MODULE **DESCRIPTOR**

MODULE TITLE	Advanced Topics in IT Security		
MODULE CODE	CO4510 (L7)	CREDIT VALUE	20 credits / 10 ECTS
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

The IT Security specialist is faced with constant changes in risks derived from emerging technology and new ways to use established technology. The purpose of this module is not to teach details but to expose students to a range of current security-related topics, and help them to develop the confidence to find and interpret relevant literature and to apply it in practice. There is an emphasis on understanding, explaining and evaluating published material, about security issues affecting real systems and about mechanisms to prevent and detect them.

It will explore the human aspect of IT security, including threats such as social engineering, and insider threat, identification and authentication issues such as password and security question issues. Students will be exposed to a holistic perspective of IT security which requires not only technical mechanisms to counter risks, but also organizational and physical mechanisms such as compliance to security policies. It will develop the students' awareness of security and privacy issues (e.g., the exposure of personal data online) in the use of IT at work and at home.

A key feature of the module will be the study of selected topics in areas such as security in cloud computing, mobile security, and security in social media, illustrated by recent examples from practice. There will be an emphasis on practical realities with the use of visiting speakers.

This module will also expose students to the practice of ethical analysis in scenarios emerging from security management and/or security research. It will develop the students' technical writing and presentation skills, and also students’ argumentation skills particularly in discussion groups.

The aims of the module are:

- To develop the students' ability to find, interpret, explain and evaluate security-related articles.
- To examine the ethical, organizational and social context of security issues.
- To explore the application of IT security to real situations.
- To discuss critically interesting issues in security research and practice.
- To develop the students’ skills through discussion and investigation.

MODULE **CONTENT**

Human factors in system security
Social engineering, Insider Threat, and other human-related threats to security. Social networking, identification and authentication issues related to humans. Password issues. Personal information and implications to security and privacy. Different authentication methods.

Managing Security
Risks and countermeasures. Technical, organizational, and physical aspect of security management. Policies in practice. Auditing, logging, training, incident response.

Ethics in Security
Principles and practical guidelines for ethical analysis.

Contemporary Issues in security
A range of issues will be discussed depending on topicality, availability of visiting speakers, practical implications in commercial situations, and their ability to generate discussion. Topics may be drawn from any aspect of IT security with implications for management of secure IT systems, such as security in cloud

computing, patch management, attack trends, emerging threats, mobile security, social engineering penetration testing, forensics in security incident response, effectiveness of security mechanisms, new practices (e.g., BYOD) and their security implications, security and privacy in social networks.

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1. Evaluate approaches to the management of IT security
2. Explain and analyse legal, ethical and social issues relevant to information security
3. Investigate, summarise and review the most relevant topics in IT security
4. Apply ideas from research and current practice to analyse and solve IT security problems

TEACHING METHODS

Lectures are used to summarise key issues and relevant technology and for visiting speakers to present current research or practice. Tutorials will be used to complement lectures with in-class reading, analysis of scenarios, experiments, and discussion to ensure the students acquire the technical background and the ability to critically evaluate published material.

Students are likely to come from a variety of backgrounds, so directed reading will also be used to help them build on their previous study in computing to understand the underlying technological context of the issues explored.

An on-line discussion group will be used to promote discussion on topics that students are investigating. Students are expected to work independently or in small teams to read around the subject and prepare summaries and critiques of published papers, which will be presented on the discussion group to allow rapid feedback from other students. To encourage participation, individual contributions to discussion will be assessed.

The examination and the article to be produced by the students will assess the students' ability to apply their understanding of the issues to unseen situations, and to summarise or explain published material. For the article, students are expected to work independently to read around the subject and prepare summaries and critiques of published papers, as well as review contemporary topics in IT security, This will also ensure that students participate fully in preparation and discussion throughout the module.

ASSESSMENT METHODS

This module is assessed through an Article (60%) and an examination (40%).