University of St.Gallen

Course and Examination Fact Sheet: Spring Semester 2025

8,731: Technologien/Technologies: Data Security and Privacy

ECTS credits: 3

Overview examination/s

(binding regulations see below)
decentral - Written work, Digital, Individual work individual grade (10%)
Examination time: Term time
decentral - Presentation, Analog, Group work individual grade (45%)
Examination time: Term time
decentral - Written work, Digital, Individual work individual grade (45%)
Examination time: Term time

Attached courses

Timetable -- Language -- Lecturer
8,731,1.00 Technologien/Technologies: Data Security and Privacy -- English -- Mitrokotsa Katerina

Course information

Course prerequisites

None

Learning objectives

By the end of the course the students are expected to:

- Get familiar with current security and privacy-preserving protocols, techniques that can be used to achieve secure and privacy-preserving communications for different applications;
- Understand the main security threats, risks associated with the covered applications;
- Gain ability to read current scientific paper;
- Improve presentation and scientific writing skills;
- Develop the ability to understand and explain technologies in their historical and social context;
- Be able to understand that technologies are built upon social forces and previous developments;
- Develop the capacity to critically reflect on the relationship between technologies and societies;
- Be encouraged to reflect on the role that technologies can play in addressing social problems.

The students will participate in the course and will:

- Synthesize some existing work on security and privaty-preserving protocols/primitives;
- Present a lecture on the topic;
- Provide some feedback and questions on all topics covered (in the form of a short review);
- Analyze a security and/or privacy-preserving mechanism.

Course content

This is a seminar course that introduces the participants to the current trends, problems, and methods in the area of cybersecurity and privacy. We will look at today's most popular security and privacy-preserving protocols, techniques, and problems that will play an emerging role in the future of secure and private communications. Also, the seminar will cover methods to model and analyze such security and privacy-preserving protocols and mechanisms. Topics would include but will

not be limited to: cryptocurrencies (bitcoin), contactless authentication (distance-bounding), privacy-preserving biometric authentication, security and privacy in contact tracing applications.

Course structure and indications of the learning and teaching design

This course will be held as a seminar (2 hours of lectures in a weekly rhythm), in which the students actively participate. Some introductory lectures will be given to familiarize the students with the main areas, cryptographic primitives and protocols. The topics (with associated source papers) will be assigned to students, and each student will have to give a 45 minutes talk, react to other students' questions (reviews), and write a 3-4 pages summary of their talk.

This course counts 3 credits credits. Accordingly, the total workload for students is 90 hours. This includes self-study, campus time and all examinations. The structure of the contact study is planned as follows: 2 hours of lectures in a weekly rhythm.

Contextual Studies are considered part of **Contact Learning**; thus, taking part properly implies **regular attendance**. It is the students' own responsibility to ensure that there is **no timetable clash** between the courses they have chosen. A detailed course outline and all relevant documents will be made available on **StudyNet**. Only the current timetable as published on **Courses** does apply.

Course literature

The literature includes some book chapters that will be used as material in the introductory lectures as well as the selected papers associated with each covered topic.

Introductory chapters from the book: Cryptography & Network Security Principles and Practice, Willian Stallings will be covered in order to understand better important security concepts and cryptographic primitives.

Additional course information

Prof. Dr. Katerina Mitrokotsa is a full professor and chair of Cybersecurity at the School of Computer Science. Before joining the HSG, she was a professor at Chalmers University of Technology in Sweden.

Examination information

Examination sub part/s

1. Examination sub part (1/3)

Examination modalities

Examination type	Written work
Responsible for organisation	decentral
Examination form	Written work
Examination mode	Digital
Time of examination	Term time
Examination execution	Asynchronous
Examination location	On Campus
Grading type	Individual work individual grade
Weighting	10%
Duration	--

Examination languages

Question language: English
Answer language: English

Remark

--

Examination-aid rule

Free aids provision

Basically, students are free to choose aids. Any restrictions are defined by the faculty members in charge of the examination under supplementary aids.

Supplementary aids
--

2. Examination sub part (2/3)

Examination modalities

Examination type	Presentation
Responsible for organisation	decentral
Examination form	Oral examination
Examination mode	Analog
Time of examination	Term time
Examination execution	Asynchronous
Examination location	On Campus
Grading type	Group work individual grade
Weighting	45%
Duration	--

Examination languages
Question language: English
Answer language: English

Remark
--

Examination-aid rule
Free aids provision

Basically, students are free to choose aids. Any restrictions are defined by the faculty members in charge of the examination under supplementary aids.

Supplementary aids
--

3. Examination sub part (3/3)

Examination modalities

Examination type	Written work
Responsible for organisation	decentral
Examination form	Written work
Examination mode	Digital
Time of examination	Term time
Examination execution	Asynchronous
Examination location	On Campus
Grading type	Individual work individual grade
Weighting	45%
Duration	--

Examination languages
Question language: English
Answer language: English

Remark
--

Examination-aid rule
Free aids provision

Basically, students are free to choose aids. Any restrictions are defined by the faculty members in charge of the examination under supplementary aids.

Supplementary aids
--

Examination content

The topics (with associated source papers) will be assigned to students, and each student will have to give a 45 minutes talk, react to other students' questions (reviews), and write a 3-4 pages summary of their talk. Group presentation and Examination Paper are expected to synthesize some existing work on security and privacy-preserving protocols/primitives and to analyze a security and/or privacy-preserving mechanism in the covered applications.

1. Examination paper written at home (individual) (10%) The students are required to write questions before each topic presentation in the form of a short review and submit them through an indicated online form.
2. Presentation (individual in groups - individual grades) (45%) The topics (with associated source papers) will be assigned to groups, and each group will have to give a 45 minutes talk and react to other students' questions (reviews).
3. Examination paper written at home (individual) (45%) A summary paper of the talk given, including important reviews and their ensuing discussion (at least 12000 characters incl. spaces or 2200 words).

Examination relevant literature

The covered literature include some book chapters of general concepts in cybersecurity (cryptographic primitives e.g. digital signatures, cryptographic hash functions) as well as a collection of papers that describe in detail a topic of cybersecurity for a specific application (e.g., biometric authentication, contact-tracing applications).

University of St.Gallen

Please note

Please note that only this fact sheet and the examination schedule published at the time of bidding are binding and takes precedence over other information, such as information on StudyNet (Canvas), on lecturers' websites and information in lectures etc.
Any references and links to third-party content within the fact sheet are only of a supplementary, informative nature and lie outside the area of responsibility of the University of St.Gallen.

Documents and materials are only relevant for central examinations if they are available by the end of the lecture period (CW21) at the latest. In the case of centrally organised mid-term examinations, the documents and materials up to CW 13 (Monday, 25 March 2025) are relevant for testing.

Binding nature of the fact sheets:

- Course information as well as examination date (organised centrally/decentrally) and form of examination: from bidding start in CW 04 (Thursday, 23 January 2025);
- Examination information (supplementary aids, examination contents, examination literature) for decentralised examinations: in CW 12 (Monday, 17 March 2025);
- Examination information (supplementary aids, examination contents, examination literature) for centrally organised mid-term examinations: in CW 14 (Monday, 31 March 2025);
- Examination information (regulations on aids, examination contents, examination literature) for centrally organised examinations: two weeks before ending with de-registration period in CW 15 (Monday, 07 April 2025).