Faculty of Health, Science and Technology
Computer Science

Syllabus

Internet Security and Privacy

Course Code:	DVAD23
Course Title:	Internet Security and Privacy *Säkerhet och integritet på internet*
Credits:	7.5
Degree Level:	Master's level
Progressive Specialisation:	Second cycle, has only first-cycle course/s as entry requirements (A1N)

Major Field of Study:
DVA (Computer Science)

Course Approval
The syllabus was approved by the Faculty of Health, Science and Technology 2022-02-24, and is valid from the Autumn semester 2022 at Karlstad University.

Prerequisites
7.5 ECTS credits in each of the areas security, computer networking, operating systems, and programming, plus upper secondary level English 6, or equivalent

Learning Outcomes
Upon completion of the course, students should be able to:
1. explain basic cryptographic primitives used in common communication protocols on the Internet,
2. categorise communication protocols based on the highest possible level of security that can be attained based on the selected cryptographic primitives and current recommendations,
3. apply modern cryptographic software libraries correctly and securely,
4. apply modern technologies for secure and privacy-preserving communication,
5. compare technologies for secure and privacy-preserving communication based on

different users threat models, and
6. describe ethical aspects and societal interests that influence the development and use of technologies for secure and privacy-preserving communication on the Internet.

Content
The course is focused on how communication on the Internet is made secure and privacy-preserving by means of cryptography and sound engineering.

The first part of the course covers applied cryptography with a focus on cryptographic primitives, security definitions, and current recommendations regarding the choice of primitives and parameters. The goal is to create a toolbox based on an understanding of primitives, their strengths and weaknesses, and how they are used in practice in software.

The second part of the course applies the toolbox created in the first part. Communication protocols and other technologies for secure and privacy-preserving communication that are common on the Internet are studied in detail, with a focus on the technical design for reaching different levels and types of protection in relation to different threat models. Examples are Transport Layer Security, WireGuard, and the anonymity network Tor.

Throughout the course, students engage in laboratory sessions and hand-in assignments which include oral and written presentations. The course concludes with an oral presentation of a group project which requires students to analyse a protocol or technology independently. The analysis includes technical, ethical, and societal aspects related to the area of use, target users, developers, and other driving forces of the technology in question.

Reading List
See separate document.

Examination
Assessment is based on:
- an individual written exam
- oral and written presentations of hand-in assignments, completed individually and in groups
- laboratory reports, completed individually and in groups

If students have a decision from Karlstad University entitling them to Targeted Study Support due to a documented disability, the examiner has the right to give such students an adapted examination or to examine them in a different manner.

Grades
One of the grades 5 (Pass with Distinction), 4 (Pass with Some Distinction), 3 (Pass), or U (Fail) is awarded in the examination of the course.

Quality Assurance
Follow-up relating to learning conditions and goal-fulfilment takes place both during and upon completion of the course in order to ensure continuous improvement. Course evaluation is partly based on student views and experiences obtained in accordance with current regulations and partly on other data and documentation. Students will be informed of the result of the evaluation and of any measures to be taken.

Course Certificate
A course certificate will be provided upon request.

Additional information

The local regulations for studies at the Bachelor and Master levels at Karlstad University stipulate the obligations and rights of students and staff.