

Database Security and Forensics

Introduction

Mr Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Site ⇒ www.al-moualime.com)



University of Skikda — Computer Science Department

1st Year Master in Information Security (IS)

Academic Year 2025-2026

Version v1.0 — 2026-09-21 à 19:20:38



Outline

- 1 Objectives
- 2 The Stakes
- 3 Organization

Course Presentation

Practical Information

- **Course:** Database Security and Forensics
- **Level:** Master 1 Information Security, Semester 2
- **Code:** UEF21 (*Fundamental Teaching Unit*)
- **Schedule:** 1.5h lecture + 1.5h lab per week
- **Evaluation:** 40% Lab (3 grades) + 60% Final Exam
- **Credits:** 4 (Coefficient 3)

Reference Book

Database Security

Authors: Alfred Basta & Melissa Zgola (2011)

Publisher: Cengage Learning

Course Motto

This course was designed with a focus on pedagogical effectiveness, active understanding, and practical application of knowledge.

Course Vision: Database Security and Investigation

Three Fundamental Skills to Master

1. Secure — Before the Attack

- Configure a DBMS (*Database Management System*) according to best practices
- Implement strong authentication and access controls
- Encrypt and protect sensitive data

2. Detect — During the Incident

- Monitor activity logs in real-time
- Identify anomalies and suspicious behavior
- React quickly to limit impacts

3. Analyze — After the Incident

- Reconstruct the attack timeline
- Collect and preserve digital evidence
- Write an analysis report and propose corrective measures

Why Study This Subject?

A Global Problem

Today, everything is digital:

- Your bank data → In a database
- Your medical records → In a database
- Your online purchases → In a database
- Your Facebook messages → In a database

Result: Databases are the first target for data hackers!

Concrete Examples: Every Minute Worldwide

- 5.9 million Google searches
- 231 million emails sent
- 400,000 banking transactions

All this data is stored in databases.

CIA Model Applied to Databases

The CIA Model — Foundation of Data Security

C — Confidentiality

- Prevent unauthorized access to data
- Examples: encryption, strong authentication, access control
- Risk: personal or financial data leakage

I — Integrity

- Ensure data is not illegally modified
- Examples: logging, signatures, database constraints
- Risk: alteration of bank accounts or results

A — Availability

- Ensure the database remains accessible to legitimate users
- Examples: backups, replication, anti-DDoS protection
- Risk: interruption of critical services

Real Attack Cycle Against a Database

Typical Steps Observed in Real Incidents

- 1 Reconnaissance — Server scanning and vulnerability research
- 2 Intrusion — Exploitation (SQL Injection, weak password)
- 3 Privilege Escalation — Administrator access
- 4 Lateral Movement — Access to other systems
- 5 Exfiltration — Progressive data theft
- 6 Trace Erasure — Deletion or modification of logs

Link with the Course

Secure → prevents intrusion Detect → identifies ongoing attack Analyze → reconstructs the timeline

Course Thread Scenario

Case Study: Compromised E-commerce Platform

A company has a PostgreSQL database containing:

- Customer accounts and passwords
- Banking transactions
- Order history

An attacker exploits SQL injection and accesses the database.

Your Mission Throughout the Course

- Security chapter: prevent the attack
- Detection chapter: identify the intrusion
- Forensic chapter: analyze the traces
- Final chapter: produce a professional report

What Data is at Risk?

Three Types of Critical Data

1. Personal Data

- Identity, contacts, photos, messages
- Browsing and purchase history

2. Financial Data

- Credit cards, accounts, transactions

3. Business Secrets

- Secret formulas, strategies, customers

Why is This Serious?

This data is worth money on the black market!

What You Will Learn (1/2)

Technical Skills — Protect

By the end of the course, you will know how to:

Secure a Database

- 1 Install and configure PostgreSQL in secure mode
- 2 Create strong passwords and access controls
- 3 Encrypt sensitive data (make it unreadable)
- 4 Prevent SQL Injection attacks

Transferable Skills

The principles learned apply to all DBMS (*Database Management Systems*): Oracle, MySQL, SQL Server, MongoDB, etc.

What You Will Learn (2/2)

Technical Skills — Investigation

Investigation After an Attack

- 1 Read and analyze system logs
- 2 Reconstruct the timeline of events (investigation approach)
- 3 Collect and preserve digital evidence with legal value
- 4 Write a professional investigation report

This Course Prepares You For

- Administering secure databases
- Working as a digital forensic analyst
- Preparing for certifications from international cybersecurity references (CEH Certified Ethical Hacker, CISSP Certified Information Systems Security Professional, CISM Certified Information Security Manager)

The Major Security Problem

Where Does Security Money Go?

Companies spend a lot of money on security:

- 40% to protect the network (Internet, WiFi)
- 35% to protect computers and software
- Only 10% to protect databases

But Watch Out!

80% of sensitive data is in databases!

It's like having a house with:

- An armored door (secure network)
- Windows with bars (protected computers)
- But an open safe (unprotected database)

Who Attacks Databases? (1/2)

Two Types of Attackers

1. External Hackers (45%)

- Use techniques like SQL Injection
- Look for system vulnerabilities
- Steal thousands of accounts at once

2. Insider Threats (55% — DANGER!!)

2. Insider Threats

- Human errors, misconfiguration
- Negligent or malicious users
- Privilege abuse

Source: Verizon DBIR and IBM reports — significant portion of incidents involve insiders or human errors

The Paradox

55% of breaches are internal, but 80% of budgets are spent against external threats!

Who Attacks Databases? (2/2)

The Four Main Attack Vectors

1. Social Engineering

- Phishing and human manipulation
- Involved in the vast majority of incidents

Source: Verizon Data Breach Investigations Report (DBIR) — human factor present in over two-thirds of breaches

2. Web Vulnerabilities

- SQL Injection, XSS (*Cross-Site Scripting*), CSRF (*Cross-Site Request Forgery*)

3. Malware

- Viruses, Worms, Trojans, Ransomware

4. Deceptive Applications

- Fake sites that imitate real ones to steal your data

How Much Does a Cyberattack Cost?

Average Cost of a Data Breach

According to the **IBM Cost of a Data Breach** report:

- **Global average cost:** approximately 4.4 million USD
- **In the United States:** approximately 10 million USD
- **Healthcare sector:** often the most expensive

Source: IBM Cost of a Data Breach Report (Ponemon Institute analysis)

Why Is It So Expensive?

- Regulatory fines (GDPR, PCI-DSS)
- Loss of trust and customers
- Business interruption
- Forensic investigation and remediation

Attack Detection Time

Average Breach Duration

Industry studies indicate that a data breach can take on average **between 240 and 280 days** to be detected and contained.

Source: IBM Cost of a Data Breach Report

Consequences of Delay

- Progressive data exfiltration
- Disappearance or alteration of evidence
- Reinfection or persistent access
- Significant cost increase

Famous Real Cases

Three Cyberattacks That Made History

1. Equifax (2017) — United States

- 147 million people hacked
- Social security numbers, driver's licenses stolen
- Cost: Over 1.4 billion dollars
- Cause: An uncorrected software bug

2. Yahoo (2013-2014)

- 3 billion compromised accounts (all users!)
- Passwords and security questions stolen
- Yahoo lost 350 million in its sale to Verizon

3. Marriott (2018) — Hotels

- 500 million customers affected
- Passport numbers and credit cards stolen
- Hackers remained hidden for 4 years!

Digital Forensics: Principle

What is Digital Forensics?

Same logic as a physical crime scene:

- Methodical search for clues
- Documentation before any handling
- Evidence copied and sealed
- Timeline reconstruction

Objective: understand precisely what happened in the system.

Application to Databases

We analyze:

- Access and modification logs
- Authentication traces
- Suspicious data modifications
- User actions

Investigation: Steps and Traceability

Digital Investigation Cycle

- 1 **Preparation** — tools and procedures
- 2 **Identification** — locate evidence
- 3 **Preservation** — copy without alteration
- 4 **Collection** — extraction of traces
- 5 **Analysis** — reconstruction of facts
- 6 **Report** — documented conclusions

Chain of Custody

Complete traceability of evidence: who → when → where → how.

Broken chain = legally fragile evidence.

Course Content Overview

Main Chapters

Chapter 1 — Threats and Malware

- Identification of external and internal threats
- The 5 malware families: Viruses, Worms, Trojans, Ransomware, Botnets
- Security cycle and defense in depth

Chapter 2 — Secure Architecture

- Secure PostgreSQL configuration
- Data encryption and protection

Chapter 3 — Access Control

- User and permission management
- Least privilege principles

Chapter 4 — Forensic Investigation

- Log analysis and attack reconstruction
- Legal evidence collection

Course Organization

Lectures to Understand Theory — 1.5h/week

- Database security concepts
- Attack techniques and strategies
- Real case analysis
- Standards: ISO 27001, NIST (*National Institute of Standards and Technology*), GDPR

Practical Work for Implementation — 1.5h/week

- Secure PostgreSQL installation and configuration
- User and permission management
- Sensitive data encryption
- Attack testing in controlled environment
- Log analysis after simulation

What You Should Already Know (1/2)

Essential Knowledge

Databases (IMPORTANT!)

- Know what a table, primary key, foreign key are
- Understand the relational model
- Master SQL: SELECT, INSERT, UPDATE, DELETE
- Know joins and views

Systems and Networks

- Use Linux command line
- Understand TCP/IP, HTTP, HTTPS
- Know what an IP address, a port are

What You Should Already Know (2/2)

Essential Knowledge (continued)

Basic Security

- Understand: Confidentiality, Integrity, Availability (CIA)
- Know what encryption is
- Know common threats (viruses, phishing)

If You Have Gaps

- Review SQL on **SQLZoo.net** (free)
- Practice Linux on **Ubuntu** in virtual machine
- Read chapters 1-2 of the reference book

What Tools to Use? (1/2)

Software to Install

Database

- **PostgreSQL 14+**: The DBMS we will use
- **pgAdmin 4**: Graphical interface for PostgreSQL
- **DBeaver**: Practical SQL editor

Why PostgreSQL?

- **Industrial**: Used by Apple, Instagram, Spotify
- **Open source**: Free, accessible source code
- **Educational**: Concepts valid for all DBMS

What Tools to Use? (2/2)

Security Tools

- **sqlmap**: Automated SQL injection testing
- **Wireshark**: Network traffic analysis
- **OpenSSL**: Encryption and certificates

Operating System

- Linux (Ubuntu recommended)
- Or Linux virtual machine on Windows

Do This Now

Install PostgreSQL to practice at home.
Installation guide provided in course resources.

Where to Find Help? (1/2)

Official Documentation

Course Reference

- Database Security — Basta & Zgola (2011)

Online Documentation (free!)

- Official PostgreSQL Security Documentation
- OWASP (*Open Web Application Security Project*) — Database Security Guide
- NIST SP 800-53 — Security Standards

Where to Find Help? (2/2)

To Stay Updated

- **The Hacker News** — Cybersecurity news
- **Krebs on Security** — Expert blog
- **CVE** (*Common Vulnerabilities and Exposures*) — List of discovered vulnerabilities

Important Laws to Know

- **GDPR**: European personal data protection law
- **PCI-DSS** (*Payment Card Industry Data Security Standard*): Credit card security standard
- Violation = Fines up to 4% of revenue!

What Jobs After This Course? (1/2)

Career Opportunities (Accessible Jobs)

- **Security DBA:** Secure database administrator
- **Forensic Analyst:** Digital investigation expert
- **Pentester:** Ethical hacker who tests security
- **Security Auditor:** Checks if company is well protected
- **CISO** (*Chief Information Security Officer*): Responsible for all IT security

What Jobs After This Course? (2/2)

Sectors That Are Hiring

- Banks and insurance companies
- Hospitals and pharmacies
- E-commerce sites
- Government and military
- Cybersecurity consulting firms

Job Market

- **3.5 million vacant positions** in cybersecurity worldwide
- Growth of **+30% per year**
- Salaries among the **highest** in IT
- Secure database specialists = Highly sought after!

Final Word

Welcome!

Why This Course is Exciting?

- You will learn to think like a hacker (to better defend yourself)
- You will play digital detective
- You will protect critical data
- You will have a sought-after and well-paid job

Course Philosophy

- **Understand** rather than memorize
- **Practice** rather than just read
- **Question** rather than accept
- **Learn continuously** (security evolves every day)