RUHR UNIVERSITÄT BOCHUM

RUB

isits
International School of IT Security AG

Module handbook

of the remote postgraduate program

"Applied IT Security"

(Master of Science)

isits AG
International School of IT Security

Ruhr Universität Bochum
Faculty of Computer Science

Table of contents

1 Introduction

The module handbook describes the modules of the postgraduate remote study program "Applied IT Security". In addition to the learning objectives, the requirements to successfully complete a module are specified. The form of the exams is regulated by Sec. 6 of the examination regulations of the master's degree program "Applied IT Security". The scope and duration of the examinations are based on the credit points to be awarded.

Glossary:

Bonus points: Bonus points are awarded for additional efforts during the semester (submission tasks); the successful completion of a module with full points is possible without bonus points.

Case studies: Special form of the submission task in module 9, e.g. in the module "Introduction to BSI Basic Protection and ISO 27001".

Contact time: The master program "Applied IT Security" is offered as a distance learning program. Due to this form of study, attendance and contact times are usually not provided. Supervision and teaching do not take place face-to-face as in traditional courses of study, but online and are not included in the calculation of contact times.

Elective modules: Modules to be chosen from the range of modules offered in the optional compulsory area (module 9).

Mandatory modules: Compulsory modules that have to be successfully completed.

Oral exam: Form of the final module examination. Usually 20 to 30 minutes in length. The oral examination can be conducted by telephone, online video-call or in person. The examination result must be recorded.

Reading Assignments: Reading assignments for self-study on current topics in a compulsory optional module; Reading Assignments are subject of the module final examination.

Submission tasks: Written exercises to monitor learning success during the semester; the processing of the submissions is voluntary; bonus points can be earned by successfully completing the submissions.

Written exam: Form of the module final examination. Usually 3 hours for a 10 CP module and 2 hours for a 5 CP module.

Written term paper: Form of the module final examination. Size: approx. 20 pages.

2 Exemplary Study Plan

EXEMPLARY STUDY PLAN (6 Semesters)

Semester	Module										
	1 (10 CP)	2 (10 CP)	3 (10 CP)	4 (10 CP)	5 (10 CP)	6 (10 CP)	7 (10 CP)	8 (5 CP)	9 (20 CP)	Thesis (25 CP)	CP
1.	Introduction to Cryptography	Discrete Mathmatics									
	10 CP	10 CP									20
2.			Computer Science				Cryptography				
			10 CP				10 CP				20
3.				Information Technology	Network Security						
				10 CP	10 CP						20
4.						Security Protocols		Security Management	Elective I		
						10 CP		5 CP	5 CP		20
5.									Elective II	Thesis	
									5 CP		
									Elective III	*(25 CP - 6 or 12 months)*	
									5 CP		
									Elective IV		
									5 CP	5 CP	20
6.										*Thesis*	
										20 CP	20
Total											120

EXEMPLARY STUDY PLAN (8 Semesters)

Semester	Module										
	1 (10 CP)	2 (10 CP)	3 (10 CP)	4 (10 CP)	5 (10 CP)	6 (10 CP)	7 (10 CP)	8 (5 CP)	9 (20 CP)	Thesis (25 CP)	CP
1.	Introduction to Cryptography	Discrete Mathmatics									
	10 CP	10 CP									20
2.							Cryptography	Security Management			
							10 CP	5 CP			15
3.			Computer Science						Elective I		
			10 CP						5 CP		15
4.					Network Security				Elective II		
					10 CP				5 CP		15
5.						Security Protocols			Elective III		
						10 CP			5 CP		15
6.				Information Technology					Elective IV		
				10 CP					5 CP		15
7.										Thesis	
										(25 CP - 6 or 12 months)	25
8.											
										25 CP	
Total											120

3 Modules in the Mandatory Section

Mandatory module:
Module 1: Introduction to Cryptography

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	1st academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Introduction to Cryptography		0 h	300 h	Max. 50

Requirements for participation

None

Learning outcomes

After successful completion of the module, students have gained knowledge of the basic applications of symmetrical, asymmetrical and hybrid processes. They are able to decide under which conditions certain methods are used in practice and how safety parameters are to be selected. They are familiar with the basics of abstract thinking in IT security technology.

On the other hand, students achieve an algorithmic and technical understanding for practical application through descriptions of selected practice-relevant algorithms (such as AES or RSA algorithm). The students get an overview of the solutions used in companies and are able to defend a certain solution with arguments.

Contents

The module offers a general introduction to the functionality of modern cryptography and data security. Basic terms and mathematical/technical procedures of cryptography and data security are explained. Practically relevant symmetric and asymmetric procedures and algorithms are introduced and explained with practice-relevant examples.

The lecture can be divided into three parts: The first part of the course deals with the functioning of symmetric cryptography including the description of historically important symmetric encryption methods (Caesar cipher, Affine cipher) and current symmetric methods (Data Encryption Standard, Advanced Encryption Standard, Stream Ciphers, One Time Pad).

The second part begins with an introduction to asymmetric procedures and their most important representatives (RSA, Diffie-Hellman, elliptic curves). An introduction to the basics of number theory is given to ensure a basic understanding of the procedures (e.g. rings of integers, groups, solids, discrete logarithms, Euclidean algorithm). Nevertheless, the focus is on the algorithmic introduction of asymmetric procedures, which include both encryption algorithms and digital signatures. This part is completed by hash functions, which play a major role for digital signatures and message authentication codes (MACs or crypto graphical checksums).

The third part of the lecture discusses the basics of security solutions based on the concepts of symmetric and asymmetric cryptography. Especially the solutions necessary and used in companies (PKI, digital certificates etc.) will be discussed.

Special forms of teaching
Lecture in distance learning (eLearning): Interactive learning platform, textbook with exercises, video content available in German and English. Voluntary submissions are offered to accompany the lecture. Feedback is provided by a tutor who communicates with the students via a forum and e-mail.
Examination forms
Written exam (3 hours)
Requirements for the allocation of credit points
Successfully passing the final module exam.
Use of the module in other study programs
No
Value of the grade for the final grade
1/12
Module supervisor
Prof. Dr. Christof Paar
Literature
Paar, Christof/Pelzl, Jan: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2009
Other information

Mandatory module:
Module 2: Discrete Mathematics for IT Security

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	1st academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Discrete Mathematics for IT Security		0 h	300 h	Max. 50

Requirements for participation

None

Learning outcomes

After successful completion of the module, students have learned the professional handling of abstract, discrete structures.

They know the underlying terminology, proof methods and algorithms from elementary number theory, combinatorics and graph theory and can apply them independently. They can model concrete structures mathematically cleanly and prove properties of the models.

Contents

The lecture "Discrete Mathematics" deals with discrete structures. It is divided into 5 parts.

Part 1: Algebraic basics.

Properties of the integers, rational and real numbers are described axiomatically and abstract reasoning is taught.

Part 2: Number Representations.

Various representations of numbers are discussed and described through polynomial arithmetic.

Part 3: Integer Arithmetic.

Basic knowledge of elementary number theory is taught, number theoretic algorithms are introduced, and concludes with cryptographic applications.

Part 4: Counting Combinatorics.

The binomial theorems are discussed, and inductively described combinatorial structures are presented.

Part 5: Graph Theory.

Graphs are used to model a wide variety of application problems. Abstract properties of graphs are studied and algorithms for their study are presented.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, exercises in self-study. Feedback is provided by a tutor who communicates with students via a forum and e-mail.

Examination forms

Written exam (3 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

1/12

Module supervisor

Prof. Dr. Christian Stump, Ruhr-Universität Bochum

Literature

Script "Discrete Mathematics for IT Security"

Other information

Mandatory module:
Module 3: Computer Science for IT Security

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	1st academic year	Annually for the summer semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Computer Science for IT Security		0 h	300 h	Max. 50

Requirements for participation

None

Learning outcomes

After successful completion of the module, students have acquired knowledge about the systematic representation, storage, and processing of information.

They are able to professionally develop small programs, write them in UML and implement, generate and execute them in a high-level language. Students are able to use the services of the operating system via these programs and to manage larger data sets via a professionally designed database. Aspects of IT security are considered.

Students acquire the necessary methodological skills to solve security problems with the help of IT in a structured manner and with consideration of IT security. For the realization of the solution they receive the necessary, practice-relevant tools. They are able to describe fundamental aspects of computer science in a conversation and to apply them to new problems.

Contents

This module teaches the basics of computer science, which are also relevant for the other modules in the area of IT security.

In addition to the technical programming basics such as "Languages and automata", "Data structures", "Algorithms" and "Complexity theory", this also includes the basics of programming in an imperative and an object-oriented programming language such as C, C++ or Java.

Furthermore, this module deals with the system software (operating systems) on which the applications run. In addition to the internal structure (task, memory, IO management), the focus is on the security mechanisms of modern operating systems (rights models, access control, execution control, secure boot process).

For many application areas of the modern IT landscape, the use of data banks is also central. The module therefore also covers the design and implementation of databases based on SQL.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, guided self-study with exercises. Feedback is provided by the teacher, who communicates with the students via a forum and e-mail.

Examination forms

Written exam (3 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

1/12

Module supervisor

Prof. Dr. Jürgen Quade, University of Applied Sciences Lower Rhine, Krefeld

Literature

Script "Computer Science for IT Security"

Other information

Mandatory module:
Module 4: Information Technology for IT Security

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	1st academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Information Technology for IT Security		0 h	300 h	Max. 50

Requirements for participation

None

Learning outcomes

After successful completion of the module, students have acquired basic knowledge of the organization and functionality of modern computer systems. They have an understanding of the technical basics in digital circuits, the interaction between the computer's components, and the design of corresponding systems. They also develop a basic understanding of the relationship between software functions and hardware realization with a focus on the security threats associated with certain acceleration techniques. With this understanding, they can discuss computer hardware problems with their colleagues and correctly classify problems that arise in conversation.

Contents

The first part of the module deals with computer architecture, i.e., the organization and functionality of modern computers. Based on the basic organization according to the von Neumann structure, the interaction between the individual components and the transfer of information between internal as well as external devices is described. This is followed by an in-depth consideration of the instruction processing within microprocessors including different instruction sets, addressing types and acceleration techniques. Here, a particular focus is put on the pipelining principle and a discussion of pipeline conflicts as well as possible solutions. Another main topic is the design of an efficient memory hierarchy with main memory, cache levels and background memory as well as virtual memory management. The first part is concluded with two chapters on parallelization and prototypical computer architectures as well as on security aspects of widely used acceleration techniques.

The second part focuses on the design of the above hardware components at the digital circuit level. Based on Boolean algebra and Boolean functions, combinational and sequential circuits as well as registers and memory components are considered at the gate level, i.e. abstracting away from the physical/electronic realization details. Finally, an overview of the design process for modern VLSI technologies (standard cell, full custom, FPGA) is given.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script, online practice with voluntary submissions. The lecturer, who communicates with the students via a forum and e-mail, provides supervision.

Examination forms

Written exam (3 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

1/12

Module supervisor

Vertr.-Prof. Dr. Philipp Niemann

Literature

Script "Information Technology for IT Security"

Other information

Mandatory module:
Module 5: Network Security

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	2nd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Network Security		0 h	300 h	Max. 50

Requirements for participation

None

Learning outcomes

After successfully completing the module, students have a comprehensive understanding of the technical aspects of network security. They have realized that cryptography alone is not sufficient to solve security problems. They have acquired a comprehensive understanding of complex IT systems. By independently thinking about how to improve network security, students prepare themselves for their role in professional life. They can analyze new problems and develop new solutions. They are able to argue the benefits of the solutions they have developed. They have understood that non-technical factors such as questions of liability and the resulting costs have a significant influence on decisions regarding IT security.

Contents

When cryptography is used in a technical environment such as a computer, data or telephone network, security depends not only on purely cryptographic factors but also on the technical embedding of the encryption and signature algorithms. Prominent examples (for faulty embeddings) are EFAIL (efail.de), attacks on the WLAN encryption systems WEP and WPA (KRACK) and various attacks on TLS (Bleichenbacher, POODLE, DROWN, ROBOT).

The “Network Security” module deals with concrete networks for data transmission and examines them from all sides regarding their security. It comprises the following parts:

- Introduction “Cryptography and the Internet”
- PPP security (especially PPTP), EAP protocols
- WLAN security (WEP, WPA, Wardriving, KRACK)
- GSM and UMTS mobile radio (authentication and encryption)
- IPSec (ESP and AH, IKEv1 and v2, attacks on IPSec)
- Security of HTTP (HTTP Authentication, Secure HTTP, Architecture of SSL/TLS)
- Transport Layer Security (TLS1.2, versions SSL 2.0 to TLS 1.3)
- Attacks on SSL and TLS (BEAST, CRIME, POODLE, Lucky13, Bleichenbacher, DROWN, Heartbleed, Invalid Curve)
- Secure Shell – SSH
- File encryption with OpenPGP (data format, Efail, climatic pink)
- E-mail encryption with S/MIME (SMTP, data format, Efail, POP3, IMAP)
- Domain Name System and DNSSEC (factorizable keys)
- Web application security (HTML, URI, XSS, CSRF, SQLi, SSO)
- XML and JSON security

In addition to the systems themselves, published attacks on these systems are also discussed; the students themselves make scientific considerations for improving security.

Special forms of teaching
Lecture in distance learning (eLearning): Interactive learning platform, book and slide printouts, voluntary submissions with feedback by a tutor who communicates with students via a forum and e-mail.
Examination forms
Written exam (3 hours)
Requirements for the allocation of credit points
Successfully passing the final module exam.
Use of the module in other study programs
No
Value of the grade for the final grade
1/12
Module supervisor
Prof. Dr. Jörg Schwenk
Literature
Schwenk, Jörg: *Internet Cryptography, Theory and Practice (1. Edition 2020)* Script (supplementary slides) "Network Security"
Other information

Mandatory module:
Module 6: Security Protocols

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	2nd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Security Protocols		0 h	300 h	Max. 50

Requirements for participation

None

Learning outcomes

In this module students learn the most important methods and tools of modern security concepts and protocols, which are required for the professional design and development of secure IT systems in practice. After completing the module, students are able to analyze security aspects of given protocols, discover weaknesses in design and develop new protocols independently.

In particular, students acquire the ability to model concrete questions and requirements analyses from existing system information or system conditions. In addition to an introduction to the various concepts and terms, this also includes an in-depth study of selected areas of cryptography and security technology. The students can use these skills in their company to implement better security solutions.

Contents

After teaching basic security definitions, security objectives and trust models, the main protocol primitives, and protocols (commitments, zero knowledge, proof of knowledge, secret sharing) are discussed in detail. In addition, other aspects from the field of system security are also considered. A focus of the course is on authentication and key exchange protocols and their known vulnerabilities and resulting problems. Furthermore, aspects are considered which are important for system security, specifically for the security of computers, such as security protocols.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script, online practice with submissions. Supervision is provided by a tutor who communicates with students via a forum and via e-mail.

Examination forms

Written exam (3 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

1/12

Module supervisor

Prof. Dr. Thorsten Holz

Literature

Script "Security Protocols“

Other information

Mandatory module:
Module 7: Cryptography

Workload	Study phase	Rotation	Duration	
10 CP (300 h)	1st academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Cryptography		0 h	300 h	Max. 50

Requirements for participation

Recommended requirements: Module 1: Introduction to Cryptography, Module 2: Discrete Mathematics.

Learning outcomes

After successfully completing this module, students have developed a deep understanding of the essential mathematical methods and procedures on which modern cryptographic processes are based. Upon completion of this module, students have gained the ability to analyze and design current and future cryptographical methods at the high level of abstraction used in research on modern cryptography. Students develop an awareness of the methodology and power of different attack scenarios. They are able to create new security models themselves and to defend them with arguments.

Contents

The lecture "Cryptography" covers the basic mathematical principles of cryptographic methods. The necessary mathematical background known from algebra, number theory, complexity theory, combinatorics and probabilistic computation is deepened and completed in the lecture. The course is divided into three parts:

In part 1 of the course, essential areas of symmetric cryptography are covered. This part contains especially block and stream algorithms as well as hash functions. The mathematical background and the precise mathematical formulation are always taken into account. In contrast to module 1, attacks (differential and linear cryptanalysis) on the algorithms are presented to deepen the understanding.

Part 2 deals with the most important asymmetrical procedures. A further part deals with the RSA algorithm and the subsequent mathematical questions such as factorization of large numbers, which were not dealt with in module 1, but are necessary for a deeper understanding. Other areas are methods based on discrete logarithms and the analysis of common algorithms for digital signatures.

In the final part 3, generic groups and pairing-based cryptography are presented. In addition to module 4, this module focuses on the mathematical basics.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script with exercises, online practice. Supervision is provided by a tutor who communicates with students via a forum and via e-mail.

Examination forms

Written exam (3 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

1/12

Module supervisor

Prof. Dr. Gregor Leander

Literature

Script "Cryptography"

Other information

Mandatory module:
Module 8: Security Management

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Security Management		0 h	150 h	Max. 50

Requirements for participation

None

Learning outcomes

After completion of the module, students will know how to achieve a security level for the IT systems used that is adequate and sufficient for the intended and economically justifiable protection requirements by implementing suitable infrastructural, organizational, personnel and technical standard security measures.

The students have acquired the skills to support the management in making the appropriate decisions by creating a security concept. They have learned how to define competencies and responsibilities for security management, how to create security awareness within companies and how to implement security measures in ongoing IT operations. They are able to defend their security concepts safely against objections from colleagues and superiors and can also respond to organizational and economic arguments.

Contents

A focal point of this information management, which sees itself as a management task (therefore "management"), is IT security management, which also deals with the security-relevant aspects of operational information and communication systems (ICT systems) as a leadership and management task.

IT security management encompasses the planning, decision-making, organization, management and control of the tasks and processes designed to ensure IT security. In many companies, the tasks of IT security management include achieving the strategic IT security objectives and creating the conditions for managing IT risk so that real risks can be minimized.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script with exercises; online practice. Supervision is provided by a tutor who communicates with students via a forum and via e-mail.

Examination forms

Written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Rainer Böhme, University of Innsbruck

Literature

Script "IT Security Management"

Other information

Mandatory module:

Module 10: Legal Aspects of IT security (German program only)

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Legal Aspects of IT security		0 h	150 h	Max. 50

Requirements for participation

Required: Advanced German language skills. This module is offered in German only.

Learning outcomes

Upon completion of this module, students will have knowledge of the basics of the legal fields relevant to everyday work in the field of IT security. They have a basic understanding of the legal working methods.

Students are then able to evaluate the legal issues that usually arise in the area of IT security, such as scanning e-mails for spam and viruses, generating and analyzing log files, etc., and to handle these in accordance with the legal requirements. Students can evaluate the influence of regulatory and legal requirements on IT security and incorporate this into the creation of their own security concepts. They can argue why a technical process complies with legal requirements.

Contents

The first part of this module deals with the basics of contract law, trademark law and copyright law; in addition, data protection law, the essential parts of telecommunications law, the Telecommunications Surveillance Ordinance, the Teleservices Act, domain law and other relevant areas are covered.

After this introduction, the second part of the course will deal with current legal issues of IT security and provide information on current legal developments. By means of practical scenarios, the students will be given the tools they need to deal with many everyday legal issues in the field of IT security.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script with exercises, online practice. Supervision is provided by a tutor who communicates with students via a forum and via e-mail.

Examination forms

Written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Tobias Gostomzyk, Technische Universität Dortmund

Literature

Script "Rechtliche Aspekte der IT-Sicherheit"

Other information

Mandatory module
Module 11: Master’s Thesis

Workload	Study phase	Rotation	Duration	
25 CP (750 h)	3rd academic year	Independent of semester	1 or 2 semesters	
Courses		**Contact time**	**Self-study**	**Group size**
N.a.		0 h	750 h	N.a.

Requirements for participation

Successful completion of compulsory and elective modules of at least 80 CP.

Learning outcomes

The students document that they are able to independently work on and solve a complex problem of applied IT security with scientific methods and a time limit under supervision.

The students show that they are familiar with working methods of scientific research and project organization and that they are able to present the knowledge and work results acquired during their studies in an understandable written form.

Contents

Students choose a topic from the portfolio of the study program in the field of IT security. Within the master thesis they work on a challenging question. Students have a right of proposal for the topic to be worked on.

Students also have the opportunity to complete their Master's thesis within the framework of an industrial project.

Special forms of teaching

Independent under supervision; constant communication with the supervisor possible

Examination forms

Written examination paper

Requirements for the allocation of credit points

Successful completion of the written master thesis.

Use of the module in other study programs

No

Value of the grade for the final grade

2,5/12

Module supervisor

Prof. Dr. Jörg Schwenk (Dean of Studies)

Literature

Other information

4 Modules in the Elective Section

Elective module:
Module 9.1: Current Topics in IT Security

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	3rd academic year	Annually for the winter semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Current Topics in IT Security		8 h	142 h	Min. 3, Max. 15

Requirements for participation

Previous knowledge from modules 5 "Network Security" and 6 "Security Systems and Protocols".

Learning outcomes

In this seminar, students learn to independently understand technical literature on a specific topic and gain insight into current research topics. Through the elaboration there is an opportunity to practice writing their own texts and summarizing complex topics. Furthermore, the lecture provides the opportunity to learn how to present scientific results and to deepen the material.

Contents

The seminar gives an overview of current research results in the field of system security. The focus is on the areas of malware analysis, botnets, security of smart phones, network security and similar topics from the field of system-related IT security.

Special forms of teaching

The seminar is held as a block event towards the end of the semester – upon special announcement. Supervision is provided by a tutor who communicates with the students via a forum and e-mail.

Examination forms

Written term paper (approx. 20 pages)

Requirements for the allocation of credit points

Lecture in the context of the presence meeting and successful passing of the written elaboration of the presentation in the context of a term paper.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Thorsten Holz

Literature

Current reading recommendations

Other information

Elective module:

Module 9.2: Data Protection in Operational Practice (German program only)

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Data Protection in Operational Practice		0 h	150 h	Min. 3, Max. 50

Requirements for participation

Required: Advanced German language skills. This module is offered in German only.
Recommended: Basic knowledge of IT security analyses, IT and data protection law.

Learning outcomes

After completing the module, students have developed knowledge that enables them to act as contact persons for data protection officers and provide the information and documentation required for controls and implementation projects. By providing basic information during the module, they are also well prepared to assume the role of a data protection officer. You are able to create a data protection concept that also meets the needs of your company's data processing and to defend it with arguments.

Contents

Data protection is one of the legal contexts that must be considered when introducing and developing IT products. Under the heading of compliance, questions regarding the fulfillment of legal requirements arise in companies in various places.

IT security and data protection are closely linked and usually the same actors are involved in the practical implementation. This module therefore focuses on the questions of such a coupled consideration of data protection and IT security issues. This practical knowledge is relevant for (potential) data protection commissioners as well as for employees in companies that administrate or configure systems:

- Basic data protection requirements: In the overview, the basic data protection regulations are discussed with reference to specific issues.
- Reading workshop on legislation: Basic techniques and questions on legal texts form the basis for implementing the changing aspects of the law.
- Creation of process directories: A central document in data protection is the legally required directory of processing activities, which documents central aspects of a software system/automated procedure from a data protection perspective according to a formal scheme.
- Further documentation for data protection issues depends on the system properties. Typical documentations are discussed and implementation alternatives are shown.
- Data privacy impact assessment: For processes with special risks, legislation requires a data privacy impact assessment, a risk assessment before commissioning. The process, the organization of privacy impact assessments and appropriate documentation of the results are discussed.

The contents are conveyed using concrete practical examples.

Special forms of teaching
Lecture in distance learning (eLearning): Interactive learning platform, script, submission tasks and reading assignments. Supervision is provided by the lecturer, who communicates with students via a forum and e-mail.
Examination forms
Oral interview about the previously developed module contents and reading assignments (duration approx. 20 to 30 minutes)
Requirements for the allocation of credit points
Successful passing of the examination interview.
Use of the module in other study programs
No
Value of the grade for the final grade
0,5/12
Module supervisor
Dr. Kai-Uwe Loser
Literature
Script "Datenschutz in der betrieblichen Praxis"
Other information

Elective module:

Module 9.3: Introduction to Forensic Informatics (German program only)

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd academic year	Annually for the summer semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Introduction to Forensic Informatics		20 h	130 h	Min. 3, Max. 20

Requirements for participation

Required: Advanced German language skills. This module is offered in German only.
Recommended: Knowledge in programming; Linux knowledge or the willingness to acquire Linux knowledge during the course.

Learning outcomes

Upon successful completion of the module, students will have basic knowledge and skills in digital preservation of evidence. Students can then evaluate forensic methods and forensic reports with regard to their usefulness in an investigation. They are able to use forensic procedures for specific problems and to defend their correctness with arguments.

Contents

Digital forensics deals with the collection, preparation, and analysis of digital traces for use in court. The starting point in each case is the suspicion of a computer break-in or a crime committed with the help of digital devices.

This course provides an overview of the methodological foundation of digital forensics. The focus is on the embedding of digital forensics in classical continuous (analog) forensics and on the documentation of forensic investigations.

Special forms of teaching

Lecture in distance learning (eLearning) with study letters, exercises and tests via the interactive learning platform, online conferences, chat, and forum. Supervision is provided by a tutor who communicates with students via a forum and e-mail.

Examination forms

Oral examination interview (duration approx. 20 to 30 minutes)

Requirements for the allocation of credit points

Successful passing of the examination interview.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Felix Freiling, Friedrich-Alexander University of Erlangen-Nuremberg

Literature

Dewald, Andreas/Freiling, Felix C. (Ed.): Forensische Informatik, 2015

Other information

Elective module:
Module 9.4: Group-Oriented Communication and Application Security

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Group-Oriented Communication and Application Security		0 h	150 h	Min. 3, Max. 50

Requirements for participation

Recommended: Basic knowledge in cryptography is an advantage.

Learning outcomes

After successful completion of the module, students can apply and further develop the acquired knowledge. They are able to develop innovative digital tools for group communication and information processing as system architects or product developers. They can independently develop solutions in an examination interview and convincingly argue their security.

Contents

This online lecture is primarily concerned with cryptographic security procedures that can be used to secure group-oriented and collaboration-based communication applications. The online lecture deals among others with the following topics:

- Group-based applications, groupware
- Requirements for reliable group communication
- Centralized and distributed procedures for implementing access control in groups, trust between group members
- Secure group communication (confidentiality and authentication), key management

Anonymous group communication, digital group, and ring signatures.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script. Submissions and Reading Assignments. Supervision is provided by the lecturer, who communicates with students via a forum and e-mail.

Examination forms

Oral interview about the previously developed module contents and reading assignments (duration approx. 20 to 30 minutes)

Requirements for the allocation of credit points

Successful passing of the examination interview.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Mark Manulis, University of Surrey

Literature

Script "Group-Oriented Communication and Application Security"

Other information

Elective module:
Module 9.5: Implementation of Cryptographic Schemes

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Implementation of Cryptographic Schemes		0 h	150 h	Min. 3, Max. 50

Requirements for participation

Recommended: Basic knowledge of the programming language C++ (if only C is known, you should be willing to learn the basics of C++) and Module 1 "Introduction to Cryptography".

Learning outcomes

Students learn the basic algorithms for the efficient implementation of computational intensive cryptographic processes. After completing the module, they have understood the handling of algorithms with very long operands in particular, as well as the interplay of implementation methods and cryptographic security.

Contents

This lecture introduces methods for fast and secure implementation of cryptographic algorithms.

In the first part, methods for efficient exponentiation are discussed in detail since they are of great importance for all common asymmetrical procedures. For the widely used RSA algorithm, special acceleration methods are also presented. In the second part, algorithms for efficient long number arithmetic are developed. First, basic methods for the representation of long numbers in computers and procedures for their addition are presented. The focus of this part is on algorithms for efficient modular multiplication. Besides the Karatsuba algorithm, the Montgomery multiplication is dealt with. In the third part secure implementations are discussed. An introduction to active and passive side channel attacks is given. Active attacks against block ciphers and RSA are presented. The basics of SPA (simple power analysis) and DPA (differential power analysis) are introduced as important representatives of passive attacks.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script, evaluated online exercises and/or submissions. Each exercise sheet consists of one or more theoretical tasks and a small programming task. Supervision is provided by a tutor who communicates with the students via a forum and via e-mail.

Examination forms

written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Christof Paar

Literature

Script "Implementation of cryptographic schemes"

Other information

Elective module:
Module 9.6: Information Security Management in Practice

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Information Security Management in Practice		15 h	135 h	Min 3, Max. 50

Requirements for participation

None

Learning outcomes

The students acquire knowledge about the establishment and operation of a security organization in medium to large companies. They will learn about organizational structures, budgeting, planning, resources, architectures, and processes. After completing the module, they will be able to apply, understand and optimize industry best practice standards to existing security processes.

They can plan, implement, and measure awareness measures, determine, and evaluate key performance indicators and adapt communication to different target groups. Students have learned how to develop a vision, mission and strategy for individual security projects and security organizations, to successfully handle and document security incidents. They are able to perform and evaluate risk analyses as well as conduct, understand and apply security assessments. They can convincingly present the methods they have developed in the corporate environment, both orally and in writing.

Contents

The lecture deals with the practical application of security industry standards and with current and new challenges for security management. The following "Information Security" elements are considered analytically:

- Vision, mission, and strategy
- Planning & controlling
- Risk management - frameworks and policies and their enforcement
- Typical security organizations today: structures, roles, and challenges
- Awareness & quality/success control
- Skill management, surveys & reporting
- Operational IT Security Services vs. "Managed Security Services" - MSS
- Compliance and definition of exceptions, processes, and services
- Social engineering & other attacks
- Global security architectures in the cloud age
- Program management

Furthermore, the lecture deals with financial aspects of security management like cost-benefit analysis of security solutions, calculation of security investment volume and ROI in practice.

Finally, an overview of further training opportunities and certifications is given.

Special forms of teaching
Lecture in distance learning (eLearning) and classroom teaching. Interactive learning platform and script. Supervision is provided by a tutor who communicates with students via a forum and e-mail.
Examination forms
Written term paper (approx. 20 pages)
Requirements for the allocation of credit points
Successful completion of the written term paper.
Use of the module in other study programs
No
Value of the grade for the final grade
0,5/12
Module supervisor
Prof. Dr. Thorsten Holz
Literature
Script "Information Security Management in Practice"
Other information

Elective module:

Module 9.7: Introduction to BSI Basic Protection and ISO 27001 (German program only)

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Introduction to BSI Basic Protection and ISO 27001		15 h	135 h	Min. 3, Max. 50

Requirements for participation

Required: Advanced German language skills. This module is offered in German only.

Learning outcomes

After completing the module, students are able to apply the standards BSI Basic Protection - and ISO 27001 / ISO 27002. They can analyze and evaluate the security level within an organization with reference to these standards and develop measures for optimization. They can convincingly defend these optimizations against objections.

Contents

The lecture covers the relevant industry standards for IT and information security. For this purpose, the BSI Basic Protection and the ISO 2700X series of standards will be examined and compared in detail. In addition to dealing with definitions, goals and limits of the standards, questions of practical implementation will be dealt with using case studies.

The lecture concludes with a discussion of aspects of security certification.

Special forms of teaching

Lecture in distance learning (eLearning) and classroom teaching. Interactive learning platform and script, case studies. Supervision is provided by the lecturer, who communicates with the students via a forum and e-mail.

Examination forms

Written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Wilhelm Dolle, KPMG

Literature

Script "Einführung in BSI-Grundschutz und ISO 27001" (W. Dolle) including case studies

Other information

Elective module:
Module 9.8: Mobile Security

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Mobile Security		12 h	138 h	Min. 3, Max. 50

Requirements for participation

Recommended: Basic knowledge in the areas of computer networks and IT security.

Learning outcomes

After successfully completing this module, students will know about the typical potential dangers and main security problems when using mobile networks, systems, applications, and devices. They can integrate partial aspects into a whole and assess risks critically and holistically (mobile systems as an extension or as an integral part of an IT infrastructure) and have a general understanding of the various security technologies and standards. They are able to understand norms, standards, guidelines and guidelines for securing mobile systems and apply them to individual cases.

Contents

Flanked by a short review of the basics of IT security and security technologies, security, and data protection problems in the use of typical mobile systems and applications are discussed with the students:

- WLAN (IEEE 802.11i)
- Bluetooth (IEEE 802.15)
- Near Field Communication (NFC)
- Smartphone operating systems
- Mobile data media
- Mobile networks (2G (GSM, GPRS), 3G (UMTS), 4G (LTE) and 5G)

Furthermore, concepts and strategies for security and data protection are discussed and solutions and recommendations for action are derived from them. In addition to generally valid it security factors such as confidentiality, integrity and authenticity, specific concepts are covered such as

- Mobile Identity & Access Management (IAM)
- Bring Your Own Device (BYOD) und Corporate Owned, Personally Enabled (COPE)
- Mobile Device Management (MDM) and
- Shadow IT

Special forms of teaching

Lecture in distance education (eLearning) with Skype conference. Interactive learning platform, script, and slide printouts. Written elaboration (essay) with feedback by the lecturer, who communicates with the students via a forum, e-mail, and Skype.

Examination forms

Written term paper (approx. 20 pages) in three stages:

1. presentation of the literature research and summary (acquisition of bonus points amounting to 5% of the final grade)
2. 50% version of the term paper (30% of the final grade)
3. 3. final version (70 % of the final grade)

Requirements for the allocation of credit points

Successful completion of written term paper and presentation with partial grades.

Use of the module in other study programs
No
Value of the grade for the final grade
0,5/12
Module supervisor
Prof. Dr.-Ing. Evren Eren, University of Applied Sciences Bremen
Literature
Script "Mobile Security" as well as various thematic PowerPoint scripts (E. Eren)
Other information

Elective module:
Module 9.9: Protecting Against Malware in Enterprises

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	By semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Protecting Against Malware in Enterprises		8 h	142 h	Min. 3, Max. 50

Requirements for participation

None

Learning outcomes

After successful completion of the module, students are able to create concepts and introduce measures that protect a company and the computers used there from malware attacks. They will understand the complexity and scope of this important threat and will have gained insight into the most important current research results of a leading company in this field. They are able to communicate this current state of research adequately and understandably within their company.

Contents

The module deals with attacks originating from malware (including viruses). The special requirements of companies and other organizations are taken into account in particular.

First, the historical development as well as the range of computer malware is presented based on selected events in the past. Afterwards, computer malware is classified according to several criteria and attacks are examined more closely. Various threats are outlined and the originators and users of malware and their motivation are also examined in detail. Possible protection measures are presented and it is explained which techniques and technologies virus scanners, firewalls, intrusion detection/prevention systems and other protection technologies use to protect against malware and its consequences.

In an overview, concrete protection measures for various application scenarios are presented.

Special forms of teaching

Lecture in distance learning (eLearning) with case studies and classroom teaching. Interactive learning platform, script. Supervision is provided by the lecturer, who communicates with the students via a forum and e-mail.

Examination forms

Written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

No

Value of the grade for the final grade

0,5/12

Module supervisor

Ralf Benzmüller

Literature

Script "Protecting against Malware in Enterprises"

Other Information

Elective module:
Module 9.10: Systems Security

Workload	Study phase	Rotation	Duration
5 CP (150 h)	2nd to 3rd academic year	Anually for the summer semester	1 semester

Courses	Contact time	Self-study	Group size
System Security	8 h	142 h	Min. 3, Max. 30

Requirements for participation

Basic knowledge in programming.

Learning outcomes

The students master important theoretical and practical aspects of security mechanisms of modern software systems. They are able to analyze independently the security of a given program, to detect weaknesses in the design and to develop possible solutions and protection mechanisms. In addition, they have become familiar with basic concepts in the field of system security. They are able to create new security models on their own and to defend them with arguments.

Contents

Important theoretical and practical aspects of system security are presented and discussed in the lecture. The focus is on different aspects of software security and different attack and defense techniques are presented. At the end of the lecture series, students should be able to analyze the security of different software systems, discover weaknesses in design and implementation and develop security mechanisms on their own. In addition, other aspects of system security such as privacy and anonymity will also be considered.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script, and lecture videos. The lecture is accompanied by exercises in which the presented concepts and techniques are practiced. Supervision is provided by the lecturer who communicates with students via a forum and via e-mail.

Examination forms

Written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Thorsten Holz

Literature

Script “Systems Security”

Other information

Elective module:
Module 9.11: Program Analysis

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	Annually for the winter semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Program Analysis		8 h	142 h	Min. 3, Max. 30

Requirements for participation

Basic knowledge in programming.

Learning outcomes

Students are familiar with various concepts, techniques, and tools from the field of program analysis. This includes an overview of various concepts from the field of reverse engineering as well as binary analysis. Students have a basic understanding of both static and dynamic methods for analyzing a given program. They are able to describe different aspects of program analysis and apply them to new problems.

Contents

The lecture will cover the following topics and techniques from the field of program analysis, among others

- Static and dynamic analysis of programs
- Analysis of control and data flow
- Symbolic design
- Taint tracking
- Program slicing
- Overview of existing analysis tools

In addition, the first part of the lecture gives an introduction to x86/x64 assembler and presents the basic techniques of reverse engineering.

Special forms of teaching

Lecture in distance learning (eLearning): Interactive learning platform, script, and lecture videos. The lecture is accompanied by exercises in which the presented concepts and techniques are practiced. Supervision is provided by the lecturer who communicates with students via a forum and via e-mail.

Examination forms

written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

Value of the grade for the final grade

0,5/12

Module supervisor

Prof. Dr. Thorsten Holz

Literature

Script “Program Analysis”

Other information

Elective module:

Module 9.12: Human Behavior in IT Security (German program only)

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	Annually for the summer semester	1 semester	
Courses		**Contact time**	**Self-study**	**Group size**
Human behavior in IT security		30 h	150 h	Min. 3, Max. 30

Requirements for participation

Required: Advanced German language skills. Currently, this module is offered in German only.

Learning outcomes

The goal of the course "Human Behavior in IT Security" is to understand which factors influence security behavior of employees in companies and consumers in everyday life, and how to influence and change it.
In addition, it will be explained why existing approaches to Information Security Management (also according to ISO 27000) often do not work in practice and how we should modify or adapt them.

Cross references to other modules:

- Module 8 (Security Management)
- Module 9.6 (Information Security Management in Practice)
- Module 10 (Legal Aspects of IT Security)

Contents

After a brief introduction to human-centered security, in the course "Human Behavior in IT Security", the following topics will be covered, among others:

1. Organizations, organizational culture and security culture
2. Change management
3. Change in the security behavior of employees
4. Risk management
5. Trust in IT security
6. Conflicts in IT security
7. Economic aspects of IT security

Special forms of teaching

Lecture, exercises and quizzes.
Media forms: lecture recordings, live exercises via Zoom, co-operative learning opportunities, presentations, online quizzes'.
By regularly submitting the answers to the quizzes bonus points can be acquired (10%).

Examination forms

written exam (2 hours)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

Yes, study program „IT Security“

Value of the grade for the final grade

0,5/12

Module supervior

Prof. Dr. M. Angela Sasse, M.Sc. Jens Opdenbusch, M.Sc Markus Schöps

Literature

Excerpt from the list of literature:

- Kluge, Annette; Gronau, Norbert (2018): Intentional Forgetting in Organizations: The Importance of Eliminating Retrieval Cues for Implementing New Routines. In: Frontiers in psychology 9, S. 51.
- Adams, John (2016): Risk and culture. In: Routledge handbook of risk studies. London: Routledge, S. 83–93.
- Kirlappos, Iacovos; Parkin, Simon; Sasse, M. Angela (2014): Learning from “Shadow Security”. Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security.
- Kirlappos, Iacovos; Parkin, Simon; Sasse, M. Angela (2014): Learning from “Shadow Security”. Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. In: Matthew Smith und David Wagner (Hg.): Proceedings 2014 Workshop on Usable Security. Workshop on Usable Security. San Diego, CA, February 23, 2014. Reston, VA: Internet Society.
- Ashenden, Debi; Lawrence, Darren (2016): Security Dialogues: Building Better Relationships between Security and Business. In: IEEE Secur. Privacy 14 (3), S. 82-87.
- Flechais, I., Mascolo, C., Sasse, M.A. (2007). Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1 (1), 12-26.
- Caputo, D.D., Pfleeger, S.L., Sasse, M.A., Ammann, P., Offutt, J., Deng, L. (2016). Barriers to Usable Security? Three Organizational Case Studies. *IEEE Security and Privacy*, 14 (5), 22-32.

Other information

The course will be offered for the first time in summer semester 2021.

Elective module:
Module 9.13: Human Aspects of Cryptography Adoption and Use

Workload	Study phase	Rotation	Duration	
5 CP (150 h)	2nd to 3rd academic year	Annually for the winter semester	1 semester	
Courses		**Contact time**	**Self-Study**	**Group size**
Human Aspects of Cryptography Adoption and Use		30 h	150 h	Min. 10, Max. 30

Requirements for participation

Required: Advanced English language skills. This module is offered in English only.

Learning outcomes

The aim of the lecture is to examine the reasons why

a) cryptographic solutions – which experts agree offer good protection against most of the common attacks today – are often not adopted by individuals and organizations, and
b) end-users, developers, and system administrators who do use cryptographic solutions in some form frequently make mistakes that undermine the security protection.

We then identify effective ways to increase adoption and enable correct use of cryptography.

Contents

In 1999, Whitten & Tygar's seminal USENIX paper "Why Johnny Can't Encrypt" established that even though the problem of End-to-End Encryption is technically solved, people cannot use PGP encryption correctly, even with a graphical user interface and instruction.

Over the past 20 years, there has been a string of "Johnny" papers trying to encourage adoption or correct usage of secure tools - with mixed results.

The aim of this lecture is to systematically examine the results of these and other studies and identify effective ways of promoting adoption and enable correct use of cryptography.

This course covers the following topics

- Usability, usable security, utility, and technology adoption
- Security threat models and people's mental models
- Cryptography ecosystem – where do cryptographic standards come from?
- Complexity or simplicity – who needs to know what?
- Applying this knowledge to different cryptographic applications:
    - PGP and S/MIME: End-to-End encrypted Email
    - WhatsApp and Signal: End-to-End security for the masses?
    - TLS: A crypto protocol success story
    - End User Privacy Tools: TOR/TAILS, Disk Encryption, VPNs
    - Usability issues of „blockchain products" (wallets, key recovery), crypto scams

Special forms of teaching

Lecture, exercises, homework and quizzes.
Media forms: lecture recordings, live exercises via Zoom, co-operative learning opportunities, presentations, online quizzes'.
By regularly submitting the answers to the quizzes and homework bonus points can be acquired (10%).

Examination forms

Oral exam (20 minutes)

Requirements for the allocation of credit points

Successfully passing the final module exam.

Use of the module in other study programs

Yes, study program „IT Security"

Stellenwert der Note für die Endnote
0,5/12
Module supervior
Prof. Dr. M. Angela Sasse, M.Sc. Konstantin Fischer
Literatur
Excerpt from the literature list: • Whitten, A., & Tygar, J. D. (1999, August). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. In USENIX security symposium (Vol. 348, pp. 169-184). • Ruoti, S., & Seamons, K. (2019). *Johnny's journey toward usable secure email.* IEEE Security & Privacy, 17(6), 72-76. • Johnson-Laird, P. N. (1983). *Mental models: Towards a cognitive science of language, inference, and consciousness (No. 6)*. Harvard University Press. • Norman, D. A. (2014). *Some observations on mental models. In Mental models* (pp. 15-22). Psychology Press. • Wu, J., & Zappala, D. (2018). *When is a tree really a truck? exploring mental models of encryption*. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) (pp. 395-409). • Demjaha, A., Spring, J. M., Becker, I., Parkin, S., & Sasse, M. A. (2018). *Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption.* In Proc. USEC (Vol. 2018). Internet Society. • Wu, J., Gattrell, C., Howard, D., Tyler, J., Vaziripour, E., Zappala, D., & Seamons, K. (2019). "*Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal.* In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 137-153). • Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014, July). *Why doesn't Jane protect her privacy?*. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 244-262). Springer, Cham. • Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017, May). *Obstacles to the adoption of secure communication tools*. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 137-153). IEEE. • Herzberg, A., & Leibowitz, H. (2016, December). *Can Johnny finally encrypt? Evaluating E2E-encryption in popular IM applications*. In Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust (pp. 17-28). • Stransky, C., Wermke, D., Schrader, J., Huaman, N., Acar, Y., Fehlhaber, A. L., & Fahl, S. (2021). *On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security*. In Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021) (pp. 437-454). • Marks, L. (2012). *Between Silk and Cyanide: A Code Maker's War 1941-45*. The History Press.
Other information
The course will be offered for the first time in winter semester 22/23.