This course provides an overview of information security and privacy topics. It introduces students to the knowledge and tools they will need to deal with the security/privacy challenges they are likely to encounter in today's world. The tools are illustrated with relevant applications.

Content

- Overview of cyberthreats
- Basic exploitation of vulnerabilities
- Authentication, access control, compartmentalization
- Basic applied cryptography
- Operational security practices and failures
- Machine learning and privacy
- Data anonymization and de-anonymization techniques
- Privacy enhancing technologies
- Blockchain and decentralization

Keywords

security, privacy, protection, intrusion, anonymization, cryptography

Learning Prerequisites
Required courses
COM-301 Computer security
Basic systems programming (in C/C++) or better
Basic networking knowledge
Good scripting knowledge (Python)

Learning Outcomes
By the end of the course, the student must be able to:
• Understand the most important classes of information security/privacy risks in today's "Big Data" environment
• Exercise a basic, critical set of "best practices" for handling sensitive information
• Exercise competent operational security practices in their home and professional lives
• Understand at overview level the key technical tools available for security/privacy protection
• Understand the key technical tools available for security/privacy protection
• Exercise competent operational security practices

Expected student activities
Attending lectures, solving assigned problems and "hands-on" exercises, reading and demonstrating understanding of provided materials.

Assessment methods
• continuous control : 30% of the grade
• final exam : 70% of the grade

Resources
Moodle Link
• https://go.epfl.ch/COM-402