**COM-402 Information security and privacy**
Troncoso Carmela, Hubaux Jean-Pierre, Oechslin Philippe

<table>
<thead>
<tr>
<th>Cursus</th>
<th>Sem.</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>MA1, MA3</td>
<td>Obl.</td>
</tr>
<tr>
<td>Data Science</td>
<td>MA1, MA3</td>
<td>Obl.</td>
</tr>
<tr>
<td>Informatique et communications</td>
<td></td>
<td>Obl.</td>
</tr>
<tr>
<td>Informatique</td>
<td>MA1, MA3</td>
<td>Obl.</td>
</tr>
<tr>
<td>Ing. finance</td>
<td>MA1, MA3</td>
<td>Opt.</td>
</tr>
<tr>
<td>Mineur en Data science</td>
<td>H</td>
<td>Opt.</td>
</tr>
<tr>
<td>SC master EPFL</td>
<td>MA1, MA3</td>
<td>Obl.</td>
</tr>
<tr>
<td>Science et ing. computationelles</td>
<td>MA1, MA3</td>
<td>Opt.</td>
</tr>
</tbody>
</table>

**Summary**
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 Big Data world. The tools are illustrated with relevant applications.

**Content**
- Overview of cyberthreats
- Exploiting 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**
Basic Python programming or better
Basec networking knowledge
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

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

Assessment methods
Continuous assessment via homework exercises, quizzes, midterm exam and final written exam.