People and Security (COMP0056)

Description

Aims:
- Students will be able to specify usability criteria that a security mechanism has to meet to be workable for end-user groups and work contexts;
- Know the strengths and weaknesses of particular security mechanisms in practice, and hence be able to choose and configure mechanisms for best performance in a given organisational context;
- Be able to specify accompanying measures (policies, training, monitoring and ensuring compliance) that a user organisation needs to implement to ensure long-term security in practice;

Learning outcomes:
On successful completion of the module, a student will be able to:
1. apply their knowledge of human factors and behavioural economics to specify and implement workable and effective security solutions, and manage security behaviour;

Content:
Understanding Human Behaviour in Security:
- Systems thinking and design;
- Usability: Users, tasks and context;
- Performance and Workload;
- Productivity and performance vs risk and security;
Economics:
- Humans and Risk;
- Risk Biases and Decision-making;
- Friction and the Compliance Budget;
Authentication:
- Authentication tasks: enrolment, verification, recovery;
- Knowledge-based authentication: Passwords,
- phrases, PINs, graphical Authentication;
- Token-based authentication;
- Biometric authentication: physical and behavioural;
- Continuous authentication via devices, sensors, and biometrics;

Key information

Year: 2019/20
Credit value: 15 (150 study hours)
Delivery: PGT L7, Campus-based
Reading List: View on UCL website
Tutor: Dr Simon Parkin
Term: Term 1
Timetable: View on UCL website

Assessment

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.
- Payment systems and transaction authentication;
  Access control:
  - Different access control models, organisational impact and user workload;
  Attacks and attackers (and how to counter them):
  - Types of attacks (Guessing, observation, capture and coercion);
  - Types of attackers: motivation, resources risk propensity;
  - Social engineering attacks;
  - Insider attacks;
  Identity:
  - Online identity vs identity in the physical world;
  - National identity vs socially constructed systems;
  - Digital footprints, shadows and superidentities;
  - Identity as currency;
  Privacy:
  - Data protection and user perception;
  - Delivering privacy: Privacy by Design, the PST model;
  - Surveillance, dataveillance and sousveillance online and in the physical world (CCTV);
  Trust:
  - Model of trust in online interaction;
  - Incentivising trustworthy behaviour;
  - Reputation systems and their application in online systems;
  Influencing user behaviour:
  - Security awareness, education and training;
  - User interface design and influencing techniques;
  - Values, attitudes, security culture and security behaviour;
  - Responsibility and communication;

**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 (i) knowledge of basic information security principles; and (ii) good essay-writing skills.

Students not enrolled on MSc Information Security must attend an interview with the Module Leader.
People and Security (COMP0056)

Description

Aims:
- Students will be able to specify usability criteria that a security mechanism has to meet to be workable for end-user groups and work contexts;
- Know the strengths and weaknesses of particular security mechanisms in practice, and hence be able to choose and configure mechanisms for best performance in a given organisational context;
- Be able to specify accompanying measures (policies, training, monitoring and ensuring compliance) that a user organisation needs to implement to ensure long-term security in practice;

Learning outcomes:
On successful completion of the module, a student will be able to:
1. apply their knowledge of human factors and behavioural economics to specify and implement workable and effective security solutions, and manage security behaviour;

Content:
Understanding Human Behaviour in Security:
- Systems thinking and design;
- Usability: Users, tasks and context;
- Performance and Workload;
- Productivity and performance vs risk and security;
Economics:
- Humans and Risk;
- Risk Biases and Decision-making;
- Friction and the Compliance Budget;
Authentication:
- Authentication tasks: enrolment, verification, recovery;
- Knowledge-based authentication: Passwords, phrases, PINs, graphical Authentication;
- Token-based authentication;
- Biometric authentication: physical and behavioural;
- Continuous authentication via devices, sensors, and biometrics;

Key information

Year: 2019/20
Credit value: 15 (150 study hours)
Delivery: UGM L7, Campus-based
Reading List: View on UCL website
Tutor: Dr Simon Parkin
Term: Term 1
Timetable: View on UCL website

Assessment

For more information about the department, programmes, relevant open days and to browse other modules, visit ucl.ac.uk
- Payment systems and transaction authentication;
  Access control:
  - Different access control models, organisational impact and user workload;
  Attacks and attackers (and how to counter them):
    - Types of attacks (Guessing, observation, capture and coercion);
    - Types of attackers: motivation, resources risk propensity;
    - Social engineering attacks;
    - Insider attacks;
  Identity:
    - Online identity vs identity in the physical world;
    - National identity vs socially constructed systems;
    - Digital footprints, shadows and superidentities;
    - Identity as currency;
  Privacy:
    - Data protection and user perception;
    - Delivering privacy: Privacy by Design, the PST model;
    - Surveillance, dataveillance and sousveillance online and in the physical world (CCTV);
  Trust:
    - Model of trust in online interaction;
    - Incentivising trustworthy behaviour;
    - Reputation systems and their application in online systems;
  Influencing user behaviour:
    - Security awareness, education and training;
    - User interface design and influencing techniques;
    - Values, attitudes, security culture and security behaviour;
    - Responsibility and communication;

**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 (i) knowledge of basic information security principles; and (ii) good essay-writing skills.

Students not enrolled on MSc Information Security must attend an interview with the Module Leader.