MSc Information Security Dissertation (COMP0064)

Description
Aims:
Students will obtain experience of undertaking and completing a piece of research, applying techniques learned throughout the programme, including the technical skills of analysis, design and implementation.

Learning outcomes:
On successful completion of the module, a student will be able to:
1. Work individually developing a major project;
2. Plan and coordinate development activities;
3. Make realistic work commitments;
4. Present the research done effectively to a deadline;

Content:
Students work individually or in groups on a research topic together with a supervisor. Frequently, the supervisor is one of UCL's lecturers on the MSc in Information Security programme, but students can also work with other academic staff at UCL or with an external supervisor from industry. The workload of the thesis corresponds to four modules. The project runs from immediately after the examination period (May) with the students responsible for organising themselves and their work, with advice from their supervisor. Students are expected to meet with their supervisor on a regular basis, as agreed with the supervisor. The main report documents the results of the project. The deadline for submission is normally the last week of August. The dissertation text (defined as everything except title page, table of contents, references and appendices) should not exceed 50 pages in 12 point type and 1.5 or double spacing for an individual report. The total dissertation length (main text together with appendices) should under no circumstances exceed 100 pages for an individual report. For group projects, each extra group member increases the allowance by 30 pages in the main body, and 30 pages in the appendices.

Key information
Year 2019/20
Credit value 60 (600 study hours)
Delivery PGT L7, Campus-based
Reading List View on UCL website
Tutor Dr Steven Murdoch
Term Terms 2 and 3
Timetable View on UCL website

Assessment
- Dissertation: 100%

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.
Examples of recent project titles:
- Algebraic Attack On Smart Cards;
- Algebraic Cryptanalysis Of Ciphers;
- Anti-Phishing: Secure, Usable and Low Cost Authentication For Secure and Convenient Online Banking Security and Payment Systems;
- Comparing Authentication Methods;
- Computer Security By Strip Searching;
- Cryptanalysis Of Keeloq;
- Defence Against Profile Injection Attacks;
- Fuzzy Private Matching and Privacy Preserving;
- Implementing Default Capabilities To Fight Computer Malware;
- Integration Of Biometrics In Identity Management;
- Maliciously Created Routing Loops In Mobility Protocols;
- Mobile Phone Security;
- Model Checking Security Protocols;
- Modelling The Information Content Of Rumour Propagation;
- Perfectly Secure Communication Over General Adversary Structures In Arbitrary Networks With Feedback Channels;
- Privacy: Dataveillance As Differential Pricing and Social Sorting;
- Private Information Retrieval;
- Topological Characterisation of Email Communications;
- Trusted Computing;
- Verification of TESLA (or Variant Dining Cryptographers) Protocol Using MCMAS;

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