GHENT UNIVERSITY

Course Specifications

Valid as from the academic year 2023-2024

Network and Computer Security (E765003)

Course size *(nominal values; actual values may depend on programme)*

Credits 6.0 **Study time 170 h**

Course offerings and teaching methods in academic year 2023-2024

A (semester 1)	Dutch	Gent	lecture
			practical

Lecturers in academic year 2023-2024

Sebrechts, Merlijn	TW05	staff member
De Poorter, Eli	TW05	lecturer-in-charge

Offered in the following programmes in 2023-2024	**crdts**	**offering**
Master of Science in Information Engineering Technology	6	A
Exchange Programme Information Engineering Technology	6	A

Teaching languages

Dutch

Keywords

computer networks, security, cryptography, authentication, computer science (P170), informatics (P175), computer technology (T120)

Position of the course

The students know the most important concepts of security and authentication, they know how to implement them on all the network layers, they know the different levels of how to secure computers and networks. Of all those concepts they know the theoretical background and the algorithms, as well as the applications. They are able to configure and to secure servers and network devices in a greater context.

Contents

- General concepts. Conventional encryption and public key encryption. Key management and exchange. Authenticity and signatures.
- Network security: X.509 certificates, PGP, S/MIME, PKI, IPSec, SSL and TLS
- System security: Web service security, firewalls, passwords

Initial competences

Required starting competencies:
Students have successfully taken the course 'Computer networks' ('Computernetwerken' (E761050)) or have acquired the aspired learning competences in another way (required starting competencies as defined in the Curriculum Rules of the Faculty of Engineering and Architecture, cf. http://www.ugent.be/ea)
Advisory initial competences:
To be able to configure and manage unix servers; to be able to set up and configure a network, all the competences are described in Operating systems I and II.

Final competences

1 Knowing the key concepts and features of secrecy and authentication, and understand them.
2 Setting up security and authentication on a working network and computer configuration.
3 Knowing and understanding the different levels and ways of how a network and computers can be secured.
4 Protecting servers and network devices in a larger network configuration.

Conditions for credit contract

Access to this course unit via a credit contract is determined after successful competences assessment

Conditions for exam contract

This course unit cannot be taken via an exam contract

Teaching methods

Lecture, Practical

Extra information on the teaching methods

Lectures (24hrs), labs (36hrs; presence required; set up an secure servers en network configurations, sometimes in goup), homework (110hrs)

Learning materials and price

Slides (ENG), Note pages (ENG), reference works, tutorials on the internet.

References

Books
William Stallings, "Cryptography and Network Security, principles and practices", 6th (international) edition, Prentice Hall, 2010; ISBN-13: 9780137056323
Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone , "Handbook of Applied Cryptography", CRC Press, 2001, ISBN 0-8493-8523-7
Matt Bishop, "Computer Security: Art and Science", Addison Wesley, Pearson Education, 2003, ISBN-13: 978-0-201-44099-7

Websites
- https://crypto.stackexchange.com/
- http://www.gnupg.org
- http://www.openssl.org
- http://www.cryptool.org/en/

Course content-related study coaching

Additional explanation during the labs or after making an appointment, possibly by email.

Assessment moments

end-of-term and continuous assessment

Examination methods in case of periodic assessment during the first examination period

Written assessment

Examination methods in case of periodic assessment during the second examination period

Written assessment

Examination methods in case of permanent assessment

Skills test, Participation, Assignment

Possibilities of retake in case of permanent assessment

examination during the second examination period is not possible

Extra information on the examination methods

Lectures: written examination (partly closed book, partly open book) (70%)
Labs sessions: permanent evaluation by graded exercises and tests and deliver assignments and reports (30%)

Calculation of the examination mark

A weighted average (70% for the written examination and 30% for the lab sessions) is used to compute the final score. When the student obtains less than 8/20 for at least one of the components, they can no longer obtain a pass mark for the course unit as a whole. If the total score does turn out to be a mark of ten or more out of twenty, this is reduced to the highest fail mark (i.e. 9/20).