Privacy Enhancing Technologies (COMP0061)

Description

Aims:
Upon completion of the module the students are expected to be specialists in understanding the issues around privacy in computer systems and on-line services; aware of the best available techniques for mitigating important privacy threats through appropriate security and cryptography controls, namely the use of private communications, private authentication and private computations; be able to securely implement those techniques, as well as familiar with the process of building secure systems.

Learning outcomes:
1. Basic and advanced conceptions of privacy;
2. Techniques used for on-line tracking and pervasive surveillance infrastructures;
3. Anonymous communications and Tor;
4. Privacy in authentication;
5. Traffic analysis;
6. Privacy in databases and storage systems;
7. Censorship and censorship evasion;
8. Advanced privacy engineering topics like selective disclosure credentials, zero-knowledge proofs, and private computations;
9. Interdisciplinary aspects of privacy;

Content:
The course covers in depth major issues in computer security related to protecting privacy as well as threats to the privacy of computer users. In particular is covers the theory and practice of:
- Private communications, anonymous communications, censorship circumvention and traffic analysis;
- Advanced privacy engineering topics based on modern cryptography like selective disclosure credentials, zero-knowledge proofs, and private computations;
- Interdisciplinary (social, economic, legal, anthropologic) aspects of privacy;
- Students are introduced to both privacy threats such as

Key information

- Year: 2019/20
- Credit value: 15 (150 study hours)
- Delivery: PGT L7, Campus-based
- Reading List: View on UCL website
- Tutor: Dr Emiliano De Cristofaro
- Term: Term 2
- Timetable: View on UCL website

Assessment

- Written examination (departmentally managed): 35%
- Written examination (departmentally managed): 35%
- Coursework: 30%

Find out more

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk

Disclaimer: All information correct as of August 2019. Please note that aspects of the module may be subject to change. UCL will make best efforts to inform applicants of major changes.
pervasive surveillance, profiling, location analysis, and traffic analysis, as well as the technical mitigation techniques relying on modern cryptography and differential privacy.

Requisites:
In order to be eligible to select this module, a student must be registered on a programme for which it is a formally-approved option or elective choice AND must have taken COMP0054 or COMP0025 in Term 1.
Privacy Enhancing Technologies (COMP0061)

**Description**

**Aims:**
Upon completion of the module the students are expected to be specialists in understanding the issues around privacy in computer systems and on-line services; aware of the best available techniques for mitigating important privacy threats through appropriate security and cryptography controls, namely the use of private communications, private authentication and private computations; be able to securely implement those techniques, as well as familiar with the process of building secure systems.

**Learning outcomes:**
1. Basic and advanced conceptions of privacy;
2. Techniques used for on-line tracking and pervasive surveillance infrastructures;
3. Anonymous communications and Tor;
4. Privacy in authentication;
5. Traffic analysis;
6. Privacy in databases and storage systems;
7. Censorship and censorship evasion;
8. Advanced privacy engineering topics like selective disclosure credentials, zero-knowledge proofs, and private computations;
9. Interdisciplinary aspects of privacy;

**Content:**
The course covers in depth major issues in computer security related to protecting privacy as well as threats to the privacy of computer users. In particular is covers the theory and practice of:
- Private communications, anonymous communications, censorship circumvention and traffic analysis;
- Advanced privacy engineering topics based on modern cryptography like selective disclosure credentials, zero-knowledge proofs, and private computations;
- Interdisciplinary (social, economic, legal, anthropologic) aspects of privacy;
- Students are introduced to both privacy threats such as

**Key information**

<table>
<thead>
<tr>
<th>Year</th>
<th>2019/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit value</td>
<td>15 (150 study hours)</td>
</tr>
<tr>
<td>Delivery</td>
<td>UGM L7, Campus-based</td>
</tr>
<tr>
<td>Reading List</td>
<td><a href="#">View on UCL website</a></td>
</tr>
<tr>
<td>Tutor</td>
<td>Dr Emiliano De Cristofaro</td>
</tr>
<tr>
<td>Term</td>
<td>Term 2</td>
</tr>
<tr>
<td>Timetable</td>
<td><a href="#">View on UCL website</a></td>
</tr>
</tbody>
</table>

**Assessment**

- Written examination (departmentally managed): 35%
- Written examination (departmentally managed): 35%
- Coursework: 30%

**Find out more**

For more information about the department, programmes, relevant open days and to browse other modules, visit [ucl.ac.uk](http://ucl.ac.uk)
pervasive surveillance, profiling, location analysis, and traffic analysis, as well as the technical mitigation techniques relying on modern cryptography and differential privacy.

Requisites:
In order to be eligible to select this module, a student must be registered on a programme for which it is a formally-approved option or elective choice AND must have taken COMP0054 or COMP0025 in Term 1.