Eötvös Loránd University (ELTE)
Faculty of Informatics (IK)
Pázmány Péter sétány 1/c
1117 Budapest, Hungary

ABOUT THE COURSE

Introduction to Data Security

Imre Lendák, PhD, GICSP

2025
Budapest, Hungary

Presentation outline

- Course team
- Course contents
- About the exam!

COURSE TEAM

Course team – Lecturers

Imre Lendak

- Degree in computer science and electrical engineering
- PhD in graph analysis
- Certified cybersecurity expert
- R&D projects in the following infrastructure security sectors:
  - energy,
  - banking,
  - water management, and
  - telecommunications.
- 10+ years software engineering experience (C++, C#, Python)
- Preferred comm.channel: email (lendak@inf.elte.hu)

Péter Kiss

- Computer science MSc, ELTE/IK
- PhD in Federated Learning
- Machine learning expert
- Taught subjects:
  - Machine learning
  - Stream mining
- R&D projects in sectors:
  - Finance
  - Telecommunications
- 10+ years of software dev & ML experience (Java, Python)

COURSE CONTENTS

Broad topics covered

Brief topic list (accredited)

- Cyberspace, cybersecurity, cybercrime;
- Identity and access management;
- Data inventory and backup;
- Data encryption;
- Data loss prevention;
- Data security standards;
- **Data privacy vs machine learning (ML); →**

Data privacy & ML

- Intro & ML security Top 10
- Evasion attacks
- Model and data inversion
- Federated learning
- Synthetic data generation
- Secure ML supply chains

Draft topic list (2025)

Data Security (3)

- Data Security Overview
  - Basic definitions
- Data protection measures
  - Inventory and backup
  - Encryption in a nutshell
  - Identity & access
  - Data loss prevention (DLP)
- Legal aspects of Data Security
  - Privacy in a nutshell
  - Critical infrastructure sectors
  - Legal framework

ML Security (7)

- ML Security Intro
  - Ontology: artefacts, attacks, attackers, attack surface
  - OWASP Top 10 ML

Model

- Secure ML training
- Evasion attacks
- Misuse of ML models: poisoning, sponge, theft, inversion, supply chains

Data

- Data ‘inversion’: inference, data leaks, anonymization, de-anonymization
- Federated learning
- Synthetic data generation

Lecture and lab timing

Lectures

- Lecture start and end times on Tuesdays (2025):
  - 12:15 – 13:00 Class #1
  - 13:00 – 13:15 Break + Face-to-face consultations
  - 13:15 – 14:00 Class #2
- Consultations
  - Team-based, bi-weekly

Labs

- No labs yet (2025 Spring)

EXAM SETUP

Course & exam setup

- Classroom-based lectures
- Exam consists of three compulsory (non-optional) elements (51% to pass each):
    - (1) course project (Canvas) → see next slide (50p),
    - (1) entry test (Canvas), and
    - (2) oral exam (50p).
- Lecture attendance for extra points & benefits
    - Lecture attendance → Up to 5 extra points
    - Canvas assignments → Extra points
    - Partial quiz (3) → Can substitute final entry test

Team-based project work

Teams

- 5 members
- International as much as possible (!)

Projects

- Important (cut-off) dates:
  - Topic list published: Feb 28
    - Bi-weekly status checks
    - Detailed instructions online
  - Project submission: Apr 27
  - Project defenses: Apr 29
- Project output(s):
  - Github repository with code
  - Documentation and illustrations also on Github → Multi-page docs (!)
  - 10-slide presentation (Overleaf ?)

Thank you for your attention!