

5.0 credits	30.0 h + 15.0 h	2q
-------------	-----------------	----

Teacher(s) :	Avoine Gildas ;
Language :	Anglais
Place of the course	Louvain-la-Neuve
Prerequisites :	-- Background in computer networks (LINGI2141 or eventually ELEC2920) -- Basic knowledges in programming INFO2MS and SINF2MS students are both compliant with these prerequisites. Student who do not know if their background allows them the attend the course (e.g. students from ELEC, ELME or MAP) should contact the teaching assistant or lecturer. Weaknesses in network can be filled by reading the book "Computer Network" by Andrew Tanenbaum. The most important topics that will be used in LINGI2347 are: SMTP, Telnet, IP, TCP, ARP, MAC, OSI layered model.
Main themes :	-- Forged E-Mail, Spam and Malwares, -- Basics in cryptography, -- Network and Application Vulnerabilities: IT spoofing, session hijacking, exploits, sniffing, -- Firewalls, -- Proxies, IDS, Hacking methods, -- Passwords and time-memory trade-off, -- Secure communications, -- Security at the User Level.
Aims :	The course provides a broad view of computer system security that provides a general knowledge of the field for non-specialists and a base for future specialists. A student completing successfully this course will be able to: -- defend the need for protection and security, and the role of ethical considerations in computer use, -- identify security strenghts and weaknesses in computer systems, -- explain the problems addressed by digital forensics and outline the basic principles involved in its practice, -- compare and contrast current methods for implementing security. <i>The contribution of this Teaching Unit to the development and command of the skills and learning outcomes of the programme(s) can be accessed at the end of this sheet, in the section entitled "Programmes/courses offering this Teaching Unit".</i>
Evaluation methods :	Exam -- MCQ, 2 years and therefore a bigger problem -- written in June, oral in September Challenges made during the year
Teaching methods :	-- Lectures -- In-class exercices take place every two weeks. -- Challenges which are practical exercices that are introduced at the end of the lectures. Students solve these challenges by themselves, at home or in the computer rooms.
Content :	The course describes a wide spectrum of the security problems everyone may face when using a computer, and explain how to mitigate them. It uses a more technical than analytical approach. -- Forged E-Mail, -- Spam and Malwares, -- Basics in Cryptography (exhaustive search, RSA, birthday paradox, hash function, etc.), -- Network and Application Vulnerabilities (IP spoofing, session hijacking, exploits, sniffing), -- Firewalls, -- Proxies, IDS, Hacking method, -- Passwords and Time-memory trade-off, -- SSH, IPSec, certificates, -- SSL/TLS, -- WEP, WPA, -- Kerberos, -- PGP, -- Security viewed by a police officer.
Bibliography :	Textbooks (not mandatory) -- "Computer system security, basic concepts and solved Exercices", G. Avoine, P. Junod and Ph. Oechslin, EPFL Press; 1 edition (July 2007), ISBN-10: 1420046209 , ISBN-13: 978-1420046205. -- "Sécurité informatique", G. Avoine, P. Junod et Ph. Oechslin, Editions Vuibert. Mandatory documents : slides on the website

Other infos :	INGI2347 vs INGI2144 Class INGI2347 is an introduction to network and application security, while class INGI2144 is an advanced course on application security.
Cycle and year of study :	> Master [120] in Electrical Engineering > Master [120] in Computer Science and Engineering > Master [120] in Computer Science > Master [120] in Mathematical Engineering
Faculty or entity in charge:	INFO