Computer Security II (COMP0055)

Description
Aims:
Providing an advanced understanding of network and computer security vulnerabilities and countermeasures in real-world systems.

Learning outcomes:
Students will learn how to think critically and creatively about advanced security topics. They will learn how, when and why to apply security technologies for the most benefit, vis-à-vis advanced network, software, and system issues. Students will be challenged with the study and the design of attacks and defenses to networks, systems, and software, both from a theoretical and a practical point of view.

Content:
- Network protocols and vulnerabilities;
- Network defenses;
- Network Security tools;
- Intrusion and Anomaly Detection;
- Advanced Software and System security: threats, vulnerabilities, and countermeasures via real-world examples;
- Malware and botnets;
- Denial of Service;
- Advanced Web Security;

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 an equivalent module) in Term 1.

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 June 2019. Please note that aspects of the module may be subject to change. UCL will make best efforts to inform applicants of major changes.
Computer Security II (COMP0055)

Aims:
Providing an advanced understanding of network and computer security vulnerabilities and countermeasures in real-world systems.

Learning outcomes:
Students will learn how to think critically and creatively about advanced security topics. They will learn how, when and why to apply security technologies for the most benefit, vis-à-vis advanced network, software, and system issues. Students will be challenged with the study and the design of attacks and defenses to networks, systems, and software, both from a theoretical and a practical point of view.

Content:
- Network protocols and vulnerabilities;
- Network defenses;
- Network Security tools;
- Intrusion and Anomaly Detection;
- Advanced Software and System security: threats, vulnerabilities, and countermeasures via real-world examples;
- Malware and botnets;
- Denial of Service;
- Advanced Web Security;

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 an equivalent module) in Term 1.