Security (COMP0141)

Description
Aims:
-The module aims at giving students a foundation in computer security, cryptography and human aspects of security.
-After taking the module students should be able to identify risks and security sensitive aspects of systems, where a system can range from a small and simple solution for a specific task to a full organisation including IT infrastructure and users. They will be taught this from the experience of how systems have failed in the past and by analysing systems from an adversarial viewpoint;
-Students should also know core defensive techniques to prevent or mitigate attacks. They should be able to formulate a threat model for a system and reason about whether it is secure or insecure;
-Students should be able to deliver effective security for real-world environments: how to design and manage security in organisations to effectively protect them;

Learning outcomes:
On successful completion of the module, a student will be able to:
1. understand how to formulate a threat model including the assets to be protected, the capabilities of the adversary, and reason about whether the probability the adversary may succeed;
2. know core cryptographic methods to protect communication such as message authentication codes, digital signatures, encryption, and key exchange. Understand the security guarantees cryptographic tools provide and conversely how inappropriate use lead to vulnerabilities;
3. understand key principles and concepts related to computer and systems security. Understand the complexities of building flexible and correct access control and authentication systems, from a technical and HCI perspective. Recognize and exploit common security vulnerabilities on hosts and networks;
4. know that security involves people, processes and

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>UG L5, Campus-based</td>
</tr>
<tr>
<td>Reading List</td>
<td>View on UCL website</td>
</tr>
<tr>
<td>Tutor</td>
<td>Dr Sarah Meiklejohn</td>
</tr>
<tr>
<td>Term</td>
<td>Term 2</td>
</tr>
<tr>
<td>Timetable</td>
<td>View on UCL website</td>
</tr>
</tbody>
</table>

Assessment

- Written examination (main exam period): 100%

Find out more

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk
technology. Understand how security needs to fit with business goals and organisational processes to work effectively - rather than disrupt, create friction, and drain resources. Know the basics of how to influence and manage security behaviours of a range of organisational stakeholders - employees, managers, developers, security specialists;

**Content:**
The module gives students a foundation in computer security, cryptography and human aspects of security. Students will study attacks against system and analyse systems from an attacker’s perspective. The module will also cover core defensive techniques and develop threat models that can be used to analyse the security of a system. The module studies specific cryptographic systems for 3 weeks, core computer security for 4 weeks, and spends 3 weeks studying security for real-world environments: how to design and manage security in organisations to effectively protect them.

**Requisites:**
In order to be eligible to select this module, a student must be registered on a programme for which it is formally available.