Database Administration Security

Cybersecurity Department

Course Code: ***CBS 214***

Theoretical Lecture 1: Security Fundamentals

Halal Abdulrahman Ahmed

Lecture Outlines

Theoretical Lecture 1: Security Fundamentals

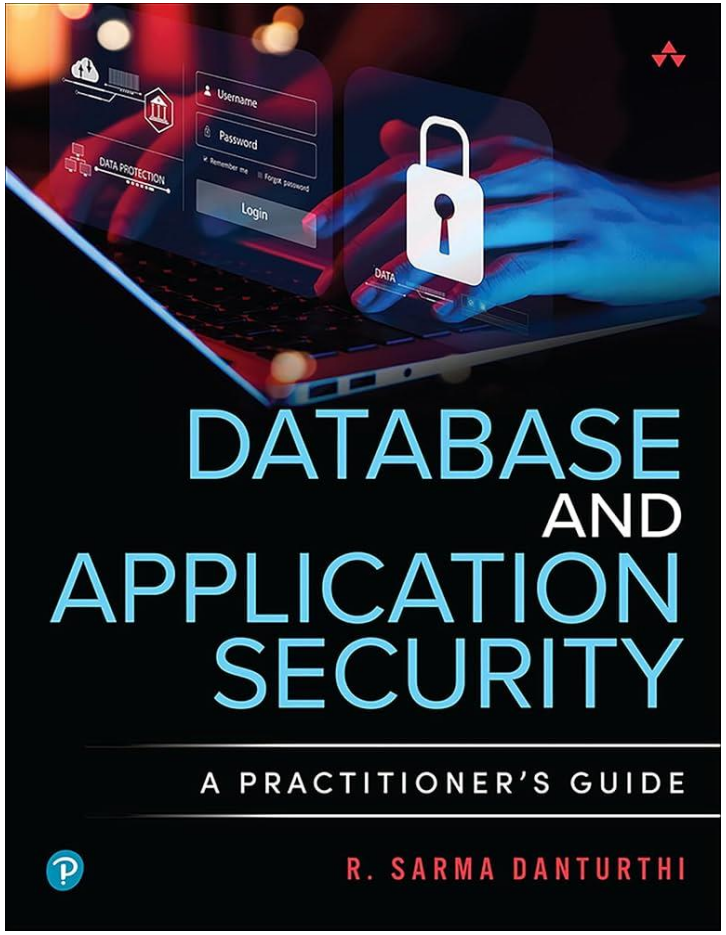
- Introduction to Cybersecurity
- Importance of Data Protection and Database Security
- Data as the Universal Currency
- Threat Actors and Common Database Attacks
- The Dirty Dozen Database Security Risks
- CIA–DAD Security Model
- I-A-A-A Security Model
- Defense in Depth Strategy

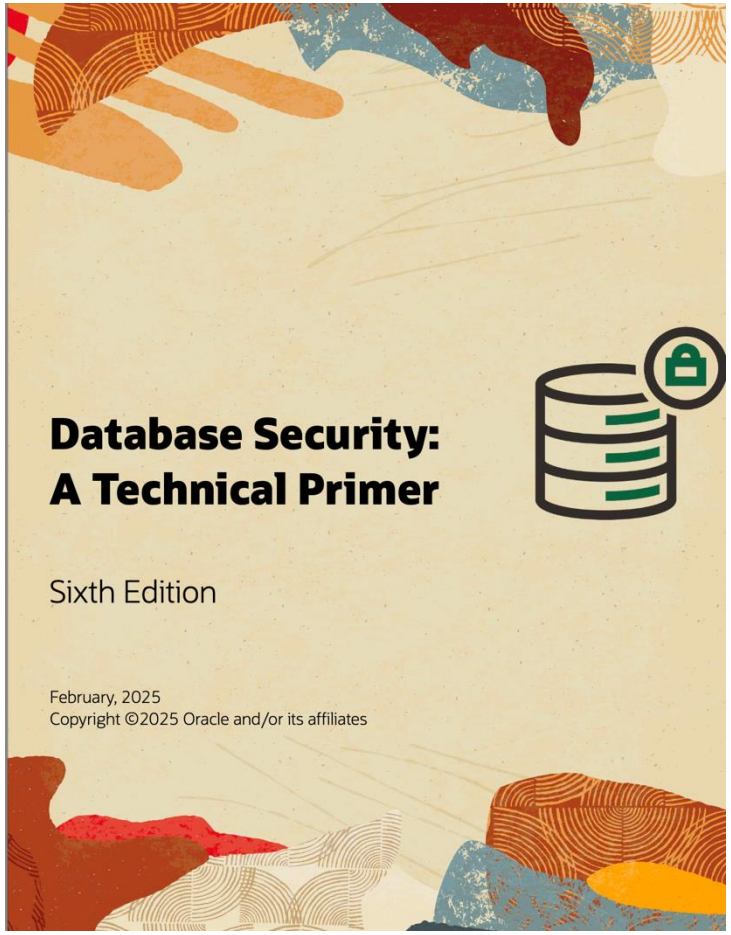
Learning Outcomes

By the end of this lecture, students will be able to:

- Explain the concept of cybersecurity and its importance
- Describe why databases are primary targets of cyberattacks
- Identify major database threats and attack vectors
- Explain the CIA–DAD security model with examples
- Explain the I-A-A-A access control model
- Understand the concept of defense in depth in database security

Materials


Username
Password
Login
DATA PROTECTION
DATA
DATABASE
AND
APPLICATION
SECURITY
A PRACTITIONER'S GUIDE
R. SARMA DANTURTHI


Database Security:
A Technical Primer
Sixth Edition
February, 2025
Copyright ©2025 Oracle and/or its affiliates

Assessment and Grading

Assessment Type	Weight	Quantity
Midterm Exam	20%	1
Quiz	10%	2
Lab Quiz	15%	2-3
Presentation	15%	1
Final Exam	40%	1

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, applications, and data from digital attacks.

Cybersecurity focuses on:

- Preventing unauthorized access
- Protecting sensitive data
- Detecting attacks early
- Reducing damage when attacks occur

Cybersecurity is important because:

- Most organizations store valuable data digitally
- Attacks can cause financial loss, legal issues, and reputation damage
- Databases are the main target of attackers

Simple example:
Protecting a university system so only authorized students can view grades.

Introduction: Why Protecting Data Matters

Modern organizations depend heavily on data to operate. This data includes personal information, financial records, intellectual property, and business-critical information. Most of this data is stored and managed inside **databases**, which makes databases the primary target of cyberattacks.

Why is data called the “universal currency”?

- Data is described as the **“universal currency”** because it has value across all sectors and industries.
- Stolen data can be sold, reused, or exploited long after a breach.
- Attackers may use data for fraud, identity theft, ransomware, or political advantage.
- Even data that seems unimportant to an organization may be valuable to attackers.
- **The value of data is not decided by the owner, but by the attacker**.

Simple example:

A list of student emails may seem harmless, but attackers can use it for phishing or social engineering attacks.

Importance of Data Security (Security is the top priority)

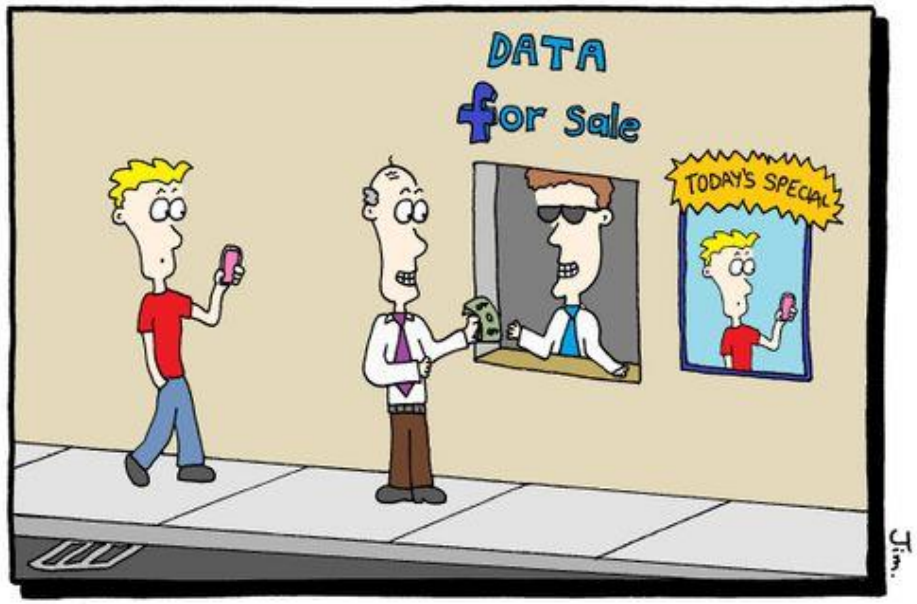
In the past, database management focused mainly on performance and availability. Today, **security has become the highest priority**. Reasons for this shift include:

- Increasing cyberattacks and ransomware
- Strict data protection regulations (such as GDPR)
- High financial and reputational cost of data breaches
- There is **no perfect or absolute security solution**. Instead, organizations rely on best practices and security controls to **reduce risk**, not eliminate it completely.

Understanding Threat Actors

Threat actors are individuals or groups that attempt to compromise data. **Types of threat actors:**

- **External attackers**
  - Hackers, cybercriminals, nation-state attackers
- **Internal attackers**
  - Employees, former employees, or trusted users abusing their access
  - Insiders can be just as dangerous as outsiders because they already have legitimate access to systems.



Common Ways Databases Are Attacked

Attackers do not always attack databases directly. They may use multiple paths, such as:

- Weak or stolen credentials
- Vulnerable applications (e.g., SQL injection)
- Misconfigured databases
- Unencrypted network traffic
- Access to database backups or copied data
- Test and development databases with weak security

Attackers often prefer **non-production systems** because they are less monitored and less protected.

The “Dirty Dozen” Database Security Risks

The **Dirty Dozen** represents the **12 most common database security risks**. They show **how attackers usually succeed**. Key risks include: They include:

- Insecure configuration and configuration drift
- Unpatched systems
- Lack of security policies
- Poor visibility into sensitive data
- Over-privileged users and administrators
- Weak authentication and shared accounts

- SQL injection vulnerabilities
- Trusting insecure networks
- Insufficient monitoring and auditing
- Sensitive data in test and development environments
- Unprotected database servers and backups
- Insecure encryption keys and secrets

Key idea: Most database breaches happen because of **basic security weaknesses**, not advanced hacking techniques.

Security Model

CIA–DAD Security Model

- The **CIA–DAD security model** is one of the most important foundational models in cybersecurity. It helps us understand two things at the same time: what information security is trying to protect, and how attackers try to break that protection. The model is divided into two parts. **CIA** represents the main security goals that organizations want to achieve, while **DAD** represents the common threats and attacks that try to violate those goals. Every security mechanism, policy, or tool exists to protect CIA and prevent DAD.
- The **CIA triad** defines the three essential goals of any secure system: **Confidentiality, Integrity, and Availability**. If any one of these goals is compromised, the system can no longer be considered secure.

Confidentiality

- **Confidentiality** means that information is accessible only to authorized users and is protected from unauthorized access. The main purpose of confidentiality is to protect privacy and sensitive information. This includes personal data, academic records, financial information, medical data, and business secrets.
- In practice, confidentiality is achieved by controlling who can see data and by protecting data from outsiders. Common techniques include user authentication (such as usernames and passwords), authorization rules, encryption, and network security mechanisms like firewalls. If confidentiality is weak, attackers may gain access to sensitive data even if the system is still running normally.
- A violation of confidentiality is called **disclosure**. Disclosure happens when confidential data is exposed to someone who is not allowed to see it.

Example: Only lecturers should be able to view exam questions before the exam. If a student or outsider gains access to those questions, confidentiality has been broken.

Integrity

- **Integrity** ensures that data remains accurate, complete, and trustworthy throughout its lifecycle. It means that information should not be changed, deleted, or corrupted unless the change is authorized and valid. Integrity is critical because incorrect data can lead to wrong decisions, financial loss, or serious legal consequences.
- Integrity is protected by access controls, validation rules, database constraints, and auditing mechanisms. Systems must ensure that only authorized users can modify data and that all changes can be traced back to the user who made them. Even accidental changes (such as human error or software bugs) are considered integrity problems if they are not controlled.
- A violation of integrity is called **alteration**, which occurs when data is modified without permission or in an unauthorized way.

Example: A student should never be able to change their own grades in the university database. If grades are modified illegally, the integrity of the academic system is compromised.

Availability

- **Availability** ensures that systems, services, and data are accessible to authorized users whenever they are needed. A system that is secure but unavailable is still a failure from a security perspective. Availability is especially important for systems that provide critical services, such as university portals, banking systems, and healthcare databases.
- Availability is protected through backups, redundancy, reliable hardware, proper maintenance, and protection against attacks such as denial-of-service (DoS). Hardware failures, power outages, software crashes, or cyberattacks can all affect availability.
- A violation of availability is called **denial**, where legitimate users are prevented from accessing the system or data.

Example: If students cannot access the registration system during enrollment due to a system crash or attack, availability has been violated.

DAD: Common Threats to Security

- The **DAD model** represents the opposite of CIA and describes how attackers typically compromise systems. Each element of DAD directly attacks one of the CIA goals.

Disclosure

- **Disclosure** occurs when confidential information is exposed to unauthorized users. This may happen due to weak passwords, stolen credentials, misconfigured permissions, unencrypted data, or insider misuse. Disclosure often leads to privacy violations, identity theft, and legal penalties for organizations.
- Disclosure does not necessarily damage the system itself, but it causes serious harm by revealing sensitive information.

Example: An attacker gaining access to student personal records or staff salary data.

DAD: Common Threats to Security (cont.)

Alteration

- **Alteration** happens when data is changed without authorization. This can be done by attackers or insiders who abuse their access. Alteration is dangerous because it makes data unreliable and untrustworthy. Organizations may continue using altered data without realizing it has been tampered with.
- Alteration attacks often occur through compromised accounts, SQL injection attacks, or lack of proper access controls.

Example: Illegally modifying financial records or academic grades in a database.

DAD: Common Threats to Security (cont.)

Denial

- **Denial** occurs when systems or data become unavailable to authorized users. This can be caused by cyberattacks such as denial-of-service, system overload, hardware failure, or even natural disasters. Denial attacks aim to disrupt services rather than steal or modify data.
- Denial can cause serious operational and financial damage, especially if systems are unavailable for long periods.

Example: A university website going offline during exam results announcement.

Relationship Between CIA and DAD

The relationship between CIA and DAD is direct and intentional:

- Confidentiality is threatened by **Disclosure**
- Integrity is threatened by **Alteration**
- Availability is threatened by **Denial**

Security controls are designed to **protect CIA goals** and **prevent DAD threats**.

CIA–DAD and Security Controls

Every security control exists for a reason related to CIA–DAD:

- Encryption protects confidentiality and prevents disclosure
- Access control protects integrity and prevents alteration
- Backups and redundancy protect availability and reduce denial impact
- Auditing helps detect disclosure, alteration, and denial attempts
- Understanding this relationship helps students analyze real-world security problems and explain why certain controls are necessary.

I-A-A-A Model

The **I-A-A-A security model** explains **how users are controlled and monitored** when they access a computer system, application, or database. While the CIA–DAD model focuses on *what* security tries to protect, the I-A-A-A model focuses on *how* access to systems is managed. It ensures that only the right users can access the system, perform only allowed actions, and be held accountable for their activities. The four components of this model work **in sequence** and **together** to enforce secure system access.

- **Identification**
- Authentication
- **Authorization**
- **Accounting (Auditing)**

Identification

Identification is the first step in the access control process. It is the act of a user **claiming an identity** to the system. At this stage, the system does not verify the user; it only receives an identity claim. Common identification methods include:

- Username
- Email address
- Student or employee ID
- Identification alone does not provide security because anyone can claim an identity.

Example: Typing a username on a login screen.

Authentication

Authentication is the process of **verifying that the claimed identity is real**. It confirms that the user is who they say they are. Authentication is critical because it prevents unauthorized users from accessing systems by pretending to be someone else. Authentication can be based on:

- Something you know (password, PIN)
- Something you have (smart card, OTP)
- Something you are (fingerprint, face recognition)
- Using more than one factor (multi-factor authentication) increases security.

Example: Entering a password after typing a username.

Authorization

Authorization determines **what an authenticated user is allowed to do** within the system. Even after a user is authenticated, they should not have unlimited access. Authorization enforces the principle of **least privilege**, which means users receive only the permissions necessary to perform their tasks. Authorization controls:

- Read, write, and delete permissions
- Access to specific files, tables, or applications
- Administrative privileges

Example: A student can view grades but cannot modify them, while a lecturer can update grades.

Accounting (Auditing)

- **Accounting**, also known as **auditing**, is the process of **tracking and recording user activities** in the system. It ensures accountability and allows organizations to detect misuse, investigate incidents, and meet legal and regulatory requirements. Audit records typically include:
- Who performed an action
- What action was performed
- When the action occurred
- From where the action originated
- Auditing does not prevent attacks directly, but it helps detect and respond to them.

Example: Recording which lecturer changed a grade and the exact time of the change.

How the I-A-A-A Model Works Together

The four steps work in this order:

- The user **identifies** themselves.
- The system **authenticates** the identity.
- The system **authorizes** allowed actions.
- The system **accounts** for all activities.
- If any step is missing, security is weakened.

Model	Category	Focus
CIA–DAD	Security goals model	*What must be protected*
I-A-A-A	Access control model	*How users are controlled*

Defense-in-Depth: A Layered Security Approach

Defense-in-depth means using **multiple layers of security controls** instead of relying on a single protection mechanism. Security layers may include:

- Network security
- Application security
- Database security
- Physical security
- If one layer fails, other layers continue to protect the data.

Example: Even if an attacker steals a password, encryption and auditing can still limit damage.

Core Database Security Goals

Database security efforts into **four main goals**:

- **Assess security posture**

  Identify weaknesses, misconfigurations, and risks.

- **Control access to data**

  Ensure users can only access what they are authorized to use.

- **Monitor user activity**

  Detect suspicious behavior and support investigations.

- **Protect data against theft**

  Prevent attackers from stealing usable data.

All security tasks should support at least one of these goals.

Goals vs Tasks in Security Management

- A **goal** describes what needs to be achieved (e.g., secure authentication).
- A **task** is the action taken to reach that goal (e.g., enabling multi-factor authentication).

Security work should focus on **high-value tasks** that directly reduce risk. Tasks that do not support a clear goal may waste time and resources.

Next Lecture

- Introduction of Database Security

Research Task

- What are the key roles in a database security environment?
- What is the General Data Protection Regulation (GDPR)?

"Normally, this project would require weeks of research and verification...but luckily there's an app for it."

References

- **Danturthi, S.** (2019). *Database and application security: A practitioner's guide*. Apress.

- **Oracle Corporation.** (2015). *Database security: A technical primer* (6th ed.). Oracle.


Any
Question