  - Maintenance plans

Layers of Physical Security

- Security works in distinct layers:
  - **Perimeter Security**:
    - Fences and walls
    - Bollards and barriers
    - Security lighting
    - Surveillance systems
  - **Building Security**:
    - Access control systems
    - Security personnel
    - Hardened entrances
    - Emergency systems

Perimeter Protection: Bollards and Barriers

- **Bollards** protect against vehicle-based threats
- Types of bollards include:
  - Fixed permanent posts
  - Retractable systems
  - Removable barriers
  - Decorative options
- Implementation considerations:
  - Proper spacing requirements
  - Impact resistance ratings
  - Emergency access needs
  - Aesthetic integration

Access Control Vestibules

Security Vestibule Purpose

Creates a secure buffer zone where credentials can be verified before granting entry

- **Access control vestibules** prevent unauthorized entry
- Required components:
  - Two interlocked doors
  - Authentication systems
  - Surveillance cameras
  - Emergency overrides
- Security features:
  - Anti-tailgating measures
  - Contraband detection
  - Physical isolation

Fencing and Physical Barriers

- Types of security fencing:
  - **Chain-link**:
    - Basic perimeter marking
    - Can add barbed wire
    - Cost-effective solution
  - **Anti-climb**:
    - Mesh design prevents footholds
    - Higher security rating
    - Often used for sensitive areas
  - **Crash-rated**:
    - Stops vehicle attacks
    - Reinforced construction
    - Used at critical facilities

Video Surveillance Systems

Modern CCTV: More Than Just Cameras

Today's systems use AI to detect suspicious behavior automatically

- **Video surveillance** combines cameras, storage, and intelligent monitoring.
- Modern systems can detect unusual activities like:
- People in restricted areas or at unusual times.
- Objects left behind or removed.
- Suspicious behavior patterns.
- Facial recognition can track known threats.
- Systems maintain searchable archives for investigations.
- Integration with access control provides better security.

Security Guards and Human Elements

- **Security personnel** provide crucial functions that technology cannot:
- Make complex decisions in unusual situations.
- Respond to emergencies with appropriate judgment.
- Interact with visitors and employees professionally.
- Notice subtle behavioral cues that machines might miss.
- Key responsibilities include:
  - Access control enforcement
  - Patrol and monitoring
  - Emergency response
  - Visitor management
  - Incident reporting

Access Badges and Credentials

Badge Type	Security Features
Basic ID	Photo, name, expiration date
Magnetic Stripe	Encoded data, swipe access
Proximity	Contactless, encrypted, harder to clone
Smart Card	Multiple credentials, high encryption
Multi-factor	Combined with PIN or biometrics

- Badges should be visibly worn at all times.
- Lost badges must be reported immediately.
- Regular audits ensure only active badges work.

Security Lighting Fundamentals

Essential Consideration

Security lighting must be on emergency power - darkness creates vulnerability

Security lighting serves multiple critical purposes:

- Deters criminal activity by increasing visibility
- Enables effective camera surveillance at night
- Supports security personnel in monitoring
- Creates safe paths for emergency evacuation

Types of Security Lighting

Common security lighting approaches:

- **Continuous Lighting**:
  - Constant illumination
  - Most common method
  - Higher energy usage
  - Best for high-security areas
- **Standby Lighting**:
  - Motion-activated operation
  - Energy efficient design
  - Psychological deterrent
  - Good for low-traffic areas

Introduction to Security Sensors

Security sensors act as the nervous system of physical security, detecting various types of threats.

- Key deployment factors:
  - Environmental conditions
  - Coverage requirements
  - False alarm rates
  - Integration capabilities
- Performance considerations:
  - Detection accuracy
  - Response time
  - Maintenance needs
  - Failure modes

Types of Security Sensors

Sensor Type	Detection Method	Best Use Case
Infrared	Heat detection	Indoor motion detection
Pressure	Weight/force changes	Secure entry points
Microwave	Movement detection	Large open areas
Ultrasonic	High-frequency sound	Small enclosed spaces

Implementation guidelines:

- Combine multiple sensor types for reliability
- Test regularly under various conditions
- Maintain proper calibration schedules

Infrared Sensor Technology

How Infrared Sensors Work

These sensors detect heat signatures from people, animals, and objects

- **Passive Infrared (PIR)** sensors detect changes in heat patterns:
  - Monitor temperature differences
  - Identify movement through detection zones
  - Work well in complete darkness
  - Can be fooled by rapid temperature changes
- Modern PIR sensors include:
- Advanced signal processing to reduce false alarms.
- Pet-immune variations for home security.
- Integration with video systems for verification.

Pressure and Contact Sensors

- **Pressure sensors** detect physical force or weight changes:
- Common applications include:
  - Floor mats near secure entries
  - Fence and wall monitoring
  - Underground intrusion detection
  - Vehicle detection systems
- Advanced features now include:
- Weight range discrimination for different threats.
- Pattern recognition for normal versus suspicious activity.
- Integration with access control systems.
- Weatherproof designs for outdoor use.

Wave-Based Detection Systems

- Two main types of wave-based sensors:
  - **Microwave**:
    - Uses radio waves
    - Covers large areas
    - Penetrates thin walls
    - Good for outdoor use
  - **Ultrasonic**:
    - Uses high-frequency sound
    - Best for enclosed spaces
    - Doesn't penetrate walls
    - Very sensitive to movement
- Both types can work through darkness, smoke, or fog.

Introduction to Deception Technology

A New Approach to Security

Instead of just defending, deception technology tricks attackers into revealing themselves

- **Deception technology** creates traps and decoys to catch attackers:
- Looks like legitimate systems but monitors for unauthorized access.
- Provides early warning of potential attacks.
- Wastes attacker time and resources.
- Helps gather information about attack methods.
- Can be both physical and digital deceptions.

Understanding Honeypots

Security Note

While honeypots are powerful tools, they must be carefully isolated from production systems to prevent them from becoming a security risk.

- **Honeypots** are decoy systems designed to attract potential attackers
- Types of honeypots include:
  - High-interaction: Full system emulation
  - Medium-interaction: Service emulation
  - Low-interaction: Port monitoring only
- Common implementation targets:
  - Web servers and applications
  - Database systems
  - IoT device simulations

Honeynets: Networks of Deception

- A **honeynet** combines multiple honeypots in a network
- Standard components include:
  - Fake web servers and services
  - Simulated databases
  - Decoy file shares
  - Mock user accounts
- Key benefits:
  - Early attack detection
  - Threat pattern analysis
  - Attacker technique study
  - Automated response testing

Honeyfiles and Document Tracking

Honeyfile Type	**Purpose**
Password Lists	Detect credential theft attempts
Fake Documents	Track unauthorized access
Decoy Spreadsheets	Monitor data exfiltration
Configuration Files	Identify system probing

- **Honeyfiles** are decoy documents that alert when accessed
- Deployment strategies include:
  - Strategic placement in shared drives
  - Integration with DLP systems
  - Automated alert mechanisms

Honeytokens: Digital Breadcrumbs

- **Honeytokens** are pieces of fake data designed to detect theft
- Common implementations:
  - Fake login credentials
  - Invalid credit card numbers
  - Decoy API keys
  - Bogus email addresses
- Detection capabilities:
  - Data breach tracking
  - Insider threat identification
  - Exfiltration monitoring
  - Attack attribution