St. Pölten University of Applied Sciences

/computer science & security

/fh/// st.pölten

Computing Module

Academic Year 2020/21
Summer Semester

Language of Instruction: English

Last update: 22 October 2020
www.fhstp.ac.at

St. Pölten University of Applied Sciences GmbH, Matthias Corvinus-Straße 15, 3100 St. Pölten, T: +43 (2742) 313 228, F: +43 (2742) 313 228-339, E: csc@fhstp.ac.at, I: www.fhstp.ac.at

Computing Module

Summer Semester 2021

Subject Code	Subject	Sem.	ECTS Credits
MCS	Computer Science – Data Science (ILV)	2	5
MCS	Legal Aspects of Research (ILV)	2	2
MCS	Research Ethics (ILV)	2	1
MCS	Sources of Innovation (ILV)	2	2
MCS	Systematic Innovation (ILV)	2	3
MCS	Writing in technical disciplines and research (ILV)	2	5
MIS	Industrial Security and Safety	4	5
MCR	Application Security and Pentesting (ILV)	2	5
MCR	Audit Interview Skills (ILV)	2	1
MCR	Digital Forensics and Incident Handling (ILV)	2	4
MCR	Dual Project: Risk Management (PT)	2	4
MCR	Mentoring: Risk Management (SE)	2	1
MCR	Professional Report Writing (ILV)	2	1
MCR	Secure Networks (ILV)	2	5
MCR	Security Auditing (ILV)	2	4
MCR	Threat Modeling & Information Sharing (ILV)	2	5
-	German Language and Austrian Culture	-	6
	TOTAL		**59**

PLEASE NOTE: All courses are subject to changes until the beginning of the semester!

Detailed course description:

Computer Science – Data Science (5 ECTS credits)

Content:
The offered course with a scope of 5 ECTS covers important in-depth content of data analysis for the chosen field of study in coordination with the supervisor.

Important topics include (but are not limited to):
Preparation & Preprocessing:
• Sample design, planning of statistical data collection, data selection
• Data types, measurement scales, dissimilarity measures, similarity measures, sequence relations, text relations
• Understanding of data and data quality (+metadata), metadata management, knowledge modelling, knowledge representation
• Feature generation
• Error types, normalisation, filtering, transformation, consolidation
Analysis methods:
• Correlation, regression vs. classification: generative models, discriminative models, probabilistic and non-probabilistic models, non-parametric models, clustering, text mining, sentiment analysis, anomaly detection
Follow-up:
• Evaluation, documentation, critical reflection of results

Legal Aspects of Research (2 ECTS credits)

Content:
Intellectual Property & Competition Law
• Exploitation of rights in the national and international environment
• Trade with rights, patents and licenses with special regard to Digital Rights Management and Dual Licensing, Open Source, Open Data, Open Innovation
Data Protection
• Data protection, privacy and freedom of information,
• EU General Data Protection Regulation and other relevant laws
• Rights and obligations of businesses & consumers
General Data Protection Regulation and other relevant laws

Research Ethics (1 ECTS credits)

Content:
• Introduction to ethics, basic concepts of ethics (legitimacy, morality, justice, trust, human dignity, values)
• Ethical thinking and its importance for IT, special problems of modern information ethics, hacker ethics, ...
• Distinction between ethics of principles vs. utilitarian approaches, examples of problems in the field of artificial intelligence, ...
• Ethics and research, examples from science
• Human rights as an anchor of ethics, intersection of ethics and law

Sources of Innovation (2 ECTS credits)

Content:
This course provides an introduction to the sources of innovation. Students will get an overview of the different internal and external knowledge sources for innovation and of how to use selected sources effectively. In this context, open and closed innovation approaches will be discussed. A special focus is on the interaction of innovation, exploration, use and search as well as the growing importance of efficient search approaches across distributed innovation sources. Another important aspect is the role of users and user communities as sources of innovation. Finally, concrete applications for the generation of inputs for innovation processes of companies, such as the lead user method or crowdsourcing, are examined in more detail.

Systematic Innovation (3 ECTS credits)

Content:
Introduction to the theory of inventive problem solving (TRIZ)
• History, Objectives, Terms
• Basic principles, theses of G.S. Altschuller
• Method overview
Selected TRIZ methods for the different phases of an inventive problem solution:
• Define and analyze the development problem:
• (S-curve analysis, 9-field thinking, function and object modeling, ideality)
• Generate solutions for contradictions
• Evaluate ideas, work them out and prioritise solutions

Writing in technical disciplines and research (5 ECTS credits)

Content:

The adequate use of language plays an increasingly important role, especially in the technical field. Students have to practice how to express themselves comprehensibly in writing. Furthermore, self-reflection and editorial work in small groups are also trained in this course. Students will write their own texts with the main focus on comprehensibility beyond the realm of technical language. Spelling and grammar as well as formal design and stylistics will also be taken into account.

• Text comprehension (technical texts)
• Explanation and description of technical processes
• Short presentations
• Case studies
• Expansion of vocabulary, especially in the field of technology
• Improvement of writing and speaking skills through working on selected technical texts and through suitable simulations of specific situations

Industrial Security and Safety (5 ECTS credits)

Content:

- Definition Industrial Control System (ICS) Security
- Security goals Industrial Security
- Understanding of SCADA-/DCS architectures
- ICS security risks and threats
- Security requirements of the industrial security sector
- Difference Industrial Security vs. IT Security
- Overview ICS network protocols
- Known ICS threats and analysis
- Critical Infrastructure Protection Standards

Key aspects of the design, implementation and analysis of safety-critical computer systems are addressed. This includes special development methods such as Model Checking. The course also addresses areas of application of safety-critical systems, analysis of requirements and identification of potential hazards (hazard analysis), analysis of system design (fault tolerance design) and methods for the proof of safety (reliability modeling).

Application Security and Pentesting (5 ECTS credits)

Content:

- Basics of application security and penetration testing
- Establishment of a suitable hacking lab
- Procedures of a professional penetration tester
- Frameworks, tools and methods for penetration testing
- OWASP Top 10 / OWASP Testing Guides

Audit Interview Skills (1 ECTS credits)

Content:

- Basics of question technique
- Conducting audit interviews

Digital Forensics and Incident Handling (4 ECTS credits)

Content:
Overview of practices and procedures in digital forensics and incident handling
- integrity
- chain of custody
- order of volatility
- Forensic process
    - o Identification
    - o Digital preservation of evidence (acquisition)
    - o Analysis
    - o Reporting
- profiling

Standards:
- ISO/IEC 27037:2012
- ISO/IEC 27041:2015
- ISO/IEC 27042:2015
- ISO/IEC 27043:2015
- ISO/IEC 27050:2016+

Incident response and digital forensics with focus on company processes

Incident handling process (preparation, identification, containment, remediation, recovery)

Log Analysis for Incident Responders
file system forensics
- NTFS
- ext

- iOS
- android

live forensics
- Monitoring tools for recording file system activity
- Tracing tools for API or Native/System calls
- Integration of network traffic into the forensic process

Application forensics (databases of concrete applications), e.g:
- browser data
- User communication (instant messaging, e-mail)

Dual Project: Risk Management (4 ECTS credits)

Ahead of the dual phase, students are taught the fundamentals of project management and requirements analysis. Within the framework of a project at an organisation, students deepen their knowledge and application competence in the technical or organisational area of risk management. At regular intervals, mandatory mentoring units (remote or physical) take place to continuously measure and promote the students' learning success.

Mentoring: Risk Management (1 ECTS credits)

Content:
As an accompanying activity of the dual project, mentoring by the FH takes place in small groups. This is to ensure that students are individually supported and that the dual project achieves the desired learning effect.

Professional Report Writing (1 ECTS credits)

Content:
- Target group analysis
- Types of reports
- Structuring of reports
- Joint preparation of reports
- Targeted writing (e.g.: forensic expert opinion for court)

Secure Networks (5 ECTS credits)

Content:
- WLAN: basic mechanisms (congestion avoidance, virtual carrier sensing, 802.11n, 802.11ac, bridging, hotspot solutions,...)

- Difference between security requirements and LANs
- Authentication infrastructures and their practical implementation (RADIUS and TACACS+).
- Protocol 802.1X and various forms of EAP authentication (PEAP, EAP-TLS, EAP-FAST,...).
- Integration of an enterprise PKI and implementation in a typical Active Directory infrastructure.

Security Auditing (4 ECTS credits)

Content:

- Tasks and function of an auditor
- Internal control systems (structure, ...)
- Audit process:
  - defining the audit objectives and scope
  - audit planning
  - audit execution
  - reporting
- Important standards and good practices

Threat Modeling & Information Sharing (5 ECTS credits)

Content:

Threat modeling

- Fundamentals of Modeling
  - o Properties of models
  - o Information theory (syntax, semantics, pragmatics)
  - o Abstraction
- Aspects of threat modelling
  - o Actors and motivation
  - o Tactics, Techniques and Procedures (TTPs)
  - o Observables or compromise indicators (IoCs)
- Common threat modelling techniques and models, including
  - o Attack Trees and Attack-Defense Trees
  - o STRIDE and PASTA
  - o Kill Chains
- Attack Patterns and Vulnerabilities
  - o Mapping of attack techniques and attack phases in the environment of IT systems (CAPEC, ATT&CK, etc.)
  - o Modelling and quantification of software weak points and vulnerabilities (CVSS, CWE)
- Visualization and creative techniques, among others:
  - o Persona non Grata
  - o Security Cards
  - o Gamification and Serious Games
- Integrated threat modeling
  - o Interfaces to organizational processes

o Interaction with the operational risk analysis

- Exchange of information at organisational and technical level
- Threat Intelligence: Collection, Evaluation, Analysis, Structuring
  - o Strategic (trends and risks)
  - o Tactical (Indicators of Compromise)
  - o Operational (technical approaches)
- Vocabularies and Formats
  - o STIX, TAXII, CybOX
- In-house preparation and communication
- Inter-organizational exchange of threat information

Computer Emergency Response Teams (CERTs)

German Language and Austrian Culture (6 ECTS credits)

Content:

Students train their speaking, writing, reading and listening skills in the German language. Furthermore, they learn about Austrian culture, e.g. history and geography, the political system, festivals, customs and traditions, food.

The course is offered at two different levels, Beginners and Advanced. The students' level of German is ascertained in the first session.