Security elective package

Security	
Offered by	Department of W&I
Language	English
Primarily interesting for	All students, but most relevant for students with background in BTW, InfS and BEI
Prerequisites	Required courses: Llinear algebra, e.g. 2DBI00, 2DBN00, or 2DE20 Programming skills, e.g. from 2IP90 – Programming Algebra – 2WF50 (for BTW students) Computer networks and security – 2IC60 (for InfS students) Recommended courses: -
Contact person	Prof. dr. T. Lange (T.Lange@tue.nl)

Content and composition

Security is a growing sector in IT and given the numerous news reports of attacks and compromises much more work is needed. IT security requires expertise in cryptographic solutions as well as in networks and security analysis. The subject is positioned at the intersection of mathematics and computer science and has relevance for applications ranging from e-government and e-commerce to access control and security in cars. Whenever ICT is deployed it is important to ensure that the infrastructure gets used only by authorized users;- only the registered voter should be allowed to cast a vote, credit card details should be safe from eavesdroppers, only authorized people should be able to enter a building and the brakes of a car should react quickly to electronic messages, but only if they come from a legitimate sender.
This course package is organized by Ei/PSI, the Eindhoven Institute for the Protection of Systems and Information and demonstrates one of the strengths of research at TU/e covering all aspects of IT security in one location.
This security package brings students up to speed on the fundamental knowledge and insight required for research and development in cryptology and computer security. It includes courses on the mathematical background, network security, cryptology, and hands-on experiments with attacks. It is an ideal preparation for the IST master track on Information Security and Technology within Computer Security and the DAM master track in mathematics.
The default packages are

- for BTW students: 2IC60, 2WF80, 2IC80
- for InfS students: 2WF90, 2WF80, 2IC80
- for other students: 2IC60, 2WF90, 2EF80; they can also take 2IC80 in addition as a 4th topic

BTW students may make a package including 2WF70 if they do not yet count it as part of the major, either to get a package of 4 or instead of 2IC80. For BTW students 2IC60 + 2WF80 can be considered a coherent package, but they are encouraged to also take 2IC80; for InfS students 2WF90 + 2WF80 can be considered a coherent package, but they are encouraged to also take 2IC80. Students may take 2WF50 + 2WF70 in place of 2WF90.

Make sure to check the course requirements on the individual course pages.

Security elective package

Course code	Course name	Level classification
2IC60	Computer networks and security (not for InfS, for BTW and other students)	3.
2WF70	Algorithmic algebra and number theory (for BTW, and students who have taken Algebra)	3.
2WF90	Algebra for security (not for BTW; for all students not taking 2WF70)	2.
2WF80	Introduction to Cryptology	3.
2IC80	Laboratory on Offensive Computer Security (for InfS and BTW students if 2WF70 is part of the major)	3.

Course description

Computer networks and security (for all students other than InfS) (2IC60)
Connectivity is becoming a necessity of life. Networks should be stable, high-performing but also secure. This course aims to provide an introduction to computer networks and information security. We highlight the organization of computer networks and related issues, in particular regarding the Internet on the one hand, and identify common security problems and their underlying causes on the other hand. We seek to understand the essential choices, basic threats and fundamental solution principles. We analyze simple network protocols and security mechanisms, providing the student a basis to independently understand the more advanced ones.

Algorithmic algebra and number theory (for BTW students if not counted in major) (2WF70) Algorithmic-Algebra part shows how Gröbner bases work and presents an algorithm to compute them. They are used in a variety of applications in algebra. The Algorithmic-Number Theory part is about methods and techniques from Number Theory that are important in cryptography.

Algebra for security (for all students other than BTW) (2WF90)
The algbra part covers algebraic structures such as rings, groups and fields, with an emphasis on finite fields and with overall an algorithmic focus. The number-theory part covers multi-precision arithmetic, modular arithmetic, quadratic reciprocity, prime number distribution, continued fraction, lattices. This course serves as a preparation for the mathematics needed for cryptology.

Introduction to Cryptology (for all students) (2WF80)
Keeping information private from preying eyes and ears and making sure that even small modifications introduced to a message in transmission get detected is the goal of cryptography. The art and science of secret writing goes back to at least to Julius Caesar who described encryption in „De Bello Gallico“. This course gives an introduction to cryptology, covering historical encryption schemes as well as RSA (the most common system on the Internet) and Diffie-Hellman to show how the systems work and are attacked.

Laboratory on Offensive Computer Security (for all students) (2IC80)
This course will cover an introduction to practical aspects of computer security threats and defences. The course will present theoretical aspects of computer security as well as practical examples of real attacks and laboratory activities. The student will learn

- the characteristics of software vulnerabilities and their impact on system security
- malware types, functionalities, and propagation mechanisms
- vectors for attack delivery
- the different types of network and host defenses, and their limitations
- how to engineer a working attack and deploy effective defenses