Bachelor in Cybersecurity Engineering

Titles, contents and timetable

Escuela Técnica Superior de Ingeniería Informática

Universidad Rey Juan Carlos

Contents

Prologue

This document contains information about titles, contents and timetable of subjects taught in the Bachelor in Cybersecurity Engineering, offered at Rey Juan Carlos University, Escuela Técnica Superior de Ingeniería Informática. This information pretends to be helpful to international students interested in visiting our University.

Contents in this document referred to subjects taught during course 2021-2022. More information can be consulted in

`https://www.urjc.es/estudios/grado/3100-ingenieria-de-la-ciberseguridad`.

1

First Course

1.1 First Semester

1.1.1 Introduction to Cybersecurity

Bits and bytes. Computer architecture. Cybersecurity? Concepts and definitions. Operating systems and protection. Compilers and programming languages. The human factor and cybersecurity economics. Networks and the Internet. Databases and information repositories. Threats and cyber attacks. Privacy.

6 ECTS credits.

1.1.2 Introduction to Programming

Introduction to Programming, Basis of C language, operators and expressions, control and selection structures, pointers, functions, arrays and strings, structs and enums, dynamic memory management, files

6 ECTS credits.

1.1.3 Logic

Introduction to Set Theory. Propositional logic (Syntax, Semantics and Gentzen Natural Deduction System). First order logic (Syntax, Semantics and Gentzen Natural Deduction System).

6 ECTS credits.

1.1.4 Discrete Math and Linear Algebra

Discrete Math: Fundaments. Modular arithmetic. Introduction to combinatorics. Graph Theory. Linear Algebra: Matrices and systems of linear equations. Vector spaces. Linear maps. Matrix diagonalization.

6 ECTS credits.

1.1.5 Physical Basis of Computing

The fundamental laws of Electromagnetism Direct current circuits. Ohm's law. Kirchhoff's law. Thevenin equivalent circuits Semiconductors. PN junction. Diodes. LED diodes. Zener diodes. Circuits with diodes. BJT Transistors. Circuits with BJT transistors. MOSFET Transistors. Circuits with MOSFET transistors. Logic gates. Digital electronics. Sequential and combinational circuits. Mealy machine.

6 ECTS credits.

1.2 Second Semester

1.2.1 Statistics

Descriptive statistics: Description of data Basic concepts. Types of variables. Graphical summary of data. Numerical summary of data. Description of bivariate data. Summary of bivariate data. Covariance, correlation. Regression. Probability: random events, definition and interpretation of probability. Properties. Conditional probability. Independence of events. Total Probability and Bayes theorem. Random variables. Definition of random variable. Types of variables. Mass function and density function. Distribution function. Mean and variance. Special distributions. Statistical Inference: Introduction. Sampling. Central Limit Theorem. Estimation for means, proportions and variances. Hypothesis tests

6 ECTS credits.

1.2.2 Calculus

The real line. Complex numbers. Functions: Overview. Limits and continuity. Derivatives. Derivative computation. Taylor polynomial. Study and graphical representation of functions. Primitive computation. Definite integrals. Fundamental Theorem of Calculus. Areas calculation. Sequences of numbers. Series of numbers.

6 ECTS credits.

1.2.3 Cryptography

Symmetric Cryptoraphy (Preliminaries. Historic introduction. Symmetric Encryption. Hash Functions. MACs). Asymmetic Cyptography (Public Key Encryption, Key Exchange, Digital Signatures. Commitment Schemes. Secret Sharing)

6 ECTS credits.

1.2.4 Data Structures

Algorithm complexity. Abstract Data Types. Lists. Stacks and Queues. Sets. Binary Trees. Graphs. Hash tables.

6 ECTS credits.

1.2.5 Dimensions and Security Models

This course explores national security. To do this, public policies, procedures and administrative networks that anticipate and respond to plausible threats of political violence are reviewed. The main contents are: Security and globalization. Dynamics of transformation in global security (Evolution and implications of globalization for the construction of secure societies). New public security paradigms. Public security policies (Dynamics and administrative networks). Institutional responses: The EU internal security strategy, The spanish national security strategy. Cybersecurity. Terrorism, radicalisation and violent extremism. Organized Crime and Serious Crime. Global common spaces. Critical infrastructures.

6 ECTS credits.

2

Second Course

2.1 First Semester

2.1.1 Operational and Statistical Management Methods

Introduction: The company and its purposes. Organization and structure of the company. The role of operations research in the companies. Mathematical Programming: Optimization models for management. Introduction to the solution methods. Postoptimization. Examples. Decision Theory: Introduction. Decision analysis. Multiobjective decision making. Examples. Project Management: Planning a project. Critical activities. Gantt chart. Cost balance and resource constraints. Other management methods. Quality management and design of experiments: X-R control charts. Design of experiments in quality control.

6 ECTS credits.

2.1.2 Basic Legal Principles Applied to Cybersecurity

This course helps students to understand the rules that the law imposes on the activity they are studying. The syllabus The course covers the legal, technical and soft law rules that govern the activity of IT operators and cybersecurity players, rules that determine their possible responsibilities towards the State and third parties. cybersecurity, rules that determine their possible responsibilities towards the State and third parties.

Cybersecurity legal regulation. Legal framework of cybersecurity law. The legal regulation of information services. The protection of personal data. Introduction to Cybersecurity Criminal Law. Professional ethics, ethical hacking and business models. The importance of professional ethics. Ethical Hacking. Software licensing and business models.

6 ECTS credits.

2.1.3 Advanced Programming

Java: platform and language. What is Java: development platform and programming language. Language evolution. Development environments. Syntax and basic semantics of Java language. Object Oriented Programming Basis of OOP. Elements of Object Oriented Programming. Classes and objects. Object Oriented Programs Introduction. Program development. Relationships between classes. Instance vs. class. Packages. Standard Library. Enumerated. Inheritance and Polymorphism. Introduction to the concept of inheritance. Inheritance by Extension. Inheritance by Implantation. Benefits of Inheritance. Introduction to the concept of polymorphism. Benefits of polymorphism. Polymorphism vs. Overloading. Type compatibility. Exceptions. Exception handling. Exception management. Throwing and declaring exceptions. Chained exceptions. Finally block. Advantages of exceptions. Data Structures. Generics. Lists, sets and maps. Traversing a collection. Sorting and searching. Equals and hashcode. Collections with primitive types. Advantages of collections. Modularity and Documentation. Introduction. Java libraries. Creation of a library. Introduction to documentation. JavaDoc. Creation of .jar files

6 ECTS credits.

2.1.4 Hacking Techniques

Information gathering techniques: footprinting, OSINT, fingerprinting, social engineering. System hacking: processors and firmware hacking, vulnerability exploiting in Windows and Linux. Web and application hacking: reverse engineering, overflows, injections and forgeries. Network and communication hacking: poisoning, hijacking, and denial of service attacks.

6 ECTS credits.

2.1.5 Computer networks

The Computer Networks course aims to provide basic training in the technical aspects of computer communication to undergraduate students of Computer Engineering, Software Engineering and Computer Engineering.

Computer networks concepts: protocols and technologies organized in a layered architecture. In this way, students will be able understand the different concepts and protocols and how all the parts fit together. Introduction to Internet. The Application Layer. Highlighting the technologies that support the Web, e-mail and P2P file sharing. The Transport Layer. It will be addressed explaining the reliable communication over an unreliable network layer, connection establishment and closure, and the agreement process, congestion and flow control, and multiplexing. The Network Layer. Fundamental topics such as route determination between two routers will be studied and the interconnection of a large number of heterogeneous networks. The Data Link Layer and the Physical Layer. Fundamental problems such as the sharing of a multiple access channel, addressing, local area networks and the physical media used to transmit information.

At the end of the course, the student should be able to adequately design a computer network for a company, taking into account cost, performance and needs criteria.They should also be able to understand the technical description or documentation of a communications product, as well as the physical means used to transmit information.

6 ECTS credits.

2.2 Second Semester

2.2.1 Databases

Information systems; database concept; databases management systems; file management systems; data models; conceptual model; data models clasification; data models in database design; E/R model extended; database design; sql.

6 ECTS credits.

2.2.2 Secure Web Development

HTML, CSS, JavaScript; Spring ajax; sql injection; XSS, spring data; spring security; cookies; oauth; SAML; OpenID

6 ECTS credits.

2.2.3 Computer Structure

This course is part of the subject "Technological Foundations of Cybersecurity" and begins with an in-depth study of the internal structure of computers. The classical von Neumann model will be used as a starting point to identify the functional units into which the components of a computer are currently classified. In this particular course, special attention will be paid to the central processing unit (CPU). For this purpose, a simple processor such as MIPS has been chosen, from which the basics of programming it will be learned. The basics of low-level programming in assembly language will be learned, with two implementations of the data and the control path (unicycle/multicycle). As an introduction, two other families of two very popular processors on the market will also be studied: ARM, present in numerous mobile devices, and Intel, omnipresent in desktop and laptop computers.

6 ECTS credits.

2.2.4 Network Security

Introduction to Network security. Perimeter protection (firewalls and DMZ). Network segmentation (VLAN). Intrusion Detection and Prevention Systems. Virtual Private Networks (IPSec and TLS). Wireless networks security.

6 ECTS credits.

3

Third Course

3.1 First Semester

3.1.1 Algorithms Design and Analysis

Analysis of algorithms: Mathematical preliminaries; Computational complexity and asymptotic notation; Memory and runtime analysis of iterative and recursive algorithms. Algorithm design techniques: Introduction to recursion; Divide and conquer; Backtracking; Greedy algorithms.

6 ECTS credits.

3.1.2 Operating Systems

Bash; shell; virtual machines, unix basic administration; input/output; debugging; threads; memory management; files;

6 ECTS credits.

3.1.3 Security in Databases

Introduction to database security, Confidentiality, Integrity and Availability in commercials DBMS; Mandatory and Discretionary Access Control, Data Ciphered in commercials DBMS; User privileges, roles and profiles management, backup copies and recovering, and auditoring in commercials DBMS.

6 ECTS credits.

3.1.4 Software Engineering

Knowledge and application of the principles, methodologies and life cycles of software engineering. Ability to develop, maintain and evaluate software services and systems that meet all user requirements and behave reliably and efficiently, are affordable to develop and maintain and meet quality standards, applying the theories, principles, methods and practices of the Software engineering. Ability to identify, evaluate and

manage potential risks that may occur. Ability to design appropriate solutions in one or more application domains using software engineering methods that integrate ethical, social, legal and economic aspects. Ability to actively participate in the specification, design, implementation and maintenance of information and communication systems.

6 ECTS credits.

3.1.5 Operating Systems

This subject shows how operating systems work. Specifically, the student will understand the basic concepts of operating systems and will become familiar with their programming, understanding their principles and forms of application. The student will acquire knowledge related to the management of processes, memory and file system.

6 ECTS credits.

3.2 Second Semester

3.2.1 Artificial Intelligence

Introduction to Artificial Intelligence, Problem solving through search (Uninformed search, Heuristic search, Advanced heuristic search, Multiagent search, Constraint satisfaction problems), Knowledge Representation (Description logic, Ontologies and Web services, Reasoning with imprecision), Machine Learning (Supervised learning/Decision Trees, Neural Networks, Reinforcement learning /Q-learning).

3 ECTS credits.

3.2.2 Information Systems

The organizational structure of a corporation. Basic concepts of Information Systems. Management Information Systems. On Line Analitical Processing (OLAP) Business

Intelligence. Data analysis Security in Information Systems.

6 ECTS credits.

3.2.3 Artificial Vision applied to Cybersecurity

Introduction to Computer Vision. Basic Image Processing Techniques Image operations Detection and description of points of interest Simple geometric structures detection Pattern recognition. Biometrics. Types of biometric systems Advantages and disadvantages of biometric systems Multibiometry Open aspects. Presentation attacks on biometric systems Types of attacks on biometric systems Presentation attacks Presentation attack detection and countermeasures. Case studies and application environments Intelligent video surveillance systems Airports and critical infrastructure. Borders and identity documents

3 ECTS credits.

3.2.4 Malware and Targeted Threats

History of Malware. Taxonomy. Propagation vectors and infection. Propagation, replication, protection and malware control. Static and dynamic analysis. Anti-malware solutions. Targeted Threats and APTs. Cyberweapons.

6 ECTS credits.

3.2.5 Methodologies for Secure Software Development

Identification of the most critical vulnerabilities and weaknesses in software and analyze their causes associated with development. Secure software development techniques. Trusted operating systems and the aspects of protection and security that they guarantee to the applications. Security fundamentals and best practices in the most widespread programming languages. Static and/or dynamic code analysis, and other test mechanisms.

6 ECTS credits.

3.2.6 Advanced Networking and Cloud Computing

Traffic modelling and queuing theory. Traffic engineering, dynamic routing and MPLS. Introduction to cloud computing and network function virtualization. Software defined networks. Advanced Network Security.

6 ECTS credits.

4

Fourth Course

4.1 First Semester

4.1.1 Pentesting

This course is intended as an introductory course to penetration testing. Penetration testing, or pentesting, consists of simulating real attacks to evaluate the risk associated with potential security breaches. The objective is to discover and exploit vulnerabilities to evaluate what a potential malicious attacker could gain access to. This subject is taught in the first quarter of the fourth year of the degree. For the completion of this course knowledge of previous subjects such as programming, networks, system administration, web applications and others, will be necessary.

3 ECTS credits.

4.1.2 Audit

Introduction to IT and information security auditing. Internal vs. external auditing. Types of auditing: conformance, certification, strategic (risks, maturity, service), quality, etc. Privacy audits. Relationship between IT audits and governance, risk management, quality, and conformance. Fraud prevention and detection. IT and security auditing methodologies. Steps and structure of a cybersecurity audit program. Computer-assisted audit techniques and tools. Standards and best practices for security audits. IIA, ISACA, ISO, and individual certifications.

3 ECTS credits.

4.1.3 Security Intelligence

Ability to conceive, write, organize, plan, develop and sign documents that are intended to define, plan, specify, summarize projects and plans in the field of cybersecurity. Be able to define, evaluate and select countermeasures for the protection of technological assets, understanding the peculiarities of the different contexts in which they must be deployed. Being able to design, deploy, evaluate and improve incident response

and business continuity plans. Ensure availability, fault tolerance and / or resilience to the appropriate levels for each context. Collect and analyze digital evidence to draw post-incident conclusions and perform forensic analysis. Define and implement security master plans, being able to prioritize the initiatives and projects included in these plans.

6 ECTS credits.

4.2 Second Semester

4.2.1 Risk Analysis and Management

Introduction to cyber risk. Approaches for risk management. Methodologies, standards and frameworks. Qualitative methods. Quantitative methods. Probability and impact. Other inputs for risk analysis. Particular scenarios. Risk mitigation. Risk transfer. The role of the CISO.

6 ECTS credits.

4.2.2 Critical Infrastructure Protection

Critical infrastructures, industrial systems and cyber-physical systems. ISA levels, basic concepts and definitions. Specific aspects. Critical infrastructure protection. National and international legislation and regulatory frameworks. Attacks on critical infrastructures and industrial systems. Cascading effects. Hybrid threats. Methodologies and strategies for the protection of critical infrastructures and industrial systems. Risk analysis and management in these contexts.

3 ECTS credits.

4.2.3 Security Regulation and Governance

Regulation. Civil vs. criminal legislation. International regulatory framework: Sarbanes-Oxley Act (SOX), PCI DSS, etc. European regulatory framework: NIS directive, etc. National regulatory framework: National Security Scheme, National Security Act, etc. Governance and its relationship with Regulation. Definition of a security strategy and planning. Environment and external factors. Corporate culture. Security management in the organization. Security policy and control model. Best practices, guidelines and recommendations for Security Governance. Internal governance: COSO, ERM. IT governance: COBIT, ITIL. Security governance: ISO 27001, ISO 27002, NIST framework.

3 ECTS credits.