WM281-15 Behavioural Cyber Security

27/28

Department
WMG
Level
Undergraduate Level 2
Module leader
Harjinder Lallie
Credit value
15
Module duration
10 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Human-computer interaction (HCI) is concerned with designing interactions between human activities and the computational systems that support them, and with constructing interfaces to afford those interactions. Interaction between users and computational artefacts occurs at an interface that includes both software and hardware. Human behaviour should influence interface design and implementation of core functionality. For end-users, the interface is the system, meaning design in this domain must be interaction-focused and human-centred. It is therefore imperative that during the design phase of this human-computer interface cyber security component of human behaviour is addressed. One of the most significant challenges in the cyber domain is the transfer of meaning between the fully human agent, and the fully digital sub-system. Failure to correctly align human behaviour with computing sub-system behaviour has contributed to numerous, historic cyber security problems.

In addition, psychological traits and individual differences among computer system users can further explain vulnerabilities to cyber security attacks and crimes, as cognitive biases can make individuals more susceptible to exploitation by cyber criminals. Cyber security procedures and policies are prevalent countermeasures for protecting organisations from cybercrimes and security incidents, however, without considering human behaviours, implementing these countermeasures will remain to no effect or even become counterproductive.

Consequently, this module places the person at the centre of the cyber domain by addressing

issues of usability and human factors. As such, the focus is on trade-offs between usability and security on the one hand, and human psychology and human error on the other hand. Human vulnerabilities will be addressed in detail to build greater cyber resilience, and narrative around security awareness/training programmes and security culture will be also introduced for understanding broader, non-technical influences on security through minimising human related risks.

Module aims

1. To provide students with high levels of skills, knowledge, and competency around human factors (HFs) and human-computer interaction (HCI) research.
2. To provide students with the opportunity to contextualise and apply learning in the field of HCI by undertaking an independent usability assessment of an online system to address trade-offs with security using appropriate methodological and analytical techniques.
3. To provide students with in-depth knowledge of human psychology and human error to understand human traits and behaviours commonly exploited by malevolent actors.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The content of this module will be taught from a cyber security perspective, and will include:

- Background: development and scope of human factors; practical goals.
- User-centred design and testing.
- Usable security incl. trade-offs.
- Human factors and security.

Specifically, the module will cover:

- Cognitive hacking, incl. psychological levers used by cyber criminals.
- Human error and insider threat.
- Approaches and frameworks for changing behaviour.
- Nudging and persuasion towards better cyber security.
- Human capabilities and limitations.
- Cyber security culture and hygiene.

Learning outcomes

By the end of the module, students should be able to:

- Select, analyse and critically evaluate the different factors that are pertinent to the security and usability of secure systems in their contexts of use. [CITP 2.1.1., 2.1.2., 2.1.4.]
- Critically analyse complex trade-offs between usability and security in system design, including formulating strategies to optimize both aspects effectively. [CITP 2.2.2., 3.1.3.]
- Select, analyse and critically evaluate key concepts, theories and frameworks related to human factors in cyber security. [CITP 2.1.1., 3.1.3.]

- Analyse and critically evaluate the role of human factors in contributing to cyber security vulnerabilities and defences. [CITP 2.2.3.]
- Explain how relevant theories and frameworks related to human behaviour and decision-making can be applied to influence human behaviour in cyber security contexts. [CITP 2.1.2]

Indicative reading list

Reading lists can be found in Talis

Specific reading list for the module

Research element

Practical lab exercises use desk-based research approach.

Interdisciplinary

The module uses insights from Psychology and Sociology to understand usability issues, human behaviour, requirements gathering and innovation processes relevant for cyber security.

Subject specific skills

Designing and evaluating usable systems as they pertain to cyber security.
Applying different disciplinary perspectives to solve design and deployment challenges, and to plan for HFs in organisations.
Locating and summarising examples of recent controversy and progress in HFs, including initiating critical analysis.

Transferable skills

Researching literature.
Communication, critical thinking, and problem solving.
Time management.
Teamwork.
Competence in multi-disciplinary research.
Presenting to peers a critical evaluation of own research work.
Defending their own work to an audience of peers.

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Supervised practical classes	20 sessions of 1 hour (13%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Assessment component			
Security and usability trade-offs	70%	42 hours	Yes (extension)
Students will be asked to analyse the security and usability of a system focusing on trade-offs.			
Reassessment component			
Security and usability trade-offs			No
Students will be asked to analyse the security and usability of a system focusing on trade-offs.			
Assessment component			
Unseen, face to face, closed book test	30%	18 hours	No
Reassessment component			

	Weighting	Study time	Eligible for self-certification
Unseen, face to face, closed book test			No

Feedback on assessment

Written feedback for each assignment.
Verbal feedback during tutorial sessions.
Summative feedback on assignments.

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security