WM241-18 Human Behavior in Cyber Systems

23/24

Department
WMG
Level
Undergraduate Level 2
Module leader
Elzbieta Titis
Credit value
18
Module duration
30 weeks
Assessment
Multiple
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 and impaired brain health can make individuals more susceptible to exploitation by cyber criminals. Cyber security procedures and policies are prevalent countermeasures for protecting organizations from cybercrimes and security incidents, however, without considering human

behaviours, implementing these countermeasures will remain useless.

Consequently, this module places the person at the centre of the cyber domain by addressing the problematic of human factors in general and usable security in particular. 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 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:

- Foundations;
- 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.

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.

Learning outcomes

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

- Select and critically evaluate the usability criteria that security mechanisms must meet to be usable in their contexts of use.
- Apply techniques from interaction design and security engineering to design and evaluate secure systems.
- Analyse the relationship between user behaviour in digital space and cyber security consequences, including psychological traits and individual differences among computer system users that are commonly exploited by malevolent actors.

Indicative reading list

Rogers et al. (2007). Interaction Design: Beyond Human-Computer Interaction. Forth Edition. John Wiley and Sons.
Corradini (2020). Building a cybersecurity culture in organizations. How to Bridge the Gap Between People and Digital Technology (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing.
Thaler and Sunstein (2009). Nudge: Improving decisions about health, wealth, and happiness. Penguin Books Ltd.

View reading list on Talis Aspire

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

Knowledge of issues and problems in HCI.
Understanding of different disciplinary perspectives and ability to apply them to solve design and deployment challenges pertaining to cyber security.
Devising, planning, and executing requirements investigations and system evaluation, and presenting findings in a clear and effective manner.
Demonstrating awareness of current areas of research in human factors by locating and summarising examples of recent controversy and progress.

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
Supervised practical classes	18 sessions of 2 hours 30 minutes (25%)
Private study	63 hours (35%)
Assessment	72 hours (40%)
Total	180 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 A3

	Weighting	Study time	Eligible for self-certification
Security and usability trade-offs	50%	36 hours	Yes (extension)

In this coursework students will be asked to analyse the security and usability of a system based on a security-usability threat model by Kainda et al. (2010). To do so, they will employ usage scenarios and threat scenarios to understand and identify both system and external elements that are threats to a system's usability, security, or both. They will then offer recommendations to redesign the system according to usability heuristics for user interface design followed by addressing subsequent security consequences.

A critical essay on a given topic	50%	36 hours	Yes (extension)

Students will be asked to produce a portfolio of research papers discussed in the class and write a critical essay on one topic from the portfolio.

	Weighting	Study time	Eligible for self-certification

There will be three reading sessions each term (six total) and students will be expected to come to class prepared each time to discuss in groups the readings and respond to the questions posed by the module tutor and their colleagues during the student-led reading discussions. Individually students will create the portfolio constituting a short overview of the readings and a summary of what was discussed, including critical appraisal of the literature, research gaps and avenues for future research.

They will then be asked to choose one topic from the portfolio to engage in academic debates and research happening in the subject area.

Assessment group R1

	Weighting	Study time	Eligible for self-certification
Reassessment assignment	100%		Yes (extension)

For the purpose of the resit question, students will write an individual report comprised of a) usability evaluation of a given case study, including list of all the good features and usability problems discovered, a brief explanation for each feature/problem mapped to Nielsen’s heuristics, and improvement suggestions, followed by b) critical discussion on defensive function of the design in terms of guiding users’ activity online to keep them safe from choosing something they don't want, including considerations for avoiding cyber security threats.

Feedback on assessment

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

Availability

Courses

This module is Core for:

- Year 2 of UWMA-H651 Undergraduate Cyber Security