MODULE HANDBOOK

Bachelor of Science

Bachelor Cyber Security (FS-BACSE)

180 ECTS

Distance Learning

INTERNATIONAL
UNIVERSITY OF
APPLIED SCIENCES

Classification: Undergraduate

Contents

---

3. Semester

---

4. Semester

---

5. Semester

2021-05-01

1. Semester

Operating Systems, Computer Networks, and Distributed Systems

Module Code: DLBIBRVS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Paul Libbrecht (Operating Systems, Computer Networks, and Distributed Systems)

Contributing Courses to Module

- Operating Systems, Computer Networks, and Distributed Systems (DLBIBRVS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Operating systems
- Computer networks
- Distributed systems
- Mobile computing

Learning Outcomes

Operating Systems, Computer Networks, and Distributed Systems

On successful completion, students will be able to

- explain the basic functions of operating systems.
- compare different operating systems.
- explain and compare the OSI reference model and the TCP/IP protocol stack.
- explain the most important IP-based protocols and services and their application.
- explain and compare different architectures for distributed systems.
- explain and compare the main mobile communication networks.
- explain basic challenges of the security on the Internet and their solutions.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Operating Systems, Computer Networks, and Distributed Systems

Course Code: DLBIBRVS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Operating systems are a central component of computers and provide their basic functions. To an increasing extent, however, computers do not stand alone, but are integrated into networks within which data and functions of other computer systems can be accessed. This enables distributed systems in which data and functions are systematically assigned to different computers in order to perform jointly defined tasks. While in the past, the various computers were stationary, many mobile computers are now also in use, which leads to completely new application scenarios in both private and business contexts.

Course Outcomes

On successful completion, students will be able to

- explain the basic functions of operating systems.
- compare different operating systems.
- explain and compare the OSI reference model and the TCP/IP protocol stack.
- explain the most important IP-based protocols and services and their application.
- explain and compare different architectures for distributed systems.
- explain and compare the main mobile communication networks.
- explain basic challenges of the security on the Internet and their solutions.

Contents

1. Foundations of Operating Systems
   - 1.1 Basic Structure of Computer Systems
   - 1.2 File Systems
   - 1.3 Memory Management
   - 1.4 Processes and Threads
2. Common Operating Systems
   - 2.1 Basic Concepts: Windows
   - 2.2 Basic Concepts: Unix and Linux
   - 2.3 Basic Concepts: Apple Operating Systems
   - 2.4 Mobile Operating Systems

3. Computer Networks
   - 3.1 Principles of Data Transmission
   - 3.2 The OSI Reference Model
   - 3.3 Network Topologies

4. TCP/IP And Internet
   - 4.1 Historical background
   - 4.2 TCP/IP Protocol Stack
   - 4.3 Selected IP-Based Protocols and Services
   - 4.4 Online Security

5. Architectures of Distributed Systems
   - 5.1 Client-Server Systems and Distributed Applications
   - 5.2 Basic Concepts of Distributed Systems: Concurrency, Semaphores, Deadlock
   - 5.3 Communication in Distributed Systems
   - 5.4 Service Orientation: SOA, Web Services and Microservices
   - 5.5 Cloud Applications
   - 5.6 Transactions in Distributed Systems
   - 5.7 High-Performance Computing Cluster

6. Mobile Computing
   - 6.1 Basics, Techniques and Protocols for Mobile Computing
   - 6.2 Mobile Internet and its Applications
   - 6.3 Mobile Communication Networks
   - 6.4 Security And Data Protection in Mobile Systems

Literature

Compulsory Reading

Further Reading

- Baun, C. (2020): Operating Systems /Betriebsysteme (bilingual edition). Springer, London.
- Cowley, J. (2013): Communications and Networking, An Introduction. Springer, London.
- Grigorik, I. (2013): High Performance Browser Networking. (URL: hpbn.co [last accessed 2020-08-20]).
- O'Regan, G. (2016): History of Operating Systems. In: Introduction to the History of Computing. Undergraduate Topics in Computer Science. Springer International Publishing, Cham.
- Parsons, J. J./Oja, D. (2017): Computer Concepts 2018. Cengage Learning, Boston, MA.
- Richardson, L./Ruby, S. (2007): RESTful Web Services. (URL: http://restfulwebapis.org/RESTful_Web_Services/ [last accessed 2020-08-20]).

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBIBRVS01_E

Introduction to Data Protection and Cyber Security

Module Code: DLBCSIDPITS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Ralf Kneuper (Introduction to Data Protection and Cyber Security)

Contributing Courses to Module

- Introduction to Data Protection and Cyber Security (DLBCSIDPITS01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Fundamentals of IT Security
- Data Protection
- IT Security Management
- Network and Communication Security

Learning Outcomes

Introduction to Data Protection and Cyber Security

On successful completion, students will be able to

- explain the terms and concepts of IT security and know the typical procedures and techniques which exist in each area.
- cite the legal regulations on data protection and explain their implementation.
- discuss in-depth IT security management and suitable measures for implementation.
- use their overview knowledge of activities and strategies for IT security in software and system development.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field(s) of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field(s).

Introduction to Data Protection and Cyber Security

Course Code: DLBCSIDPITS01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, the students are familiarized with important concepts from the field of IT security. Basic terms are introduced and discussed, and typical application fields, areas of IT security application, and typical procedures and techniques are introduced and described.

Course Outcomes

On successful completion, students will be able to

- explain the terms and concepts of IT security and know the typical procedures and techniques which exist in each area.
- cite the legal regulations on data protection and explain their implementation.
- discuss in-depth IT security management and suitable measures for implementation.
- use their overview knowledge of activities and strategies for IT security in software and system development.

Contents

1. Fundamentals of Data Protection and IT Security
   - 1.1 Conceptual Bases, Protection Goals
   - 1.2 Attacks and Threats
   - 1.3 Security Strategy
   - 1.4 Legal Regulations (IT Security Law, etc.)

2. Data Protection
   - 2.1 Data Protection as a Personal Right
   - 2.2 Basic Principles of Data Protection (Data Economy, Consent, etc.)
   - 2.3 Federal Data Protection Act
   - 2.4 EU Data Protection Basic Regulation
   - 2.5 Further International Regulations on Data Protection (EU, USA)
   - 2.6 Cross-Border Data Flow, e.g., in Cloud Computing
   - 2.7 Data Protection in Everyday Life (Search Engines, Anonymous Surfing, Social Networks, Use of Mobile Devices and Data Carriers, etc.)

3. Basic Functions of IT Security and Their Implementation
   - 3.1 Identification and Authentication (Knowledge/Biometrics)
   - 3.2 Rights Management
   - 3.3 Rights Check
   - 3.4 Preservation of Evidence
   - 3.5 Reprocessing
   - 3.6 Guarantee of Functionality

4. IT Security Management
   - 4.1 IT Basic Protection (Basic Protection Catalogues, Protection Needs Analysis, etc.)
   - 4.2 Series of Standards ISO 2700x

5. IT Security Management in Everyday Life
   - 5.1 Password Management
   - 5.2 Data Backup
   - 5.3 Email Security
   - 5.4 Protection Against Viruses and Other Pests
   - 5.5 Protection Against Social Engineering Attacks

6. Network and Communication Security
   - 6.1 Firewall Technology
   - 6.2 Network Separation
   - 6.3 Security in WLAN, Mobile Networks (UMTS/LTE), Bluetooth, and NFC

7. IT Security in the Development of Software and Systems
   - 7.1 Protection of the Development Environment
   - 7.2 Secure Development (Protection Against SQL Injection, XSS, Filtering of Input Data)
   - 7.3 Common Criteria

Literature

Compulsory Reading

Further Reading

- Eckert, C. (2014): IT-Sicherheit. Konzepte – Verfahren – Protokolle. 9. Auflage, De Gruyter, München.
- Poguntke, W. (2013): Basiswissen IT-Sicherheit. Das Wichtigste für den Schutz von Systemen & Daten. 3. Auflage, W3l, Dortmund.
- Witt, B. C. (2010): Datenschutz kompakt und verständlich. 2. Auflage, Vieweg+Teubner, Wiesbaden.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSIDPITS01

Mathematics: Analysis

Module Code: DLBDSMFC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Timo Heinisch (Mathematics: Analysis)

Contributing Courses to Module

- Mathematics: Analysis (DLBDSMFC01)

Module Exam Type

Module Exam	Split Exam
Study Format: Berufsbegleitendes Studium Exam, 90 Minutes Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Sequences and series
- Functions & reverse functions
- differential calculus
- integral calculus

Learning Outcomes

Mathematics: Analysis

On successful completion, students will be able to

- summarize the basic concepts of analysis.
- illustrate the terms "consequences" and "series".
- explain the concept of function and to understand the concept of the inverse function.
- explain basic statements of the differential and integral calculus.
- explain the relationship between differentiation and integration.
- master the derivation of higher-dimensional functions.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field of Methods	All Bachelor Programmes in the IT & Technology fields

Mathematics: Analysis

Course Code: DLBDSMFC01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Analysis is one of the essential basic subjects of mathematics. Originally developed to be able to formulate and solve problems of classical mechanics mathematically, in its present rigorous form it has become indispensable in numerous applications in the natural sciences and technology. This module aims to introduce the basic hand tool of differential and integral calculus and to explain their mutual interrelations. In addition, the differential calculus is generalized to multidimensional spaces.

Course Outcomes

On successful completion, students will be able to

- summarize the basic concepts of analysis.
- illustrate the terms "consequences" and "series".
- explain the concept of function and to understand the concept of the inverse function.
- explain basic statements of the differential and integral calculus.
- explain the relationship between differentiation and integration.
- master the derivation of higher-dimensional functions.

Contents

1. Sequences and series
   - 1.1 Sequences and series
   - 1.2 Convergence of infinite series
   - 1.3 power series
2. Functions and reverse functions
   - 2.1 Continuous functions
   - 2.2 Exponential and logarithm function
   - 2.3 Trigonometric functions and their inverse functions
3. Differential calculus
   - 3.1 Derivatives and higher derivatives
   - 3.2 curve discussion
   - 3.3 Rules (chain rule, product rule, quotient rule ...)
   - 3.4 Taylor Rows

4. Integral calculus
   - 4.1 The Riemann Integral
   - 4.2 Specific and indefinite integrals
   - 4.3 The fundamental theorem of differential and integral calculus
   - 4.4 Volumes and shells of rotary bodies
   - 4.5 Paths and lengths

5. Differential calculus in the Rn
   - 5.1 Partial Derivation
   - 5.2 Total Derivation
   - 5.3 Gradients of vector-valued functions and matrices

Literature

Compulsory Reading

Further Reading

- Arens, T. et al. (2013): Basic knowledge of mathematics studies. Analysis and Linear Algebra with Cross Connections. Springer, Berlin/Heidelberg.
- Boas, M. L. (2006): Mathematical methods in the physical sciences. Third edition. Wiley. Hoboken, NJ.
- Deisenroth, M. P./Faisal, A./Ong C.-S.: Math for ML. Cambridge University Press.
- Heuser, H. (2009): Textbook of Analysis. Vieweg + Teubner (studies). Wiesbaden.
- Modler, F./Kreh, M. (2014): Tutorial Analysis 1 and Linear Algebra 1. Mathematics explained and commented by students for students. 3rd edition, Springer Spektrum, Berlin/Heidelberg.
- Papula, L. (2014): Mathematics for engineers and scientists. Vol. 1: A textbook and workbook for basic studies. Springer Vieweg, Wiesbaden.

Study Format Berufsbegleitendes Studium

Study Format	Course Type
Berufsbegleitendes Studium	Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☑ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☑ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Introduction to Academic Work

Module Code: DLBCSIAW

Module Type	Admission Requirements	Study Level	CP	Student Workload
s. Curriculum/see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	
s. Curriculum/see curriculum	Minimum 1 semester	WiSe/SoSe	

Module Coordinator

Prof. Dr. Maya Stagge (Introduction to Academic Work)

Contributing Courses to Module

- Introduction to Academic Work (DLBCSIAW01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Workbook	

Weight of Module

s. Curriculum/see curriculum

Module Contents

- Scientific Theoretical Foundations and Research Paradigms
- Application of Good Scientific Practice
- Methodology
- Librarianship: Structure, Use, and Literature Management
- Forms of Scientific Work at IUBH

Learning Outcomes

Introduction to Academic Work

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,/On successful completion, students will be able to

- understand and apply formal criteria of a scientific work.
- distinguish basic research methods and identify criteria of good scientific practice.
- describe central scientific theoretical basics and research paradigms and their effects on scientific research results.
- use literature databases, literature administration programs, and other library structures properly; avoid plagiarism; and apply citation styles correctly.
- apply the evidence criteria to scientific texts.
- define a research topic and derive a structure for scientific texts.
- compile a list of literature, illustrations, tables, and abbreviations for scientific texts.
- understand and distinguish between the different forms of scientific work at IUBH.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field of Methods	All Bachelor Programmes in the Business & Management field

Introduction to Academic Work

Course Code: DLBCSIAW01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The application of good scientific practice is one of the basic academic qualifications that should be acquired while studying. This course deals with the distinction between everyday knowledge and science. This requires a deeper understanding of the theory of science, as well as the knowledge of basic research methods and instruments for writing scientific texts. The students therefore gain initial insight into academic research and are introduced to the basic knowledge that will help them in the future to produce scientific papers. In addition, the students receive an overview of the different IUBH examination forms and insight into their requirements and implementation.

Course Outcomes

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,/On successful completion, students will be able to

- understand and apply formal criteria of a scientific work.
- distinguish basic research methods and identify criteria of good scientific practice.
- describe central scientific theoretical basics and research paradigms and their effects on scientific research results.
- use literature databases, literature administration programs, and other library structures properly; avoid plagiarism; and apply citation styles correctly.
- apply the evidence criteria to scientific texts.
- define a research topic and derive a structure for scientific texts.
- compile a list of literature, illustrations, tables, and abbreviations for scientific texts.
- understand and distinguish between the different forms of scientific work at IUBH.

Contents

1. Theory of Science
   - 1.1 Introduction to Science and Research
   - 1.2 Research Paradigms
   - 1.3 Fundamental Research Decisions
   - 1.4 Effects of Scientific Paradigms on Research Design

2. Application of Good Scientific Practice
   - 2.1 Research Ethics
   - 2.2 Evidence Teaching
   - 2.3 Data Protection and Affidavit
   - 2.4 Orthography and Shape
   - 2.5 Identification and Delimitation of Topics
   - 2.6 Research Questions and Structure

3. Research Methods
   - 3.1 Empirical Research
   - 3.2 Literature and Reviews
   - 3.3 Quantitative Data Collection
   - 3.4 Qualitative Data Collection
   - 3.5 Mix of Methods
   - 3.6 Critique of Methods and Self-Reflection

4. Librarianship: Structure, Use, and Literature Management
   - 4.1 Plagiarism Prevention
   - 4.2 Database Research
   - 4.3 Literature Administration
   - 4.4 4.4 Citation and Author Guidelines
   - 4.5 4.5 Bibliography

5. Scientific Work at the IUBH – Research Essay

6. Scientific Work at the IUBH - Project Report

7. Scientific Work at the IUBH - Case Study

8. Scientific Work at the IUBH - Bachelor Thesis

9. Scientific Work at the IUBH – Oral Assignment

10. Scientific Work at the IUBH – Oral Project Report

11. Scientific Work at the IUBH - Colloquium

12. Scientific Work at the IUBH - Portfolio

13. Scientific Work at the IUBH - Exam

Literature
Compulsory Reading
Further Reading ▪ Bortz, J./Döring, N. (2012): Forschungsmethoden und Evaluation. Für Human- und Sozialwissenschaftler. 5. Auflage, Springer Medizin Verlag, Heidelberg. ▪ Braunecker, C. (2016): How to do Empirie, how to do SPSS – eine Gebrauchsanleitung. Facultas Verlags- und Buchhandels AG, Wien. ▪ Engelen, E.M. et al. (2010): Heureka – Evidenzkriterien in den Wissenschaften, ein Kompendium für den interdisziplinären Gebrauch. Spektrum akademischer Verlag, Heidelberg. ▪ Flick, U. et al. (2012): Handbuch Qualitative Sozialforschung. Grundlagen, Konzepte, Methoden und Anwendungen. 3. Auflage, Beltz Verlag, Weinheim. ▪ Hug, T./Poscheschnik, G. (2015): Empirisch Forschen, 2. Auflage, Verlag Huter & Roth KG, Wien. ▪ Hussy, W. et al. (2013): Forschungsmethoden in Psychologie und Sozialwissenschaften. 2. Auflage, Springer Medizin Verlag, Heidelberg.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Workbook

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Introduction to Programming with Python

Module Code: DLBDSIPWP

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr.-Ing. Reza Shahbazfar (Introduction to Programming with Python)

Contributing Courses to Module

- Introduction to Programming with Python (DLBDSIPWP01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Python as a programming language for data science
- Variables and built-in datatypes
- Statements and functions
- Error and exception handling
- Important Python data science modules

Learning Outcomes

Introduction to Programming with Python

On successful completion, students will be able to

- use fundamental Python syntax.
- recollect common elementary data types.
- recognize foundational programming concepts and their realization in Python.
- understand error handling and logging.
- create working programs.
- list the most important libraries and packages for data science.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field(s) of Data Science & Artificial Intelligence.	All Bachelor Programmes in the IT & Technology field(s).

Introduction to Programming with Python

Course Code: DLBDSIPWP01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course provides students with a foundational understanding of the Python programming language. Following an introductory exposition to the importance of Python for data science-related programming tasks, students will be acquainted with fundamental programming concepts like variables, data types, and statements. Building on this basis, the important notion of a function is explained and errors, exception handling, and logging are explicated. The course concludes with an overview of the most widely-used library packages for data science.

Course Outcomes

On successful completion, students will be able to

- use fundamental Python syntax.
- recollect common elementary data types.
- recognize foundational programming concepts and their realization in Python.
- understand error handling and logging.
- create working programs.
- list the most important libraries and packages for data science.

Contents

1. Introduction
   - 1.1 Why Python?
   - 1.2 Obtaining and installing Python
   - 1.3 The Python interpreter , IPython, and Jupyter
2. Variables and Data Types
   - 2.1 Variables and value assignment
   - 2.2 Numbers
   - 2.3 Strings
   - 2.4 Collections
   - 2.5 Files

3. Statements
   - 3.1 Assignment, expressions, and print
   - 3.2 Conditional statements
   - 3.3 Loops
   - 3.4 Iterators and comprehensions

4. Functions
   - 4.1 Function declaration
   - 4.2 Scope
   - 4.3 Arguments

5. Errors and Exceptions
   - 5.1 Errors
   - 5.2 Exception handling
   - 5.3 Logs

6. Modules and Packages
   - 6.1 Usage
   - 6.2 Namespaces
   - 6.3 Documentation
   - 6.4 Popular data science packages

Literature

Compulsory Reading

Further Reading

- Barry, P. (2016): Head first Python: A brain-friendly guide. 2nd ed., O'Reilly, Sebastopol, CA.
- Lubanovic, B. (2019): Introducing Python. 2nd ed., O'Reilly, Sebastopol, CA.
- Lutz, M. (2013): Learning Python. 5th ed., O'Reilly, Sebastopol, CA.
- Matthes, E. (2019): Python crash course: A hands-on, project-based introduction to programming. 2nd ed., No Starch Press, San Francisco, CA.
- Ramalho, L. (2015): Fluent Python: Clear, concise, and effective programming. O'Reilly, Sebastopol, CA.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Statistics: Probability and Descriptive Statistics

Module Code: DLBDSSPDS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Dr. Stefan Stöckl (Statistics: Probability and Descriptive Statistics)

Contributing Courses to Module

- Statistics: Probability and Descriptive Statistics (DLBDSSPDS01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Probability
- Random variables
- Joint distributions
- Expectation and variance
- Inequalities and limit theorems

Learning Outcomes

Statistics: Probability and Descriptive Statistics

On successful completion, students will be able to

- define probability, random variable, and probability distribution.
- understand the concept of Bayesian statistics.
- grasp the definition of joint and marginal distributions.
- calculate expectation values and higher moments.
- comprehend important inequality equations and limit theorems.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the field of Methods	All Bachelor Programmes in the Business & Management fields

Statistics: Probability and Descriptive Statistics

Course Code: DLBDSSPDS01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Statistical description and analysis are the foundations for data-driven analysis and prediction methods. This course introduces the fundamentals, beginning with a formal definition of probabilities and introduction to the concepts underlying Bayesian statistics.Random variables and probability density distributions are then discussed, as well as the concept of joint and marginal distributions. The importance of various discrete and continuous distributions and their applications is stressed.Characterizing distributions is an important aspect of describing the behavior of probability distributions. Students are familiarized with expectation values, variance, and covariance. The concepts of algebraic and central moments and moment-generating functions complement the characterization of probability distributions.Finally, this course focuses on important inequalities and limit theorems such as the law of large numbers or the central limit theorem.

Course Outcomes

On successful completion, students will be able to

- define probability, random variable, and probability distribution.
- understand the concept of Bayesian statistics.
- grasp the definition of joint and marginal distributions.
- calculate expectation values and higher moments.
- comprehend important inequality equations and limit theorems.

Contents

1. Probability
   - 1.1 Definitions
   - 1.2 Independent events
   - 1.3 Conditional probability
   - 1.4 Bayesian statistics
2. Random Variables
   - 2.1 Random Variables
   - 2.2 Distribution functions and probability mass functions
   - 2.3 Important discrete probability distributions
   - 2.4 Important continous probability distributions

3. Joint Distributions
   - 3.1 Joint distributions
   - 3.2 Marginal distributions
   - 3.3 Independent random variables
   - 3.4 Conditional distributions

4. Expectation and Variance
   - 4.1 Expectation of a random variable, conditional expectations
   - 4.2 Variance and covariance
   - 4.3 Expectations and variances of important probability distributions
   - 4.4 Algebraic and central moments
   - 4.5 Moment-generating functions

5. Inequalities and Limit Theorems
   - 5.1 Probability inequalities
   - 5.2 Inequalities for expectations
   - 5.3 The law of large numbers
   - 5.4 Central limit theorem

Literature

Compulsory Reading

Further Reading

- Bruce, P., & Bruce, A. (2017). Practical statistics for data scientists: 50 essential concepts. Sebastopol, CA: O'Reilley.
- Downey, A. B. (2014). Think stats (2nd ed.). Sebastopol, CA: O'Reilly.
- Downey, A. B. (2013). Think Bayes. Sebastopol, CA: O'Reilly.
- Reinhart, A. (2015). Statistics done wrong: The woefully complete guide. San Francisco, CA: No Starch Press.
- Wassermann, L. (2004). All of statistics: A concise course in statistical inference. New York, NY: Springer Science+Business Media.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☑ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBDSSPDS01

2. Semester

Object-oriented Programming with Java

Module Code: DLBCSOOPJ

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Damir Ismailovic (Object-oriented Programming with Java)

Contributing Courses to Module

- Object-oriented Programming with Java (DLBCSOOPJ01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Introduction to the Java language
- Java language constructs
- Introduction to object-oriented system developement
- Inheritance
- Object-oriented concepts
- Exception handling
- Interfaces

Learning Outcomes **Object-oriented Programming with Java** On successful completion, students will be able to ▪ describe the basic concepts of object-oriented modeling and programming, distinguishing them from one another. ▪ describe the basic concepts and elements of the Java programming language and have some experience in their use. ▪ independently create Java programs to solve concrete problems.	
Links to other Modules within the Study Program This module is similar to other modules in the field(s) of Computer Science & Software Development.	**Links to other Study Programs of IUBH** All Bachelor Programmes in the IT & Technology field(s).

Object-oriented Programming with Java

Course Code: DLBCSOOPJ01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Operational information systems are usually planned and programmed to be object-oriented. Therefore, this course teaches the basic skills of object-oriented programming. Theoretical concepts are presented and practiced directly with the programming language Java.

Course Outcomes

On successful completion, students will be able to

- describe the basic concepts of object-oriented modeling and programming, distinguishing them from one another.
- describe the basic concepts and elements of the Java programming language and have some experience in their use.
- independently create Java programs to solve concrete problems.

Contents

1. Introduction to Object-Oriented System Development
   - 1.1 Object Orientation as a Way of Looking at Complex Systems
   - 1.2 The Object as a Basic Concept of Object Orientation
   - 1.3 Phases in the Object-Oriented Development Process
   - 1.4 Basic Principle of Object-Oriented System Development

2. Introduction to Object-Oriented Modeling
   - 2.1 Structuring Problems With Classes
   - 2.2 Identifying Classes
   - 2.3 Attributes as Properties of Classes
   - 2.4 Methods as Functions of Classes
   - 2.5 Associations between Classes
   - 2.6 Unified Modeling Language (UML)

Literature
Compulsory Reading
Further Reading ▪ Java (Hrsg.): Java Platform Standard Edition API Specification. (URL: http://www.oracle.com/technetwork/java/api-141528.html [letzter Zugriff: 21.11.2016]). ▪ Krüger G./Stark T. (2011): Handbuch der Java-Programmierung. 7. Auflage, Addison-Wesley, Salt Lake City. ▪ Lahres, B./Raýman, G. (2006): Praxisbuch Objektorientierung. Galileo Computing, Bonn. ▪ Oestereich B. (2012): Analyse und Design mit der UML 2.5. Objektorientierte Softwareentwicklung. 10. Auflage, Oldenbourg, München. ▪ Ratz, D. et al. (2011): Grundkurs Programmieren in Java. 6. Auflage, Carl Hanser Verlag, München. ▪ Ullenboom C. (2011): Java ist auch eine Insel. 10. Auflage, Galileo Computing, Bonn.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Mathematics: Linear Algebra

Module Code: DLBDSMFLA

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Moustafa Nawito (Mathematics: Linear Algebra)

Contributing Courses to Module

- Mathematics: Linear Algebra (DLBDSMFLA01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Matrix algebra
- Vector spaces
- Linear and affine transformations
- Analytical geometry
- Matrix decomposition

Learning Outcomes

Mathematics: Linear Algebra

On successful completion, students will be able to

- explain fundamental notions in the domain of linear equation systems.
- exemplify properties of vectors and vector spaces.
- summarize characteristics of linear and affine mappings.
- identify important relations in analytical geometry.
- utilize different methods for matrix decomposition.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field of Methods	All Bachelor Programmes in the IT & Technology fields

Mathematics: Linear Algebra

Course Code: DLBDSMFLA01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Linear algebra is a fundamental subject in mathematics. Its historical origin lies in the development of solution techniques for systems of linear equations arising from geometric problems. Numerous scientific and engineering applications can be solved using its methods. This course introduces the foundations of linear algebra and its basic notions like vectors and matrices. It then builds upon this foundation by introducing the derivation of solution techniques for problems in analytical geometry.

Course Outcomes

On successful completion, students will be able to

- explain fundamental notions in the domain of linear equation systems.
- exemplify properties of vectors and vector spaces.
- summarize characteristics of linear and affine mappings.
- identify important relations in analytical geometry.
- utilize different methods for matrix decomposition.

Contents

1. Fundamentals
   - 1.1 Systems of linear equations
   - 1.2 Matrices as compact representations of linear equations
   - 1.3 Matrix algebra
   - 1.4 Inverse and trace
2. Vector Spaces
   - 2.1 Definition
   - 2.2 Linear combination and linear dependance
   - 2.3 Base, span, and rank
3. Linear and affine mappings
   - 3.1 Matrix representations of linear mappings
   - 3.2 Image and kernel
   - 3.3 Affine spaces and sub-spaces
   - 3.4 Affine mappings

4. Analytical Geometry
   - 4.1 Norms
   - 4.2 Inner and dot product
   - 4.3 Orthogonal projections
   - 4.4 Rotations

5. Matrix Decomposition
   - 5.1 Determinant and trace
   - 5.2 Eigenvalues and eigenvectors
   - 5.3 Cholesky decomposition
   - 5.4 Eigenvalue decomposition and diagonalisation
   - 5.5 Singular value decomposition

Literature

Compulsory Reading

Further Reading

- Arfken, G./Weber, H. J./Harris, F. E. (2012): Mathematical methods for physicists. 7th ed., Academic Press, Cambridge, MA.
- Boas, M. L. (2006): Mathematical methods in the physical sciences. 3rd ed.,Wiley, Hoboken, NJ.
- Deisenroth, M. P./Faisal, A./Ong C. S. (2019): Math for machine learning. (URL: https://mml-book.com).
- Riley, K. F./Hobson, M. P./Bence, S. J. (2006): Mathematical methods for physics and engineering. Cambridge University Press, Cambridge.
- Strang, G. (2016): Introduction to linear algebra, 5th ed., Wellesley-Cambridge Press, Wellesley, MA.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☑ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBDSMFLA01

Collaborative Work

Module Code: DLBCSCW

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Karin Halbritter (Collaborative Work)

Contributing Courses to Module

- Collaborative Work (DLBCSCW01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Oral Assignment	

Weight of Module

see curriculum

Module Contents

- Self-Directed and Collaborative Learning
- Networking and Cooperation
- Performance in (Virtual) Teams
- Communication, Arguments, and Being Convincing
- Potentials for Conflict and Managing Conflicts
- Self-Management and Personal Skills

Learning Outcomes

Collaborative Work

On successful completion, students will be able to

- design their own self-directed and collaborative learning processes with analog and digital media.
- initiate local and virtual cooperation and select suitable methods for shaping cooperation.
- assess different forms of communication in relation to the goals and requirements of different situations and reflect one's own communication and argumentation behaviour.
- explain potentials for conflict and the role of emotions in conflicts and describe the use of systemic methods in the target- and solution-oriented handling of conflicts.
- form an idea of one's own resources, present methods of self-management and self-motivation, and derive appropriate strategies.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Business Administration & Management	All Bachelor Programmes in the Business & Management fields

Collaborative Work

Course Code: DLBCSCW01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The course supports the students in building up and expanding important interdisciplinary competences for our networked world, and in doing so, students can take advantage of the opportunities for constructive cooperation with others. It presents essential forms and design possibilities of collaborative learning and working, imparts basic knowledge and tools for self-managed, flexible, and creative thinking, learning and acting and familiarizes students with the topics of empathy and emotional intelligence. Students are also encouraged to use the course contents. In this way, they promote their autonomous competence to act and their competence in the interactive application of tools and in interacting in heterogeneous groups.

Course Outcomes

On successful completion, students will be able to

- design their own self-directed and collaborative learning processes with analog and digital media.
- initiate local and virtual cooperation and select suitable methods for shaping cooperation.
- assess different forms of communication in relation to the goals and requirements of different situations and reflect one's own communication and argumentation behaviour.
- explain potentials for conflict and the role of emotions in conflicts and describe the use of systemic methods in the target- and solution-oriented handling of conflicts.
- form an idea of one's own resources, present methods of self-management and self-motivation, and derive appropriate strategies.

Contents

1. Learning for a Networked World in a Networked World
   - 1.1 Requirements and Opportunities of the VUCA World
   - 1.2 Learning, Information, and Dealing with Knowledge and Ignorance
   - 1.3 C-Model: Collective – Collaborative – Continuous – Connected
   - 1.4 Checking Your Own Learning Behaviour
2. Networking and Cooperation
   - 2.1 Finding and Winning Suitable Cooperation Partners
   - 2.2 Sustainable Relationships: Digital Interaction and Building Trust
   - 2.3 Collaboration: Organizing Locally and Virtually and Using Media
   - 2.4 Social Learning: Agile, Collaborative, and Mobile Planning of Learning Processes

3. Performance in (Virtual) Teams
   - 3.1 Goals, Roles, Organization and Performance Measurement
   - 3.2 Team Building and Team Flow
   - 3.3 Scrum as a Framework for Agile Project Management
   - 3.4 Design Thinking, Kanban, Planning Poker, Working-in-Progress-Limits & Co

4. Communicate and Convince
   - 4.1 Communication as Social Interaction
   - 4.2 Language, Images, Metaphors, and Stories
   - 4.3 It's the Attitude that Counts: Open, Empathetic, and Appreciative Communication
   - 4.4 Listen Actively - Argue - Convince - Motivate
   - 4.5 Analyze Your Own Conversational and Argumentational Skills

5. Recognize Conflict Potentials - Handle Conflicts - Negotiate Effectively
   - 5.1 Respecting Diversity - Seizing Opportunities
   - 5.2 Developing Empathy for Yourself and Others
   - 5.3 Systemic Work Solutions and Reframing
   - 5.4 Negotiate Constructively: Finding Clear Words - Interests Instead of Positions

6. Realize Your Own Projects
   - 6.1 Set Goals Effectively - Focus - Reflect
   - 6.2 The Agile Use of One's Own Time
   - 6.3 (Self-)Coaching and Inner Team
   - 6.4 Strategies and Methods for Self-Management and Self-Motivation

7. Mobilize Your Resources
   - 7.1 Recognizing Resources - Regulating Emotions
   - 7.2 Reflection and Innovation - Lateral Thinking and Creativity
   - 7.3 Transfer Strength and Willpower: Analyzing and Controlling Condition Factors

8. Construction Kit: Overview of Concepts, Tools, and Methods
   - 8.1 Communicate, Cooperate, Negotiate, Argue
   - 8.2 Think, Reflect, Develop Ideas, Decide, Lead Yourself

Literature
Compulsory Reading
Further Reading ▪ Baber, A. (2015): Strategic connections. The new face of networking in a collaborative world. Amacom, New York. ▪ Goleman, D. (2013): Focus. The hidden driver of excellence. Harper Collins USA, New York. ▪ Kaats, E./Opheij, W. (2014): Creating conditions for promising collaboration. Alliances, networks, chains, strategic partnerships. Springer Management, Berlin. ▪ Lang, M. D. (2019): The guide to reflective practice in conflict resolution. Rowman & Littlefield, Lanham/Maryland. ▪ Martin, S. J./Goldstein, N. J./Cialdini, R. B. (2015): The small BIG. Small changes that spark BIG influence. Profile Books, London.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Introduction to Network Forensics

Module Code: DLBCSEINF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBIBRVS01_E or DLBIBRVS01	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Introduction to Network Forensics)

Contributing Courses to Module

- Introduction to Network Forensics (DLBCSEINF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Network protocols and services
- World Wide Web
- Log data analysis
- Network forensics

Learning Outcomes

Introduction to Network Forensics

On successful completion, students will be able to

- interact with the network at a low level.
- understand the idiosyncrasies of Internet protocols.
- understand how to read RFCs in self-study when protocols are modified, or new ones added.
- understand common attacks against these protocols.
- understand how encryption is used in the Internet, and how it can be subverted.
- deploy and use IDPS systems.
- recognize security events in a SIEM that uses the IDPS data.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Introduction to Network Forensics

Course Code: DLBCSEINF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBIBRVS01_E or DLBIBRVS01

Course Description

Network forensics is the art and science of capturing, recording and analysis of network events in order to discover attacks. This requires an in-depth knowledge of the core Internet protocols, how they are used and how they can be attacked.In this course, we will look at the most commonly used network protocols in Internet-based networking. We take a practical approach and look at actual network traces to discover how protocols are layered on each other. At its core there is TCP/IP. Other protocols, like HTTP, are built on that layer. Others, like DNS are based on the alternative UDP protocol. The major services that make up the Internet will be discussed. For instance, DNS is a protocol, but also a distributed database system. The ICANN organization oversees IP addresses and they are allocated to regional organizations and distributed to Autonomous Systems. This requires routing which is handled by other protocols.Encryption is provided for confidentiality of data but often also for authentication and integrity reasons. It is implemented in a variety of forms with an equal variety of trade-offs.The forensic practitioner requires a variety of tools, ranging from simple probing tools to collection and analysis tools. These are usually packaged as Intrusion Detection and Prevention Systems as well as SIEMs for the actual analysis. However, security event data usually needs to be augmented with external data sources for accurate diagnosis, and a variety of data sources will be discussed.

Course Outcomes

On successful completion, students will be able to

- interact with the network at a low level.
- understand the idiosyncrasies of Internet protocols.
- understand how to read RFCs in self-study when protocols are modified, or new ones added.
- understand common attacks against these protocols.
- understand how encryption is used in the Internet, and how it can be subverted.
- deploy and use IDPS systems.
- recognize security events in a SIEM that uses the IDPS data.

Contents

6. Domain Name System
   - 6.1 Host name hierarchy
   - 6.2 DNS as a distributed database
   - 6.3 DNSSEC
   - 6.4 SPF, DMARC and other special records

7. Common application layer protocols
   - 7.1 HTTP
   - 7.2 HTTP/2
   - 7.3 SMTP

8. Transport Layer Encryption
   - 8.1 SSH
   - 8.2 IPSEC
   - 8.3 TLS
   - 8.4 Man in the middle attacks
   - 8.5 Certificates and certificate authorities

9. Intrusion detection and prevention systems
   - 9.1 Sensor and event types
   - 9.2 Netflow monitoring
   - 9.3 Rules, false positive and false negatives
   - 9.4 SIEMs
   - 9.5 Attack prevention technologies

10. Correlation and enrichment data sources
    - 10.1 Enrichment of data
    - 10.2 DNS data sources: DNSBLs, passive DNS, DNS repositories
    - 10.3 AS numbers, IP blocks, GeoIP and WhoIs data
    - 10.4 Certificate Transparency
    - 10.5 Correlation methods

Literature
Compulsory Reading
Further Reading ▪ Fall, K. R. / Stevens, W. R. (2012): TCP/IP Illustrated, Volume 1: The Protocols. 2nd edition, Addison-Wesley, Upper Saddle River, NJ. ▪ Matthews, J. (2005): Computer Networking: Internet Protocols in Action. Wiley, Hoboken, NJ. ▪ Stevens, W. R. (1996): TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols. Addison-Wesley, Upper Saddle River, NJ. ▪ Wright, G.R. / Stevens, W. R. (1995): TCP/IP Illustrated, Volume 2: The Implementation. Addison-Wesley, Upper Saddle River, NJ.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSEINF01_E

Requirements Engineering

Module Code: DLBCSRE

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Tobias Brückmann (Requirements Engineering)

Contributing Courses to Module

- Requirements Engineering (DLBCSRE01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basics of requirements engineering
- Enterprise modeling
- Requirement determination techniques
- Techniques of requirements documentation
- Testing and coordination of requirements
- Managing requirements

Learning Outcomes

Requirements Engineering

On successful completion, students will be able to

- describe models of enterprise modeling relevant to IT support and have experience in modeling.
- understand techniques and methods for determining requirements of IT systems and be able to distinguish them from each other.
- understand techniques for the documentation of requirements on IT systems and have experience in their use.
- describe techniques for testing, coordinating, and managing the requirements of IT systems and be able to distinguish between them.
- independently select suitable techniques and methods of requirements engineering for given project situations.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field(s) of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field(s).

Requirements Engineering

Course Code: DLBCSRE01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The early phases of software development are largely characterized by the fact that functional and technical requirements for the IT system have to be determined. The determination of these requirements must be carried out extremely carefully because all of the following activities in the SW development process are planned and executed on the basis of documented requirements. In this course, procedures, methods, and models are covered, which make it possible to have a structured and methodical determination and documentation of requirements for operational information systems.

Course Outcomes

On successful completion, students will be able to

- describe models of enterprise modeling relevant to IT support and have experience in modeling.
- understand techniques and methods for determining requirements of IT systems and be able to distinguish them from each other.
- understand techniques for the documentation of requirements on IT systems and have experience in their use.
- describe techniques for testing, coordinating, and managing the requirements of IT systems and be able to distinguish between them.
- independently select suitable techniques and methods of requirements engineering for given project situations.

Contents

1. Fundamentals and Terms of Requirements Engineering
   - 1.1 Requirements Engineering in the Software Process
   - 1.2 Core Activities in Requirements Engineering
   - 1.3 What is a Requirement?
2. Determination of Requirements
   - 2.1 Determination of the System Context
   - 2.2 Determination of the Sources of Requirements
   - 2.3 Selection of the Appropriate Investigative Techniques
   - 2.4 Determine Requirements Using Techniques

3. Selected Investigative Techniques
   - 3.1 Creativity Techniques
   - 3.2 Interview Techniques
   - 3.3 Observation Techniques
   - 3.4 Prototyping

4. Documentation of Requirements
   - 4.1 Activities for Documenting Requirements
   - 4.2 Typical Elements of Requirements Documentation
   - 4.3 Forms of Documentation

5. Modeling of Processes
   - 5.1 Basics and Terms
   - 5.2 Modeling with the Business Process Model and Notation
   - 5.3 Modeling with Event Driven Process Chains

6. Modeling of Systems
   - 6.1 Fundamentals of Unified Modeling Language
   - 6.2 UML Use Case Diagram
   - 6.3 UML Activity Diagram
   - 6.4 UML Class Diagram
   - 6.5 UML State Diagram

7. Checking and Reconciling Requirements
   - 7.1 Activities for Checking and Reconciling Requirements
   - 7.2 Test Criteria
   - 7.3 Test Principles
   - 7.4 Testing Techniques
   - 7.5 Coordination of Requirements

8. Management of Prioritization Requirements and Techniques
   - 8.1 Managing Requirements
   - 8.2 Techniques for Prioritizing Requirements

Literature

Compulsory Reading

Further Reading

- Allweyer, T. (2009): BPMN 2.0. Business Process Model and Notation. Einführung in den Standard für die Geschäftsprozessmodellierung. 2. Auflage, Books on Demand, Norderstedt.
- Balzert, H. (2010): UML 2 kompakt mit Checklisten. 3. Auflage, Spektrum, Heidelberg.
- Booch, G./Rumbaugh, J./Jacobson, I. (2006): Das UML Benutzerhandbuch. Addison-Wesley, Bonn.
- Cohn, M. (2010): User Stories für die agile Software-Entwicklung mit Scrum, XP u.a. mitp, Frechen.
- Freund, J./Rücker, B. (2012): Praxishandbuch BPMN 2.0. 3. Auflage, Hanser. München.
- Gadatsch, A. (2012): Grundkurs Geschäftsprozess-Management. Methoden und Werkzeuge für die IT-Praxis. Eine Einführung für Studenten und Praktiker. 7. Auflage, Vieweg+Teubner, Wiesbaden.
- Pohl, K. (2008): Requirements Engineering. Grundlagen, Prinzipien, Techniken. 2. Auflage, dpunkt.verlag, Heidelberg.
- Pohl, K./Rupp, C. (2011): Basiswissen Requirements Engineering. Aus- und Weiterbildung nach IREB-Standard zum Certified Professional for Requirements Engineering Foundation Level. 3. Auflage, dpunkt.verlag, Heidelberg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

System Pentesting Basics

Module Code: DLBCSESPB_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Jesus Luna Garcia (System Pentesting Basics)

Contributing Courses to Module

- System Pentesting Basics (DLBCSESPB01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Penetration testing process
- Host-based penetration testing
- Exploitation of network services
- Web App penetration testing
- System hardening
- Ethical hacking

Learning Outcomes

System Pentesting Basics

On successful completion, students will be able to

- understand the basic organizational and compliance needs for penetration testing.
- identify the relevant components of modern-day IT system that may be exploitable.
- understand the underlying processes comprising a penetration testing.
- understand the most common attack vectors associated to hosts, networks and Web Apps as well as how to defend against those.
- familiarize themselves with real-world tools used by professional penetration testers.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

System Pentesting Basics

Course Code: DLBCSESPB01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

System penetration testing is a vital process for finding and supporting the mitigation of vulnerabilities in IT systems before the attackers can exploit them. For that reason, many organizations employ such “pentesters”, or ethical hackers, to test their software and hardware base (connectivity included) and fix the security issues that are found. This has become a cornerstone of modern security concepts. However, in order to be successful in this endeavor, a good knowledge of the different types of targeted IT systems is required. We refer to hosts, networks, Web Apps, and even cloud computing. In this course we present the fundamental aspects of IT systems, along with the processes, tools and techniques that comprise the industrial practice of penetration testing. Equipped with this knowledge, students will understand the mechanisms of a given attack, and start down the path of pentesting themselves.

Course Outcomes

On successful completion, students will be able to

- understand the basic organizational and compliance needs for penetration testing.
- identify the relevant components of modern-day IT system that may be exploitable.
- understand the underlying processes comprising a penetration testing.
- understand the most common attack vectors associated to hosts, networks and Web Apps as well as how to defend against those.
- familiarize themselves with real-world tools used by professional penetration testers.

Contents

1. Penetration Testing Goals and Industrial Perspective
   - 1.1 Organizational Benefits
   - 1.2 Ethical Hacking Framework
   - 1.3 Legal and Compliance Aspects
   - 1.4 Responsible Disclosure of Vulnerabilities
   - 1.5 Professional Penetration Testing Services and Certifications

2. Background Concepts
   - 2.1 Operating Systems
   - 2.2 Hardware Architectures
   - 2.3 Networking and Protocols
   - 2.4 Web-Based Applications
   - 2.5 Cloud Computing

3. Penetration Testing Process
   - 3.1 Planning and Reconnaissance
   - 3.2 Whitebox, Blackbox and Graybox Scanning
   - 3.3 Gaining Access
   - 3.4 Maintaining Access
   - 3.5 Analysis and Reporting
   - 3.6 Hardening and Mitigation

4. Operating System-Based Penetration Testing
   - 4.1 Common Misconfigurations
   - 4.2 Shellcode Attacks
   - 4.3 Memory Corruption and Buffer Overflow Vulnerabilities
   - 4.4 Metasploit and Kali Tools
   - 4.5 Operating System Hardening

5. Network Penetration Testing
   - 5.1 Network Infrastructure Scoping and Recon
   - 5.2 Exploiting Network Services
   - 5.3 Lateral Movement in the Network
   - 5.4 Kerberos Attacks
   - 5.5 Toolset: Nmap, PowerShell, Bloodhound, and Tcpdump
   - 5.6 Devising Corrective Actions

6. Web App Penetration Testing
   - 6.1 The OWASP Methodology
   - 6.2 Open Source Intelligence (OSINT)
   - 6.3 Commonly Exploited Web App Vulnerabilities
   - 6.4 Exploitation Toolset: BurpSuite, sqlmap, BeEF and ExploitDB
   - 6.5 Reporting Findings and Mitigation Actions

7. Specialized Penetration Testing at a Glance
   - 7.1 Exploit Development
   - 7.2 Ethical Hacking
   - 7.3 Wireless and Mobile Device Penetration Testing
   - 7.4 Cloud Threat and Vulnerability Assessment

Literature

Compulsory Reading

Further Reading

- Erickson, J. (2007): Hacking. The Art of Exploitation. No Starch Press, San Francisco.
- Gollmann, D. (2011): Computer Security. 3rd edition, Wiley, Hoboken, NJ.
- Kim, P. (2014): The Hacker Playbook. A Practical Guide to Penetration Testing. CreateSpace Independent Publishing Platform, North Charleston.
- Lin, X. (2018): Introductory Computer Forensics. A Hands-on Practical Approach. Springer International Publishing, Cham.
- Stuttard, D. (2011): The Web Application Hacker's Handbook. Finding and Exploiting Security Flaws. Wiley, Hoboken, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

3. Semester

Intercultural and Ethical Decision-Making

Module Code: DLBCSIDM

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Jürgen Matthias Seeler (Intercultural and Ethical Decision-Making)

Contributing Courses to Module

- Intercultural and Ethical Decision-Making (DLBCSIDM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Basics of Intercultural Competence
- Cultural Concepts
- Culture and Ethics
- Implications of Current Ethical Problems in the Area of Interculturality, Ethics, and Diversity
- Intercultural Learning and Working
- Case Studies for Cultural and Ethical Conflicts

Learning Outcomes

Intercultural and Ethical Decision-Making

On successful completion, students will be able to

- explain the most important terms in the areas of interculturality, diversity, and ethics.
- distinguish different explanatory patterns of culture.
- understand culture at different levels.
- plan processes of intercultural learning and working.
- understand the interdependencies of culture and ethics.
- independently work on a case study on intercultural competence.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Business Administration & Management	All Bachelor Programs in the Business & Management fields

Intercultural and Ethical Decision-Making

Course Code: DLBCSIDM01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students acquire the necessary knowledge to understand intercultural competencies and current developments in the fields of diversity and ethics. Students will understand how to systematically plan and implement learning processes for the development of competences important in these areas. First, important terms are clarified and differentiated from each other, and cultural aspects are explained from different perspectives. In addition, students learn that cultural issues are relevant at different levels, for example, within a state, company, or other group. In this context, students also recognize the connection between ethics and culture with different interdependencies. On the basis of this knowledge, students are then familiarized with the different possibilities and potentials of intercultural and ethical learning and working. Practical cases are used to illustrate the importance of the relationships learned for today's work context in many companies. The students then work on a case study in which the acquired knowledge is systematically applied.

Course Outcomes

On successful completion, students will be able to

- explain the most important terms in the areas of interculturality, diversity, and ethics.
- distinguish different explanatory patterns of culture.
- understand culture at different levels.
- plan processes of intercultural learning and working.
- understand the interdependencies of culture and ethics.
- independently work on a case study on intercultural competence.

Contents

1. Basics of Intercultural and Ethical Competence to Act
   - 1.1 Subject Areas, Terms, and Definitions
   - 1.2 Relevance of Intercultural and Ethical Action
   - 1.3 Intercultural Action - Diversity, Globalization, Ethics
2. Cultural Concepts
   - 2.1 Hofstedes Cultural Dimensions
   - 2.2 Culture Differentiation According to Hall
   - 2.3 Locus of Control Concept to Rotter

3. Culture and Ethics
   - 3.1 Ethics - Basic Terms and Concepts
   - 3.2 Interdependence of Culture and Ethics
   - 3.3 Ethical Concepts in Different Regions of the World

4. Current Topics in the Area of Interculturality, Ethics, and Diversity
   - 4.1 Digital Ethics
   - 4.2 Equality and Equal Opportunities
   - 4.3 Social Diversity

5. Intercultural Learning and Working
   - 5.1 Acculturation
   - 5.2 Learning and Working in Intercultural Groups
   - 5.3 Strategies for Dealing with Cultural Conflicts

6. Case Studies for Cultural and Ethical Conflicts
   - 6.1 Case Study: Interculturality
   - 6.2 Case Study: Diversity
   - 6.3 Case Study: Interculturality and Ethics

Literature

Compulsory Reading

Further Reading

- Emrich, C. (2011): Interkulturelles Management: Erfolgsfaktoren im globalen Business. Kohlhammer-Verlag, Stuttgart/Berlin/Köln.
- Erll, A./Gymnich, M. (2015): Uni-Wissen Interkulturelle Kompetenzen: Erfolgreich kommunizieren zwischen den Kulturen – Kernkompetenzen. 4. Auflage, Klett Lerntraining, Stuttgart.
- Eß, O. (2010): Das Andere lehren: Handbuch zur Lehre Interkultureller Handlungskompetenz. Waxmann Verlag, Münster.
- Hofstede, G./ Hofstede, G. J./Minkov, M. (2017): Lokales Denken, globales Handeln Interkulturelle Zusammenarbeit und globales Management. 6. Auflage, Beck, München.
- Leenen, W.R./Groß, A. (2018): Handbuch Methoden Interkultureller Bildung und Weiterbildung. Verlag Vandenhoeck & Ruprecht, Göttingen.
- Thomas, A. (2011): Interkulturelle Handlungskompetenz. Versiert, angemessen und erfolgreich im internationalen Geschäft. Gabler-Verlag, Wiesbaden.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Case Study

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

DLBCSIDM01

Introduction to the Internet of Things

Module Code: DLBINGEIT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Marian Benner-Wickner (Introduction to the Internet of Things)

Contributing Courses to Module

- Introduction to the Internet of Things (DLBINGEIT01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Internet of Things Fundamentals
- Social and Economic Significance
- Communication Standards and Technologies
- Data Storage and Processing
- Design and Development
- Applicability

Learning Outcomes

Introduction to the Internet of Things

On successful completion, students will be able to

- grasp the distinctive features of Internet of Things (IoT) and IoT systems.
- understand the social and economic importance of Internet of Things.
- identify the most important standards for communication between IoT devices.
- differentiate between various techniques for storing and processing data in IoT systems.
- identify different architectures and technologies for structuring IoT systems.
- recognize challenges of data protection and data security in IoT systems.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software	All Bachelor Programmes in the IT & Technology fields

Introduction to the Internet of Things

Course Code: DLBINGEIT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of this course is to give students an insight into technical and theoretical basics of the Internet of Things (IoT) and its fields of application. In addition to the general structure of IoT systems and the technology standards used in them, students are also taught the importance of Internet of Things for economy and society. Furthermore, this course demonstrates how data is exchanged, stored and processed in IoT.

Course Outcomes

On successful completion, students will be able to

- grasp the distinctive features of Internet of Things (IoT) and IoT systems.
- understand the social and economic importance of Internet of Things.
- identify the most important standards for communication between IoT devices.
- differentiate between various techniques for storing and processing data in IoT systems.
- identify different architectures and technologies for structuring IoT systems.
- recognize challenges of data protection and data security in IoT systems.

Contents

1. Internet of Things Fundamentals
   - 1.1 The Internet of Things - Basics and Motivation
   - 1.2 Evolution of the Internet - Web 1.0 to Web 4.0
2. Social and Economic Significance
   - 2.1 Innovations for Consumers and Industry
   - 2.2 Implications on People and the World of Work
   - 2.3 Data Protection and Data Security
3. Communication Standards and Technologies
   - 3.1 Network Topologies
   - 3.2 Network Protocols
   - 3.3 Technologies

4. Data Storage and Processing
   - 4.1 Networked Storage with Linked Data and RDF(S)
   - 4.2 Analysis of Networked Data using a Semantic Reasoner
   - 4.3 Processing of Data Streams with Complex Event Processing
   - 4.4 Operation and Analysis of Large Data Clusters using NoSQL and MapReduce

5. Design and Development
   - 5.1 Software Engineering for Distributed and Embedded Systems
   - 5.2 Architecture Styles and Patterns of Distributed Systems
   - 5.3 Platforms: Microcontrollers, Monoboard Computers, One-Chip Systems

6. Applicability
   - 6.1 Smart Home / Smart Living
   - 6.2 Ambient Assisted Living
   - 6.3 Smart Energy / Smart Grid
   - 6.4 Smart Factory
   - 6.5 Smart Logistics

Literature

Compulsory Reading

Further Reading

- Buyya, R./Vahid Dastjerdi, A. (Hrsg.) (2016): Internet of things. Principles and paradigms. Morgan Kaufmann, Cambridge, MA.
- Fleisch, E. (Hrsg.) (2005): Internet der dinge. Ubiquitous Computing und RFID in der Praxis. Springer, Berlin.
- Gilchrist, A. (2016): Industry 4.0. The industrial internet of things. Apress, New York, NY.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBINGEIT01_E

Algorithms, Data Structures, and Programming Languages

Module Code: DLBCSL

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

N.N. (Algorithms, Data Structures, and Programming Languages)

Contributing Courses to Module

- Algorithms, Data Structures, and Programming Languages (DLBCSL01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Data structures
- Algorithm design
- Important algorithms
- Programming paradigms and the basic terms of programming languages
- Programme analysis tools
- Overview of common programming languages

Learning Outcomes

Algorithms, Data Structures, and Programming Languages

On successful completion, students will be able to

- explain basic data structures and compare and apply them in concrete applications.
- explain basic algorithms.
- design, select and apply suitable algorithms and data structures for specific applications
- analyse sketched or programmed algorithms when or before running them
- explain and compare the common programming paradigms and programming languages.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the field(s) of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field(s).

Algorithms, Data Structures, and Programming Languages

Course Code: DLBCSL01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Programming essentially consists of selecting suitable algorithms and data structures for a specific task and converting them into program code. There are many different programming languages, which are based on different procedures and in which algorithms and data structures are implemented differently. In this module, these concepts, which have so far been dealt with using concrete examples, are systematically presented and applied more broadly in order to give students the necessary tools to develop a systematic approach to programming.

Course Outcomes

On successful completion, students will be able to

- explain basic data structures and compare and apply them in concrete applications.
- explain basic algorithms.
- design, select and apply suitable algorithms and data structures for specific applications
- analyse sketched or programmed algorithms when or before running them
- explain and compare the common programming paradigms and programming languages.

Contents

1. Basic Concepts
   - 1.1 Algorithms, Data Structures, and Programming Languages as the Basics of Programming
   - 1.2 Detailing and Abstraction
   - 1.3 Control Structures
   - 1.4 Types of Data
   - 1.5 Basic Data Structures (List, Chain, Tree)

2. Data Structures
   - 2.1 Advanced Data Structures: Queue, Heap, Stack, Graph
   - 2.2 Abstract Data Types, Objects, and Classes
   - 2.3 Polymorphism

3. Algorithm Design
   - 3.1 Induction, Iteration, and Recursion
   - 3.2 Methods of Algorithm Design
   - 3.3 Correctness and Verification of Algorithms
   - 3.4 Efficiency (complexity) of algorithms

4. Basic Algorithms
   - 4.1 Traversing and Linearization of Trees
   - 4.2 Search Algorithms
   - 4.3 Sorting Algorithms
   - 4.4 Search in Strings
   - 4.5 Hash Algorithms
   - 4.6 Pattern Recognition

5. Measuring Programmes
   - 5.1 Type inference and IDE interactive support
   - 5.2 Cyclomatic and referential complexity
   - 5.3 Digesting code documentation
   - 5.4 Compiler optimization
   - 5.5 Code coverage
   - 5.6 Unit and integration testing
   - 5.7 Heap analysis

6. Programming Languages
   - 6.1 Programming Paradigms
   - 6.2 Execution of Programs
   - 6.3 Types of Programming Languages
   - 6.4 Syntax, Semantics, and Pragmatics
   - 6.5 Variables and Type Systems

7. Overview of Important Programming Languages
   - 7.1 Assembler and Webassembly
   - 7.2 C and C++
   - 7.3 Java and C#
   - 7.4 Haskell, Lisp
   - 7.5 JavaScript and its relatives
   - 7.6 Other imperative programming languages

Literature
Compulsory Reading
Further Reading ▪ Gumm H. P. /Sommer M. (2013): Einführung in die Informatik. 10. Auflage. Oldenbourg, München. ▪ Harel, D. (2006): Algorithmik. Die Kunst des Rechnens. Springer, Berlin/Heidelberg/New York. ▪ Cormen, T.,Leiserson, C., Rivest, R., Stein, C. (2009) Introduction to Algorithms, 3rd edition, MIT Press, Cambridge, Mass., USA

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Theoretical Computer Science and Mathematical Logic

Module Code: DLBCSTCSML

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N. N. (Theoretical Computer Science and Mathematical Logic)

Contributing Courses to Module

- Theoretical Computer Science and Mathematical Logic (DLBCSTCSML01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Proposition and predicate logic
- Finite automata
- Formal languages
- Computability and Turing machines
- Complexity theory
- Petri nets

Learning Outcomes

Theoretical Computer Science and Mathematical Logic

On successful completion, students will be able to

- formulate and translate predicate logical relationships into programming languages.
- use finite automatons and regular expressions to describe technical facts.
- explain the Chomsky hierarchy.
- identify the limits of provability and predictability.
- explain the meaning and relevance of the P=NP problem.
- apply Petri nets for the description of technical facts.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field(s) of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field(s).

Theoretical Computer Science and Mathematical Logic

Course Code: DLBCSTCSML01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Theoretical computer science and mathematical logic form the theoretical basics of computer science. However, this is not "pure theory", as these fundamentals are applied in many areas of computer science. These include, for example, the formulation of conditions in SQL queries or other programs based on statement and predicate logic, the use of finite state machines to specify systems with state transition diagrams, and the modeling of business and other processes with Petri nets. In addition, theoretical computer science and mathematical logic analyze the limits of computer science and computability, which cannot be exceeded irrespective of the technologies and algorithms used.

Course Outcomes

On successful completion, students will be able to

- formulate and translate predicate logical relationships into programming languages.
- use finite automatons and regular expressions to describe technical facts.
- explain the Chomsky hierarchy.
- identify the limits of provability and predictability.
- explain the meaning and relevance of the P=NP problem.
- apply Petri nets for the description of technical facts.

Contents

1. Propositional Logic
   - 1.1 Basic Concepts
   - 1.2 Interpretation and Satisfiability
   - 1.3 Normal Forms
   - 1.4 Proof by Contradiction and Resolution
   - 1.5 Completeness
2. Predicate Logic
   - 2.1 Basic Concepts
   - 2.2 Completeness and Incompleteness
   - 2.3 Logic Programming with Prolog

3. Finite Automata and Regular Expressions
   - 3.1 Basic Concepts of Finite Automata
   - 3.2 Regular Expressions
   - 3.3 Practical Applications

4. Formal Languages and Grammars
   - 4.1 Basic Concepts
   - 4.2 The Chomsky Hierarchy
   - 4.3 Regular Languages
   - 4.4 Context Free Languages
   - 4.5 Context Sensitive Languages

5. Computability and Turing Machines
   - 5.1 Models of Computability
   - 5.2 Turing Machines
   - 5.3 Recursive Functions
   - 5.4 Computability and Decidability
   - 5.5 The Halting Problem

6. Complexity Theory
   - 6.1 Basic Concepts
   - 6.2 Complexity Classes
   - 6.3 P=NP?

7. Petri Nets
   - 7.1 Basic Concepts of Graphs and Petri Nets
   - 7.2 Invariants, Liveliness, and Safety
   - 7.3 Process Modeling and Analysis with Petri Nets

8. Applications of Mathematical Logic and Theoretical Computer Science
   - 8.1 Parser and Compiler
   - 8.2 Program Verification
   - 8.3 Artificial Intelligence

Literature
Compulsory Reading
Further Reading ▪ Dewdney, A.K. (1995): Der Turing Omnibus. Eine Reise durch die Informatik mit 66 Stationen. Springer, Berlin/Heidelberg/New York. ▪ Erk, K./Priese, L. (2008): Theoretische Informatik. 3. Auflage. Springer eXamen.press, Berlin/ Heidelberg. ▪ Priese, L./Wimmerl, H. (2008): Petri-Netze. 2. Auflage. Springer eXamen.press, Berlin/ Heidelberg. ▪ Schöning, U. (2000): Logik für Informatiker. 5. Auflage. Spektrum Verlag, Heidelberg/ Berlin. ▪ Schöning, U. (2008): Ideen der Informatik. Grundlegende Modelle und Konzepte der Theoretischen Informatik, 3. Auflage. Oldenbourg, München.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** yes
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

IT Project Management

Module Code: DLBCSEITPAM1

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (IT Project Management)

Contributing Courses to Module

- IT Project Management (DLBCSEITPAM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basic terms and foundations of IT project management
- Large and small planning techniques
- Techniques for prioritization, cost-estimation, and project controlling
- Techniques for stakeholder, communication, and risk management
- Organization and structure in IT project management
- Schools of thought in IT project management

Learning Outcomes

IT Project Management

On successful completion, students will be able to

- explain and differentiate between the basic principles and tasks of IT project management.
- explain the important practical techniques and methods necessary for the implementation of IT project management.
- describe the basic procedural models and explain their advantages and disadvantages as well as their possible applications.
- identify possible project risks on the basis of given practical scenarios and select suitable measures from IT project management in order to minimize them in a targeted manner.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

IT Project Management

Course Code: DLBCSEITPAM01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, typical problems in the management of Software projects are discussed and the methods and techniques used to address challenges conveyed.In addition, standard procedural models for IT project management are explained and their strengths and weaknesses specifically identified.

Course Outcomes

On successful completion, students will be able to

- explain and differentiate between the basic principles and tasks of IT project management.
- explain the important practical techniques and methods necessary for the implementation of IT project management.
- describe the basic procedural models and explain their advantages and disadvantages as well as their possible applications.
- identify possible project risks on the basis of given practical scenarios and select suitable measures from IT project management in order to minimize them in a targeted manner.

Contents

1. Basics Terms and Foundations of IT Project Management
   - 1.1 Definition of a Project and Types of IT Projects
   - 1.2 IT Project Lifecycle
   - 1.3 Multi-Project Management – The Project in the Context of the Organization
2. Planning Techniques
   - 2.1 Large-Scale Planning: Milestones, Sub-tasks, and Work Packages
   - 2.2 Large-Scale Planning: Gantt Charts
   - 2.3 Planning and Organization of Work Packages: Kanban Board
3. Prioritization, Estimation of Costs, Project Controlling
   - 3.1 Prioritization
   - 3.2 Estimation of Costs
   - 3.3 Project Controlling

4. Stakeholder, Communication and Risk Management
   - 4.1 Stakeholder Management
   - 4.2 Communication Management
   - 4.3 Risk Management

5. Organization and Structure in IT Project Management
   - 5.1 Overview and Levels of Management from PRINCE2
   - 5.2 Management Processes in PRINCE2
   - 5.3 Pragmatic IT Project Management (PITPM)
   - 5.4 Configuration of an IT Project in PITPM
   - 5.5 Management of a project in PITPM

6. Schools of Thought in IT Project Management
   - 6.1 Agile Software Development
   - 6.2 Value-Based Software Engineering

Literature

Compulsory Reading

Further Reading

- Berkun, S. (2009): Die Kunst des IT-Projektmanagements. 2. Auflage, O'Reilly, Sebastopol, CA.
- DeMarco, T. (2003): Bärentango. Mit Risikomanagement Projekte zum Erfolg führen. Carl Hanser Verlag, München.
- Geirhos, M. (2011): IT-Projektmanagement. Was wirklich funktioniert – und was nicht. Galileo Computing, Bonn.
- Höhn, R./Höppner S. (2008): Das V-Modell XT. Grundlagen, Methodik und Anwendungen. Springer, Berlin/Heidelberg.
- Malik, M. (2006): Führen, Leisten, Leben. Wirksames Management für eine neue Zeit. Campus, Frankfurt a. M.
- Mangold, P. (2009): IT-Projektmanagement kompakt. 3.Auflage, Spektrum.
- Motzel, E./Pannenbäcker, O. (1998): Projektmanagement-Kanon. Der deutsche Zugang zum Project Management Body of Knowledge. TÜV-Verlag, Köln.
- Patzak, G./Rattay, G.: Projektmanagement. Leitfaden zum Management von Projekten, Projektportfolios und projektorientierten Unternehmen. 5. Auflage, Linde Verlag, Wien.
- Phillips, J. (2010): IT Project Management. On Track from Start to Finish. 3. Auflage, McGraw-Hill, New York, NY.
- Pichler, R. (2007): Scrum. Agiles Projektmanagement erfolgreich einsetzen. dpunkt.verlag, Heidelberg.
- Schwalbe, K. (2010): Information Technology Project Management. 6. Auflage, Course Technology, Independence, KY.
- Tiemeyer, E. (2010): Handbuch IT-Projektmanagement. Vorgehensmodelle, Managementinstrumente, Good Practices. Hanser, München.
- Versteegen, G. (2000): Projektmanagement: mit dem Rational Unified Process. Springer, Berlin/Heidelberg.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DevSecOps and Common Software Weaknesses

Module Code: DLBCSEDCSW_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSESPB01_E or DLBCSESPB01_D	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (DevSecOps and Common Software Weaknesses)

Contributing Courses to Module

- DevSecOps and Common Software Weaknesses (DLBCSEDCSW01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Written Assessment: Written Assignment	

Weight of Module

see curriculum

Module Contents

- Common code bugs
- Software Development Lifecycle
- DevOps
- DevSecOps
- Vulnerability reporting and bug bounty programs
- Patch management

Learning Outcomes

DevSecOps and Common Software Weaknesses

On successful completion, students will be able to

- avoid common software implementation and design mistakes.
- design a software development lifecycle process based on DevSecOps principles.
- incorporate vulnerability reporting and response into the SDL.
- organize and manage a bug bounty program.
- implement and manage a corporate patch management process.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

DevSecOps and Common Software Weaknesses

Course Code: DLBCSEDCSW01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSESPB01_E or DLBCSESPB01_D

Course Description

Modern organizations are run by software to some degree or another. In many cases, it is the custom software in business processes or products that is the key differentiator. But even companies that do no development of their own, are dependent on software and understanding software vulnerabilities is vital to their operations, as recent ransomware attacks have shown.In this course, we look at modern software development and lifecycle processes. Since its beginnings with Extreme Programming, there has been a shift away from the waterfall design to an agile development process. More recently, the Shift-Left movement has advocated for security to be considered from the start and not as an afterthought.In order to design secure software, it is naturally important to understand how insecurities creep into code. We look at the most important enumerations of software bugs: OWASP and Mitre's CWEs. Lastly, patch management has become the most import defensive tool for an organization. We look at this topic both from a software development perspective as well as from the customer's point of view.

Course Outcomes

On successful completion, students will be able to

- avoid common software implementation and design mistakes.
- design a software development lifecycle process based on DevSecOps principles.
- incorporate vulnerability reporting and response into the SDL.
- organize and manage a bug bounty program.
- implement and manage a corporate patch management process.

Contents

1. Introduction to the software development process
   - 1.1 Traditional software development: Waterfall design
   - 1.2 Iterative design
   - 1.3 Agile software development
   - 1.4 Operations as a separate process
   - 1.5 Infrastructure as code
   - 1.6 Merging Development and Operations: DevOps

2. DevOps best practices
   - 2.1 Coding: code development and review, source code management tools, code merging.
   - 2.2 Building: continuous integration tools, build status.
   - 2.3 Testing: continuous testing tools that provide quick and timely feedback on business risks.
   - 2.4 Packaging: artifact repository, application pre-deployment staging.
   - 2.5 Releasing: change management, release approvals, release automation.
   - 2.6 Configuring: infrastructure configuration and management, infrastructure as code tools.
   - 2.7 Monitoring: applications performance monitoring, end-user experience.

3. Sources of security bugs
   - 3.1 General classes of bugs
   - 3.2 Looking at the OWASP top ten
   - 3.3 Looking at the Mitre CWE™

4. DevSecOps
   - 4.1 Protection goals
   - 4.2 Threat modeling
   - 4.3 Choice of programming language, tool chain and infrastructure
   - 4.4 Linting for code security issues
   - 4.5 Testing for security
   - 4.6 Security by design/Shifting Left
   - 4.7 Security as a people problem
   - 4.8 Designing in a bug reporting and response process
   - 4.9 Managing a bug bounty program

5. Patch management
   - 5.1 Dilemma: software update churn vs security
   - 5.2 Vulnerability disclosures and the Mitre CVE™ process
   - 5.3 Coordinated vulnerability disclosure
   - 5.4 Program security vs Software-as-a-Service patching
   - 5.5 Deployment strategies for catching bugs early

6. Summary and research problems

Literature
Compulsory Reading
Further Reading ▪ Anderson, R. (2020): Security Engineering. 3rd edition, Wiley, Hoboken, NJ. ▪ Mitre CVEs: https://cwe.mitre.org ▪ OWASP Top-ten: https://owasp.org/www-project-top-ten/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

4. Semester

IT-Service Management

Module Code: DLBCSITSM

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (IT-Service Management)

Contributing Courses to Module

- IT-Service Management (DLBCSITSM01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Fundamentals and terms of IT Service Management
- IT Infrastructure Library (ITIL)
- ITIL - Service Design
- ITIL - Service Transition
- ITIL - Service Operation
- Information Security Management with the IT-Baseline Protection-Framework of the BSI

Learning Outcomes

IT-Service Management

On successful completion, students will be able to

- identify the basics and challenges of IT service management.
- describe the motivation and structure of the IT Infrastructure Library (ITIL) in order to determine its main elements and distinguish concrete activities in the service life cycle.
- present and compare the activities of ITIL governance and ITIL operational processes and develop concrete solutions using these activities.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field(s) of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field(s).

IT-Service Management

Course Code: DLBCSITSM01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT Service Management is an approach to aligning and understanding a company's IT as a service provider and supporter of operational and business processes. Quality management and the handling of daily operations are at the forefront.This course covers the use of the IT Infrastructure Library (ITIL) in order to teach concepts, procedures, and best practice in IT Service Management (IT Operations).The course therefore considers the management of activities within the SW life cycle, which take place after the development of an IT system, and IT operation as a ongoing process in the day-to-day operation of a company’s IT department.

Course Outcomes

On successful completion, students will be able to

- identify the basics and challenges of IT service management.
- describe the motivation and structure of the IT Infrastructure Library (ITIL) in order to determine its main elements and distinguish concrete activities in the service life cycle.
- present and compare the activities of ITIL governance and ITIL operational processes and develop concrete solutions using these activities.

Contents

1. Fundamentals and Terms of IT Service Management
   - 1.1 IT Services
   - 1.2 IT Service Management
2. IT Infrastructure Library (ITIL)
   - 2.1 Service Life Cycle and Process Groups in ITIL
   - 2.2 Service Strategy
   - 2.3 Continual Service Improvement
3. ITIL – Service Design
   - 3.1 Service Level Management
   - 3.2 Service Catalog Management
   - 3.3 Availability Management
   - 3.4 Further Processes in the Service Transition

4. ITIL – Service Transition
   - 4.1 Transition Planning and Support
   - 4.2 Change Management
   - 4.3 Service Asset and Configuration Management (SACM)
   - 4.4 Further Processes in the Service Transition

5. ITIL – Service Operation
   - 5.1 Event Management
   - 5.2 Incident Management
   - 5.3 Problem Management
   - 5.4 Further Processes in the Service Operation

6. Information Security Management with the IT-Baseline Protection Framework of the BSI
   - 6.1 Structure and Elements of BSI Basic Protection
   - 6.2 The Information Security Process

Literature

Compulsory Reading

Further Reading

- Beims, M. (2012): IT-Service Management in der Praxis mit ITIL. Hanser, München.
- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2008): BSI-Standard 100-1. Managementsysteme für Informationssicherheit (ISMS). (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile [letzter Zugriff: 27.02.2017]).
- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2008): BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise. (URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile [letzter Zugriff: 27.02.2017]).
- Bundesamt für Sicherheit und Informationstechnik (Hrsg.) (2014): IT-Grundschutz-Kataloge. 14. Ergänzungslieferung. (URL: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2014_EL14_DE.pdf [letzter Zugriff: 27.02.2017]).
- Renner, B./Moser, U./Schmid, D. (2006): IT-Service-Management. Transparente IT-Leistungen & Messbare Qualität. BPX Edition, Rheinfelden.
- Tiemeyer, E. (Hrsg.) (2011): Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. Hanser, München.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Cryptography

Module Code: DLBCSCT

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Cryptography)

Contributing Courses to Module

- Cryptography (DLBCSCT01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Protection targets, vulnerabilities, and threats
- Foundations of cryptology and its core components
- Basic cryptographic applications
- Authentication
- Single computer security
- Security communication network
- Security E-Commerce
- Secure software development

Learning Outcomes

Cryptography

On successful completion, students will be able to

- give an overview of different classes of cryptographic systems.
- give a basic description of symmetric cryptographic methods, in particular One-Time Pad, DES, and AES, and describe their operating principles by means of simple, concrete examples.
- describe the basic hash functions.
- describe basic asymmetric cryptographic methods, especially RSA, and their operating principles by means of simple, concrete examples.
- describe the areas of application of cryptographic procedures and their application scenarios.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Developement	All Bachelor Programmes in the IT & Technology fields

Cryptography

Course Code: DLBCSCT01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course covers basic and targeted in-depth knowledge of cryptographic processes and the practical use of cryptographic systems. After an overview of cryptographic methods, hash functions, symmetric methods, and asymmetric methods are presented. The theoretical basics of selected procedures are taught and practically explained using simple examples. In addition, areas of application and application scenarios for cryptographic procedures are presented.

Course Outcomes

On successful completion, students will be able to

- give an overview of different classes of cryptographic systems.
- give a basic description of symmetric cryptographic methods, in particular One-Time Pad, DES, and AES, and describe their operating principles by means of simple, concrete examples.
- describe the basic hash functions.
- describe basic asymmetric cryptographic methods, especially RSA, and their operating principles by means of simple, concrete examples.
- describe the areas of application of cryptographic procedures and their application scenarios.

Contents

1. Protection Goals, Vulnerabilities, and Threats
   - 1.1 Protection Goals
   - 1.2 Vulnerabilities and Threats
2. Foundations of Cryptology and its Core Components
   - 2.1 Encoding
   - 2.2 Symmetrical Encryption
   - 2.3 Asymmetric Encryption
   - 2.4 One-way Functions and Cryptographic Hash Functions

3. Basic Cryptographic Applications
   - 3.1 Key exchange and Hybrid Processes
   - 3.2 Digital Signature
   - 3.3 Message Authentication Code
   - 3.4 Steganographic Methods

4. Authentication
   - 4.1 Passwords and Public-Key-Certificates
   - 4.2 Challenge-Response-Procedure and Zero-Knowledge-Procedure
   - 4.3 Biometric Methods
   - 4.4 Authentication in Distributed Systems
   - 4.5 Identities Through Smartcards

5. Security of Single Computers
   - 5.1 Malware and Cookies
   - 5.2 Some Special Features of Operating Systems
   - 5.3 Web Server Security

6. Security in Communication Networks
   - 6.1 Security Problems and Defense Concepts
   - 6.2 Internet Standards for Communication Security
   - 6.3 Identity and Anonymity
   - 6.4 Security in Mobile and Wireless Communications

7. Security in E-Commerce
   - 7.1 Email Security
   - 7.2 Online Banking and Online Payments
   - 7.3 Electronic Money

8. Secure Software Development
   - 8.1 Threat Modeling
   - 8.2 Secure Software Design
   - 8.3 Techniques for Safe Programming

Literature
Compulsory Reading
Further Reading ▪ Baumann, U./Franz, E./Pfitzmann, A. (2014): Kryptographische Systeme. Springer Vieweg, Wiesbaden. ▪ Beutelspacher, A. (2014): Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. 10. Auflage, Springer Spektrum, Wiesbaden. ▪ Eckert, C. (2014): IT-Sicherheit. Konzepte – Verfahren – Protokolle. 9. Auflage, De Gruyter Oldenbourg, München. ▪ Ertel, W. (2010): Angewandte Kryptographie. 4. Auflage, Hanser, München. ▪ Spitz, S./Pramateftakis, M./Swoboda, J. (2011): Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen. 2. Auflage, Vieweg+Teubner; Wiesbaden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☑ Exam Template	

IT Law

Module Code: DLBCSIITL

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (International IT Law)

Contributing Courses to Module

- International IT Law (DLBCSIITL01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Written Assessment: Case Study, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Basic Concepts of Legal Systems
- Internet and Domain Law
- Contracts
- Intellectual Property
- Data Protection / Privacy

Learning Outcomes

International IT Law

On successful completion, students will be able to

- describe basic concepts of IT law.
- provide examples of different approaches to IT law in different countries.
- identify legal questions as they arise in IT.
- apply the core ideas of data protection and privacy in their work.
- distinguish the different types of contracts and intellectual property as they relate to IT.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the field(s) of Computer Science & Software Developement.	All Bachelor Programmes in the IT & Technology field(s).

International IT Law

Course Code: DLBCSIITL01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The application of IT is embedded in a legal framework which computer scientists need to know and adhere to in their work. This applies to the way their own work is performed which, for example, may be governed by contracts with suppliers and/or customers. Computer scientists create and use intellectual property, and this leads to questions of copyright, software patents, etc. Beyond this, IT strongly influences the social environment and therefore needs to abide by regulations such as data protection. The goal of this module is to provide students with a basic understanding of these legal aspects so they can take them into account, apply them in simple cases, and recognize when more specialised legal knowledge is required. Since IT is a topic that connects different countries and legal frameworks, the course looks at some of the common legal questions as they are handled in the European Union, the USA, and India.

Course Outcomes

On successful completion, students will be able to

- describe basic concepts of IT law.
- provide examples of different approaches to IT law in different countries.
- identify legal questions as they arise in IT.
- apply the core ideas of data protection and privacy in their work.
- distinguish the different types of contracts and intellectual property as they relate to IT.

Contents

1. Basic Concepts of Legal Systems
   - 1.1 The Role of Law in IT
   - 1.2 Basic Concepts of the Legal System in the European Union
   - 1.3 Basic Concepts of the Legal System in the USA
   - 1.4 Basic Concepts of the Legal System in India
2. Internet and Domain Law
   - 2.1 Web Sites and the Law
   - 2.2 Net Neutrality
   - 2.3 Domain Registration
   - 2.4 Internet Crime

3. Contracts
   - 3.1 Types of IT Contracts
   - 3.2 Electronic Contracts and Electronic Signatures
   - 3.3 Licences
   - 3.4 Free and Open Source Software
   - 3.5 Buying and Selling Off-the-Shelf Software
   - 3.6 Software Development Contracts

4. Intellectual Property
   - 4.1 Brands, Trade Marks and Domain Names
   - 4.2 Copyright
   - 4.3 Software Patents
   - 4.4 Digital and Data Ownership

5. Data Protection/Privacy
   - 5.1 Basic Concepts of Data Protection
   - 5.2 Data Protection in the European Union: the GDPR
   - 5.3 Data Protection in the USA
   - 5.4 Data Protection in India
   - 5.5 Trans-Border Data Flows

Literature

Compulsory Reading

Further Reading

- Hoeren, T., & Pinelli, S. (2018). Agile programming – Introduction and current legal challenges. Computer Law & Security Review, 34(5), pp. 1131-1138. Retrieved from www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Hr.-Hoeren-29.10.pdf
- Lloyd, I. (2018). Information technology law (8th ed.). Oxford: Oxford University Press.
- Murray, A. (2019). Information technology law: The law and society (4th ed.). Oxford: Oxford University Press.
- Soma, J. T. (2014). Privacy law in a nutshell. St. Paul, MN: West Academic.
- Wikia.org. (n.d.). The IT law wiki [web encyclopedia]. Retrieved from https://itlaw.wikia.org/wiki/The_IT_Law_Wiki#

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Case Study

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Case Study, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Host and Software Forensics

Module Code: DLBCSEHSF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSESPB01_E or DLBCSESPB01_D	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Host and Software Forensics)

Contributing Courses to Module

- Host and Software Forensics (DLBCSEHSF01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Tools and methods for host forensics
- Malware sandboxing and reverse engineering
- Report and presentation writing

Learning Outcomes

Host and Software Forensics

On successful completion, students will be able to

- understand the requirements on system forensics analysis.
- know the available tools and methods for evidence collection and analysis.
- understand the principles of Malware sandboxing and reversing.
- write reports and presentations with the target audience in mind.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Host and Software Forensics

Course Code: DLBCSEHSF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSESPB01_E or DLBCSESPB01_D

Course Description

Security officers will encounter security incidents on a regular basis nowadays and will be called upon to examine the damage. We look at both criminal and business policy violation investigations. In particular how to collect and evaluate evidence.We look at different types of unwanted activity and how these manifest themselves in the data we collect. With the appropriate tools, the evidence can be collected and if necessary, a Chain of Custody ensured using appropriate cryptographic methods.Capturing the files on the disk is standard practice in computer forensics. However, a part of the evidence collection process is also capturing information from the running system which includes memory and process capture.The collected evidence must be evaluated appropriately, and logical conclusions drawn from it. Often, possible Malware is found on the victim system. We look at two methods of analyzing the Malware: Sandboxing and Reverse engineering.The results are put in a report and consideration needs to be taken who the target audience of the report and possible presentation will be. Good communication is vital here.

Course Outcomes

On successful completion, students will be able to

- understand the requirements on system forensics analysis.
- know the available tools and methods for evidence collection and analysis.
- understand the principles of Malware sandboxing and reversing.
- write reports and presentations with the target audience in mind.

Contents

1. Principles of computer forensics
   - 1.1 Investigation basics: Criminal vs. Business policy
   - 1.2 Policies, Legal frameworks and standards
   - 1.3 Expert witnesses

2. Digital evidence
   - 2.1 Types of evidence
   - 2.2 Acquisition and Chain of Custody considerations
   - 2.3 Identification
   - 2.4 Evaluation
   - 2.5 Presentation

3. Types of computer crime
   - 3.1 Crime under the law
   - 3.2 Computer crime
   - 3.3 Jurisdiction

4. Host evidence collection
   - 4.1 Software tools
   - 4.2 Hardware support
   - 4.3 Cryptographic methods to ensure integrity and Chain of Custody
   - 4.4 Steps for crime scene search
   - 4.5 Cloud computing considerations
   - 4.6 SSD specific considerations
   - 4.7 Mobile device considerations
   - 4.8 Email considerations
   - 4.9 Encrypted file systems

5. System forensics
   - 5.1 Memory analysis
   - 5.2 Process dumps and analysis
   - 5.3 Windows forensics
   - 5.4 Linux forensics
   - 5.5 Mac OS-X forensics
   - 5.6 Apple iOS forensics
   - 5.7 Cloud forensics
   - 5.8 Web site forensics

6. Sandboxing Malware
   - 6.1 Commercial and open source tools
   - 6.2 Example: Cuckoo Sandbox
   - 6.3 Guest system considerations
   - 6.4 Spoonfeeding unwilling, slow or delayed Malware
   - 6.5 Reading sandbox reports
   - 6.6 Sandboxing as a part of operations

7. Principles of reverse engineering
   - 7.1 Clean room environment
   - 7.2 Machine code
   - 7.3 Principles of disassembly
   - 7.4 Decompilation
   - 7.5 What to look for
   - 7.6 Operating system interactions
   - 7.7 Using IDA-Pro
   - 7.8 Using Ghidra

8. Evaluation
   - 8.1 Connecting the dots
   - 8.2 Finding the root cause
   - 8.3 Mapping to Mitre ATT&CK® Techniques, Tactics and Procedures
   - 8.4 Avoiding jumping to conclusions

9. Presentation
   - 9.1 Report writing
   - 9.2 Law enforcement collaboration
   - 9.3 Preparation for court presentation
   - 9.4 Preparation for presentation to management

Literature

Compulsory Reading

Further Reading

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. https://attack.mitre.org/.
- Newman, R. C. (2007): Computer Forensics: Evidence Collection and Management. Auerbach Publications, Boca Raton, FL.
- Reddy, N. (2019): Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations. Apress, New York City, NY.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSEHSF01_E

Artificial Intelligence

Module Code: DLBDSEAIS1

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Artificial Intelligence)

Contributing Courses to Module

- Artificial Intelligence (DLBDSEAIS01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- chart the historical developments in artificial intelligence.
- understand the approach of contemporary AI systems.
- comprehend the concepts behind reinforcement learning.
- analyze natural language using basic NLP techniques.
- scrutinize images and their contents.

Learning Outcomes

Artificial Intelligence

On successful completion, students will be able to

- chart the historical developments in artificial intelligence.
- understand the approach of contemporary AI systems.
- comprehend the concepts behind reinforcement learning.
- analyze natural language using basic NLP techniques.
- scrutinize images and their contents.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology fields

Artificial Intelligence

Course Code: DLBDSEAIS01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The quest for artificial intelligence (AI) has captured humanity's interest for many decades and has been an active research area since the 1960s. This course will give a detailed overview of the historical developments, successes, and set-backs in AI, as well as modern approaches in the development of artificial intelligence.This course gives an introduction to reinforcement learning, a process similar to how humans and animals experience the world: exploring the environment and inferring the best course of action.This course also covers the principles of natural language processing and computer vision, both of which are key ingredients for an artificial intelligence to be able to interact with its environment.

Course Outcomes

On successful completion, students will be able to

- chart the historical developments in artificial intelligence.
- understand the approach of contemporary AI systems.
- comprehend the concepts behind reinforcement learning.
- analyze natural language using basic NLP techniques.
- scrutinize images and their contents.

Contents

1. History of AI
   - 1.1 Historical developments
   - 1.2 AI winter
   - 1.3 Expert systems
   - 1.4 Notable advances
2. Modern AI Systems
   - 2.1 Narrow versus general AI
   - 2.2 Application areas
3. Reinforcement Learning
   - 3.1 What is reinforcement learning?
   - 3.2 Markov Chains and value function
   - 3.3 Time-difference and Q Learning

4. Natural Language Processing (NLP)
   - 4.1 Introduction to NLP and application areas
   - 4.2 Basic NLP techniques
   - 4.3 Vectorizing data

5. Computer Vision
   - 5.1 Pixels and filters
   - 5.2 Feature detection
   - 5.3 Distortions and calibration
   - 5.4 Semantic segmentation

Literature

Compulsory Reading

Further Reading

- Bear, F./Barry, W./Paradiso, M. (2006): Neuroscience: Exploring the brain. 3rd ed., Lippincott Williams and Wilkins, Baltimore, MD:
- Bird S./Klein, E./Loper, E. (2009): Natural language processing with Python. 2nd ed., O'Reilly, Sebastopol, CA.
- Chollet, F. (2017): Deep learning with Python. Manning, Shelter Island, NY.
- Fisher, R. B., et al. (2016) : Dictionary of computer vision and image processing. John Wiley & Sons, Chichester.
- Geron, A. (2017): Hands-on machine learning with Scikit-Learn and TensorFlow. O'Reilly, Boston, MA.
- Goodfellow, I./Bengio, Y./Courville, A. (2016): Deep learning. MIT Press, Boston, MA.
- Grus, J. (2019): Data science from scratch: First principles with Python. O'Reilley, Sebastopol, CA.
- Jurafsky, D./Martin, J. H. (2008): Speech and language processing. Prentice Hall, Upper Saddle River, NJ.
- Nilsson, N. (2009): The quest for artificial intelligence. Cambridge University Press, Cambridge.
- Russell, S./Norvig, P. (2009): Artificial intelligence: A modern approach. 3rd ed., Pearson, Essex.
- Sutton, R./Barto, A. (2018): Reinforcement learning: An introduction. 2nd ed., MIT Press, Boston, MA.
- Szelski, R. (2011): Computer vision: Algorithms and applications. 2nd ed., Springer VS, Wiesbaden.
- Szepesvári, C. (2010): Algorithms for reinforcement learning. Morgan & Claypool, San Rafael, CA.
- Wiering, M./Otterlo, M. (2012): Reinforcement learning: State of the art. Springer, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBDSEAIS01

Information Security Standards

Module Code: DLBCSEISS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Information Security Standards)

Contributing Courses to Module

- Information Security Standards (DLBCSEISS01_E)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Written Assessment: Case Study	

Weight of Module

see curriculum

Module Contents

- Structure of the Information Security Standards
- Information Security Controls
- Information Security Management System (ISMS)
- Risk Management and Assessment

Learning Outcomes

Information Security Standards

On successful completion, students will be able to

- understand the general structure of information security standards.
- understand the normative content of the frameworks and standards.
- remember the required security controls.
- analyze existing Information Security Management Systems.
- evaluate Information Security Management Systems.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Information Security Standards

Course Code: DLBCSEISS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	None

Course Description

Information security includes digital as well as non-digital information. The subset IT-Security deals only with electronical processed, stored and transferred information. Thus, information security is about the security referring to digital and non-digital assets of an organization.

Course Outcomes

On successful completion, students will be able to

- understand the general structure of information security standards.
- understand the normative content of the frameworks and standards.
- remember the required security controls.
- analyze existing Information Security Management Systems.
- evaluate Information Security Management Systems.

Contents

1. Introduction to Information Security
   - 1.1 Basic Definitions, Security Concepts and Information Security Objectives
   - 1.2 Standards and Regulatory Frameworks
   - 1.3 Security Standards: ISO 27000 Family and BSI Standards
   - 1.4 Information Security Management System (ISMS)
2. Initiating an Information Security Management System
   - 2.1 Initial Setup for the ISMS
   - 2.2 Analysis of the Organization
   - 2.3 Analysis of the Existing ISMS and Determination of the Maturity
   - 2.4 Defining the ISMS Scope and Security Policies
3. Implementation of the Information Security Management System
   - 3.1 Risk Assessment
   - 3.2 Statement of Applicability (SoA)
   - 3.3 Definition of the Organizational Structure for Information Security
   - 3.4 Document Management and Communication Plan
   - 3.5 Definition of Controls and Procedures

4. Controlling of the Information Security Management System
   - 4.1 Monitoring, Measurement, Analysis and Evaluation
   - 4.2 Internal Auditing
   - 4.3 Management Review

5. Improving of the Information Security Management System
   - 5.1 Treatment of Challenges and Non-conformities
   - 5.2 Continual Improvement
   - 5.3 Corrective and Preventive Action Plans

6. Controls of the Information Security Management System
   - 6.1 General Structure of Controls
   - 6.2 Controls of the ISO 27001 – Annex A
   - 6.3 Management of Controls
   - 6.4 Evaluating the Effectiveness of Controls

Literature

Compulsory Reading

Further Reading

- Alexander, D./Finch, A./Sutton, D. (2013): Information Security Management Principles. Second edition, BCS, the Chartered Institute for IT, Swindon, UK.
- Chopra, A./Chaudhary, M. (2020): Implementing an information security management system. Security management based on ISO 27001 guidelines. Apress, New York.
- Awad, A. I./Yen, N./Fairhurst, M. (2018): Information Security. Foundations, Technologies and Applications. The Institution of Engineering and Technology, London.
- van Publishing, H. (2015): Foundations of information security based on ISO27001 and ISO27002. 2nd Edition, Van Haren Publishing, Hertogenbosch.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Case Study

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

DLBCSEISS01_E

5. Semester

Seminar: Current Topics in Computer Science

Module Code: DLBCSSCTCS

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Seminar: Current Topics in Computer Science)

Contributing Courses to Module

- Seminar: Current Topics in Computer Science (DLBCSSCTCS01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Written Assessment: Research Essay	

Weight of Module

see curriculum

Module Contents

- This seminar deals with current topics of computer science. Students make a dive deep into a specific topic within a sub-discipline of their choice.

Learning Outcomes

Seminar: Current Topics in Computer Science

On successful completion, students will be able to

- discuss in-depth and insightfully a given topic in the field of computer science.
- write about a certain computer science topic in terms of important characteristics, connections, and insights in the form of a research essay.
- execute the basics of scientific work and implement them in the context of a research essay.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the field(s) of Computer Science & Software Developement.	All Bachelor Programmes in the IT & Technology field(s).

Seminar: Current Topics in Computer Science

Course Code: DLBCSSCTCS01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This seminar is an opportunity for students to deepen the broad knowledge they will have gained over the previous four semesters of the study program. Students will choose a topic of specific individual interest that is connected to a sub-discipline of computer science. If a student, for example, is interested in the application of artificial intelligence in a specific context, elaborating context-specific use cases from a literature review can be the theme of the essay. Feedback provided by the tutor will help students strengthen any weaknesses they may have in scientific writing and academic work and prepare students for writing their bachelor thesis.

Course Outcomes

On successful completion, students will be able to

- discuss in-depth and insightfully a given topic in the field of computer science.
- write about a certain computer science topic in terms of important characteristics, connections, and insights in the form of a research essay.
- execute the basics of scientific work and implement them in the context of a research essay.

Contents

- Computer science is a broad subject area with many very different facets, depending on the specific sub-discipline. This seminar will address this diversity by taking up current trends in the context of individually-prepared texts. Each participant must create an essay for this purpose. Possible topics include Java and web development, data modeling and database systems, requirements engineering, and core computer science disciplines like operating systems, computer networks, distributed systems, algorithms, data structures, and programming languages.

Literature
Compulsory Reading
Further Reading ▪ Brookshear, G. / Bylow, D. (2014): Computer science: An overview. 12th edition, Pearson, Boston, MA. ▪ Gruhn,V. / Striemer, R. (Eds.) (2018): The essence of software engineering. Springer International Publishing, Cham. ▪ Springer. (n.d.) Lecture Notes in Computer Science. Springer, Heidelberg. ▪ Tardos, E. (Ed.). (n.d.) Journal of the ACM.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Advanced Data Analysis

Module Code: DLBDSEDA1

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Advanced Data Analysis)

Contributing Courses to Module

- Advanced Data Analysis (DLBDSEDA01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Business performance analytics
- Text mining
- Web- and social media analytics
- Experimentation and testing

Learning Outcomes

Advanced Data Analysis

On successful completion, students will be able to

- identify important design considerations for business KPIs.
- explain various topics in business process analytics.
- utilize established techniques for web data analytics.
- understand analytical approaches to text mining and semantic analysis.
- disambiguate relevant questions in social media analytics.
- use the techniques and methods for experimentation and testing.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology fields

Advanced Data Analysis

Course Code: DLBDSEDA01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

This course introduces several advanced analytics subjects of practical relevance. The subject areas covered span from business performance measurement and analytics, text mining, and web- and social media analytics to current trends in experimental design and setup. Along this journey topics such as the design of key performance indicators (KPIs), business process analytics, word frequency and semantic analysis, data science on clickstreams, social media interactions, and multi-armed bandit testing are addressed.

Course Outcomes

On successful completion, students will be able to

- identify important design considerations for business KPIs.
- explain various topics in business process analytics.
- utilize established techniques for web data analytics.
- understand analytical approaches to text mining and semantic analysis.
- disambiguate relevant questions in social media analytics.
- use the techniques and methods for experimentation and testing.

Contents

1. Business Performance Analytics
   - 1.1 KPI design considerations
   - 1.2 Common business performance indicators
   - 1.3 Business process mining
2. Text Analytics
   - 2.1 Word and document frequency (TF-IDF)
   - 2.2 Semantic analysis
3. Web Analytics
   - 3.1 Web metrics
   - 3.2 Clickstream analytics
   - 3.3 Recommender systems

4. Social Network Mining
   - 4.1 Introduction to social media analytics
   - 4.2 Mining common social media platforms

5. Testing and Experimentation
   - 5.1 Practical A/B testing
   - 5.2 Multivariate tests
   - 5.3 Multi-armed bandit testing

Literature

Compulsory Reading

Further Reading

- Hapke, H. / Howard, C. / Lane, H. (2019): Natural language processing in action.: Manning Publications, Shelter Island, NY.
- Kaushik, A. (2009): Web analytics 2.0: The art of online accountability and science of customer centricity. Sybex, Hoboken, NJ.
- Klassen, M. / Russell, M. A. (2019): Mining the social web. 3rd edition. O'Reilly Media, Sebastopol, CA.
- Marr, B. (2012): Key Performance Indicators (KPI). Pearson, Boston, MA.
- Neely, A. (Ed.) (2011): Business performance measurement: Unifying theory and integrating practice. 2nd edition, Cambridge University Press, Cambridge.
- Ojeda, T. / Bilbro, R. / Bengfort, B. (2018): Applied text analysis with Python. O'Reilly Media, Sebastopol, CA.
- Parmenter, D. (2015): Key performance indicators: Developing, implementing, and using winning KPIs. 3rd edition, John Wiley & Sons, Chichester.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Data Analysis

Module Code: DLBDSEDA2

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Project: Data Analysis)

Contributing Courses to Module

- Project: Data Analysis (DLBDSEDA02)

Module Exam Type

Module Exam	Split Exam
Study Format: Fernstudium Portfolio	

Weight of Module

see curriculum

Module Contents

Transfer of methodological knowledge to the implementation of real-world analytics use cases from the above-mentioned problem domains.

Learning Outcomes

Project: Data Analysis

On successful completion, students will be able to

- formulate and implement a real-world analytical use case.
- analyze the suitability of different possible approaches with respect to the project task.
- transfer acquired specialized analytical knowledge to real-world use cases.
- derive relevant design choices from the given project setting.
- make apposite choices with respect to implementation alternatives.
- select appropriate resources

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Data Science & Artificial Intelligence	All Bachelor Programs in the IT & Technology fields

Project: Data Analysis

Course Code: DLBDSEDA02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The focus of this course is the implementation of a real-world, advanced analytics use case in the form of a student project. Primary subject areas for this practical work include business performance analytics, text mining, web- and social analytics, and experimentation and testing.The goal is for students to demonstrate they can transfer the theoretical knowledge acquired in Advanced Data Analysis (DLBDSEDA01) to an implementation scenario that closely mimics project work in a professional data science setting.

Course Outcomes

On successful completion, students will be able to

- formulate and implement a real-world analytical use case.
- analyze the suitability of different possible approaches with respect to the project task.
- transfer acquired specialized analytical knowledge to real-world use cases.
- derive relevant design choices from the given project setting.
- make apposite choices with respect to implementation alternatives.
- select appropriate resources

Contents

- This course covers the practical implementation of the approaches and techniques covered in the course Advanced Data Analysis (DLBDSEDA01) in a project-oriented setting. Each participant must produce a project report detailing and documenting their work. Project tasks are chosen from a list or suggested by the students in accord with the tutor.

Literature
Compulsory Reading
Further Reading ▪ Hapke, H. / Howard, C. / Lane, H. (2019): Natural language processing in action.: Manning Publications, Shelter Island, NY. ▪ Kaushik, A. (2009): Web analytics 2.0: The art of online accountability and science of customer centricity. Sybex, Hoboken, NJ. ▪ Klassen, M. / Russell, M. A. (2019): Mining the social web. 3rd edition. O'Reilly Media, Sebastopol, CA. ▪ Marr, B. (2012): Key Performance Indicators (KPI). Pearson, Boston, MA. ▪ Neely, A. (Ed.) (2011): Business performance measurement: Unifying theory and integrating practice. 2nd edition, Cambridge University Press, Cambridge. ▪ Ojeda, T. / Bilbro, R. / Bengfort, B. (2018): Applied text analysis with Python. O'Reilly Media, Sebastopol, CA. ▪ Parmenter, D. (2015): Key performance indicators: Developing, implementing, and using winning KPIs. 3rd edition, John Wiley & Sons, Chichester.

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Portfolio

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods

- ☐ Learning Sprints®
- ☐ Course Book
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Exam Template
- ☐ Review Book
- ☐ Creative Lab
- ☑ Guideline
- ☑ Live Tutorium/Course Feed

Cloud Computing

Module Code: DLBDSCC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Cloud Computing)

Contributing Courses to Module

- Cloud Computing (DLBDSCC01)

Module Exam Type

Module Exam	Split Exam
Study Format: Distance Learning Exam, 90 Minutes	

Weight of Module

see curriculum

Module Contents

- Cloud computing fundamentals
- Relevant enabling technologies for cloud computing
- Introduction to serverless computing
- Established cloud platforms
- Cloud offerings for data science and analytics

Learning Outcomes

Cloud Computing

On successful completion, students will be able to

- understand the fundamentals of cloud computing and cloud service models.
- recognize enabling technologies that underlie current cloud offerings.
- cite the principles of serverless computing.
- analyze characteristics of established cloud offerings.
- describe cloud options for data science and machine learning

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Data Science & Artificial Intelligence	All Bachelor Programmes in the IT & Technology fields

Cloud Computing

Course Code: DLBDSCC01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Many of the recent advances in data science, particularly machine learning and artificial intelligence, rely on comprehensive data storage and computing power. Cloud computing is one way of providing that power in a scalable way, without considerable upfront investment in hardware and software resources. This course introduces the area of cloud computing together with its enabling technologies. Moreover, the most cutting-edge advances like serverless computing and storage are illustrated. Finally, a thorough overview on popular cloud offerings, especially in regard to analytics capabilities, is given.

Course Outcomes

On successful completion, students will be able to

- understand the fundamentals of cloud computing and cloud service models.
- recognize enabling technologies that underlie current cloud offerings.
- cite the principles of serverless computing.
- analyze characteristics of established cloud offerings.
- describe cloud options for data science and machine learning

Contents

1. Introduction to Cloud Computing
   - 1.1 Fundamentals of Cloud computing
   - 1.2 Cloud Service Models
   - 1.3 Benefits and Risks
2. Enabling Technology
   - 2.1 Virtualization and Containerization
   - 2.2 Storage Technology
   - 2.3 Networks and RESTful Services
3. Serverless Computing
   - 3.1 Introduction to Serverless Computing
   - 3.2 Benefits
   - 3.3 Limitations

4. Established Cloud Platforms
   - 4.1 Google Cloud Platform
   - 4.2 Amazon Web Services
   - 4.3 Microsoft Azure

5. Data Science in the Cloud
   - 5.1 Google Data Science and Machine Learning Services
   - 5.2 Amazon Web Services Data Science and Machine Learning Services
   - 5.3 Microsoft Azure Data Science and Machine Learning Services

Literature

Compulsory Reading

Further Reading

- Chapin, J., & Roberts, M. (2017). What is serverless? Sebastopol, CA: O'Reilly Media.
- Goessling, S., & Jackson, K. L. (2018). Architecting cloud computing solutions. Birmingham: Packt Publishing.
- Kavis, M. J. (2014). Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS). Hoboken, NJ: Wiley.
- Mahmood, Z., Puttini, R., & Erl, T. (2013). Cloud computing: Concepts, technology & architecture. Boston, MA: Prentice Hall.
- Rafaels, R. (2018). Cloud computing (2nd ed.). Scotts Valley, CA: CreateSpace Independent Publishing Platform.
- Sehgal, N. K., & Bhatt, P. C. P. (2018). Cloud computing: Concepts and practices. Cham: Springer.
- Zonooz, P. Farr, E., Arora, K., & Laszewski, T. (2018). Cloud native architectures. Birmingham: Packt Publishing.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBDSCC01

IT Security Consulting

Module Code: DLBCSEEISC_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEEISC01_E or DLBCSEEISC01_D ▪ none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Technical and Operational IT Security Concepts) / N.N. (Project: Configuration and Application of SIEM Systems)

Contributing Courses to Module

- Technical and Operational IT Security Concepts (DLBCSEEISC01_E)
- Project: Configuration and Application of SIEM Systems (DLBCSEEISC02_E)

Module Exam Type

Module Exam	Split Exam
	Technical and Operational IT Security Concepts • Study Format "Distance Learning": Exam, 90 Minutes Project: Configuration and Application of SIEM Systems • Study Format "Fernstudium": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Technical and Operational IT Security Concepts

- Network analysis and evaluation
- Protection Profiles
- Intrusion Detection Systems
- Network Monitoring
- Security Information and Event Management (SIEM)
- IT-Security evaluation and assessment

Project: Configuration and Application of SIEM Systems

- Network analysis and evaluation
- Protection Profiles
- Intrusion Detection Systems
- Network Monitoring
- Security Information and Event Management (SIEM)
- IT-Security evaluation and assessment

Learning Outcomes

Technical and Operational IT Security Concepts

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Project: Configuration and Application of SIEM Systems

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Technical and Operational IT Security Concepts

Course Code: DLBCSEEISC01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-Systems and Networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructure require higher security mechanism regarding confidentiality, integrity and availability. Based on specific “Protection Profiles” high sophisticated tools, mechanisms and procedures need to be designed, implemented, configurated and operated.With this course the student will be able to evaluate given IT-Infrastructure, support the security-design of new IT-Systems and Networks by developing specific Protection Profiles, evaluate which technical and operational security measures and application are required and how these are integrated, configured and operated.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Contents

1. Network Analysis and Evaluation
   - 1.1 Layer Specific Threats and Vulnerabilities
   - 1.2 DATA Flow, Interdependencies and Interrelationships
   - 1.3 Vulnerability Scanning and Detection
   - 1.4 Supporting Tools and Techniques

2. Protection Profiles
   - 2.1 Reference Architecture Technology and Networking
   - 2.2 Risk Assessment, Residual Risk and Risk Management
   - 2.3 Security Requirements and Safeguards
   - 2.4 Security Evaluation of IT-Security Products
   - 2.5 Accreditation of IT-Systems and Networks

3. Intrusion Detection Systems
   - 3.1 Detection Strategy
   - 3.2 Data Sources, Sensors
   - 3.3 Analytics
   - 3.4 Indicators of Compromise

4. Network Monitoring
   - 4.1 Threat Protection Systems
   - 4.2 Wireless Sensor Networks Technology
   - 4.3 Threat Information Sharing

5. Security Information and Event Management (SIEM)
   - 5.1 Technical and Operational DATA Sources
   - 5.2 DATA Fusion
   - 5.3 Network Norm Behavior
   - 5.4 Big Data Analysis – Transferring Technical Data for Operational Information
   - 5.5 Security Situation Picture, Situational Awareness
   - 5.6 Incident Response Strategies and Automated Responses

6. IT-Security Evaluation and Assessment
   - 6.1 IT-Security Metrics
   - 6.2 IT-Security Assessment

Literature
Compulsory Reading
Further Reading ▪ Federal Office for Information Security (BSI) (2018): IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT. ▪ Hayden, L. (2010): IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education, New York City, NY. ▪ McNab, C. (2016): Network Security Assessment: Know Your Network. 3. Auflage, O'Reilly UK Ltd., London. ▪ Miller, D. R. et al. (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Configuration and Application of SIEM Systems

Course Code: DLBCSEEISC02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEEISC01_E or DLBCSEEISC01_D

Course Description

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats. Furthermore, students will face the challenge to transfer technical data into operational Information to initiate valid responses. By the end of this course, students will have obtained well-founded knowledge of the integration of SIEM into enterprise IT infrastructure, applications and services.

Course Outcomes

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Contents

- This course focuses on practical aspects of the implementation of a SIEM into an enterprise IT infrastructure environment. Students start with a chosen use case and SIEM and then evaluate requirements which need to be fulfilled so that the SIEM can be used as part of an enterprise IT system / network. Students need to evaluate requirements for sensors, network monitoring, intrusion detection, data fusion, big data analytics, and translating technical data into operational information.
- Based on the available information, valid responses – including automated responses - will be identified and processed.
- All relevant artifacts and considerations are documented by the students in a project report.

Literature
Compulsory Reading
Further Reading ▪ Al-Sakib, K. P. (2016): The State of the Art in Intrusion Prevention and Detection. Routledge, Abingdon. ▪ Miller, D. et al (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY. ▪ Mitchell, H. B. (2007): Multi-Sensor Data Fusion: An Introduction. Springer Verlag, Berlin.

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Social Engineering

Module Code: DLBCSEESE_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSEESE01_E or DLBCSEESE01_D	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Social Engineering and Insider Threats) / N.N. (Project: Social Engineering)

Contributing Courses to Module

- Social Engineering and Insider Threats (DLBCSEESE01_E)
- Project: Social Engineering (DLBCSEESE02_E)

Module Exam Type

Module Exam	Split Exam
	Social Engineering and Insider Threats • Study Format "Distance Learning": Written Assessment: Case Study Project: Social Engineering • Study Format "Distance Learning": Oral Project Report

Weight of Module

see curriculum

Module Contents

Social Engineering and Insider Threats

- Social engineering methods
- Legal aspects of social engineering
- Compliance, code of conduct
- Insider threat detection
- Security policies and regulations
- National and international cooperation and information exchange

Project: Social Engineering

- Social engineering methods
- Legal aspects of social engineering
- Compliance, code of conduct
- Insider threat detection
- Security policies and regulations
- National and international cooperation and information exchange

Learning Outcomes

Social Engineering and Insider Threats

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Project: Social Engineering

On successful completion, students will be able to

- recognize the importance of the “Human Factor” in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Social Engineering and Insider Threats

Course Code: DLBCSEESE01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-systems and networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructures are of high interest for attackers to gain information (Cyber Espionage) to manipulate or destroy information and data as well as interrupt basic functions and services by compromising these systems and enterprises. One attack vector is targeted to the users and operators to misuse these people as workforce to break security policies and regulations. Social Engineering or social manipulation is widely used by adversaries to gain the necessary information to compromise IT-Infrastructures and to achieve their specific goals. Using methods of social engineering is very close to the so called “Insider Threat”. People from inside the organization act for various reasons against the security policies and regulations of their own enterprise. Revenge, dissatisfaction or sometimes criminal intent are reasons for such behavior. A combination of social engineering and “hostile insiders” is a gold nugget for all adversaries. Therefore, technical and organizational measures have to be developed and implemented to avert such threats. With this course, students will be able to recognize methods of social engineering and identify insider threats. They will be able to develop and implement preventive security policies and regulations as well as responsive security measures to counter these threats.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Contents

1. Social engineering methods
   - 1.1 Phishing, spear phishing
   - 1.2 Quid pro quo, baiting, media dropping
   - 1.3 Scareware, CEO-Fraud
   - 1.4 Pretexting, tailgating

2. Legal aspects of social engineering,
   - 2.1 Compliance, code of conduct
   - 2.2 Identity theft
   - 2.3 Data privacy

3. Insider threat detection
   - 3.1 DATA Mining for insider threat detection,
   - 3.2 Comprehensive Framework for insider threat detection and response
   - 3.3 Self-assessment tools for evaluation,
   - 3.4 Organizational learning
   - 3.5 Innovative processes
   - 3.6 Application of machine Learning methods

4. Security policies and regulations
   - 4.1 Organizational framework, compliance, code of conduct
   - 4.2 Training
   - 4.3 Incident response system
   - 4.4 Protection of classified / sensitive information
   - 4.5 Password policy
   - 4.6 Data storage and access profiles
   - 4.7 Interface monitoring and regulation (USB policy, ...)

5. National and international cooperation and information exchange.
   - 5.1 Cooperation with Internet Service Providers (ISP) and IT-Security stakeholders
   - 5.2 Exchange platforms and forums for Tactics Techniques and Procedures (TTP´s) and Best Practices
   - 5.3 Cooperation with national Security Authorities

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Hadnagy, C. (2012): Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe, MITP-Verlags GmbH & Co. KG, Frechen. ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET) ▪ Menger, A. (2016): IT-Sicherheit und Social Engineering. Grundlagen, Erscheinungsformen und Schutzmöglichkeiten. Hochschule Osnabrück.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Project: Social Engineering

Course Code: DLBCSEESE02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEESE01_E or DLBCSEESE01_D

Course Description

This project course will give students hands-on experience in the challenging task to prevent and counter social engineering attacks and eliminate or as a minimum mitigate the insider threat to the Enterprise IT-Systems and Networks. Students will need to consider practical aspects of social and psychological challenges – the so called “Human Factor” - as well as the application of technical toolkits to detect attacks driven by social engineering methods or caused by hostile insiders. Through this course Students will develop a complete overview of organizational, technical and procedural measures by analyzing the threat vector landscape, identify vulnerabilities and security gaps in the enterprise and develop and implement practical security policies and regulations, including security awareness campaigns, to prevent and recover from incidents caused by social engineering and insider threats.

Course Outcomes

On successful completion, students will be able to

- recognize the importance of the “Human Factor” in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Contents

- This project course focuses on practical aspects to prevent, detect and recover from social engineering driven attacks as well as threat deriving from hostile insiders. Students start with a chosen use case to analyze a tangible and successful social engineering campaign, identify the main attack vectors and learn how different activities on multiple levels concur to reach the objective or the attacker. Students need to analyze the security framework of the attacked enterprise, identify the vulnerability gaps and shortfalls that allowed the social engineering attack to be successful. Taking into account the “Human Factor” the students will

then develop organizational and technical security policies to show how a specific attack could have been prevented and the damage been avoided or mitigated. All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET)

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods

- ☐ Learning Sprints®
- ☐ Course Book
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Exam Template
- ☐ Review Book
- ☐ Creative Lab
- ☑ Guideline
- ☐ Live Tutorium/Course Feed

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Static and Dynamic Malware Analysis) / N.N. (Seminar: Sandbox Interpretation)

Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02_E)

Module Exam Type

Module Exam	Split Exam
	Static and Dynamic Malware Analysis • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Static and Dynamic Malware Analysis

- Objectives in Malware analysis
- Analysis Lab setup
- Tools of the trade
- Malware Classification
- Sandboxes
- Reversing
- Digging deeper

Seminar: Sandbox Interpretation

This course is about the practical application of Malware analysis techniques to real sandbox log files.

Learning Outcomes

Static and Dynamic Malware Analysis

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Seminar: Sandbox Interpretation

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Malware is a top compromise vector in cyber attacks. Analyzing the attacking Malware gives the security analyst insights into the methodology and intension of the attacker. There are a number of ways that Malware can be analyzed and this course will introduce the most common ones.

Course Outcomes

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Contents

1. Objectives in Malware analysis
   - 1.1 Forensics
   - 1.2 Root cause analysis
   - 1.3 Mitigation
2. Analysis Lab setup
   - 2.1 Stealth
   - 2.2 Isolation
   - 2.3 Honeypots
3. Tools of the trade
   - 3.1 Virtual machines
   - 3.2 Debugger
   - 3.3 Disassembler

4. Malware Classification
   - 4.1 Antivirus
   - 4.2 Virustotal
   - 4.3 Yara
   - 4.4 Clustering with PEID, TELFHASH, TLSH, SSDEEP, etc

5. Sandboxes
   - 5.1 Levels of interaction
   - 5.2 Instrumentation
   - 5.3 Online sandboxing services, Virustotal
   - 5.4 Scripting for sandboxes
   - 5.5 Corporate sandbox considerations

6. Reversing
   - 6.1 Unpacking, decrypting and de-obfuscation
   - 6.2 Debugging techniques
   - 6.3 Control flow analysis
   - 6.4 Library and system calls

7. Digging deeper
   - 7.1 Domain and IP information
   - 7.2 Analysis of Javascript code
   - 7.3 Memory forensics
   - 7.4 Kernel debugging rootkits
   - 7.5 Theoretical underpinnings of program analysis

Literature

Compulsory Reading

Further Reading

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. https://attack.mitre.org/
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020)

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E

Course Description

In this course, we explore the most important tool in Malware analysis, the Sandbox and extract from the Sandbox logs the potential attacks exhibited by the Malware.

Course Outcomes

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Contents

- This course is about the practical application of Malware analysis techniques to real sandbox log files and extract the indicators of compromise and Malware objectives into a report.

Literature

Compulsory Reading

Further Reading

- Gregg, M. (2008): Build Your Own Security Lab: A Field Guide for Network Testing. Wiley, Hoboken, NJ.
- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEHF02_E

DevSecOps

Module Code: DLBCSEEDSO_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ IWNF01_E or IWNF01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Techniques and methods for agile software development) / N.N. (Project: Agile DevSecOps Software Engineering)

Contributing Courses to Module

- Techniques and methods for agile software development (IWNF01_E)
- Project: Agile DevSecOps Software Engineering (DLBCSEEDSO01_E)

Module Exam Type

Module Exam	Split Exam
	Techniques and methods for agile software development • Study Format "Distance Learning": Exam, 90 Minutes Project: Agile DevSecOps Software Engineering • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Techniques and methods for agile software development

- Characteristics and principles of agility
- Agility in small teams with SCRUM
- Agile portfolio and project management
- Agile requirements and IT architecture management
- Agile Testing
- Agile Delivery and Deployment

Project: Agile DevSecOps Software Engineering

This module provides the fundamental security principles for leveraging DevOps in software engineering, also known as the DevSecOps paradigm. Given a security-relevant scenario, this module will illustrate good DevSecOps practices like definition of security baselines, threat modelling approaches, and security automation as part of the continuous integration/continuous development (CI/CD) pipeline.

Learning Outcomes

Techniques and methods for agile software development

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Project: Agile DevSecOps Software Engineering

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Techniques and methods for agile software development

Course Code: IWNF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The goal of the course is to give students a deeper insight into the topic of agile software development. First of all, the basic characteristics and principles of agility are presented and discussed. Afterwards, it is shown how small projects and teams can use agile software engineering and how agile principles can be transferred and applied to large projects. Afterwards, agile techniques are taught for selected core activities in software engineering, with a focus on testing, delivery and deployment.

Course Outcomes

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Contents

1. Characteristics and Principles of Agility
   - 1.1 Features and Challenges of Software Projects
   - 1.2 Classification of Uncertainty
   - 1.3 Comparison of Agile and Classic Software Development
   - 1.4 Principles of Agility
2. Agility in Small Teams with Scrum
   - 2.1 Basics and General Structure with SCRUM
   - 2.2 Central Management Artifact: Product Backlog
   - 2.3 Other Management Artifacts

3. Agile Portfolio and Project Management
   - 3.1 Planning Levels in Agile Project Management
   - 3.2 Agile Portfolio Management
   - 3.3 Organization of Several Teams in One Project
   - 3.4 Product and Release Planning

4. Agile Requirements and IT Architecture Management
   - 4.1 Requirements Engineering in Agile Projects
   - 4.2 Architecture Management in Agile Projects

5. Agile Testing
   - 5.1 Basic Principles and Requirements for the QA Organization
   - 5.2 Test Levels and Agility
   - 5.3 Test Automation

6. Agile Delivery and Deployment
   - 6.1 Basics and Continuous Delivery Pipeline
   - 6.2 Continuous Build and Continuous Integration
   - 6.3 Acceptance Tests, Load Tests and Continuous Deployment

Literature

Compulsory Reading

Further Reading

- Biffl, S. et al. (Hrsg.) (2005): Value-Based Software Engineering. Springer, Berlin/Heidelberg.
- Cockburn, A. (2007): Agile Software Development. The Cooperative Game. 2nd edition, Addison-Wesley, Upper Saddle River, NJ.
- Cohn, M. (2005): Agile Estimating and Planning. Prentice Hall, Upper Saddle River, NJ.
- Crispin, L. (2008): Agile Testing: A Practical Guide for Testers and Agile Teams. Addison Wesley, Upper Saddle River, NJ.
- Highsmith, J. (2009): Agile Project Management: Creating Innovative Products. Addison Wesley, Upper Saddle River, NJ.Layton, M. C. (2012): Agile project management for dummies. John Wiley & Sons, New York, NY.
- Rubin, K. S. (2012): Essential Scrum: A Practical Guide to the Most Popular Agile Process. Addison Wesley, Upper Saddle River, NJ.
- Schwaber, K. (2014): Agile Project Management with Scrum. Microsoft Press, Redmond, WA.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Agile DevSecOps Software Engineering

Course Code: DLBCSEEDSO01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	IWNF01_E or IWNF01

Course Description

This course covers the basic security principles for leveraging the DevSecOps approach in software engineering scenarios. The content of this course will illustrate the adoption of DevSecOps to continuously and holistically improve the security of an organization, rather than just focusing on protecting the underlying software infrastructure (as in the case of traditional non-agile methodologies). By presenting DevSecOps principles like threat modelling, definition of security baselines, security automation/tools, and continuous compliance monitoring, this course will teach how security can be integrated while developing a software engineering product.

Course Outcomes

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Contents

- Despite the broad adoption of DevOps in the industry, the integration of security principles into this paradigm (i.e., DevSecOps) is still an open challenge for many practitioners. In this course the students will learn fundamental DevSecOps concepts like threat modelling, definition of security baselines, continuous compliance monitoring, and integration of security automation in DevOps.

Literature
Compulsory Reading
Further Reading ▪ Johnson, E. (2020): Secure DevOps. A Practical Introduction. (URL: https://www.sans.org/ondemand/course/secure-dev-ops-a-practical-introduction [Retrieved: 15.08.2020]). ▪ Hsu, T. (2018): Hands-On Security in DevOps. Packt Publishing, UK. ▪ Microsoft. (2020): Secure DevOps. Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity. (URL: https://www.microsoft.com/en-us/securityengineering/devsecops [Retrieved: 15.08.2020]). ▪ Schneider, C. (2015): Security DevOps. Staying secure in agile projects. (URL: https://owaspappseceurope2015.sched.com/event/378l/security-devops-staying-secure-in-agile-projects [Retrieved: 15.08.2020]). ▪ Yasar, H. (2016): An Introduction to Secure DevOps. Including Security in the Software Lifecycle. (URL: https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html [Retrieved: 15.08.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Security in Complex Networks

Module Code: DLBCSEESCN_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSEITPAM02 or IAMG01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (IT Architecture Management) / N.N. (Project: IT Security Architecture)

Contributing Courses to Module

- IT Architecture Management (DLBCSEITPAM02)
- Project: IT Security Architecture (DLBCSEESCN01_E)

Module Exam Type

Module Exam	Split Exam
	IT Architecture Management • Study Format "Distance Learning": Exam, 90 Minutes Project: IT Security Architecture • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

IT Architecture Management

- Basic terms and foundations of IT enterprise architectures management
- IT application portfolio management
- Architecture governance
- Modeling of IT enterprise architectures
- Frameworks using TOGAF as an example
- Reference models and sample catalogues

Project: IT Security Architecture

Using well-known methods and techniques from the field of IT architecture management, students will be able to develop a well-grounded overview of IT-infrastructure regarding IT-strategy and strategic management. Students will understand and take advantage of typical concepts, methods and models for all tasks in the framework of architecture management. Emphasis will be taken to the security aspects of the IT infrastructure by designing and implementing IT-security architecture in the overall framework.

Learning Outcomes

IT Architecture Management

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Project: IT Security Architecture

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

IT Architecture Management

Course Code: DLBCSEITPAM02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In addition to concrete IT projects, such as the development of a new IT system or the introduction of standard software, a strategic management system for organizational-wide IT infrastructure – that is, for all IT hardware and software systems – must be used.Strategic management is the responsibility of the IT enterprise architect, who operates IT architecture management. Their task is to strategically align IT infrastructure with an organization's business and IT strategy.This course covers the typical concepts, methods, procedures, and IT models of architecture management.

Course Outcomes

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Contents

1. Basic Terms and Foundation for the Management of IT Enterprise Architectures
   - 1.1 IT Enterprise Architecture
   - 1.2 Goals of Enterprise Architecture Management
   - 1.3 Processes in the Management of IT Enterprise Architectures
2. IT Application Portfolio Management
   - 2.1 IT Application Portfolio Management Overview
   - 2.2 Application Manual
   - 2.3 Portfolio Analysis
   - 2.4 Development Planning

3. Architecture Governance
   - 3.1 Organizational Structure
   - 3.2 Policy Development and Enforcement
   - 3.3 Project Support

4. Modeling of IT Enterprise Architectures
   - 4.1 Models in the Context of IT Architecture Management
   - 4.2 Forms of Documentation for Processes and Applications
   - 4.3 Forms of Documentation for Systems and Technologies

5. Frameworks Using the Example of TOGAF
   - 5.1 Fundamentals and Use of IT Architecture Frameworks
   - 5.2 Overview and Categories of EAM Frameworks
   - 5.3 The Open Group Architecture Framework (TOGAF)

6. Reference Models and Sample Catalogues
   - 6.1 Architecture Reference Models
   - 6.2 EAM Design Sample Catalogue

Literature

Compulsory Reading

Further Reading

- Hanschke, I. (2011): Enterprise Architecture Management. Einfach und effektiv. Hanser, München.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt.verlag, Heidelberg.
- Keuntje. J. H./Barkow, R. (Hrsg.) (2010): Enterprise Architecture. Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen. Symposion Publishing, Ettlingen.
- Ross, J. W./ Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston, MA.
- Schwarzer, B. (2009): Einführung in das Enterprise Architecture Management. Verstehen – Planen – Umsetzen. Books on Demand, Norderstedt.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: IT Security Architecture

Course Code: DLBCSEESCN01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEITPAM02 or IAMG01

Course Description

Using methods and techniques from the field IT architecture management, students will work independently on a practical question of IT security architecture. By the end of this course students will be able to independently develop IT security architecture models, based on an existing IT-system / network architecture.

Course Outcomes

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Contents

- Implementation and documentation of practical questions regarding IT security in the framework of IT architecture management. Typical scenarios are, for example, “Implementation of IT security devices in complex networks”, “Design of processes for security updates and patch management” and “using in-house resources or outsourcing of IT security tasks”.

Literature

Compulsory Reading

Further Reading

- Bartsch, M. / Frey, S. (2014): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien, Wiesbaden.
- Müller, K.-R. (2014): IT-Sicherheit mit System. Springer Fachmedien, Wiesbaden.
- Pfister, M. (2019): In 3 einfachen (aber wichtigen) Schritten zur Enterprise IT-Sicherheitsarchitektur (URL: https://www.infoguard.ch/de/blog/in-3-schritten-zur-enterprise-it-sicherheitsarchitektur [Retrieved: 17.07.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E ▪ DLBCSEINF01_E or DLBCSEINF01_D	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Protocols, Log- and Dataflow-Analysis in Depth) / N.N. (Seminar: Threat Hunting, Analysis and Incident Response)

Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02_E)

Module Exam Type

Module Exam	Split Exam
	Protocols, Log- and Dataflow-Analysis in Depth • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Threat Hunting, Analysis and Incident Response • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Introduction
- Basic protocol layering
- Operating system logs
- HTTP server
- IP Firewall
- Web application filter
- Authentication servers
- Databases
- Intrusion Detection and Protection System (IDPS)
- Email systems
- Content filters
- SSH
- Less common systems
- Context
- Log management Infrastructure
- Security Information and Event Management (SIEM)
- Visualization
- Security Operations Centers (SOC)
- Logging in the cloud
- Dataflow monitoring
- Attacks against logging
- Analysis techniques
- Reporting

Seminar: Threat Hunting, Analysis and Incident Response

- Mitre ATT&CK TTPs
- APT actors
- Security coverage gap analysis

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Seminar: Threat Hunting, Analysis and Incident Response

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Contents

1. Introduction
   - 1.1 Network protocols
   - 1.2 Applications of log files
   - 1.3 Operating system log files
   - 1.4 Application log files
   - 1.5 Network log files
   - 1.6 Dataflow logs
   - 1.7 Security log files

2. Basic protocol layering
   - 2.1 Internet protocol hierarchy
   - 2.2 TCP connection
   - 2.3 Frame layer
   - 2.4 Ethernet layer
   - 2.5 Internet Protocol layer
   - 2.6 Transport Control Protocol
   - 2.7 UDP packets
   - 2.8 TCP/IP in relation to the OSI layer model
   - 2.9 Reading RFCs and related documentation

3. Operating system logs
   - 3.1 Syslog
   - 3.2 System events
   - 3.3 Audit events

4. HTTP server
   - 4.1 Common server vendors
   - 4.2 Apache log format
   - 4.3 Web edge logging
   - 4.4 Logs from Content delivery networks

5. IP Firewall

6. Web application filter

7. Authentication servers

8. Databases

9. Intrusion Detection and Protection System (IDPS)

10. Email systems
    - 10.1 SMTP
    - 10.2 POP
    - 10.3 Exchange

11. Content filters
    - 11.1 Spam and Phish filters
    - 11.2 Malware filters
    - 11.3 Data leak prevention
12. SSH
13. Less common systems
    - 13.1 MQTT
    - 13.2 CoAP
    - 13.3 XMPP
    - 13.4 BGP
    - 13.5 RIP
    - 13.6 DNS
14. Context
    - 14.1 Asset management
    - 14.2 Known vulnerable systems
    - 14.3 Network topology
15. Log management Infrastructure
    - 15.1 Log generation
    - 15.2 Storage
    - 15.3 Analysis
    - 15.4 Monitoring
    - 15.5 Security and privacy of logs
    - 15.6 Roles and responsibility
    - 15.7 Policies
    - 15.8 Long term log storage
16. Security Information and Event Management (SIEM)
17. Visualization
18. Security Operations Centers (SOC)
19. Logging in the cloud
20. Dataflow monitoring

21. Attacks against logging

22. Analysis techniques
    - 22.1 Entry Normalization
    - 22.2 Semantics of log events
    - 22.3 Prioritizing entries
    - 22.4 Aggregation
    - 22.5 Rule based systems
    - 22.6 Anomaly detection
    - 22.7 Machine learning
    - 22.8 Triaging incidents
    - 22.9 Working with filters

23. Reporting
    - 23.1 Indicators of compromise
    - 23.2 Mapping to the Mitre ATT&CK framework
    - 23.3 STIX, TAXII
    - 23.4 Written reports and presentations

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- NIST Special Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

6. Semester

Business Intelligence

Module Code: DLBCSEBI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Sebastian Werning (Business Intelligence) / Prof. Dr. Sebastian Werning (Project: Business Intelligence)

Contributing Courses to Module

- Business Intelligence (DLBCSEBI01)
- Project: Business Intelligence (DLBCSEBI02)

Module Exam Type

Module Exam	Split Exam
	Business Intelligence • Study Format "Distance Learning": Exam, 90 Minutes Project: Business Intelligence • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Business Intelligence

- Basics of mobile software development
- Android system architecture
- Development environment
- Core components of an Android app
- Interaction between application components
- Advanced techniques

Project: Business Intelligence

Conception, implementation, and documentation of small, mobile applications on the basis of a concrete task.

Learning Outcomes

Business Intelligence

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Project: Business Intelligence

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Business Intelligence

Course Code: DLBCSEBI01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Business Intelligence (BI) is used to obtain information from company data that is relevant for targeted corporate management and the optimization of business activities. This course introduces and discusses techniques, procedures, and models for data provision, information generation, and analysis, as well the distribution of the information obtained. You will then be able to explain the various subject areas of data warehousing and independently select methods and techniques to meet specific requirements.

Course Outcomes

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Contents

1. Motivation and Conceptualization
   - 1.1 Motivation and Historical Development
   - 1.2 BI as a Framework
2. Data Provision
   - 2.1 Operative and Dispositive Systems
   - 2.2 The Data Warehouse Concept
   - 2.3 Architectural Variations
3. Data Warehouse
   - 3.1 ETL Process
   - 3.2 DWH and Data Mart
   - 3.3 ODS and Metadata

4. Modelling of Multidimensional Data Spaces
   - 4.1 Data Modeling
   - 4.2 OLAP Cubes
   - 4.3 Physical Storage
   - 4.4 Star and Snowflake Scheme
   - 4.5 Historicization

5. Analysis Systems
   - 5.1 Free Data Research and OLAP
   - 5.2 Reporting Systems
   - 5.3 Model-Based Analysis Systems
   - 5.4 Concept-Oriented Systems

6. Distribution and Access
   - 6.1 Information Distribution
   - 6.2 Information Access

Literature

Compulsory Reading

Further Reading

- Bachmann, R./Kemper, G. (2011): Raus aus der BI-Falle. Wie Business Intelligence zum Erfolg wird. 2. Auflage, mitp, Heidelberg.
- Bauer, A./Günzel, H. (2008): Data Warehouse Systeme. Architektur, Entwicklung, Anwendung. 3. Auflage, dpunkt.verlag, Heidelberg.
- Betz, R. (2015): Werde Jäger des verlorenen Schatzes. In: Immobilienwirtschaft, Heft 5, S. 1614–1164. (URL https://www.haufe.de/download/immobilienwirtschaft-ausgabe-052015-immobilienwirtschaft-fachmagazin-fuer-management-recht-praxis-303530.pdf [letzter Zugriff: 27.02.2017]).
- Bodendorf, F. (2006): Daten- und Wissensmanagement. 2. Auflage, Springer, Berlin.
- Chamoni, P./Gluchowski, P. (Hrsg.) (2006): Analytische Informationssysteme Business Intelligence-Technologien und -Anwendungen. Springer, Berlin.
- Engels, C. (2008): Basiswissen Business Intelligence. W3L, Herdecke/Witten.
- Gansor, T./Totok, A./Stock, S. (2010): Von der Strategie zum Business Intelligence Competency Center (BICC). Konzeption – Betrieb – Praxis. Hanser, München.
- Gluchowski, P./Gabriel, R./Dittmar, C. (2008): Management Support Systeme und Business Intelligence. Computergestützte Informationssysteme für Fach- und Führungskräfte. 2. Auflage, Springer, Berlin/Heidelberg.
- Grothe, M. (2000): Business Intelligence. Aus Informationen Wettbewerbsvorteile gewinnen. Addison-Wesley, München.
- Gutenberg, E. (1983): Grundlagen der Betriebswirtschaft, Band 1. Die Produktion. 18. Auflage, Springer, Berlin/Heidelberg/New York.
- Hannig, U. (Hrsg.) (2002): Knowledge Management und Business Intelligence. Springer, Berlin.
- Hansen, H.-R./Neumann, G. (2001): Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 8. Auflage, Lucius & Lucius UTB, Stuttgart.
- Humm, B./Wietek, F. (2005): Architektur von Data Warehouses und Business Intelligence Systemen. In: Informatik Spektrum, S. 3–14. (URL: https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm__Wietek_-_Architektur_DW__Informatik-Spektrum_2005-01_.pdf [letzter Zugriff: 27.02.2017]).
- Kemper, H.-G./Baars, H./Mehanna, W. (2010): Business Intelligence – Grundlagen und praktische Anwendungen. Eine Einführung in die IT-basierte Managementunterstützung. 3. Auflage, Vieweg+Teubner, Stuttgart.
- Turban, E. et al. (2010): Business Intelligence. A Managerial Approach. 2. Auflage, Prentice Hall, Upper Saddle River (NJ).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Business Intelligence

Course Code: DLBCSEBI02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using well-known methods and techniques from the field of Business Intelligence, students will work independently on a practical question in this course.At the end of the course you will be able to independently design and prototype Business Intelligence applications based on concrete requirements.

Course Outcomes

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Contents

- Implementation and documentation of practical questions regarding the use of Business Intelligence applications. Typical scenarios are, for example, “Management of BI projects”, “Design of multidimensional data models” and “Prototypical implementation of small BI applications”.

Literature

Compulsory Reading

Further Reading

- Brenner, W./Uebernickel, F. (2015): Design Thinking. Das Handbuch. Frankfurter Allgemeine Buch, Frankfurt a. M.
- Brown, T. (2008): Design Thinking. In: Harvard Business Review, Heft Juni, S. 84–95.
- Meinel, C./Weinberg, U./Krohn, T. (Hrsg.) (2015): Design Thinking Live. Wie man Ideen entwickelt und Probleme löst. Murmann, Hamburg.
- Uebernickel, F./Brenner, W. (2016): Design Thinking. In: Hoffmann, C. P. et al. (Hrsg.): Business Innovation: Das St. Galler Modell. Springer, Wiesbaden, S. 243–265.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Future Threats

Module Code: DLBCSEEFT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSRE01 or IREN01, DLBCSEEFT01_E or DLBCSEEFT01_D ▪ DLBCSRE01 or IREN01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Threat Modeling) / N.N. (Project: Threat Modeling)

Contributing Courses to Module

- Threat Modeling (DLBCSEEFT01_E)
- Project: Threat Modeling (DLBCSEEFT02_E)

Module Exam Type

Module Exam	Split Exam
	Threat Modeling • Study Format "Distance Learning": Exam, 90 Minutes Project: Threat Modeling • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Threat Modeling

- Thinking C.I.A. and beyond
- Measuring the Cyber Threat
- Threat Modeling
- Attack libraries
- Rules, Regulations, and Law Enforcement
- Risk management
- Threat Mitigation

Project: Threat Modeling

This course covers the theory and practice of discovering and modeling threats in a given system, architecture or scenario. It covers common methodologies and sources for common threat patterns. In a project, the theory is translated to practice by analyzing a given situation for threats.

Learning Outcomes

Threat Modeling

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Project: Threat Modeling

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Threat Modeling

Course Code: DLBCSEEFT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01

Course Description

When a system or architecture is being created it is vital that possible threats are evaluated at the same time. By using both modeling methodologies and past observed attack patterns, it is possible to take a new or existing system and examine it for possible threats. With this analysis, possible risks and mitigations can be derived. While the most common methodologies are based on Attack Trees and the STRIDE model, recently attack modelling has also been using repositories of attacker techniques, tactics and procedures for inspiration.

Course Outcomes

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Contents

1. Thinking C.I.A. and beyond
   - 1.1 Confidentiality
   - 1.2 Integrity
   - 1.3 Availability
   - 1.4 Safety and other concerns
2. Measuring the Cyber Threat
   - 2.1 Measurement and Management
   - 2.2 Cyber Threat Metrics
   - 2.3 Measuring the Threat for an Organization
   - 2.4 The Likelihood of Major Cyber Attacks
   - 2.5 Black Swan events

3. Threat Modeling
   - 3.1 Attack Tree methodology
   - 3.2 STRIDE
   - 3.3 DREAD
   - 3.4 Pyramid of Pain

4. Attack libraries
   - 4.1 CAPEC
   - 4.2 Solove's Taxonomy of Privacy
   - 4.3 Modeling with Mitre ATT&CK®
   - 4.4 Identifying new types of attacks

5. Rules, Regulations, and Law Enforcement
   - 5.1 Cyber Laws
   - 5.2 Compliance and Law Enforcement

6. Risk management
   - 6.1 Changing Approaches to Risk Management
   - 6.2 Incident Response and Crisis Management
   - 6.3 Factoring in black swan events
   - 6.4 Continuous reevaluation

7. Threat Mitigation
   - 7.1 Defensive Tactics and Technologies
   - 7.2 Risk mitigation strategies
   - 7.3 Validation of defenses
   - 7.4 Security and Privacy by Design
   - 7.5 Implementing threat mitigation in an organization

Literature
Compulsory Reading
Further Reading ▪ CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/ ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Mitre ATT&CK®. https://attack.mitre.org/ ▪ Pfleeger, C. P. / Pfleeger, S. L. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London. ▪ Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Threat Modeling

Course Code: DLBCSEEFT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01, DLBCSEEFT01_E or DLBCSEEFT01_D

Course Description

Threats to modern computer systems are diverse and ever evolving. In this project, the student will have the opportunity to apply the art and science of threat modeling to a scenario to be defined by the instructor together with the student. The basis will be case studies, real or fictive, to which the student will be expected to identify and report on the threats using an appropriate methodology. This can be selected from methodologies such as Attack Trees, STRIDE, DREAD or a justified enumeration of CAPEC or Mitre ATT&CK® TTPs as the student feels most appropriate. The results will be presented as a report.

Course Outcomes

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Contents

- To a given case or scenario, the student will model the threats using one of the established methodologies and then submit the report and, if appropriate, any code and data. Specific problems and contexts will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber
- Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS.
- Palmer, C. C. (2001): Ethical Hacking. In: IBM Systems Journal. 40 (3):769.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBDSCC01 or DLBDSCC01_D ▪ DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Security Controls in the Cloud) / N.N. (Project: Security by Design in the Cloud)

Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECS01_E)
- Project: Security by Design in the Cloud (DLBCSEECS02_E)

Module Exam Type

Module Exam	Split Exam
	Security Controls in the Cloud • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Security Controls in the Cloud

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

Project: Security by Design in the Cloud

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Learning Outcomes

Security Controls in the Cloud

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Project: Security by Design in the Cloud

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Security Controls in the Cloud

Course Code: DLBCSEECS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Contents

1. Cloud security is different
   - 1.1 Shared responsibility model
   - 1.2 Infrastructure as code
   - 1.3 The Private, Public and Hybrid Cloud
   - 1.4 Types of virtualization
   - 1.5 Cloud threat models: Mitre Cloud ATT&CK

2. Losing the intranet
   - 2.1 Identify and Access Management
   - 2.2 Principle of least privilege and fine-grained cloud access control
   - 2.3 Using Software Defined Networks, virtual private clouds and subnets
   - 2.4 Moving to a serverless architecture
   - 2.5 Defense in depth

3. Security by design
   - 3.1 Orchestration: Infrastructure as Code
   - 3.2 The Automate-Everything principle, Updating and Repeatability
   - 3.3 Reuse of good design patterns
   - 3.4 Container security
   - 3.5 Identification and Authentication

4. Secure cloud coding
   - 4.1 Software supply chain security
   - 4.2 Continuous Integration and Deployment
   - 4.3 Testing in code integration for security
   - 4.4 Canaries in code deployment
   - 4.5 Policy engines

5. Confidentiality aspects
   - 5.1 Secrets management
   - 5.2 Encryption of data at rest
   - 5.3 Encryption of data in transit
   - 5.4 Data leakage and exfiltration

6. Availability
   - 6.1 Storage tiers and locality
   - 6.2 Backup strategies
   - 6.3 Data and process redundancy
   - 6.4 Data lifecycle configuration
   - 6.5 DDoS mitigation

7. Locality
   - 7.1 Compliance requirements
   - 7.2 Geography of data/processes
   - 7.3 Redundancy of data centers
   - 7.4 Colocation for performance reasons

8. Monitoring and Audit
   - 8.1 Centralized logging
   - 8.2 Auditing orchestration scripts
   - 8.3 Detecting misconfigurations
   - 8.4 Cloud Forensics

9. Summary and Research topics
   - 9.1 Homomorphic encryption
   - 9.2 Attestation
   - 9.3 Proof-carrying data
   - 9.4 Side-channel attacks
   - 9.5 Conclusions

Literature

Compulsory Reading

Further Reading

- Mitre Cloud ATT&CK. https://attack.mitre.org/matrices/enterprise/cloud/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E

Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Literature

Compulsory Reading

Further Reading

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Principles of Ethical Hacking) / N.N. (Project: Pentesting)

Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEEPT01_E)
- Project: Pentesting (DLBCSEEPT02_E)

Module Exam Type

Module Exam	Split Exam
	Principles of Ethical Hacking • Study Format "Distance Learning": Exam, 90 Minutes Project: Pentesting • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module
see curriculum

Module Contents

Principles of Ethical Hacking

- History of ethical hacking
- Ethical and legal frameworks
- Planning phase
- Social Engineering & OSINT
- Tools
- RATs, Rootkits and Command & Control
- Data exfiltration
- Red/Blue Teams
- Bug Bounty programs
- Report writing

Project: Pentesting

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

Learning Outcomes

Principles of Ethical Hacking

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Project: Pentesting

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Contents

1. History of ethical hacking

2. Ethical and legal frameworks
   - 2.1 Certifications
   - 2.2 Defining parameters of engagement
   - 2.3 Contracts

3. Planning phase
   - 3.1 Using Mitre PreATT&CK® for reconnaissance
   - 3.2 User Mitre Enterprise ATT&CK® for tool selection
   - 3.3 Documentation

4. Social Engineering & OSINT

5. Tools
   - 5.1 Web application pentesting tools
   - 5.2 Remote execution testing tools
   - 5.3 Password cracking
   - 5.4 OSINT tools
   - 5.5 Fuzzing tools
6. RATs, Rootkits and Command & Control
7. Data exfiltration
8. Red/Blue Teams
9. Bug Bounty programs
10. Report writing

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Pentesting

Course Code: DLBCSEEPT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E

Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEPT02_E

Industrial Systems Technology

Module Code: DLBCSEEIST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBINGEIT01_E or DLBINGEIT01 ▪ none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Marian Benner-Wickner (Software Engineering Principles) / N.N. (Internet of Things Security)

Contributing Courses to Module

- Software Engineering Principles (IGIS01_E)
- Internet of Things Security (DLBCSEEIST01_E)

Module Exam Type

Module Exam	Split Exam
	Software Engineering Principles • Study Format "Distance Learning": Exam, 90 Minutes Internet of Things Security • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Software Engineering Principles

- binary system
- Structure and function of computer systems
- Structure and function of communication networks
- Software life cycle
- Roles, phases, activities in software engineering

Internet of Things Security

Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Learning Outcomes

Software Engineering Principles

On successful completion, students will be able to

- students can perform simple calculations in the binary system (Boolean algebra).
- students can describe the structure of computer systems and communication networks.
- students can distinguish between the phases of a SW life cycle.
- students can distinguish roles and phases in the software process.
- the students know different process models of SW development.
- the students know typical challenges and risks of enterprise SW development.
- the students know different programming paradigms and their application.

Internet of Things Security

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Software Engineering Principles

Course Code: IGIS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to give students an insight into the technical and theoretical basics of software engineering. In addition to the general structure of computer systems, students are taught typical challenges in the development of enterprise information systems. Furthermore, the typical phases and activities in software engineering are presented to address these risks.

Course Outcomes

On successful completion, students will be able to

- students can perform simple calculations in the binary system (Boolean algebra).
- students can describe the structure of computer systems and communication networks.
- students can distinguish between the phases of a SW life cycle.
- students can distinguish roles and phases in the software process.
- the students know different process models of SW development.
- the students know typical challenges and risks of enterprise SW development.
- the students know different programming paradigms and their application.

Contents

1. Structure and organization of information systems
   - 1.1 0 and 1 as the basis of all IT systems
   - 1.2 Von Neumann Architecture
   - 1.3 Distributed systems and communication networks
   - 1.4 Enterprise information systems

2. Risks and challenges of enterprise software engineering
   - 2.1 Properties of enterprise software systems
   - 2.2 Software Engineering
   - 2.3 Risks and typical problems
   - 2.4 Cause study
   - 2.5 Challenges in Software Engineering

3. Software life cycle: from planning to replacement
   - 3.1 The software life cycle at a glance
   - 3.2 Planning
   - 3.3 Development
   - 3.4 Operation
   - 3.5 Maintenance
   - 3.6 Shutdown

4. Requirements engineering and specification
   - 4.1 requirements engineering
   - 4.2 Specification

5. Architecture and implementation
   - 5.1 Architecture
   - 5.2 Implementation

6. Testing, operation and evolution
   - 6.1 Testing
   - 6.2 Operation
   - 6.3 Evolution

7. Roles in Software Engineering
   - 7.1 Idea of the role-based approach
   - 7.2 Typical roles

8. Organization of software projects
   - 8.1 From process paradigm towards software process
   - 8.2 Process Paradigms
   - 8.3 Product life cycle

9. Software Process Frameworks
   - 9.1 V-model XT
   - 9.2 Rational Unified Process (RUP)
   - 9.3 Scrum

Literature
Compulsory Reading
Further Reading ▪ Gumm, H. P./Sommer, M. (2011): Introduction to Computer Science. 9th edition, Oldenbourg, Munich. ▪ Hansen, H. R./Neumann, G. (2009): Information Systems 1. Fundamentals and Applications. 10th edition, UTB, Stuttgart. ▪ Ludewig, J./Lichter, H. (2010): Software Engineering. Basics, people, processes, techniques. 2nd edition, dpunkt.verlag, Heidelberg. ▪ Sommerville, I. (2015): Software Engineering. 10th edition, Pearson, Munich.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Internet of Things Security

Course Code: DLBCSEEIST01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBINGEIT01_E or DLBINGEIT01

Course Description

Internet of Things (IoT) is a mega trend. It covers end consumer systems as well as industrial systems and technologies (Industrial IoT, or IIoT). There is an increasing amount of interconnected devices that composes the Internet of Things. In general, the Internet of Things architecture consists of terminal devices, cloud solutions and actors/sensors. Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Course Outcomes

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Contents

1. Basics of the Internet of Things (IoT)
   - 1.1 Introduction
   - 1.2 Architecture
   - 1.3 Non-Industrial Internet of Things
   - 1.4 Industry 4.0 (Industrial IoT)
2. Internet of Things Attacks
   - 2.1 Vulnerabilities, Threats and Risks
   - 2.2 Cyber Attacks and Countermeasures
3. Security by Design
   - 3.1 Project Management / Secure Development Life Cycle
   - 3.2 Static Testing
   - 3.3 Dynamic Testing
   - 3.4 DevSecOps

4. Securing Internet of Things Devices
   - 4.1 Security Risks
   - 4.2 Design Objectives

5. Operational Security
   - 5.1 Information and Cyber Security Management System
   - 5.2 Network Security
   - 5.3 Device Configuration
   - 5.4 Authentication and Authorization

6. Cloud Security
   - 6.1 Concept of the Fog
   - 6.2 Threats to Cloud Internet of Things Services
   - 6.3 Cloud-Based Security Services
   - 6.4 Securing the Cloud Solution

7. Big Data / Artificial Intelligence
   - 7.1 Supervised Learning
   - 7.2 Unsupervised Learning

Literature

Compulsory Reading

Further Reading

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSEEIST01_E

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLBCSEECTI01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01_E)
- Project: Defense against APTs (DLBCSEECTI02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Threat Feeds • Study Format "Distance Learning": Exam, 90 Minutes Project: Defense against APTs • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Attack Models and Threat Feeds

- Apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model
- Determine what data is already available
- Do a gap analysis on what is detection or defense technology is missing
- Determine what extern threat feed data is required
- Utilize threat intelligence systems for diagnosis

Project: Defense against APTs

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a “table top exercise” which data is already available and which extern threat feed data is required. After analyzing the “attack side” students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

Learning Outcomes

Attack Models and Threat Feeds

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Project: Defense against APTs

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Attack Models and Threat Feeds

Course Code: DLBCSEECTI01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data.It is rare that internal data is enough for a complete analysis and in practice the threat analysist must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience.After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Contents

1. Threat actors
   - 1.1 Script kiddies
   - 1.2 eCrime threat actors
   - 1.3 Advanced Persistent Threat actors (APT)
   - 1.4 Threat researchers

2. Modeling an attack
   - 2.1 Phases of an attack
   - 2.2 Lockheed Martin Kill-Chain
   - 2.3 Attack Trees
   - 2.4 STRIDE
   - 2.5 DREAD
   - 2.6 The Diamond Model of attack analysis
   - 2.7 Pyramid of pain
   - 2.8 Techniques, Tactics and Procedures

3. Attack preparation TTPs
   - 3.1 Observability of attack preparations
   - 3.2 Operational security of an organization

4. Enterprise TTPs
   - 4.1 Behaviors of the attacker
   - 4.2 Observable data in an enterprise

5. ICS TTPs
   - 5.1 Critical infrastructure
   - 5.2 Special considerations with IoT/ICS defense

6. Threat data exchange
   - 6.1 Indicators of Compromise
   - 6.2 Threat intelligence reports
   - 6.3 Ad-hoc data formats
   - 6.4 STIX format, TAXII protocol
   - 6.5 Mitre ATT&CK, CVEs, etc.
   - 6.6 The semantics of threat data
   - 6.7 Other sources of data for CTI analysis

7. Examples of threat analysis platforms
   - 7.1 ACT Platform
   - 7.2 MISP
   - 7.3 OpenCTI

8. Examples of threat actors and their modus operandi
   - 8.1 Threat model
   - 8.2 Relevant indicator data
   - 8.3 Relevant CTI data
   - 8.4 Diagnosing the threat
   - 8.5 Data coverage gap analysis

9. Reporting
   - 9.1 Mapping raw data to Mitre ATT&CK
   - 9.2 Making defensive recommendations
   - 9.3 Writing reports for technical staff
   - 9.4 Writing reports for management
   - 9.5 Working with law enforcement

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Defense against APTs

Course Code: DLBCSEECTI02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT´s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures. To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT´s, ISP´s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of

their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT´s, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Mobile Threats

Module Code: DLBCSEEMT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBIBRVS01_E or DLBIBRVS01; DLBCSEINF01_E or DLBCSEINF01_D ▪ none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Wireless and Telecom Security) / N.N. (Software Architectures of Mobile Devices)

Contributing Courses to Module

- Wireless and Telecom Security (DLBCSEEMT01_E)
- Software Architectures of Mobile Devices (DLBCSEEMT02_E)

Module Exam Type

Module Exam	Split Exam
	Wireless and Telecom Security • Study Format "Distance Learning": Exam, 90 Minutes Software Architectures of Mobile Devices • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Wireless and Telecom Security

- Wireless protocols overview
- Wireless basics
- Telecom protocol classes
- Telecom architecture
- Handset and device security
- Threats
- Other wireless applications
- Protections

Software Architectures of Mobile Devices

- Handset technology stack
- Hardware
- Android operating system
- Apple iOS operating system
- Mobile devices
- Software ecosystems and security
- Mobile handset threats
- Mobile Device Management

Learning Outcomes

Wireless and Telecom Security

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Software Architectures of Mobile Devices

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Wireless and Telecom Security

Course Code: DLBCSEEMT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBIBRVS01_E or DLBIBRVS01; DLBCSEINF01_E or DLBCSEINF01_D

Course Description

The number of devices that can connect wirelessly to networks has already overtaken the number of desktop and laptop computers that connect to a local area network via a cable. In particular, phones and tablets dominate the market, and these connect to the wireless telecommunication networks. But there are also many other forms of wireless communication that devices use. The idiosyncrasies of these wireless systems need to be understood to integrate them in a complete security concept. Wireless protocols often force the user to trust in a system that they have no insights into and in this course, we will shine light onto the subject.

Course Outcomes

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Contents

1. Wireless protocols overview
   - 1.1 Personal area network protocols (Bluetooth, RFID, NFC, and more)
   - 1.2 Wireless local area network protocols (802.11a,b, g, ac , p and more)
   - 1.3 Wide area network protocols (Telecom protocols, LoRa, Satellite protocols, and more)
   - 1.4 Key exchange and cryptography in wireless networking
2. Wireless basics
   - 2.1 Frequencies
   - 2.2 Modulations
   - 2.3 Data Encodings
   - 2.4 Trade-offs

3. Telecom protocol classes
   - 3.1 Telecom vs IT terminology and technologies
   - 3.2 Telecom standards
   - 3.3 Legacy digital protocols
   - 3.4 LTE
   - 3.5 5G

4. Telecom architecture
   - 4.1 Overall architecture
   - 4.2 Core architecture
   - 4.3 Software defined networking
   - 4.4 5G Campus Networks
   - 4.5 Application layer security

5. Handset and device security
   - 5.1 Requirements
   - 5.2 Typical hardware design
   - 5.3 IoT Devices

6. Threats
   - 6.1 Common attack vectors against devices and handsets
   - 6.2 Common attack vector against the core network
   - 6.3 Potential attacks against 5G campus networks

7. Other wireless applications
   - 7.1 Aviation and Nautical wireless protocols
   - 7.2 Proprietary device protocols
   - 7.3 Wide area sensor networks (LoRa, Sigfox, ...)
   - 7.4 Digital voice/data technologies (DECT/GAP, TETRA, ...)
   - 7.5 Satellite communications

8. Protections
   - 8.1 Integrating mobile technology securely
   - 8.2 Monitoring mobile devices

Literature
Compulsory Reading
Further Reading ▪ Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G. ▪ Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187. ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Software Architectures of Mobile Devices

Course Code: DLBCSEEMT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Mobile devices have supplanted desktops and laptops as the most common end-user device. The smart phone has become a central business tool. Users run their entire lives from them. Furthermore, the Internet of Things are also using these mobile platforms. But too often, the risks and opportunities associated with these mobile devices are opaque to the security administrators in particular as these devices often operate outside the traditional Intranet. In this course, we examine how the dominant players, Android and Apple iOS, handle security in their software stack and ecosystem. We also look at the overlooked problem of IoT Security and wrap up with organizational solutions.

Course Outcomes

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Contents

1. Handset technology stack
   - 1.1 Hardware
   - 1.2 Firmware
   - 1.3 Operating system
   - 1.4 Applications
   - 1.5 Ecosystem
2. Hardware
   - 2.1 RF modules
   - 2.2 PDA module
   - 2.3 Trusted Execution Environment component
   - 2.4 Biometric devices
   - 2.5 Location technology

3. Android operating system
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel and Hardware abstraction layer
   - 3.4 Sandboxing and virtualization
   - 3.5 Code signing

4. Apple iOS operating system
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel and Frameworks
   - 4.4 Sandboxing and virtualization
   - 4.5 Code signing

5. Mobile devices
   - 5.1 The Internet of things
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android on devices
   - 5.5 Other common embedded operating systems

6. Software ecosystems and security
   - 6.1 Google play
   - 6.2 Apple store
   - 6.3 Security providers
   - 6.4 The role of the Cloud

7. Mobile handset threats
   - 7.1 Historic examples of handset attacks
   - 7.2 Taxonomy of Handset threats
   - 7.3 Jailbreaking

8. Mobile Device Management
   - 8.1 The threats of BYOD
   - 8.2 Unique threats to mobile devices
   - 8.3 Patch and policy management

Literature
Compulsory Reading
Further Reading ▪ Gupta, A. (2014): Learning Pentesting for Android Devices ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ N.A. (2020): Android Enterprise Security White Paper. ▪ N.A. (2019): iOS Security iOS 12.3. https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf ▪ Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSEEMT02_E

IT Security Consulting

Module Code: DLBCSEEISC_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEEISC01_E or DLBCSEEISC01_D ▪ none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Technical and Operational IT Security Concepts) / N.N. (Project: Configuration and Application of SIEM Systems)

Contributing Courses to Module

- Technical and Operational IT Security Concepts (DLBCSEEISC01_E)
- Project: Configuration and Application of SIEM Systems (DLBCSEEISC02_E)

Module Exam Type

Module Exam	Split Exam
	Technical and Operational IT Security Concepts • Study Format "Distance Learning": Exam, 90 Minutes Project: Configuration and Application of SIEM Systems • Study Format "Fernstudium": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Technical and Operational IT Security Concepts

- Network analysis and evaluation
- Protection Profiles
- Intrusion Detection Systems
- Network Monitoring
- Security Information and Event Management (SIEM)
- IT-Security evaluation and assessment

Project: Configuration and Application of SIEM Systems

- Network analysis and evaluation
- Protection Profiles
- Intrusion Detection Systems
- Network Monitoring
- Security Information and Event Management (SIEM)
- IT-Security evaluation and assessment

Learning Outcomes

Technical and Operational IT Security Concepts

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Project: Configuration and Application of SIEM Systems

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Technical and Operational IT Security Concepts

Course Code: DLBCSEEISC01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-Systems and Networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructure require higher security mechanism regarding confidentiality, integrity and availability. Based on specific “Protection Profiles” high sophisticated tools, mechanisms and procedures need to be designed, implemented, configurated and operated.With this course the student will be able to evaluate given IT-Infrastructure, support the security-design of new IT-Systems and Networks by developing specific Protection Profiles, evaluate which technical and operational security measures and application are required and how these are integrated, configured and operated.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate IT systems and networks and detect vulnerabilities.
- develop enterprise specific protection profiles.
- design and implement tools for sensor based network monitoring, intrusion detection and response.
- use Big Data fusion mechanisms, evaluate and assess the IT-system network security status and decide and initiate incident response measures.
- evaluate the security status of IT systems and networks and provide guidance for improvement.

Contents

1. Network Analysis and Evaluation
   - 1.1 Layer Specific Threats and Vulnerabilities
   - 1.2 DATA Flow, Interdependencies and Interrelationships
   - 1.3 Vulnerability Scanning and Detection
   - 1.4 Supporting Tools and Techniques

2. Protection Profiles
   - 2.1 Reference Architecture Technology and Networking
   - 2.2 Risk Assessment, Residual Risk and Risk Management
   - 2.3 Security Requirements and Safeguards
   - 2.4 Security Evaluation of IT-Security Products
   - 2.5 Accreditation of IT-Systems and Networks

3. Intrusion Detection Systems
   - 3.1 Detection Strategy
   - 3.2 Data Sources, Sensors
   - 3.3 Analytics
   - 3.4 Indicators of Compromise

4. Network Monitoring
   - 4.1 Threat Protection Systems
   - 4.2 Wireless Sensor Networks Technology
   - 4.3 Threat Information Sharing

5. Security Information and Event Management (SIEM)
   - 5.1 Technical and Operational DATA Sources
   - 5.2 DATA Fusion
   - 5.3 Network Norm Behavior
   - 5.4 Big Data Analysis – Transferring Technical Data for Operational Information
   - 5.5 Security Situation Picture, Situational Awareness
   - 5.6 Incident Response Strategies and Automated Responses

6. IT-Security Evaluation and Assessment
   - 6.1 IT-Security Metrics
   - 6.2 IT-Security Assessment

Literature
Compulsory Reading
Further Reading ▪ Federal Office for Information Security (BSI) (2018): IT-Grundschutz Profiles - Structural Description - COMMUNITY DRAFT. ▪ Hayden, L. (2010): IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education, New York City, NY. ▪ McNab, C. (2016): Network Security Assessment: Know Your Network. 3. Auflage, O'Reilly UK Ltd., London. ▪ Miller, D. R. et al. (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Configuration and Application of SIEM Systems

Course Code: DLBCSEEISC02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEEISC01_E or DLBCSEEISC01_D

Course Description

This course will give students hands-on experience in the challenging task of implementing a Security Incident Event Management (SIEM) Tool into an Enterprise IT-Environment. Students will need to consider practical aspects such as different data sources, data fusion and big data analytics methods and processing, as well as constraints such as data availability and multiple data formats. Furthermore, students will face the challenge to transfer technical data into operational Information to initiate valid responses. By the end of this course, students will have obtained well-founded knowledge of the integration of SIEM into enterprise IT infrastructure, applications and services.

Course Outcomes

On successful completion, students will be able to

- understand the challenges of integrating a SIEM into an existing enterprise IT infrastructure.
- evaluate the constraints the implementation project imposes on the execution of a SIEM.
- identify the necessary intrusion detection and monitoring components required for reliable execution of the SIEM tool.
- analyze requirements regarding data acquisition, data fusion, analysis, and processing.
- identify deviation from normal behavior in IT systems / networks.
- initiate further deep investigation of malware samples and apply relevant response strategies - including automated responses.

Contents

- This course focuses on practical aspects of the implementation of a SIEM into an enterprise IT infrastructure environment. Students start with a chosen use case and SIEM and then evaluate requirements which need to be fulfilled so that the SIEM can be used as part of an enterprise IT system / network. Students need to evaluate requirements for sensors, network monitoring, intrusion detection, data fusion, big data analytics, and translating technical data into operational information.
- Based on the available information, valid responses – including automated responses - will be identified and processed.
- All relevant artifacts and considerations are documented by the students in a project report.

Literature
Compulsory Reading
Further Reading ▪ Al-Sakib, K. P. (2016): The State of the Art in Intrusion Prevention and Detection. Routledge, Abingdon. ▪ Miller, D. et al (2011): Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, New York City, NY. ▪ Mitchell, H. B. (2007): Multi-Sensor Data Fusion: An Introduction. Springer Verlag, Berlin.

Study Format Fernstudium

Study Format	Course Type
Fernstudium	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Social Engineering

Module Code: DLBCSEESE_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSEESE01_E or DLBCSEESE01_D	BA	5	150 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Social Engineering and Insider Threats) / N.N. (Project: Social Engineering)

Contributing Courses to Module

- Social Engineering and Insider Threats (DLBCSEESE01_E)
- Project: Social Engineering (DLBCSEESE02_E)

Module Exam Type

Module Exam	Split Exam
	Social Engineering and Insider Threats • Study Format "Distance Learning": Written Assessment: Case Study Project: Social Engineering • Study Format "Distance Learning": Oral Project Report

Weight of Module

see curriculum

Module Contents

Social Engineering and Insider Threats

- Social engineering methods
- Legal aspects of social engineering
- Compliance, code of conduct
- Insider threat detection
- Security policies and regulations
- National and international cooperation and information exchange

Project: Social Engineering

- Social engineering methods
- Legal aspects of social engineering
- Compliance, code of conduct
- Insider threat detection
- Security policies and regulations
- National and international cooperation and information exchange

Learning Outcomes

Social Engineering and Insider Threats

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Project: Social Engineering

On successful completion, students will be able to

- recognize the importance of the “Human Factor” in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Social Engineering and Insider Threats

Course Code: DLBCSEESE01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

IT-systems and networks containing and processing highly sensitive information and data as well as IT-Infrastructure in support of business-critical processes or national critical infrastructures are of high interest for attackers to gain information (Cyber Espionage) to manipulate or destroy information and data as well as interrupt basic functions and services by compromising these systems and enterprises. One attack vector is targeted to the users and operators to misuse these people as workforce to break security policies and regulations. Social Engineering or social manipulation is widely used by adversaries to gain the necessary information to compromise IT-Infrastructures and to achieve their specific goals. Using methods of social engineering is very close to the so called “Insider Threat”. People from inside the organization act for various reasons against the security policies and regulations of their own enterprise. Revenge, dissatisfaction or sometimes criminal intent are reasons for such behavior. A combination of social engineering and “hostile insiders” is a gold nugget for all adversaries. Therefore, technical and organizational measures have to be developed and implemented to avert such threats. With this course, students will be able to recognize methods of social engineering and identify insider threats. They will be able to develop and implement preventive security policies and regulations as well as responsive security measures to counter these threats.

Course Outcomes

On successful completion, students will be able to

- analyze and evaluate social engineering methods against IT -systems and networks and detect vulnerabilities in their own enterprise.
- develop enterprise specific technical and organizational security policies and regulations.
- design and implement tools for network monitoring to detect and log appliance to security policies and regulations.
- use „Big Data“ fusion and machine learning mechanisms to evaluate and assess the IT-system network as well as user and administrator security status and decide and initiate response measures to recover from social engineering and insider threat generated incidents.
- evaluate the security status and the security awareness in the enterprise on all levels and generate advice for improvement.

Contents

1. Social engineering methods
   - 1.1 Phishing, spear phishing
   - 1.2 Quid pro quo, baiting, media dropping
   - 1.3 Scareware, CEO-Fraud
   - 1.4 Pretexting, tailgating

2. Legal aspects of social engineering,
   - 2.1 Compliance, code of conduct
   - 2.2 Identity theft
   - 2.3 Data privacy

3. Insider threat detection
   - 3.1 DATA Mining for insider threat detection,
   - 3.2 Comprehensive Framework for insider threat detection and response
   - 3.3 Self-assessment tools for evaluation,
   - 3.4 Organizational learning
   - 3.5 Innovative processes
   - 3.6 Application of machine Learning methods

4. Security policies and regulations
   - 4.1 Organizational framework, compliance, code of conduct
   - 4.2 Training
   - 4.3 Incident response system
   - 4.4 Protection of classified / sensitive information
   - 4.5 Password policy
   - 4.6 Data storage and access profiles
   - 4.7 Interface monitoring and regulation (USB policy, ...)

5. National and international cooperation and information exchange.
   - 5.1 Cooperation with Internet Service Providers (ISP) and IT-Security stakeholders
   - 5.2 Exchange platforms and forums for Tactics Techniques and Procedures (TTP´s) and Best Practices
   - 5.3 Cooperation with national Security Authorities

Literature
Compulsory Reading
Further Reading ▪ Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane. ▪ Company: TrustedSec. (Internet DEMO Version to subscribe) ▪ Hadnagy, C. (2012): Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe, MITP-Verlags GmbH & Co. KG, Frechen. ▪ Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford. ▪ Kennedy, D.: The Social-Engineer Toolkit (SET) ▪ Menger, A. (2016): IT-Sicherheit und Social Engineering. Grundlagen, Erscheinungsformen und Schutzmöglichkeiten. Hochschule Osnabrück.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Case Study

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Project: Social Engineering

Course Code: DLBCSEESE02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEESE01_E or DLBCSEESE01_D

Course Description

This project course will give students hands-on experience in the challenging task to prevent and counter social engineering attacks and eliminate or as a minimum mitigate the insider threat to the Enterprise IT-Systems and Networks. Students will need to consider practical aspects of social and psychological challenges – the so called “Human Factor” - as well as the application of technical toolkits to detect attacks driven by social engineering methods or caused by hostile insiders. Through this course Students will develop a complete overview of organizational, technical and procedural measures by analyzing the threat vector landscape, identify vulnerabilities and security gaps in the enterprise and develop and implement practical security policies and regulations, including security awareness campaigns, to prevent and recover from incidents caused by social engineering and insider threats.

Course Outcomes

On successful completion, students will be able to

- recognize the importance of the “Human Factor” in regard to the security of enterprise IT-systems and networks, and consider the legal constraints in regard to social engineering and insider threat detection.
- analyse and evaluate the security framework and identify security gaps and shortfalls.
- develop and implement organizational, technical and security policies and regulations.
- develop and run security awareness campaigns to enhance the resilience against the application of social engineering methods.
- cooperate with different stakeholders like national security authorities, security companies and Internet service providers.

Contents

- This project course focuses on practical aspects to prevent, detect and recover from social engineering driven attacks as well as threat deriving from hostile insiders. Students start with a chosen use case to analyze a tangible and successful social engineering campaign, identify the main attack vectors and learn how different activities on multiple levels concur to reach the objective or the attacker. Students need to analyze the security framework of the attacked enterprise, identify the vulnerability gaps and shortfalls that allowed the social engineering attack to be successful. Taking into account the “Human Factor” the students will

then develop organizational and technical security policies to show how a specific attack could have been prevented and the damage been avoided or mitigated. All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- Blokdyk, G. (2019): Insider Threat Detection Solutions a Complete Guide - 2020 Edition. Emereo Pty Limited, Brisbane.
- Company: TrustedSec. (Internet DEMO Version to subscribe)
- Gelles, M. G. (2016): Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, Oxford.
- Kennedy, D.: The Social-Engineer Toolkit (SET)

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Oral Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Host Forensics

Module Code: DLBCSEEHF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Static and Dynamic Malware Analysis) / N.N. (Seminar: Sandbox Interpretation)

Contributing Courses to Module

- Static and Dynamic Malware Analysis (DLBCSEEHF01_E)
- Seminar: Sandbox Interpretation (DLBCSEEHF02_E)

Module Exam Type

Module Exam	Split Exam
	Static and Dynamic Malware Analysis • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Sandbox Interpretation • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Static and Dynamic Malware Analysis

- Objectives in Malware analysis
- Analysis Lab setup
- Tools of the trade
- Malware Classification
- Sandboxes
- Reversing
- Digging deeper

Seminar: Sandbox Interpretation

This course is about the practical application of Malware analysis techniques to real sandbox log files.

Learning Outcomes

Static and Dynamic Malware Analysis

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Seminar: Sandbox Interpretation

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Static and Dynamic Malware Analysis

Course Code: DLBCSEEHF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Malware is a top compromise vector in cyber attacks. Analyzing the attacking Malware gives the security analyst insights into the methodology and intension of the attacker. There are a number of ways that Malware can be analyzed and this course will introduce the most common ones.

Course Outcomes

On successful completion, students will be able to

- know what protected Malware analysis environment entails.
- read sandbox reports and glean attack information from them.
- know the principles of Malware reversing, what to keep in mind and avoid.
- get to know more advanced methods and principles of program analysis.

Contents

1. Objectives in Malware analysis
   - 1.1 Forensics
   - 1.2 Root cause analysis
   - 1.3 Mitigation
2. Analysis Lab setup
   - 2.1 Stealth
   - 2.2 Isolation
   - 2.3 Honeypots
3. Tools of the trade
   - 3.1 Virtual machines
   - 3.2 Debugger
   - 3.3 Disassembler

4. Malware Classification
   - 4.1 Antivirus
   - 4.2 Virustotal
   - 4.3 Yara
   - 4.4 Clustering with PEID, TELFHASH, TLSH, SSDEEP, etc

5. Sandboxes
   - 5.1 Levels of interaction
   - 5.2 Instrumentation
   - 5.3 Online sandboxing services, Virustotal
   - 5.4 Scripting for sandboxes
   - 5.5 Corporate sandbox considerations

6. Reversing
   - 6.1 Unpacking, decrypting and de-obfuscation
   - 6.2 Debugging techniques
   - 6.3 Control flow analysis
   - 6.4 Library and system calls

7. Digging deeper
   - 7.1 Domain and IP information
   - 7.2 Analysis of Javascript code
   - 7.3 Memory forensics
   - 7.4 Kernel debugging rootkits
   - 7.5 Theoretical underpinnings of program analysis

Literature

Compulsory Reading

Further Reading

- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Lin, X. (2018): Introductory Computer Forensics: A Hands-on Practical Approach. Springer International Publishing, Cham.
- Mitre ATT&CK®. https://attack.mitre.org/
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.
- Yurichev, D. (2020): Reverse Engineering for Beginners. URL: https://beginners.re/ (last accessed: 24 August 2020)

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Sandbox Interpretation

Course Code: DLBCSEEHF02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEHSF01_E or DLBCSEHSF01_D; DLBCSEEHF01_E

Course Description

In this course, we explore the most important tool in Malware analysis, the Sandbox and extract from the Sandbox logs the potential attacks exhibited by the Malware.

Course Outcomes

On successful completion, students will be able to

- read a sandbox log.
- extract Indicators of Compromise.
- determine the Malware's mode of operation.

Contents

- This course is about the practical application of Malware analysis techniques to real sandbox log files and extract the indicators of compromise and Malware objectives into a report.

Literature

Compulsory Reading

Further Reading

- Gregg, M. (2008): Build Your Own Security Lab: A Field Guide for Network Testing. Wiley, Hoboken, NJ.
- Ligh, M. H. et al (2011): Malware Analyst's Cookbook and DVD. Wiley, Hoboken, NJ.
- Szőr, P. (2005): The Art of Computer Virus Research and Defense. Addison-Wesley, Upper Saddle River, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEHF02_E

DevSecOps

Module Code: DLBCSEEDSO_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ IWNF01_E or IWNF01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Techniques and methods for agile software development) / N.N. (Project: Agile DevSecOps Software Engineering)

Contributing Courses to Module

- Techniques and methods for agile software development (IWNF01_E)
- Project: Agile DevSecOps Software Engineering (DLBCSEEDSO01_E)

Module Exam Type

Module Exam	Split Exam
	Techniques and methods for agile software development • Study Format "Distance Learning": Exam, 90 Minutes Project: Agile DevSecOps Software Engineering • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Techniques and methods for agile software development

- Characteristics and principles of agility
- Agility in small teams with SCRUM
- Agile portfolio and project management
- Agile requirements and IT architecture management
- Agile Testing
- Agile Delivery and Deployment

Project: Agile DevSecOps Software Engineering

This module provides the fundamental security principles for leveraging DevOps in software engineering, also known as the DevSecOps paradigm. Given a security-relevant scenario, this module will illustrate good DevSecOps practices like definition of security baselines, threat modelling approaches, and security automation as part of the continuous integration/continuous development (CI/CD) pipeline.

Learning Outcomes

Techniques and methods for agile software development

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Project: Agile DevSecOps Software Engineering

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Techniques and methods for agile software development

Course Code: IWNF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The goal of the course is to give students a deeper insight into the topic of agile software development. First of all, the basic characteristics and principles of agility are presented and discussed. Afterwards, it is shown how small projects and teams can use agile software engineering and how agile principles can be transferred and applied to large projects. Afterwards, agile techniques are taught for selected core activities in software engineering, with a focus on testing, delivery and deployment.

Course Outcomes

On successful completion, students will be able to

- analyse and evaluate problems and risks of industrial SW development and their consequences for development processes.
- know and understand the basic principles of No-Frills Software Engineering.
- analyse practical scenarios and independently apply suitable methods and tools of No-Frills Software Engineering.

Contents

1. Characteristics and Principles of Agility
   - 1.1 Features and Challenges of Software Projects
   - 1.2 Classification of Uncertainty
   - 1.3 Comparison of Agile and Classic Software Development
   - 1.4 Principles of Agility
2. Agility in Small Teams with Scrum
   - 2.1 Basics and General Structure with SCRUM
   - 2.2 Central Management Artifact: Product Backlog
   - 2.3 Other Management Artifacts

3. Agile Portfolio and Project Management
   - 3.1 Planning Levels in Agile Project Management
   - 3.2 Agile Portfolio Management
   - 3.3 Organization of Several Teams in One Project
   - 3.4 Product and Release Planning

4. Agile Requirements and IT Architecture Management
   - 4.1 Requirements Engineering in Agile Projects
   - 4.2 Architecture Management in Agile Projects

5. Agile Testing
   - 5.1 Basic Principles and Requirements for the QA Organization
   - 5.2 Test Levels and Agility
   - 5.3 Test Automation

6. Agile Delivery and Deployment
   - 6.1 Basics and Continuous Delivery Pipeline
   - 6.2 Continuous Build and Continuous Integration
   - 6.3 Acceptance Tests, Load Tests and Continuous Deployment

Literature

Compulsory Reading

Further Reading

- Biffl, S. et al. (Hrsg.) (2005): Value-Based Software Engineering. Springer, Berlin/Heidelberg.
- Cockburn, A. (2007): Agile Software Development. The Cooperative Game. 2nd edition, Addison-Wesley, Upper Saddle River, NJ.
- Cohn, M. (2005): Agile Estimating and Planning. Prentice Hall, Upper Saddle River, NJ.
- Crispin, L. (2008): Agile Testing: A Practical Guide for Testers and Agile Teams. Addison Wesley, Upper Saddle River, NJ.
- Highsmith, J. (2009): Agile Project Management: Creating Innovative Products. Addison Wesley, Upper Saddle River, NJ.Layton, M. C. (2012): Agile project management for dummies. John Wiley & Sons, New York, NY.
- Rubin, K. S. (2012): Essential Scrum: A Practical Guide to the Most Popular Agile Process. Addison Wesley, Upper Saddle River, NJ.
- Schwaber, K. (2014): Agile Project Management with Scrum. Microsoft Press, Redmond, WA.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Agile DevSecOps Software Engineering

Course Code: DLBCSEEDSO01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	IWNF01_E or IWNF01

Course Description

This course covers the basic security principles for leveraging the DevSecOps approach in software engineering scenarios. The content of this course will illustrate the adoption of DevSecOps to continuously and holistically improve the security of an organization, rather than just focusing on protecting the underlying software infrastructure (as in the case of traditional non-agile methodologies). By presenting DevSecOps principles like threat modelling, definition of security baselines, security automation/tools, and continuous compliance monitoring, this course will teach how security can be integrated while developing a software engineering product.

Course Outcomes

On successful completion, students will be able to

- apply basic thread modelling into DevOps scenarios,
- familiarize with relevant DevOps security baselines from international standards and industrial good practices,
- select the appropriate tools and automation approaches for DevSecOps,
- design continuous compliance monitoring into Infrastructure-as-a-Code scenarios.

Contents

- Despite the broad adoption of DevOps in the industry, the integration of security principles into this paradigm (i.e., DevSecOps) is still an open challenge for many practitioners. In this course the students will learn fundamental DevSecOps concepts like threat modelling, definition of security baselines, continuous compliance monitoring, and integration of security automation in DevOps.

Literature
Compulsory Reading
Further Reading ▪ Johnson, E. (2020): Secure DevOps. A Practical Introduction. (URL: https://www.sans.org/ondemand/course/secure-dev-ops-a-practical-introduction [Retrieved: 15.08.2020]). ▪ Hsu, T. (2018): Hands-On Security in DevOps. Packt Publishing, UK. ▪ Microsoft. (2020): Secure DevOps. Making security principles and practices an integral part of DevOps while maintaining improved efficiency and productivity. (URL: https://www.microsoft.com/en-us/securityengineering/devsecops [Retrieved: 15.08.2020]). ▪ Schneider, C. (2015): Security DevOps. Staying secure in agile projects. (URL: https://owaspappseceurope2015.sched.com/event/378l/security-devops-staying-secure-in-agile-projects [Retrieved: 15.08.2020]). ▪ Yasar, H. (2016): An Introduction to Secure DevOps. Including Security in the Software Lifecycle. (URL: https://insights.sei.cmu.edu/devops/2016/11/an-introduction-to-secure-devops-including-security-in-the-software-lifecycle.html [Retrieved: 15.08.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Security in Complex Networks

Module Code: DLBCSEESCN_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	DLBCSEITPAM02 or IAMG01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (IT Architecture Management) / N.N. (Project: IT Security Architecture)

Contributing Courses to Module

- IT Architecture Management (DLBCSEITPAM02)
- Project: IT Security Architecture (DLBCSEESCN01_E)

Module Exam Type

Module Exam	Split Exam
	IT Architecture Management • Study Format "Distance Learning": Exam, 90 Minutes Project: IT Security Architecture • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

IT Architecture Management

- Basic terms and foundations of IT enterprise architectures management
- IT application portfolio management
- Architecture governance
- Modeling of IT enterprise architectures
- Frameworks using TOGAF as an example
- Reference models and sample catalogues

Project: IT Security Architecture

Using well-known methods and techniques from the field of IT architecture management, students will be able to develop a well-grounded overview of IT-infrastructure regarding IT-strategy and strategic management. Students will understand and take advantage of typical concepts, methods and models for all tasks in the framework of architecture management. Emphasis will be taken to the security aspects of the IT infrastructure by designing and implementing IT-security architecture in the overall framework.

Learning Outcomes

IT Architecture Management

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Project: IT Security Architecture

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

IT Architecture Management

Course Code: DLBCSEITPAM02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In addition to concrete IT projects, such as the development of a new IT system or the introduction of standard software, a strategic management system for organizational-wide IT infrastructure – that is, for all IT hardware and software systems – must be used.Strategic management is the responsibility of the IT enterprise architect, who operates IT architecture management. Their task is to strategically align IT infrastructure with an organization's business and IT strategy.This course covers the typical concepts, methods, procedures, and IT models of architecture management.

Course Outcomes

On successful completion, students will be able to

- describe and explain the basic principles of IT strategy, governance, and architecture management, differentiating between them.
- explain and differentiate the typical activities of IT architecture management, their interrelationships, and their dependencies.
- explain suitable models of IT architecture management, distinguish between them, and explain their intended purpose.
- explain and describe selected IT architectural frameworks as well as reference models and sample catalogues.

Contents

1. Basic Terms and Foundation for the Management of IT Enterprise Architectures
   - 1.1 IT Enterprise Architecture
   - 1.2 Goals of Enterprise Architecture Management
   - 1.3 Processes in the Management of IT Enterprise Architectures
2. IT Application Portfolio Management
   - 2.1 IT Application Portfolio Management Overview
   - 2.2 Application Manual
   - 2.3 Portfolio Analysis
   - 2.4 Development Planning

3. Architecture Governance
   - 3.1 Organizational Structure
   - 3.2 Policy Development and Enforcement
   - 3.3 Project Support

4. Modeling of IT Enterprise Architectures
   - 4.1 Models in the Context of IT Architecture Management
   - 4.2 Forms of Documentation for Processes and Applications
   - 4.3 Forms of Documentation for Systems and Technologies

5. Frameworks Using the Example of TOGAF
   - 5.1 Fundamentals and Use of IT Architecture Frameworks
   - 5.2 Overview and Categories of EAM Frameworks
   - 5.3 The Open Group Architecture Framework (TOGAF)

6. Reference Models and Sample Catalogues
   - 6.1 Architecture Reference Models
   - 6.2 EAM Design Sample Catalogue

Literature

Compulsory Reading

Further Reading

- Hanschke, I. (2011): Enterprise Architecture Management. Einfach und effektiv. Hanser, München.
- Keller, W. (2012): IT-Unternehmensarchitektur. Von der Geschäftsstrategie zur optimalen IT-Unterstützung. 2. Auflage, dpunkt.verlag, Heidelberg.
- Keuntje. J. H./Barkow, R. (Hrsg.) (2010): Enterprise Architecture. Management in der Praxis. Wandel, Komplexität und IT-Kosten im Unternehmen beherrschen. Symposion Publishing, Ettlingen.
- Ross, J. W./ Weill, P./Robertson, D. C. (2006): Enterprise Architecture as Strategy. Creating a Foundation for Business Execution. Harvard Business Review Press, Boston, MA.
- Schwarzer, B. (2009): Einführung in das Enterprise Architecture Management. Verstehen – Planen – Umsetzen. Books on Demand, Norderstedt.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: IT Security Architecture

Course Code: DLBCSEESCN01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEITPAM02 or IAMG01

Course Description

Using methods and techniques from the field IT architecture management, students will work independently on a practical question of IT security architecture. By the end of this course students will be able to independently develop IT security architecture models, based on an existing IT-system / network architecture.

Course Outcomes

On successful completion, students will be able to

- use IT-architecture management tools and techniques from the perspective of IT security.
- independently analyze IT architecture models regarding IT security shortfalls.
- design IT security architecture models and integrate them in the overall IT architecture management.
- identify and explain problems within the linked systems of operational, financial and management needs and IT security requirements.

Contents

- Implementation and documentation of practical questions regarding IT security in the framework of IT architecture management. Typical scenarios are, for example, “Implementation of IT security devices in complex networks”, “Design of processes for security updates and patch management” and “using in-house resources or outsourcing of IT security tasks”.

Literature

Compulsory Reading

Further Reading

- Bartsch, M. / Frey, S. (2014): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Springer Fachmedien, Wiesbaden.
- Müller, K.-R. (2014): IT-Sicherheit mit System. Springer Fachmedien, Wiesbaden.
- Pfister, M. (2019): In 3 einfachen (aber wichtigen) Schritten zur Enterprise IT-Sicherheitsarchitektur (URL: https://www.infoguard.ch/de/blog/in-3-schritten-zur-enterprise-it-sicherheitsarchitektur [Retrieved: 17.07.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Network Forensics

Module Code: DLBCSEENF_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E ▪ DLBCSEINF01_E or DLBCSEINF01_D	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Protocols, Log- and Dataflow-Analysis in Depth) / N.N. (Seminar: Threat Hunting, Analysis and Incident Response)

Contributing Courses to Module

- Protocols, Log- and Dataflow-Analysis in Depth (DLBCSEENF01_E)
- Seminar: Threat Hunting, Analysis and Incident Response (DLBCSEENF02_E)

Module Exam Type

Module Exam	Split Exam
	Protocols, Log- and Dataflow-Analysis in Depth • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Threat Hunting, Analysis and Incident Response • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Protocols, Log- and Dataflow-Analysis in Depth

- Introduction
- Basic protocol layering
- Operating system logs
- HTTP server
- IP Firewall
- Web application filter
- Authentication servers
- Databases
- Intrusion Detection and Protection System (IDPS)
- Email systems
- Content filters
- SSH
- Less common systems
- Context
- Log management Infrastructure
- Security Information and Event Management (SIEM)
- Visualization
- Security Operations Centers (SOC)
- Logging in the cloud
- Dataflow monitoring
- Attacks against logging
- Analysis techniques
- Reporting

Seminar: Threat Hunting, Analysis and Incident Response

- Mitre ATT&CK TTPs
- APT actors
- Security coverage gap analysis

Learning Outcomes

Protocols, Log- and Dataflow-Analysis in Depth

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Seminar: Threat Hunting, Analysis and Incident Response

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Protocols, Log- and Dataflow-Analysis in Depth

Course Code: DLBCSEENF01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D

Course Description

Logging is done for a variety of diagnosis reasons, but these logs can be very useful in finding security incidents. In this course, we look at a variety of sources of log files. These range from operating system logs, to application logs and network traffic logs. Context and additional information also need to be collected. All this data is then consolidated in a Security Information and Event Management system where it can be analyzed and triaged for action. Finally, major incidents need to be documented and communicated to the relevant parties.

Course Outcomes

On successful completion, students will be able to

- locate and evaluate security relevant log data.
- operate a typical SIEM system.
- create and understand SOC procedures.
- report findings in written and machine readable forms.

Contents

1. Introduction
   - 1.1 Network protocols
   - 1.2 Applications of log files
   - 1.3 Operating system log files
   - 1.4 Application log files
   - 1.5 Network log files
   - 1.6 Dataflow logs
   - 1.7 Security log files

2. Basic protocol layering
   - 2.1 Internet protocol hierarchy
   - 2.2 TCP connection
   - 2.3 Frame layer
   - 2.4 Ethernet layer
   - 2.5 Internet Protocol layer
   - 2.6 Transport Control Protocol
   - 2.7 UDP packets
   - 2.8 TCP/IP in relation to the OSI layer model
   - 2.9 Reading RFCs and related documentation
3. Operating system logs
   - 3.1 Syslog
   - 3.2 System events
   - 3.3 Audit events
4. HTTP server
   - 4.1 Common server vendors
   - 4.2 Apache log format
   - 4.3 Web edge logging
   - 4.4 Logs from Content delivery networks
5. IP Firewall
6. Web application filter
7. Authentication servers
8. Databases
9. Intrusion Detection and Protection System (IDPS)
10. Email systems
    - 10.1 SMTP
    - 10.2 POP
    - 10.3 Exchange

11. Content filters
    - 11.1 Spam and Phish filters
    - 11.2 Malware filters
    - 11.3 Data leak prevention
12. SSH
13. Less common systems
    - 13.1 MQTT
    - 13.2 CoAP
    - 13.3 XMPP
    - 13.4 BGP
    - 13.5 RIP
    - 13.6 DNS
14. Context
    - 14.1 Asset management
    - 14.2 Known vulnerable systems
    - 14.3 Network topology
15. Log management Infrastructure
    - 15.1 Log generation
    - 15.2 Storage
    - 15.3 Analysis
    - 15.4 Monitoring
    - 15.5 Security and privacy of logs
    - 15.6 Roles and responsibility
    - 15.7 Policies
    - 15.8 Long term log storage
16. Security Information and Event Management (SIEM)
17. Visualization
18. Security Operations Centers (SOC)
19. Logging in the cloud
20. Dataflow monitoring

21. Attacks against logging

22. Analysis techniques
    - 22.1 Entry Normalization
    - 22.2 Semantics of log events
    - 22.3 Prioritizing entries
    - 22.4 Aggregation
    - 22.5 Rule based systems
    - 22.6 Anomaly detection
    - 22.7 Machine learning
    - 22.8 Triaging incidents
    - 22.9 Working with filters

23. Reporting
    - 23.1 Indicators of compromise
    - 23.2 Mapping to the Mitre ATT&CK framework
    - 23.3 STIX, TAXII
    - 23.4 Written reports and presentations

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- NIST Special Publicaton 800-94
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Threat Hunting, Analysis and Incident Response

Course Code: DLBCSEENF02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D; DLBCSEENF01_E

Course Description

Much of a security officer's work is with data where incidents need to be analyzed and countermeasures implemented. This course uses the Mitre ATT&CK® framework to reference TTPs (Techniques, Tactics and Procedures) that map to security events. Not all TTPs can be found in labeled security events, so Threat Hunting aims to go beyond ordinary incident response and find indicators of these TTPs also using other methods.

Course Outcomes

On successful completion, students will be able to

- understand Mitre ATT&CK® Techniques, Tactics and Procedures.
- understand how APT actors use combinations of these TTPs.
- understand how Botnets and related Malware behave in networks.
- examine where to find evidence of these TTPs.
- explore datasets for threats not picked up by existing rules.
- do a gap analysis on existing protections with respect to a given APT.
- design mitigations to given TTPs.

Contents

- In this seminar, we cover the subjects of incident response and threat hunting using the Mitre ATT&CK® framework and publicly available reports.

Literature

Compulsory Reading

Further Reading

- Kumar, P. et al (2018): Handbook of Research on Network Forensics and Analysis Techniques. IGI Global, Hershey, PA.
- Mitre ATT&CK®. https://attack.mitre.org/
- Perdisci, R. et al (2019): Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Business Intelligence

Module Code: DLBCSEBI

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Sebastian Werning (Business Intelligence) / Prof. Dr. Sebastian Werning (Project: Business Intelligence)

Contributing Courses to Module

- Business Intelligence (DLBCSEBI01)
- Project: Business Intelligence (DLBCSEBI02)

Module Exam Type

Module Exam	Split Exam
	Business Intelligence • Study Format "Distance Learning": Exam, 90 Minutes Project: Business Intelligence • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Business Intelligence

- Basics of mobile software development
- Android system architecture
- Development environment
- Core components of an Android app
- Interaction between application components
- Advanced techniques

Project: Business Intelligence

Conception, implementation, and documentation of small, mobile applications on the basis of a concrete task.

Learning Outcomes

Business Intelligence

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Project: Business Intelligence

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Business Intelligence

Course Code: DLBCSEBI01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Business Intelligence (BI) is used to obtain information from company data that is relevant for targeted corporate management and the optimization of business activities. This course introduces and discusses techniques, procedures, and models for data provision, information generation, and analysis, as well the distribution of the information obtained. You will then be able to explain the various subject areas of data warehousing and independently select methods and techniques to meet specific requirements.

Course Outcomes

On successful completion, students will be able to

- explain the motivation, use cases, and basics of Business Intelligence.
- identify and explain techniques and methods for providing and modeling data, as well as types of data relevant to BI, differentiating between them.
- explain techniques and methods for the generation and storage of information and independently select suitable methods on the basis of concrete requirements.

Contents

1. Motivation and Conceptualization
   - 1.1 Motivation and Historical Development
   - 1.2 BI as a Framework
2. Data Provision
   - 2.1 Operative and Dispositive Systems
   - 2.2 The Data Warehouse Concept
   - 2.3 Architectural Variations
3. Data Warehouse
   - 3.1 ETL Process
   - 3.2 DWH and Data Mart
   - 3.3 ODS and Metadata

4. Modelling of Multidimensional Data Spaces
   - 4.1 Data Modeling
   - 4.2 OLAP Cubes
   - 4.3 Physical Storage
   - 4.4 Star and Snowflake Scheme
   - 4.5 Historicization

5. Analysis Systems
   - 5.1 Free Data Research and OLAP
   - 5.2 Reporting Systems
   - 5.3 Model-Based Analysis Systems
   - 5.4 Concept-Oriented Systems

6. Distribution and Access
   - 6.1 Information Distribution
   - 6.2 Information Access

Literature

Compulsory Reading

Further Reading

- Bachmann, R./Kemper, G. (2011): Raus aus der BI-Falle. Wie Business Intelligence zum Erfolg wird. 2. Auflage, mitp, Heidelberg.
- Bauer, A./Günzel, H. (2008): Data Warehouse Systeme. Architektur, Entwicklung, Anwendung. 3. Auflage, dpunkt.verlag, Heidelberg.
- Betz, R. (2015): Werde Jäger des verlorenen Schatzes. In: Immobilienwirtschaft, Heft 5, S. 1614–1164. (URL https://www.haufe.de/download/immobilienwirtschaft-ausgabe-052015-immobilienwirtschaft-fachmagazin-fuer-management-recht-praxis-303530.pdf [letzter Zugriff: 27.02.2017]).
- Bodendorf, F. (2006): Daten- und Wissensmanagement. 2. Auflage, Springer, Berlin.
- Chamoni, P./Gluchowski, P. (Hrsg.) (2006): Analytische Informationssysteme Business Intelligence-Technologien und -Anwendungen. Springer, Berlin.
- Engels, C. (2008): Basiswissen Business Intelligence. W3L, Herdecke/Witten.
- Gansor, T./Totok, A./Stock, S. (2010): Von der Strategie zum Business Intelligence Competency Center (BICC). Konzeption – Betrieb – Praxis. Hanser, München.
- Gluchowski, P./Gabriel, R./Dittmar, C. (2008): Management Support Systeme und Business Intelligence. Computergestützte Informationssysteme für Fach- und Führungskräfte. 2. Auflage, Springer, Berlin/Heidelberg.
- Grothe, M. (2000): Business Intelligence. Aus Informationen Wettbewerbsvorteile gewinnen. Addison-Wesley, München.
- Gutenberg, E. (1983): Grundlagen der Betriebswirtschaft, Band 1. Die Produktion. 18. Auflage, Springer, Berlin/Heidelberg/New York.
- Hannig, U. (Hrsg.) (2002): Knowledge Management und Business Intelligence. Springer, Berlin.
- Hansen, H.-R./Neumann, G. (2001): Wirtschaftsinformatik I. Grundlagen betrieblicher Informationsverarbeitung. 8. Auflage, Lucius & Lucius UTB, Stuttgart.
- Humm, B./Wietek, F. (2005): Architektur von Data Warehouses und Business Intelligence Systemen. In: Informatik Spektrum, S. 3–14. (URL: https://www.fbi.h-da.de/fileadmin/personal/b.humm/Publikationen/Humm__Wietek_-_Architektur_DW__Informatik-Spektrum_2005-01_.pdf [letzter Zugriff: 27.02.2017]).
- Kemper, H.-G./Baars, H./Mehanna, W. (2010): Business Intelligence – Grundlagen und praktische Anwendungen. Eine Einführung in die IT-basierte Managementunterstützung. 3. Auflage, Vieweg+Teubner, Stuttgart.
- Turban, E. et al. (2010): Business Intelligence. A Managerial Approach. 2. Auflage, Prentice Hall, Upper Saddle River (NJ).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Business Intelligence

Course Code: DLBCSEBI02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using well-known methods and techniques from the field of Business Intelligence, students will work independently on a practical question in this course.At the end of the course you will be able to independently design and prototype Business Intelligence applications based on concrete requirements.

Course Outcomes

On successful completion, students will be able to

- independently design a solution to a practical problem in the field of Business Intelligence in order to then implement a prototype and document the results.
- identify and explain typical problems and challenges in the design and practical implementation of small BI solutions.

Contents

- Implementation and documentation of practical questions regarding the use of Business Intelligence applications. Typical scenarios are, for example, “Management of BI projects”, “Design of multidimensional data models” and “Prototypical implementation of small BI applications”.

Literature

Compulsory Reading

Further Reading

- Brenner, W./Uebernickel, F. (2015): Design Thinking. Das Handbuch. Frankfurter Allgemeine Buch, Frankfurt a. M.
- Brown, T. (2008): Design Thinking. In: Harvard Business Review, Heft Juni, S. 84–95.
- Meinel, C./Weinberg, U./Krohn, T. (Hrsg.) (2015): Design Thinking Live. Wie man Ideen entwickelt und Probleme löst. Murmann, Hamburg.
- Uebernickel, F./Brenner, W. (2016): Design Thinking. In: Hoffmann, C. P. et al. (Hrsg.): Business Innovation: Das St. Galler Modell. Springer, Wiesbaden, S. 243–265.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Future Threats

Module Code: DLBCSEEFT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSRE01 or IREN01, DLBCSEEFT01_E or DLBCSEEFT01_D ▪ DLBCSRE01 or IREN01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Threat Modeling) / N.N. (Project: Threat Modeling)

Contributing Courses to Module

- Threat Modeling (DLBCSEEFT01_E)
- Project: Threat Modeling (DLBCSEEFT02_E)

Module Exam Type

Module Exam	Split Exam
	Threat Modeling • Study Format "Distance Learning": Exam, 90 Minutes Project: Threat Modeling • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Threat Modeling

- Thinking C.I.A. and beyond
- Measuring the Cyber Threat
- Threat Modeling
- Attack libraries
- Rules, Regulations, and Law Enforcement
- Risk management
- Threat Mitigation

Project: Threat Modeling

This course covers the theory and practice of discovering and modeling threats in a given system, architecture or scenario. It covers common methodologies and sources for common threat patterns. In a project, the theory is translated to practice by analyzing a given situation for threats.

Learning Outcomes

Threat Modeling

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Project: Threat Modeling

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Threat Modeling

Course Code: DLBCSEEFT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01

Course Description

When a system or architecture is being created it is vital that possible threats are evaluated at the same time. By using both modeling methodologies and past observed attack patterns, it is possible to take a new or existing system and examine it for possible threats. With this analysis, possible risks and mitigations can be derived. While the most common methodologies are based on Attack Trees and the STRIDE model, recently attack modelling has also been using repositories of attacker techniques, tactics and procedures for inspiration.

Course Outcomes

On successful completion, students will be able to

- confidently think through eventual threats.
- model these threats using a common modelling methodology.
- find relevant techniques, tactics and procedures relating to a given scenario.
- calculate risk associate with the threat model.
- mitigate the risk by implementing design changes.

Contents

1. Thinking C.I.A. and beyond
   - 1.1 Confidentiality
   - 1.2 Integrity
   - 1.3 Availability
   - 1.4 Safety and other concerns
2. Measuring the Cyber Threat
   - 2.1 Measurement and Management
   - 2.2 Cyber Threat Metrics
   - 2.3 Measuring the Threat for an Organization
   - 2.4 The Likelihood of Major Cyber Attacks
   - 2.5 Black Swan events

3. Threat Modeling
   - 3.1 Attack Tree methodology
   - 3.2 STRIDE
   - 3.3 DREAD
   - 3.4 Pyramid of Pain

4. Attack libraries
   - 4.1 CAPEC
   - 4.2 Solove's Taxonomy of Privacy
   - 4.3 Modeling with Mitre ATT&CK®
   - 4.4 Identifying new types of attacks

5. Rules, Regulations, and Law Enforcement
   - 5.1 Cyber Laws
   - 5.2 Compliance and Law Enforcement

6. Risk management
   - 6.1 Changing Approaches to Risk Management
   - 6.2 Incident Response and Crisis Management
   - 6.3 Factoring in black swan events
   - 6.4 Continuous reevaluation

7. Threat Mitigation
   - 7.1 Defensive Tactics and Technologies
   - 7.2 Risk mitigation strategies
   - 7.3 Validation of defenses
   - 7.4 Security and Privacy by Design
   - 7.5 Implementing threat mitigation in an organization

Literature
Compulsory Reading
Further Reading ▪ CAPEC: Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/ ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide to Penetration Testing. Secure Planet LLC. ▪ Mitre ATT&CK®. https://attack.mitre.org/ ▪ Pfleeger, C. P. / Pfleeger, S. L. / Marguilies, J. (2015): Security in Computing. Fifth Edition, Pearson Education, London. ▪ Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Threat Modeling

Course Code: DLBCSEEFT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSRE01 or IREN01, DLBCSEEFT01_E or DLBCSEEFT01_D

Course Description

Threats to modern computer systems are diverse and ever evolving. In this project, the student will have the opportunity to apply the art and science of threat modeling to a scenario to be defined by the instructor together with the student. The basis will be case studies, real or fictive, to which the student will be expected to identify and report on the threats using an appropriate methodology. This can be selected from methodologies such as Attack Trees, STRIDE, DREAD or a justified enumeration of CAPEC or Mitre ATT&CK® TTPs as the student feels most appropriate. The results will be presented as a report.

Course Outcomes

On successful completion, students will be able to

- apply their knowledge of threat modelling to cases and scenarios.
- justify their resulting model based on sound reasoning and in relation to known techniques, tactics and procedures of attackers.
- write a report that lays out their reasoning in a systematic and understandable manner.

Contents

- To a given case or scenario, the student will model the threats using one of the established methodologies and then submit the report and, if appropriate, any code and data. Specific problems and contexts will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Case Studies (Cyber): https://www.securitymagazine.com/topics/2664-case-studies-cyber
- Karger, P. A. / Scherr, R. R. (1974): MULTICS SECURITY EVALUATION: VULNERABILITY ANALYSIS.
- Palmer, C. C. (2001): Ethical Hacking. In: IBM Systems Journal. 40 (3):769.
- Shostack, A. (2014): Threat Modeling: Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Van Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Cloud Security

Module Code: DLBCSEECS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBDSCC01 or DLBDSCC01_D ▪ DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Security Controls in the Cloud) / N.N. (Project: Security by Design in the Cloud)

Contributing Courses to Module

- Security Controls in the Cloud (DLBCSEECS01_E)
- Project: Security by Design in the Cloud (DLBCSEECS02_E)

Module Exam Type

Module Exam	Split Exam
	Security Controls in the Cloud • Study Format "Distance Learning": Exam, 90 Minutes Project: Security by Design in the Cloud • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Security Controls in the Cloud

- Cloud security
- Losing the intranet
- Security by design
- Secure cloud coding
- Confidentiality aspects
- Monitoring and Audit

Project: Security by Design in the Cloud

This module is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Learning Outcomes

Security Controls in the Cloud

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Project: Security by Design in the Cloud

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Security Controls in the Cloud

Course Code: DLBCSEECS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D

Course Description

Maintaining a datacenter is expensive and inflexible, so it is expected that most corporations will be moving their server-based processes to a private, public or hybrid cloud in the next few years. Doing so will make operations more flexible and elastic but poses challenges to security architectures and operations. The paradigm of Infrastructure as Code (IaC) has been embraced by cloud providers and is a great opportunity to architect security into the design of a system (security by design) utilizing security best practices. However, too often, we see the on-premises mentality being applied to cloud deployments resulting in less secure systems instead of utilizing the security advantages a cloud provides. This course teaches the principles of Cloud Native security and how to avoid common pitfalls.

Course Outcomes

On successful completion, students will be able to

- design a secure cloud deployment using infrastructure as code methodologies.
- understand cloud-specific attacks and threat models.
- define appropriate storage classes in compliance with security requirements.
- monitor cloud resources to detect misuse and incidents.

Contents

1. Cloud security is different
   - 1.1 Shared responsibility model
   - 1.2 Infrastructure as code
   - 1.3 The Private, Public and Hybrid Cloud
   - 1.4 Types of virtualization
   - 1.5 Cloud threat models: Mitre Cloud ATT&CK

2. Losing the intranet
   - 2.1 Identify and Access Management
   - 2.2 Principle of least privilege and fine-grained cloud access control
   - 2.3 Using Software Defined Networks, virtual private clouds and subnets
   - 2.4 Moving to a serverless architecture
   - 2.5 Defense in depth

3. Security by design
   - 3.1 Orchestration: Infrastructure as Code
   - 3.2 The Automate-Everything principle, Updating and Repeatability
   - 3.3 Reuse of good design patterns
   - 3.4 Container security
   - 3.5 Identification and Authentication

4. Secure cloud coding
   - 4.1 Software supply chain security
   - 4.2 Continuous Integration and Deployment
   - 4.3 Testing in code integration for security
   - 4.4 Canaries in code deployment
   - 4.5 Policy engines

5. Confidentiality aspects
   - 5.1 Secrets management
   - 5.2 Encryption of data at rest
   - 5.3 Encryption of data in transit
   - 5.4 Data leakage and exfiltration

6. Availability
   - 6.1 Storage tiers and locality
   - 6.2 Backup strategies
   - 6.3 Data and process redundancy
   - 6.4 Data lifecycle configuration
   - 6.5 DDoS mitigation

7. Locality
   - 7.1 Compliance requirements
   - 7.2 Geography of data/processes
   - 7.3 Redundancy of data centers
   - 7.4 Colocation for performance reasons

8. Monitoring and Audit
   - 8.1 Centralized logging
   - 8.2 Auditing orchestration scripts
   - 8.3 Detecting misconfigurations
   - 8.4 Cloud Forensics

9. Summary and Research topics
   - 9.1 Homomorphic encryption
   - 9.2 Attestation
   - 9.3 Proof-carrying data
   - 9.4 Side-channel attacks
   - 9.5 Conclusions

Literature
Compulsory Reading
Further Reading ▪ Mitre Cloud ATT&CK. https://attack.mitre.org/matrices/enterprise/cloud/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Security by Design in the Cloud

Course Code: DLBCSEECS02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSCC01 or DLBDSCC01_D, DLBCSEECS01_E

Course Description

This course provides the opportunity to implement a cloud software system using best cloud security practices. A list of ideas is provided on the online learning platform. In addition, the students can contribute use case ideas of their own after consulting with the tutor. The core aim is to apply the theoretical knowledge of cloud security methods and best practices to implement an application that is deployed as an Infrastructure-as-code project, can be monitored and audited, as well as easily and preferably automatically updated without danger. This entails reasoning about possible design and architectural choices in a rational way, as well as implementing them on a cloud platform, such as CNCF, Amazon AWS, Microsoft Azure or Google GCP.

Course Outcomes

On successful completion, students will be able to

- transfer previously acquired knowledge about cloud security to practical use cases.
- design, architect, and implement a working cloud-based system.
- reason about design choices of and how best cloud security practices are followed.
- critically evaluate said choices with respect to the stated design goal.
- describe and explain the resulting solution in a report.

Contents

- This course is about the implementation of a practical cloud application employing best security practices to arrive at a system that is practical, auditable, monitored and easily updated.

Literature

Compulsory Reading

Further Reading

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Pentesting

Module Code: DLBCSEEPT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D ▪ DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Principles of Ethical Hacking) / N.N. (Project: Pentesting)

Contributing Courses to Module

- Principles of Ethical Hacking (DLBCSEEPT01_E)
- Project: Pentesting (DLBCSEEPT02_E)

Module Exam Type

Module Exam	Split Exam
	Principles of Ethical Hacking • Study Format "Distance Learning": Exam, 90 Minutes Project: Pentesting • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module
see curriculum

Module Contents

Principles of Ethical Hacking

- History of ethical hacking
- Ethical and legal frameworks
- Planning phase
- Social Engineering & OSINT
- Tools
- RATs, Rootkits and Command & Control
- Data exfiltration
- Red/Blue Teams
- Bug Bounty programs
- Report writing

Project: Pentesting

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system.

Learning Outcomes

Principles of Ethical Hacking

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Project: Pentesting

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Principles of Ethical Hacking

Course Code: DLBCSEEPT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D

Course Description

Ethical hacking is an essential part in testing security implementations as well as discovering overlooked security issues. In this course, we will look at the principles and tools that hackers use and how ethical hacking is effectively utilized.

Course Outcomes

On successful completion, students will be able to

- understand the concepts, ethical and legal frameworks for penetration testing activity.
- plan a penetration testing campaign.
- use the tools and methods to execute the plan.
- organize a bug bounty program and work with penetration testers.
- write reports for the target audience.

Contents

1. History of ethical hacking

2. Ethical and legal frameworks
   - 2.1 Certifications
   - 2.2 Defining parameters of engagement
   - 2.3 Contracts

3. Planning phase
   - 3.1 Using Mitre PreATT&CK® for reconnaissance
   - 3.2 User Mitre Enterprise ATT&CK® for tool selection
   - 3.3 Documentation

4. Social Engineering & OSINT

5. Tools
   - 5.1 Web application pentesting tools
   - 5.2 Remote execution testing tools
   - 5.3 Password cracking
   - 5.4 OSINT tools
   - 5.5 Fuzzing tools
6. RATs, Rootkits and Command & Control
7. Data exfiltration
8. Red/Blue Teams
9. Bug Bounty programs
10. Report writing

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Pentesting

Course Code: DLBCSEEPT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEINF01_E or DLBCSEINF01_D, DLBCSEHSF01_E or DLBCSEHSF01_D, DLBCSEEPT01_E

Course Description

In a controlled setting, students use provided tools to execute a penetration test against an emulated corporate system. Students write a report outlining the vulnerabilities found, the methods used and proposals for fixing that class of vulnerability.

Course Outcomes

On successful completion, students will be able to

- execute a successful penetration test.
- write appropriate reports.

Contents

- The student will be provided with virtual environments emulating corporate systems and an attacker machine with the necessary tools.

Literature

Compulsory Reading

Further Reading

- Karger, P. A. / Scherr, R. R. (1974): Multics Security Evaluation: Vulnerability Analysis. (URL: https://www.acsac.org/2002/papers/classic-multics-orig.pdf [last accessed: 25 August 2020]).
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Palmer, C. C. (2001): Ethical Hacking. IBM Systems Journal. 2001. 40 (3):769.
- Pentesting Bible. https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBCSEEPT02_E

Industrial Systems Technology

Module Code: DLBCSEEIST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBINGEIT01_E or DLBINGEIT01 ▪ none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Marian Benner-Wickner (Software Engineering Principles) / N.N. (Internet of Things Security)

Contributing Courses to Module

- Software Engineering Principles (IGIS01_E)
- Internet of Things Security (DLBCSEEIST01_E)

Module Exam Type

Module Exam	Split Exam
	Software Engineering Principles • Study Format "Distance Learning": Exam, 90 Minutes Internet of Things Security • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Software Engineering Principles

- binary system
- Structure and function of computer systems
- Structure and function of communication networks
- Software life cycle
- Roles, phases, activities in software engineering

Internet of Things Security

Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Learning Outcomes

Software Engineering Principles

On successful completion, students will be able to

- students can perform simple calculations in the binary system (Boolean algebra).
- students can describe the structure of computer systems and communication networks.
- students can distinguish between the phases of a SW life cycle.
- students can distinguish roles and phases in the software process.
- the students know different process models of SW development.
- the students know typical challenges and risks of enterprise SW development.
- the students know different programming paradigms and their application.

Internet of Things Security

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Software Engineering Principles

Course Code: IGIS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to give students an insight into the technical and theoretical basics of software engineering. In addition to the general structure of computer systems, students are taught typical challenges in the development of enterprise information systems. Furthermore, the typical phases and activities in software engineering are presented to address these risks.

Course Outcomes

On successful completion, students will be able to

- students can perform simple calculations in the binary system (Boolean algebra).
- students can describe the structure of computer systems and communication networks.
- students can distinguish between the phases of a SW life cycle.
- students can distinguish roles and phases in the software process.
- the students know different process models of SW development.
- the students know typical challenges and risks of enterprise SW development.
- the students know different programming paradigms and their application.

Contents

1. Structure and organization of information systems
   - 1.1 0 and 1 as the basis of all IT systems
   - 1.2 Von Neumann Architecture
   - 1.3 Distributed systems and communication networks
   - 1.4 Enterprise information systems

2. Risks and challenges of enterprise software engineering
   - 2.1 Properties of enterprise software systems
   - 2.2 Software Engineering
   - 2.3 Risks and typical problems
   - 2.4 Cause study
   - 2.5 Challenges in Software Engineering

3. Software life cycle: from planning to replacement
   - 3.1 The software life cycle at a glance
   - 3.2 Planning
   - 3.3 Development
   - 3.4 Operation
   - 3.5 Maintenance
   - 3.6 Shutdown

4. Requirements engineering and specification
   - 4.1 requirements engineering
   - 4.2 Specification

5. Architecture and implementation
   - 5.1 Architecture
   - 5.2 Implementation

6. Testing, operation and evolution
   - 6.1 Testing
   - 6.2 Operation
   - 6.3 Evolution

7. Roles in Software Engineering
   - 7.1 Idea of the role-based approach
   - 7.2 Typical roles

8. Organization of software projects
   - 8.1 From process paradigm towards software process
   - 8.2 Process Paradigms
   - 8.3 Product life cycle

9. Software Process Frameworks
   - 9.1 V-model XT
   - 9.2 Rational Unified Process (RUP)
   - 9.3 Scrum

Literature
Compulsory Reading
Further Reading ▪ Gumm, H. P./Sommer, M. (2011): Introduction to Computer Science. 9th edition, Oldenbourg, Munich. ▪ Hansen, H. R./Neumann, G. (2009): Information Systems 1. Fundamentals and Applications. 10th edition, UTB, Stuttgart. ▪ Ludewig, J./Lichter, H. (2010): Software Engineering. Basics, people, processes, techniques. 2nd edition, dpunkt.verlag, Heidelberg. ▪ Sommerville, I. (2015): Software Engineering. 10th edition, Pearson, Munich.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Internet of Things Security

Course Code: DLBCSEEIST01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBINGEIT01_E or DLBINGEIT01

Course Description

Internet of Things (IoT) is a mega trend. It covers end consumer systems as well as industrial systems and technologies (Industrial IoT, or IIoT). There is an increasing amount of interconnected devices that composes the Internet of Things. In general, the Internet of Things architecture consists of terminal devices, cloud solutions and actors/sensors. Internet of Things Security brings together different topics i.e. network protocols, software, hardware, cryptography and cloud computing.

Course Outcomes

On successful completion, students will be able to

- know and understand the basic concepts of IoT architectures.
- know and understand the most common vulnerabilities, threats and risks for IoT.
- understand and apply countermeasures for IoT vulnerabilities.
- analyze an IoT architecture model/solution.

Contents

1. Basics of the Internet of Things (IoT)
   - 1.1 Introduction
   - 1.2 Architecture
   - 1.3 Non-Industrial Internet of Things
   - 1.4 Industry 4.0 (Industrial IoT)
2. Internet of Things Attacks
   - 2.1 Vulnerabilities, Threats and Risks
   - 2.2 Cyber Attacks and Countermeasures
3. Security by Design
   - 3.1 Project Management / Secure Development Life Cycle
   - 3.2 Static Testing
   - 3.3 Dynamic Testing
   - 3.4 DevSecOps

4. Securing Internet of Things Devices
   - 4.1 Security Risks
   - 4.2 Design Objectives

5. Operational Security
   - 5.1 Information and Cyber Security Management System
   - 5.2 Network Security
   - 5.3 Device Configuration
   - 5.4 Authentication and Authorization

6. Cloud Security
   - 6.1 Concept of the Fog
   - 6.2 Threats to Cloud Internet of Things Services
   - 6.3 Cloud-Based Security Services
   - 6.4 Securing the Cloud Solution

7. Big Data / Artificial Intelligence
   - 7.1 Supervised Learning
   - 7.2 Unsupervised Learning

Literature

Compulsory Reading

Further Reading

- Butun, I. (2020): Industrial IoT. Challenges, Design Principles, Applications, and Security. 1st Edition, Springer International Publishing, Cham.
- Gupta B./Quamara, M. (2020): Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. 1st edition, CRC Press, Boca Raton, FL.
- Liyanage, M. et al. (2020): IoT Security. Advances in Authentication. 1st edition, John Wiley & Sons Ltd., Hoboken, NJ.
- Russell, B./Van Duren, D. (2018): Practical Internet of Things Security. Design a security framework for an Internet connected ecosystem. 2nd edition, Packt Publishing Ltd., Birmingham.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSEEIST01_E

Cyber Threat Intelligence

Module Code: DLBCSEECTI_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLBCSEECTI01_E	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Attack Models and Threat Feeds) / N.N. (Project: Defense against APTs)

Contributing Courses to Module

- Attack Models and Threat Feeds (DLBCSEECTI01_E)
- Project: Defense against APTs (DLBCSEECTI02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Threat Feeds • Study Format "Distance Learning": Exam, 90 Minutes Project: Defense against APTs • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Attack Models and Threat Feeds

- Apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model
- Determine what data is already available
- Do a gap analysis on what is detection or defense technology is missing
- Determine what extern threat feed data is required
- Utilize threat intelligence systems for diagnosis

Project: Defense against APTs

Using well-known methods like the MITRE ATT&CK Techniques, Tactics and Procedures students will be able to produce a comprehensive threat model. Therefore, students will have to determine through simulation or a “table top exercise” which data is already available and which extern threat feed data is required. After analyzing the “attack side” students will utilize threat intelligence systems for diagnostic to do a gap analysis – especially what defense technology is missing – and will be able to give sound advice to enhance resilience and to foster response capabilities. Emphasis will be drawn on the practical aspects of the defense against a given threat actor using techniques including beyond technical solutions and determine what cooperation with CERTs and ISPs is required to effectively defend against threats.

Learning Outcomes

Attack Models and Threat Feeds

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Project: Defense against APTs

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Attack Models and Threat Feeds

Course Code: DLBCSEECTI01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, we look in depth at modeling threats and using data to diagnose, analyze and make recommendations. After a broad look at threat actors, we look at a variety of ways of modeling threats. This spans from Attack Trees to Kill Chains, but whichever method works the best, it all boils down to adversary Techniques, Tactics and Procedures. We look into the various taxonomies of these as defined by Mitre's ATT&CK and determine what can be observed in data.It is rare that internal data is enough for a complete analysis and in practice the threat analysist must use external data sources. These are available in a variety of formats, but the industry is converging on STIX and the use of software platforms like ACT to do the parsing and provide a good user experience.After looking at examples of threat actors and reports on them, we tackle the problem of making recommendations and writing reports. In some cases, engaging with law enforcement is required in which case some particularities need to be observed.

Course Outcomes

On successful completion, students will be able to

- understand a variety of threat modeling techniques.
- apply the Mitre ATT&CK Techniques, Tactics and Procedures.
- do a gap analysis on what is detection or defense technology is missing.
- utilize threat intelligence systems for diagnosis.
- write reports and recommendations.

Contents

1. Threat actors
   - 1.1 Script kiddies
   - 1.2 eCrime threat actors
   - 1.3 Advanced Persistent Threat actors (APT)
   - 1.4 Threat researchers

2. Modeling an attack
   - 2.1 Phases of an attack
   - 2.2 Lockheed Martin Kill-Chain
   - 2.3 Attack Trees
   - 2.4 STRIDE
   - 2.5 DREAD
   - 2.6 The Diamond Model of attack analysis
   - 2.7 Pyramid of pain
   - 2.8 Techniques, Tactics and Procedures

3. Attack preparation TTPs
   - 3.1 Observability of attack preparations
   - 3.2 Operational security of an organization

4. Enterprise TTPs
   - 4.1 Behaviors of the attacker
   - 4.2 Observable data in an enterprise

5. ICS TTPs
   - 5.1 Critical infrastructure
   - 5.2 Special considerations with IoT/ICS defense

6. Threat data exchange
   - 6.1 Indicators of Compromise
   - 6.2 Threat intelligence reports
   - 6.3 Ad-hoc data formats
   - 6.4 STIX format, TAXII protocol
   - 6.5 Mitre ATT&CK, CVEs, etc.
   - 6.6 The semantics of threat data
   - 6.7 Other sources of data for CTI analysis

7. Examples of threat analysis platforms
   - 7.1 ACT Platform
   - 7.2 MISP
   - 7.3 OpenCTI

8. Examples of threat actors and their modus operandi
   - 8.1 Threat model
   - 8.2 Relevant indicator data
   - 8.3 Relevant CTI data
   - 8.4 Diagnosing the threat
   - 8.5 Data coverage gap analysis

9. Reporting
   - 9.1 Mapping raw data to Mitre ATT&CK
   - 9.2 Making defensive recommendations
   - 9.3 Writing reports for technical staff
   - 9.4 Writing reports for management
   - 9.5 Working with law enforcement

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Project: Defense against APTs

Course Code: DLBCSEECTI02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBCSEECTI01_E

Course Description

This project course will give students hands-on experience in the challenging task to analyze threat vectors and real attacks of highly sophisticated, well planned, prepared and conducted attack campaigns named “Advanced Persistent Threats – APT´s” which derive from state, non-state or highly criminal attackers. Students will need to consider all practical aspects of different attack vectors using technical and non-technical (like social engineering) methods and procedures. To have the right understanding how to defend against these attacks they will use an attack simulator like Foreseeti SecureCAD or AttackIQ or conduct a “table top exercise” to figure out what data is required to analyze what security components and system configurations are needed to defend against a given, highly capable threat actor. Through this course, students will develop a complete overview what technical applications can be used to enhance resilience, foster response capabilities and recover from such attacks. Furthermore, students will have to take into account so called “soft measures” like organizational and procedural policies and regulations, bearing in mind the human factor in its social and psychological form. Through the cooperation with CERT´s, ISP´s and IT-Security Companies, academics and state agencies, students will cooperate on international level with IT-experts and experts from other disciplines to improve their expertise and to develop their personality.

Course Outcomes

On successful completion, students will be able to

- practically apply the Mitre ATT&CK Techniques, Tactics and Procedures to produce a threat model of complex and sophisticated APT attacks.
- use an attack simulator to identify internal available and develop requirements for external needed threat feed data or conduct a “table top exercise”.
- do a comprehensive gap analysis, using a threat intelligence system for diagnostic, apply the right technical and non-technical defences.
- cooperate with CERT´s, ISP´s and IT-Security companies.

Contents

- This project course focuses on practical aspects how to defend against APTs. Students will start with a given use case to analyze a real-world APT Attack against a defined IT-System / Network, identify the different attack vectors on multiple levels and make the necessary data regarding used malware and exploits, techniques and procedures available by using a simulator or conducting a “table top exercise”. With this, students will develop a comprehensive picture of vulnerabilities and security shortfalls in the IT-system / network of

their own enterprise. Students will then have to analyze and identify what technical or non-technical measures could have prevented this attack using an interdisciplinary approach taking all levels and involved actors into account. Cooperation with other national and international CERT´s, ISP, IT-Security companies and state agencies will be the basis for a sound assessment how to improve the own resilience using best practices, state of the art technologies and considering new technologies.

- All relevant artifacts and considerations are documented by the students in a comprehensive project report.

Literature

Compulsory Reading

Further Reading

- ACT Platform: https://www.mnemonic.no/research-and-development/semi-automated-cyber-threat-intelligence/
- Caltagirone, S./Pendergast, A./Betz, C. (2013): The Diamond Model of Intrusion Analysis. (URL: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf)
- Hutchins, E. M./Cloppert, M. J./Amin, R. M.(2010): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. (URL: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
- MISP Platform: https://www.misp-project.org/
- Mitre PreATT&CK. https://attack.mitre.org/matrices/pre/
- Mitre Enterprise ATT&CK. https://attack.mitre.org/matrices/enterprise/
- Mitre Mobile ATT&CK. https://attack.mitre.org/matrices/mobile/
- Mitre ICS ATT&CK: https://collaborate.mitre.org/attackics/index.php/Main_Page
- Obrst, L./Chase, P./Markeloff, R. (2012): Developing an Ontology of the Cyber Security Domain. In Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security, Fairfax, VA.
- OpenCTI: https://github.com/OpenCTI-Platform/opencti
- Semantics of threat data: http://www.ti-semantics.com
- STIX: https://www.oasis-open.org/standards#stix2.1
- TAXII: https://www.oasis-open.org/standards#taxii2.1
- Zeltzer, L.: Report Template for Threat Intelligence and Incident Response. https://zeltser.com/cyber-threat-intel-and-ir-report-template/

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Mobile Threats

Module Code: DLBCSEEMT_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLBIBRVS01_E or DLBIBRVS01; DLBCSEINF01_E or DLBCSEINF01_D ▪ none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Wireless and Telecom Security) / N.N. (Software Architectures of Mobile Devices)

Contributing Courses to Module

- Wireless and Telecom Security (DLBCSEEMT01_E)
- Software Architectures of Mobile Devices (DLBCSEEMT02_E)

Module Exam Type

Module Exam	Split Exam
	Wireless and Telecom Security • Study Format "Distance Learning": Exam, 90 Minutes Software Architectures of Mobile Devices • Study Format "Distance Learning": Exam, 90 Minutes

Weight of Module

see curriculum

Module Contents

Wireless and Telecom Security

- Wireless protocols overview
- Wireless basics
- Telecom protocol classes
- Telecom architecture
- Handset and device security
- Threats
- Other wireless applications
- Protections

Software Architectures of Mobile Devices

- Handset technology stack
- Hardware
- Android operating system
- Apple iOS operating system
- Mobile devices
- Software ecosystems and security
- Mobile handset threats
- Mobile Device Management

Learning Outcomes

Wireless and Telecom Security

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Software Architectures of Mobile Devices

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the fields of IT & Technology

Wireless and Telecom Security

Course Code: DLBCSEEMT01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBIBRVS01_E or DLBIBRVS01; DLBCSEINF01_E or DLBCSEINF01_D

Course Description

The number of devices that can connect wirelessly to networks has already overtaken the number of desktop and laptop computers that connect to a local area network via a cable. In particular, phones and tablets dominate the market, and these connect to the wireless telecommunication networks. But there are also many other forms of wireless communication that devices use. The idiosyncrasies of these wireless systems need to be understood to integrate them in a complete security concept. Wireless protocols often force the user to trust in a system that they have no insights into and in this course, we will shine light onto the subject.

Course Outcomes

On successful completion, students will be able to

- understand the basics of wireless signals used in data transmission.
- identify different types of wireless networking and understand their differences.
- understand telecommunications terminology and contrast this to IT terminology.
- understand the architectures of the most important wireless telecommunications systems.
- understand the attack vectors against the handsets and devices as well as the core network.
- find other types of networking that may be in use.

Contents

1. Wireless protocols overview
   - 1.1 Personal area network protocols (Bluetooth, RFID, NFC, and more)
   - 1.2 Wireless local area network protocols (802.11a,b, g, ac , p and more)
   - 1.3 Wide area network protocols (Telecom protocols, LoRa, Satellite protocols, and more)
   - 1.4 Key exchange and cryptography in wireless networking
2. Wireless basics
   - 2.1 Frequencies
   - 2.2 Modulations
   - 2.3 Data Encodings
   - 2.4 Trade-offs

3. Telecom protocol classes
   - 3.1 Telecom vs IT terminology and technologies
   - 3.2 Telecom standards
   - 3.3 Legacy digital protocols
   - 3.4 LTE
   - 3.5 5G

4. Telecom architecture
   - 4.1 Overall architecture
   - 4.2 Core architecture
   - 4.3 Software defined networking
   - 4.4 5G Campus Networks
   - 4.5 Application layer security

5. Handset and device security
   - 5.1 Requirements
   - 5.2 Typical hardware design
   - 5.3 IoT Devices

6. Threats
   - 6.1 Common attack vectors against devices and handsets
   - 6.2 Common attack vector against the core network
   - 6.3 Potential attacks against 5G campus networks

7. Other wireless applications
   - 7.1 Aviation and Nautical wireless protocols
   - 7.2 Proprietary device protocols
   - 7.3 Wide area sensor networks (LoRa, Sigfox, ...)
   - 7.4 Digital voice/data technologies (DECT/GAP, TETRA, ...)
   - 7.5 Satellite communications

8. Protections
   - 8.1 Integrating mobile technology securely
   - 8.2 Monitoring mobile devices

Literature
Compulsory Reading
Further Reading ▪ Bartock, M. / Cichonski, J. / Souppaya, M. (2020): 5G CYBERSECURITY: Preparing a Secure Evolution to 5G. ▪ Cichonski, J. / Franklin, J. M. / Bartock, M. (2017): Guide to LTE Security. NIST Special Publication 800-187. ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ Pavur, J. et al. (2020): A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In 2020 IEEE Symposium on Security and Privacy (S&P). IEEE. May, 2020.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Software Architectures of Mobile Devices

Course Code: DLBCSEEMT02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Mobile devices have supplanted desktops and laptops as the most common end-user device. The smart phone has become a central business tool. Users run their entire lives from them. Furthermore, the Internet of Things are also using these mobile platforms. But too often, the risks and opportunities associated with these mobile devices are opaque to the security administrators in particular as these devices often operate outside the traditional Intranet. In this course, we examine how the dominant players, Android and Apple iOS, handle security in their software stack and ecosystem. We also look at the overlooked problem of IoT Security and wrap up with organizational solutions.

Course Outcomes

On successful completion, students will be able to

- understand the hardware and software stacks of common mobile handsets.
- understand the security controls in these stack.
- see what protections and risks are associated with the devices' ecosystems.
- see what attacks have had success in the past.
- utilize mobile endpoint management to protect an organization.

Contents

1. Handset technology stack
   - 1.1 Hardware
   - 1.2 Firmware
   - 1.3 Operating system
   - 1.4 Applications
   - 1.5 Ecosystem
2. Hardware
   - 2.1 RF modules
   - 2.2 PDA module
   - 2.3 Trusted Execution Environment component
   - 2.4 Biometric devices
   - 2.5 Location technology

3. Android operating system
   - 3.1 Hardware
   - 3.2 Bootloader
   - 3.3 Kernel and Hardware abstraction layer
   - 3.4 Sandboxing and virtualization
   - 3.5 Code signing

4. Apple iOS operating system
   - 4.1 Hardware
   - 4.2 Bootloader
   - 4.3 Kernel and Frameworks
   - 4.4 Sandboxing and virtualization
   - 4.5 Code signing

5. Mobile devices
   - 5.1 The Internet of things
   - 5.2 Linux
   - 5.3 RTOS
   - 5.4 Android on devices
   - 5.5 Other common embedded operating systems

6. Software ecosystems and security
   - 6.1 Google play
   - 6.2 Apple store
   - 6.3 Security providers
   - 6.4 The role of the Cloud

7. Mobile handset threats
   - 7.1 Historic examples of handset attacks
   - 7.2 Taxonomy of Handset threats
   - 7.3 Jailbreaking

8. Mobile Device Management
   - 8.1 The threats of BYOD
   - 8.2 Unique threats to mobile devices
   - 8.3 Patch and policy management

Literature
Compulsory Reading
Further Reading ▪ Gupta, A. (2014): Learning Pentesting for Android Devices ▪ Mobile Threat Catalog, https://pages.nist.gov/mobile-threat-catalogue/ ▪ N.A. (2020): Android Enterprise Security White Paper. ▪ N.A. (2019): iOS Security iOS 12.3. https://www.apple.com/lae/business/docs/site/iOS_Security_Guide.pdf ▪ Silberschatz, Avi / Galvin, P. B. / Gagne, G. (2012): Operating System Concepts. 9th Edition, John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBCSEEMT02_E

Supply Chain Management

Module Code: DLBDSESCM

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Supply Chain Management I) / N.N. (Supply Chain Management II)

Contributing Courses to Module

- Supply Chain Management I (DLBDSESCM01)
- Supply Chain Management II (DLBDSESCM02)

Module Exam Type

Module Exam	Split Exam
	Supply Chain Management I • Study Format "Distance Learning": Module Exam (50) Supply Chain Management II • Study Format "Distance Learning": Module Exam (50)

Weight of Module

see curriculum

Module Contents

Supply Chain Management I

- Historical and terminological aspects of the SCM concept
- Motives for the creation of cross-company value creation networks
- Design principles and effects of value creation networks
- Logistical core processes and SCM
- Information technology aspects of the SCM concept
- Coordination and collaboration of the network partners
- Industry-specific solutions of the SCM

Supply Chain Management II

- Strategic aspects of SCM
- SCM Practice: Tasks and Activities in the Core Planning Process
- SCM Practice: Tasks and Activities in the Core Process of Procurement
- SCM Practice: Tasks and Activities in the Core Process Production
- SCM Practice: Tasks and Activities in the Core Distribution Process

Learning Outcomes

Supply Chain Management I

On successful completion, students will be able to

- explain the importance of cross-company value creation processes.
- understand common concepts for modeling cross-company value creation processes.
- understand dynamic effects in supply chains and can systematize their causes and effects.
- explain important theoretical concepts for describing the characteristics and challenges of cross-company value creation processes.
- explain the approaches and problem categories commonly used in the context of supply chain management.
- understand important reference and/or management models for the concretization of supply chain systems.
- name and detail important roles and tasks in the SCM network.
- deal with the coordination problem of SCM and describe the common solution approaches.

Supply Chain Management II

On successful completion, students will be able to

- systematically explain the strategic relevance of enterprise-wide value creation processes.
- understand the most important tasks and problems in the SCM core process planning.
- systematize the elements and interrelationships in the CPFR model in a differentiated way.
- be familiar with the characteristics and peculiarities of contract logistics.
- understand the most important tasks and problems in the SCM core process procurement.
- explain central elements and characteristics of a procurement strategy.
- understand the most important tasks and problems in the SCM core process production.
- explain central elements and characteristics of a modern production strategy.
- understand the most important tasks and problems in the SCM core process distribution.
- explain central elements and characteristics of the so-called ECR concept.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Logistics & Transportation	All Bachelor Programmes in the Transport & Logistics fields

Supply Chain Management I

Course Code: DLBDSESCM01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

SCM proves to be an extremely multi-faceted construct from both a theoretical and a practical point of view. An adequate understanding of the problem dimensions and modes of action of (global) cross-company value creation networks requires a multidimensional approach. It starts by considering logistical processes, with modern process, flow, and network standards forming an important basis for SCM. On the basis of such an approach, students should gain a fundamental understanding of SCM. From the point of view of a holistic approach, it also makes sense to also examine a number of other typical problem areas in addition to the logistical challenges of this concept. This includes IT aspects of SCM (e.g., APS systems), and questions to do with the collaboration and coordination of network partners. This course also considers selected industry specific SCM solutions (ECR or VMI).

Course Outcomes

On successful completion, students will be able to

- explain the importance of cross-company value creation processes.
- understand common concepts for modeling cross-company value creation processes.
- understand dynamic effects in supply chains and can systematize their causes and effects.
- explain important theoretical concepts for describing the characteristics and challenges of cross-company value creation processes.
- explain the approaches and problem categories commonly used in the context of supply chain management.
- understand important reference and/or management models for the concretization of supply chain systems.
- name and detail important roles and tasks in the SCM network.
- deal with the coordination problem of SCM and describe the common solution approaches.

Contents

1. Fundamentals of the Supply Chain Concept
   - 1.1 Terminological and Conceptual Fundamentals
   - 1.2 Supply Chain Typology According to Otto
   - 1.3 Supply Chain Typology According to Bechtel/Jayaram
   - 1.4 Dynamic Aspects of Supply Chains

2. Selected Theoretical Concepts for the Supply Chain Concept
   - 2.1 New Institutional Economics
   - 2.2 Game Theory
   - 2.3 Network Approach
   - 2.4 Other Theoretical Additions

3. Supply Chain Management
   - 3.1 Basic Information on the Goals and Scope of SCM
   - 3.2 Popular Problem Areas of the SCM
   - 3.3 Supply Chain Management as an Evolutionary Step in Logistics
   - 3.4 Supply Chain Management as Cooperation Management

4. SCM Model
   - 4.1 Basic Information on the Term SCM Models
   - 4.2 SCOR Model
   - 4.3 SCM Task Model

5. SCM as a Coordination Problem
   - 5.1 Basic Information on the Concept of Coordination
   - 5.2 Coordination Concepts, Context, and Perspectives of SCM
   - 5.3 Coordination Instruments

Literature
Compulsory Reading
Further Reading ▪ Arndt, H. (2018): Supply Chain Management. Optimierung logistischer Prozesse. 7. Auflage, Gabler, Wiesbaden. ▪ Grosche, P. (2012): Konfiguration und Koordination von Wertschöpfungsaktivitäten in internationalen Unternehmen. Eine empirische Untersuchung in der Automobilindustrie. Gabler-Verlag, Wiesbaden. ▪ Heiserich, O.E./Helbig, K./Ullmann, W. (2011): Logistik. Eine praxisorientierte Einführung. 4. Auflage, Gabler-Verlag | Springer Fachmedien, Wiesbaden 2011. ▪ Hertel, J./Zentes, J./Schramm-Klein, H. (2011): Supply-Chain-Management und Warenwirtschaftssysteme im Handel. 2. Auflage, Springer Verlag, Heidelberg. ▪ Hungenberg, H. (2014): Strategisches Management in Unternehmen. Ziele-Prozesse-Verfahren. 8. Auflage, Wiesbaden. ▪ Pfohl, H. C. (2010): Logistiksysteme. Betriebswirtschaftliche Grundlagen. 8 Auflage, Springer, Berlin. ▪ Schulte, C. (2013): Logistik. Wege zur Optimierung der Supply Chain. 6. Auflage, Vahlen, München. ▪ Werner, H. (2013): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 5. Auflage, Gabler, Wiesbaden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Module Exam

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Supply Chain Management II

Course Code: DLBDSESCM02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

From the perspective of strategic management research and practice, the activities covered by the term SCM are closely related to efforts to build and/or maintain a stable operational competitive advantage. A fundamental discussion of this relationship forms the starting point for the course. On this basis, a differentiated analysis of strategy-relevant activities and instruments in the Plan, Source, Make, Deliver, and Return process categories is then carried out using the SCOR model. Special attention is given to the practice-relevant areas of SCM, e.g., order-promising (plan), supplier-relation-management (source), postponement (make), and the ECR-concept (deliver).

Course Outcomes

On successful completion, students will be able to

- systematically explain the strategic relevance of enterprise-wide value creation processes.
- understand the most important tasks and problems in the SCM core process planning.
- systematize the elements and interrelationships in the CPFR model in a differentiated way.
- be familiar with the characteristics and peculiarities of contract logistics.
- understand the most important tasks and problems in the SCM core process procurement.
- explain central elements and characteristics of a procurement strategy.
- understand the most important tasks and problems in the SCM core process production.
- explain central elements and characteristics of a modern production strategy.
- understand the most important tasks and problems in the SCM core process distribution.
- explain central elements and characteristics of the so-called ECR concept.

Contents

1. Strategic Aspects of SCM
   - 1.1 Strategic Thinking and Action: General Information
   - 1.2 Competition Focus and SCM
   - 1.3 Competition Location and SCM
   - 1.4 Competition Rules and SCM

2. SCM Practice: Core Process Planning
   - 2.1 General Preliminary Considerations
   - 2.2 Collaborative Planning, Forecasting, and Replenishment
   - 2.3 Order Promoting
   - 2.4 Kanban
   - 2.5 Integration of X-PL Logistics Service Providers

3. SCM Practice: Core Process Procurement
   - 3.1 General Preliminary Considerations
   - 3.2 Production Synchronous Procurement
   - 3.3 Sourcing Concepts
   - 3.4 Supplier Relations Management

4. SCM Practice: Core Process Production
   - 4.1 Selected Aspects of the Problem Background
   - 4.2 Collaborative Engineering
   - 4.3 Postponement Strategies
   - 4.4 Value Added Partnership

5. SCM Practice: Core Process Distribution
   - 5.1 Basic Information on the Distribution Problem
   - 5.2 Efficient Consumer Response (ECR)
   - 5.3 Consignment Warehouse

Literature
Compulsory Reading
Further Reading ▪ Arndt, H. (2018): Supply Chain Management. Optimierung logistischer Prozesse. 7. Auflage, Gabler, Wiesbaden. ▪ Grosche, P. (2012): Konfiguration und Koordination von Wertschöpfungsaktivitäten in internationalen Unternehmen. Eine empirische Untersuchung in der Automobilindustrie. Gabler-Verlag, Wiesbaden. ▪ Heiserich, O.E./Helbig, K./Ullmann, W. (2011): Logistik. Eine praxisorientierte Einführung. 4. Auflage, Gabler-Verlag | Springer Fachmedien, Wiesbaden 2011. ▪ Hertel, J./Zentes, J./Schramm-Klein, H. (2011): Supply-Chain-Management und Warenwirtschaftssysteme im Handel. 2. Auflage, Springer Verlag, Heidelberg. ▪ Hungenberg, H. (2014): Strategisches Management in Unternehmen. Ziele-Prozesse-Verfahren. 8. Auflage, Wiesbaden. ▪ Pfohl, H. C. (2010): Logistiksysteme. Betriebswirtschaftliche Grundlagen. 8 Auflage, Springer, Berlin. ▪ Schulte, C. (2013): Logistik. Wege zur Optimierung der Supply Chain. 6. Auflage, Vahlen, München. ▪ Werner, H. (2013): Supply Chain Management. Grundlagen, Strategien, Instrumente und Controlling. 5. Auflage, Gabler, Wiesbaden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Module Exam

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBDSESCM02

Smart Factory

Module Code: DLBDSESF

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Smart Factory I) / Prof. Dr. Christian Magnus (Smart Factory II)

Contributing Courses to Module

- Smart Factory I (DLBDSESF01)
- Smart Factory II (DLBDSESF02)

Module Exam Type

Module Exam	Split Exam
	Smart Factory I • Study Format "Distance Learning": Exam, 90 Minutes Smart Factory II • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Smart Factory I

- Motivation and Definition of Terms
- Development of Automation
- Technological Basics and Standards
- Basic concepts of a Smart Factory
- Reference Architectures
- Smart Factory Engineering
- Safety and Security

Smart Factory II

A catalogue with the currently provided tasks is provided on the online platform of the module. It provides the content basis of the module and can be supplemented or updated by the seminar leader.

Learning Outcomes

Smart Factory I

On successful completion, students will be able to

- understand the term Smart Factory in the context of Industry 4.0.
- be able to trace the development of automation to a fully autonomous, non-centrally organized production plant.
- understand the basic technologies and standards used to design and operate a Smart Factory.
- understand the essential concepts of a Smart Factory.
- identify and differentiate between the individual elements of a Smart Factory using different reference architectures.
- understand the special engineering challenges in the Smart Energy context.
- understand the special safety risks of digitized and networked production plants and assign concrete recommendations for action.

Smart Factory II

On successful completion, students will be able to

- have a deeper understanding of the technologies and standards in the context of Smart Factory.
- apply technologies in the context of Smart Factory to a simple practical example.
- design a hardware or software prototype for a selected task.
- document, design, and develop activities in the form of a project report.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programmes in the IT & Technology fields

Smart Factory I

Course Code: DLBDSESF01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students will gain a deeper insight into the networking and digitization of production facilities by examining a Smart Factory. For this purpose, they will be familiarized with the basic goals of a Smart Factory in the context of the research complex Industry 4.0. After a brief introduction to the history of automation, students will learn the technical basics and standards required to design and operate a Smart Factory. Building on this, they will learn how these individual technologies are used to implement the central concepts of a Smart Factory. In order to understand which components a Smart Factory consists of, different reference architectures are presented and compared. The course concludes with the special engineering challenges of an autonomously acting and decentralized production plant. Above all, this includes IT security, which is particularly relevant due to the digital networking of production facilities and products.

Course Outcomes

On successful completion, students will be able to

- understand the term Smart Factory in the context of Industry 4.0.
- be able to trace the development of automation to a fully autonomous, non-centrally organized production plant.
- understand the basic technologies and standards used to design and operate a Smart Factory.
- understand the essential concepts of a Smart Factory.
- identify and differentiate between the individual elements of a Smart Factory using different reference architectures.
- understand the special engineering challenges in the Smart Energy context.
- understand the special safety risks of digitized and networked production plants and assign concrete recommendations for action.

Contents

1. Motivation and Definition of Terms
   - 1.1 Goals of Smart Factory
   - 1.2 Internet of Things
   - 1.3 Cyber-Physical Systems
   - 1.4 Cyber-Physical Production Systems
   - 1.5 Smart Factory as a Cyber-Physical (Production) System

2. Development of Automation
   - 2.1 Automation Pyramid
   - 2.2 Networked, Decentralized Organization of Production
   - 2.3 Future Challenges

3. Technological Basics and Standards
   - 3.1 Identification of Physical Objects
   - 3.2 Formal Description Languages and Ontologies
   - 3.3 Digital Object Memory
   - 3.4 Physical Situation Recognition
   - 3.5 (Partially) Autonomous Action and Cooperation
   - 3.6 Human-Machine Interaction
   - 3.7 Machine to Machine Communication

4. Basic Concepts of a Smart Factory
   - 4.1 Order-Controlled Production
   - 4.2 Bundling of Machine and Production Data
   - 4.3 Supporting People in Production
   - 4.4 Intelligent Products and Resources
   - 4.5 Smart Services

5. Reference Architectures
   - 5.1 Purpose and Properties of Reference Architectures
   - 5.2 Overview of Standardization Initiatives
   - 5.3 CyProS Reference Architecture
   - 5.4 RAMI 4.0 (DIN SPEC 91345)

6. Smart Factory Engineering
   - 6.1 Classification of Different Engineering Tools
   - 6.2 Virtual Engineering
   - 6.3 User-Centered Design
   - 6.4 Requirements Engineering
   - 6.5 Modelling
   - 6.6 Integration of Classic and Smart Components

Literature
Compulsory Reading
Further Reading ▪ Bangemann, T. et al. (2016): Integration of Classical Components into Industrial Cyber–Physical Systems. In: Proceedings of the IEEE, 104. Jg., Heft 5, S. 947–959. DOI: 10.1109/JPROC.2015.2510981. ▪ Bauernhansl, T./Hompel, M. ten/Vogel-Heuser, B. (Hrsg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Springer, Berlin. ▪ Bundesministerium für Wirtschaft und Energie (Hrsg.) (2016): IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten. Berlin. ▪ Geisberger, E./Broy, M. (Hrsg.) (2012): agendaCPS. Integrierte Forschungsagenda Cyber-Physical Systems. Springer, Berlin/Heidelberg. ▪ Harrison, R./Vera, D.; Ahmad, B. (2016): Engineering Methods and Tools for Cyber–Physical Automation Systems. In: Proceedings of the IEEE, 104. Jg., Heft 5, S. 973–985. DOI: 10.1109/JPROC.2015.2510665. ▪ Haupert, J. (2013): DOMeMan: Repräsentation, Verwaltung und Nutzung von digitalen Objektgedächtnissen. Akademische Verlagsgesellschaft AKA, Berlin. ▪ VDMA & Partner (2016): Leitfaden Industrie 4.0 Security. Handlungsempfehlungen für den Mittelstand. VDMA Verlag, Frankfurt a. M.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Smart Factory II

Course Code: DLBDSESF02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

In this course, students select a concrete task from the catalog of topics provided in consultation with the seminar leader. They will work on the task in a prototyping environment suited to the task, which can be either a hardware (e.g., prototyping boards) or software (e.g., technology-specific development environments) environment. To complete the task, students apply the concepts, methods, and tools taught in the Smart Factory I course. They document their results with a project report.

Course Outcomes

On successful completion, students will be able to

- have a deeper understanding of the technologies and standards in the context of Smart Factory.
- apply technologies in the context of Smart Factory to a simple practical example.
- design a hardware or software prototype for a selected task.
- document, design, and develop activities in the form of a project report.

Contents

- A catalogue with the currently provided tasks is provided on the online platform of the module. It provides the content basis of the module and can be supplemented or updated by the seminar leader.

Literature

Compulsory Reading

Further Reading

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☑ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLBDSESF02

Automation and Robotics

Module Code: DLBDSEAR

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLBDSEAR01	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Mario Boßlau (Production Engineering) / N.N. (Automation and Robotics)

Contributing Courses to Module

- Production Engineering (DLBDSEAR01)
- Automation and Robotics (DLBDSEAR02)

Module Exam Type

Module Exam	Split Exam
	Production Engineering • Study Format "Distance Learning": Exam, 90 Minutes (50) Automation and Robotics • Study Format "Distance Learning": Module Exam (50)

Weight of Module

see curriculum

Module Contents

Production Engineering

- Introduction to Manufacturing Technology
- Main Production Groups According to DIN 8580
- Additive Manufacturing Processes
- Rapid Prototyping
- Rapid Tooling
- Direct/Rapid Manufacturing
- Cyber-Physical Production Plants

Automation and Robotics

- Basics of Automation
- Fundamentals of Measurement Technology
- Sensors
- Basics of Control Engineering
- Basics of Control Technology
- Introduction to Robotics
- Kinematics of a Robot

Learning Outcomes

Production Engineering

On successful completion, students will be able to

- understand the basic concepts and interrelationships of production engineering.
- understand current changes in manufacturing technology due to technologies such as additive manufacturing and megatrends such as cyber physical systems.
- assign different manufacturing processes to the main manufacturing groups according to DIN 8580.
- understand the basic principle of additive manufacturing processes.
- distinguish between different additive manufacturing processes.
- understand the terms Rapid Prototyping, Rapid Tooling, and Direct Manufacturing and name individual processes and application examples.
- understand the elements and properties of cyber-physical production plants.

Automation and Robotics

On successful completion, students will be able to

- understand the basic aspects of automation.
- understand the different sizes and units in measurement technology.
- differentiate between different measurement methods.
- understand the basic structure of measuring equipment.
- select a suitable sensor based on various criteria.
- understand the elements of control systems.
- describe the behavior of control systems in the time and frequency domain.
- understand the basic principles of control technology.
- convert between different number systems and apply Boolean algebra.
- understand the structure of switching networks, plants, and storages.
- understand important elements of control systems such as signal generators and power amplifiers.
- design simple programmable logic controllers.
- understand the basic structure of industrial robots.
- calculate different movements and positions of jointed-arm robots.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field of Engineering	All Bachelor Programmes in the IT & Technology fields

Production Engineering

Course Code: DLBDSEAR01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

The aim of the course is to provide students with an overview of the processes that have influenced and still influence production processes through technological developments under the generic term Industry 4.0, based on traditional, standardized manufacturing techniques. These include, in particular, technological advances in additive manufacturing processes that enable applications such as rapid prototyping, rapid tooling, and direct manufacturing. Finally, the course deals with the consequences of the digitalization and networking of production facilities and their elements in the sense of a cyber-physical system.

Course Outcomes

On successful completion, students will be able to

- understand the basic concepts and interrelationships of production engineering.
- understand current changes in manufacturing technology due to technologies such as additive manufacturing and megatrends such as cyber physical systems.
- assign different manufacturing processes to the main manufacturing groups according to DIN 8580.
- understand the basic principle of additive manufacturing processes.
- distinguish between different additive manufacturing processes.
- understand the terms Rapid Prototyping, Rapid Tooling, and Direct Manufacturing and name individual processes and application examples.
- understand the elements and properties of cyber-physical production plants.

Contents

1. Introduction to Manufacturing Technology
   - 1.1 Basic Terms and Contexts in Manufacturing Theory
   - 1.2 Historical Development of Production
   - 1.3 The Discussion About the Long Tail

2. Main Production Groups According to DIN 8580
   - 2.1 Archetypes
   - 2.2 Reshaping
   - 2.3 Cutting (Cutting, Machining, Ablation)
   - 2.4 Joining
   - 2.5 Coating
   - 2.6 Substance Property Changes

3. Additive Manufacturing Processes
   - 3.1 Basic Principles and Legal Aspects
   - 3.2 Stereolithography (STL)
   - 3.3 Selective Laser Sintering and Selective Beam Melting With Laser or Electron Beam
   - 3.4 Fused Deposition Modeling (FDM)
   - 3.5 Multi-Jet Modeling (MJM) and Poly-Jet Process (PJM)
   - 3.6 3D Printing Process (3DP)
   - 3.7 Laminating Processes
   - 3.8 Mask Sintering

4. Rapid Prototyping
   - 4.1 Definition
   - 4.2 Strategic and Operational Aspects
   - 4.3 Application Areas and Examples

5. Rapid Tooling
   - 5.1 Definition, Strategic, and Operational Aspects
   - 5.2 Indirect and Direct Procedures

6. Direct/Rapid Manufacturing
   - 6.1 Potentials and Requirements for Procedures
   - 6.2 Implementation, Application Areas, and Examples

7. Cyber-Physical Production Plants
   - 7.1 Derivation of the Terms Industry 4.0 and Cyber-Physical Systems
   - 7.2 Megatrend Cyber Physical Systems (CPS)
   - 7.3 Definition Cyber-Physical Production Plant
   - 7.4 Effects on Planning and Operation of Production Facilities
   - 7.5 Dynamic Reconfiguration and Migration of Production Facilities

Literature
Compulsory Reading
Further Reading ▪ Anderson, C. (2012): Makers. The new industrial revolution. Crown Business, New York. ▪ Bauernhansl, Thomas/Hompel, M. ten/Vogel-Heuser, B. (Hrsg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung – Technologien – Migration. Springer, Wiesbaden. ▪ Gebhardt, A. (2012): Understanding Additive Manufacturing. Rapid Prototyping – Rapid Tooling – Rapid Manufacturing. Hanser, München/Cincinnati. ▪ Lachmayer, R./Lippert, R. B./Fahlbusch, T. (Hrsg.) (2016): 3D-Druck beleuchtet. Additive Manufacturing auf dem Weg in die Anwendung. Springer, Berlin/Heidelberg. ▪ Wittenstein, M. et al. (Hrsg.) (2015): Intelligente Vernetzung in der Fabrik. Industrie 4.0. Umsetzungsbeispiele für die Praxis. Fraunhofer Verlag, Stuttgart.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Automation and Robotics

Course Code: DLBDSEAR02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	DLBDSEAR01

Course Description

The aim of the course is to provide students with an insight into measurement, control, and regulation technology and convey the basics of robotics. Students will be taught which methods can be used to determine certain measured variables and how measurement errors are dealt with. Based on these fundamentals, various sensors will be presented and students will be able to select suitable sensors based on predefined criteria. The course also introduces students to the basics of control engineering. The different ways of describing the structure and behaviour of control systems are illustrated to the students. The basics of control engineering are also taught. The students receive a short introduction to binary number systems and Boolean algebra, and deal with various basal circuit and control elements. Finally, students will gain an insight into robotics with a focus on industrial robots. In this context, the students learn the description and calculation of positions and movements of individual limbs of a robot arm.

Course Outcomes

On successful completion, students will be able to

- understand the basic aspects of automation.
- understand the different sizes and units in measurement technology.
- differentiate between different measurement methods.
- understand the basic structure of measuring equipment.
- select a suitable sensor based on various criteria.
- understand the elements of control systems.
- describe the behavior of control systems in the time and frequency domain.
- understand the basic principles of control technology.
- convert between different number systems and apply Boolean algebra.
- understand the structure of switching networks, plants, and storages.
- understand important elements of control systems such as signal generators and power amplifiers.
- design simple programmable logic controllers.
- understand the basic structure of industrial robots.
- calculate different movements and positions of jointed-arm robots.

Contents

5. Basics of Control Technology
   - 5.1 Basic Principle and Elements of Control Systems
   - 5.2 Numerical Representations
   - 5.3 Boolean Algebra
   - 5.4 Switching Networks, Plants, and Storage Facilities
   - 5.5 Signal Generators and Power Amplifiers
   - 5.6 Programmable Logic Controllers
   - 5.7 Connection-Programmed Controls

6. Introduction to Robotics
   - 6.1 Terms and Classification
   - 6.2 Basic Elements
   - 6.3 Classification of Robots

7. Kinematics of a Robot
   - 7.1 Coordinate Systems and Reference Points
   - 7.2 Rotations
   - 7.3 Forward and Reverse Transformations
   - 7.4 Denavit-Hartenberg Transformation

Literature

Compulsory Reading

Further Reading

- Heinrich, B./Linke, P./Glöckler, M. (2015): Grundlagen Automatisierung. Springer, Wiesbaden.
- Hesse, S./Malisa, V. (Hrsg.) (2016): Taschenbuch Robotik – Montage – Handhabung. 2. Auflage, Carl Hanser Verlag, München.
- Jazar, R. N. (2010): Theory of Applied Robotics. 2. Auflage, Springer US, Boston (MA).
- Karaali, C. (2013): Grundlagen der Steuerungstechnik. Springer, Wiesbaden.
- Parthier, R. (2011): Messtechnik. Grundlagen und Anwendungen der elektrischen Messtechnik für alle technischen Fachrichtungen und Wirtschaftsingenieure. 6. Auflage, Vieweg & Teubner, Wiesbaden.
- Tietze, U./Schenk, C./Gamm, E. (2016): Halbleiter-Schaltungstechnik. 15. Auflage, Springer, Berlin.
- Zacher, S./Reuter, M. (2014): Regelungstechnik für Ingenieure. Springer, Wiesbaden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Module Exam

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

DLBDSEAR02

Mobile Software Engineering

Module Code: DLBCSEMSE

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

N.N. (Mobile Software Engineering I) / N.N. (Mobile Software Engineering II)

Contributing Courses to Module

- Mobile Software Engineering I (DLBCSEMSE01)
- Mobile Software Engineering II (DLBCSEMSE02)

Module Exam Type

Module Exam	Split Exam
	Mobile Software Engineering I • Study Format "Distance Learning": Exam, 90 Minutes Mobile Software Engineering II • Study Format "Distance Learning": Written Assessment: Project Report

Weight of Module

see curriculum

Module Contents

Mobile Software Engineering I

- Basics of mobile software development
- Android system architecture
- Development environment
- Core components of an Android app
- Interaction between application components
- Advanced techniques

Mobile Software Engineering II

Conception, implementation, and documentation of small, mobile applications on the basis of a concrete task.

Learning Outcomes

Mobile Software Engineering I

On successful completion, students will be able to

- recognize the differences and peculiarities of software development for mobile systems and explain them.
- differentiate between different activities, roles, and risks in the creation, operation, and maintenance of mobile software systems.
- explain and differentiate between the architecture and technical features of the Android platform.
- independently create mobile software systems to solve concrete problems for the “Android” platform.

Mobile Software Engineering II

On successful completion, students will be able to

- independently design and create a prototype of a small mobile application to solve a specific problem.
- recognize typical problems and challenges in the practical implementation of small mobile applications.
- document the conception and implementation of small, independently designed and implemented mobile applications.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the fields of Computer Science & Software Development	All Bachelor Programs in the IT & Technology fields

Mobile Software Engineering I

Course Code: DLBCSEMSE01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using the mobile platform "Android" as an example, it will be demonstrated how the programming of mobile applications (apps) differs from the development of browser-based information systems, which technologies and programming concepts are typically used, and which typical challenges there are in app development for industrial applications.

Course Outcomes

On successful completion, students will be able to

- recognize the differences and peculiarities of software development for mobile systems and explain them.
- differentiate between different activities, roles, and risks in the creation, operation, and maintenance of mobile software systems.
- explain and differentiate between the architecture and technical features of the Android platform.
- independently create mobile software systems to solve concrete problems for the “Android” platform.

Contents

1. Basics of Mobile Software Development
   - 1.1 Special Features of Mobile Devices
   - 1.2 Special Features of Mobile Software Development
   - 1.3 Classification of Mobile Devices
   - 1.4 The Android Platform
2. Android System Architecture
   - 2.1 The Android System
   - 2.2 Safety and Security
   - 2.3 Communication with Networks
3. Development Environment
   - 3.1 Android Studio
   - 3.2 First App and Emulator Test
   - 3.3 Application Deployment

4. Core Components of an Android App
   - 4.1 Overview of the Components of an Android App
   - 4.2 Activities, Layouts, and Views
   - 4.3 Resources
   - 4.4 Summary in an App
   - 4.5 Graphic Design

5. Interaction Between Application Components
   - 5.1 Intents
   - 5.2 Services
   - 5.3 Broadcast Receiver

6. Advanced Techniques
   - 6.1 Threading
   - 6.2 Application Memory

Literature

Compulsory Reading

Further Reading

- Becker, A./Pant, M. (2015): Android 5. Programmieren für Smartphones und Tablets. 4. Auflage, dpunkt.verlag, Heidelberg.Eason, J. (2014): Android Studio 1.0. (URL: https://android-developers.googleblog.com/2014/12/android-studio-10.html
- Eason, J. (2014): Android Studio 1.0. (URL: https://android-developers.googleblog.com/2014/12/android-studio-10.html [letzter Zugriff: 12.06.2015]).
- Franke, F./Ippen, J. (2012): Apps mit HTML5 und CSS3. Galileo Computing, Bonn.
- Google Inc. (Hrsg.) (2015): Android Developer Guide. (URL: http://developer.android.com/guide) [letzter Zugriff: 12.06.2015]).
- Google Inc. (Hrsg.) (2015): App Components. (URL: http://developer.android.com/guide/components/index.html [letzter Zugriff: 12.06.2015]).
- Google Inc. (Hrsg.) (2015): Installing the Android SDK. (URL: http://developer.android.com/sdk/installing/index.html[letzter Zugriff: 13.05.2015]).
- Google Inc. (Hrsg.) (2015): Resources Overview. (URL: http://developer.android.com/guide/topics/resources/overview.html[letzter Zugriff: 12.06.2015]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Mobile Software Engineering II

Course Code: DLBCSEMSE02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		5	none

Course Description

Using the knowledge gained in the course "Mobile Software Engineering using the Android platform as an example", students independently create a mobile application and document its conception and implementation.

Course Outcomes

On successful completion, students will be able to

- independently design and create a prototype of a small mobile application to solve a specific problem.
- recognize typical problems and challenges in the practical implementation of small mobile applications.
- document the conception and implementation of small, independently designed and implemented mobile applications.

Contents

- Conception, implementation, and documentation of small, mobile applications on the basis of a concrete task. Possible topics are, for example:
- A radio app to improve the exchange between listeners and stations in general, and listeners and radio presenters in particular.
- An app that allows a group of board game fans to better organize their regular evening game.
- An app that theses supervisors at IUBH can use to improve their supervision processes.

Literature
Compulsory Reading
Further Reading ▪ Eason, J. (2014): Android Studio 1.0. (URL: http://android-developers.blogspot.de/2014/12/android- studio-10.html [letzter Zugriff: 12.06.2015]). ▪ Google Inc. (Hrsg.) (2015): Android Developer Guide. (URL: http://developer.android.com/guide) ▪ Google Inc. (Hrsg.) (2015a): App Components. (URL: http://developer.android.com/guide/components/ index.html [letzter Zugriff: 12.06.2015]). ▪ Google Inc. (Hrsg.) (2015b): Installing the Android SDK. (URL: http://developer.android.com/sdk/ installing/index.html [letzter Zugriff: 13.05.2015]). ▪ Google Inc. (Hrsg.) (2015c): Resources Overview. (URL: http://developer.android.com/guide/topics/ resources/overview.html [letzter Zugriff: 12.06.2015]). ▪ Hipp, Wyrick & Company, Inc. (Hrsg.) (2015): SQLite Webseite. (URL: http://sqlite.org/index.html [letzter Zugriff: 12.06.2015]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Project

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Project Report

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Bachelor Thesis

Module Code: DLBBT

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	BA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Degree Program Advisor (SGL) (Bachelor Thesis) / Degree Program Advisor (SGL) (Colloquium)

Contributing Courses to Module

- Bachelor Thesis (DLBBT01)
- Colloquium (DLBBT02)

Module Exam Type

Module Exam	Split Exam
	Bachelor Thesis • Study Format "Distance Learning": Written Assessment: Bachelor Thesis Colloquium • Study Format "Distance Learning": Presentation: Colloquium

Weight of Module

see curriculum

Module Contents

Bachelor Thesis

- Bachelor's thesis
- Colloquium on the bachelor's thesis

Colloquium

Learning Outcomes

Bachelor Thesis

On successful completion, students will be able to

- work on a problem from their major field of study by applying the specialist and methodological skills they have acquired during their studies.
- independently analyze selected tasks with scientific methods, critically evaluate them, and develop appropriate solutions under the guidance of an academic supervisor.
- record and analyze existing (research) literature appropriate to the topic of their bachelor's thesis.
- prepare a detailed written elaboration in compliance with scientific methods.

Colloquium

On successful completion, students will be able to

- present a problem from their field of study using academic presentation and communication techniques.
- reflect on the scientific and methodological approach chosen in their bachelor's thesis.
- demonstrate that they can actively answer subject-related questions from the subject experts (reviewers of the bachelor's thesis).

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
All modules in the bachelor program	All bachelor programs in distance learning

Bachelor Thesis

Course Code: DLBBT01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		9	none

Course Description

The aim and purpose of the bachelor's thesis is to successfully apply the subject-specific and methodological competencies acquired during the course of study in the form of an academic dissertation with a thematic reference to the major field of study. The content of the bachelor's thesis can be a practical-empirical or theoretical-scientific problem. Students should prove that they can independently analyze a selected problem with scientific methods, critically evaluate it, and work out proposed solutions under the subject-methodological guidance of an academic supervisor. The topic chosen by the student from their respective field of study should meet the acquired scientific competences, deepening their academic knowledge and skills in order to meet the future needs of the field.

Course Outcomes

On successful completion, students will be able to

- work on a problem from their major field of study by applying the specialist and methodological skills they have acquired during their studies.
- independently analyze selected tasks with scientific methods, critically evaluate them, and develop appropriate solutions under the guidance of an academic supervisor.
- record and analyze existing (research) literature appropriate to the topic of their bachelor's thesis.
- prepare a detailed written elaboration in compliance with scientific methods.

Contents

- The bachelor's thesis must be written on a topic that relates to the content of the respective major field of study. In the context of the bachelor's thesis, the problem, as well as the scientific research goal, must be clearly emphasized. The work must reflect the current state of knowledge of the topic to be examined by means of an appropriate literature analysis. The student must prove their ability to use the acquired knowledge theoretically and/or empirically in the form of an independent and problem-solution-oriented application.

Literature
Compulsory Reading
Further Reading ▪ Hunziker, A.W. (2010): Spaß am wissenschaftlichen Arbeiten. So schreiben Sie eine gute Semester-, Bachelor- oder Masterarbeit. 4. Auflage, Verlag SKV, Zürich. ▪ Wehrlin, U. (2010): Wissenschaftliches Arbeiten und Schreiben. Leitfaden zur Erstellung von Bachelorarbeit, Masterarbeit und Dissertation – von der Recherche bis zur Buchveröffentlichung. AVM, München. ▪ Selection of literature according to topic

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Thesis

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** yes
Type of Exam	Written Assessment: Bachelor Thesis

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
270 h	0 h	0 h	0 h	0 h	270 h

Instructional Methods

- ☐ Learning Sprints®
- ☐ Course Book
- ☐ Vodcast
- ☐ Shortcast
- ☐ Audio
- ☐ Exam Template
- ☑ Review Book
- ☐ Creative Lab
- ☐ Guideline
- ☐ Live Tutorium/Course Feed

Colloquium

Course Code: DLBBT02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
BA	English		1	none

Course Description

The colloquium will take place after the submission of the bachelor's thesis. This is done at the invitation of the experts. During the colloquium, students must prove that they have independently produced the content and results of the written work. The content of the colloquium is a presentation of the most important work contents and research results by the student as well as the answering of questions by experts.

Course Outcomes

On successful completion, students will be able to

- present a problem from their field of study using academic presentation and communication techniques.
- reflect on the scientific and methodological approach chosen in their bachelor's thesis.
- demonstrate that they can actively answer subject-related questions from the subject experts (reviewers of the bachelor's thesis).

Contents

- The colloquium includes a presentation of the most important results of the bachelor's thesis, followed by the student answering the reviewers' technical questions.

Literature

Compulsory Reading

Further Reading

- Renz, K.-C. (2016): Das 1 x 1 der Präsentation. Für Schule, Studium und Beruf. 2. Auflage, Springer Gabler, Wiesbaden.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Thesis Defense

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** yes
Type of Exam	Presentation: Colloquium

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
30 h	0 h	0 h	0 h	0 h	30 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	