Fall 2019
Sébastien Combéfis

I5020 Computer Security

Competencies List

This document provides the list of basic and advanced competencies, with a precise description, that can be acquired through the *I5020 Computer Security* course.

Basic Competencies

Basic competencies are specific to a teaching unit or activity and a 100% mastery level for all of them is required to succeed the teaching unit or activity (10/20).

Code	The learner is able to...
Computer Security Principle	
CS001	understand the CIA triad and use it to explain the key objectives of computer security.
CS002	define and explain the basic security concepts and the relations between them.
CS003	identify weaknesses in a computer system or infrastructure and propose solutions.
Cryptography	
CS101	encrypt and decrypt messages with “historical” ciphers.
CS102	make connections between cryptographic tools and the CIA triad.
CS103	compare symmetric and asymmetric encryption schemes.
CS104	write a program that encrypts data with the suitable libraries.
Secured Design	
CS201	discuss about general design principles for protection mechanisms.
CS202	understand software protections that can be installed on a computer system.
CS203	understand hardware protections that can be installed on a computer system.
CS204	discuss about the differences and importance of authentication and access control.
CS205	identify security risks related to operating systems, network, database, cloud and IoT and propose solutions to decrease them.
Secured Programming	
CS301	write robust code that checks precisely all the external data (environment, file, form...).
CS302	write robust code that resists to SQL, PHP injections and XSS attack.
CS303	apply code design principles in developed software.
GP301	write robust code with good error management.
Security Audit	
CS401	identify vulnerabilities in a system and propose countermeasures for them.
CS402	capture network traffic with WireShark to perform basic analyses.
CS403	discuss about the risks that a company assets are exposed to and propose solutions to decrease them.
CS404	perform a basic internal code audit of a given program.

Advanced Competencies

Advanced competencies could be transversal to several teaching units or activities and increasing the mastery level of any of them is global to all the teaching units and activities where it is declared.

Code	The learner is able to...
Computer Security Principle	
CS004	compare the CIA triad, the CIAA quarted and the parkerian hexad.
CS005	make links between attacks and threat consequences with the CIA triad.
CS006	identify residual risks that come from a countermeasure.
Cryptography	
CS105	describe formally a given cryptosystem and manually encryt/decrypt messages formally.
CS106	compare different cryptographic architecture choices for a given problem.
CS107	identify the suitable cryptographic tool for a given security issue.
CS108	understand how RSA can be used as an encryption and as a signature scheme.
Secured Design	
CS206	choose the suitable compromise between security and usability for a given application and argue the choice.
CS207	write an application that stores passwords securely.
CS208	explain techniques that can be used to protect a system against malware.
CS209	choose a relevant software architecture to improve security related quality aspects.
Secured Programming	
CS304	program, configure and launch a secured HTTPS server.
CS305	perform a pentest analysis on a given code and refactor it according to the result.
CP213	write a code that is free of memory leaks and check it with `valgrind`.
Security Audit	
GA001	make a complete code audit, propose changes and argue them with quality criteria.
CS405	use the McCumber cube framework to discuss about actions to take regarding security of a computer system.
CS406	perform a basic external security audit of a website with open source tools.
CS407	analyse a news article about a computer security problem with a security model.
CS408	perform an advanced audit of a website with an open source linux distribution.