SAPIENZA
UNIVERSITÀ DI ROMA

ATTACHMENT – DESCRIPTION OF CURRICULUM

INFORMATION IDENTIFYING THE HOLDER OF THE QUALIFICATION
Family name(s): DAVOLI
Given name(s): ANTONIO
Date of birth (day/month/year):14/03/1964
Student identification number or code (if available): 756696

1 FORMATIVE ACTIVITY (code): Statistics (1055043)
FORMATIVE AIMS: The course includes topics and themes of specific relevance for cybersecurity. Intensive work is carried out on the computer, actually coding statistical algorithms, Monte Carlo Methods and simulations in order to acquire a solid understanding of actual implementation of statistical methods. Last generation OOP languages and IDEs are used. Students are also required to maintain a blog with all their researches carried out during the course upon indication of the instructor. Knowledge and Understanding To understand the fundamental statistical concepts including sampling, experimentation, variability, distribution, association, causation, estimation, confidence, hypothesis testing, and significance; to review and analyze statistical arguments, and to appreciate the relevance and importance of statistics. Applying Knowledge and Understanding The student will acquire the following skills: collecting, organizing and interpreting numerical data; interpreting and communicating the results of a statistical analysis. Understanding and making sensible decisions based on the analysis of numerical information.
COURSE CONTENTS: Classical topics in Statistics, useful for the Cybersecurity curriculum
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

2 FORMATIVE ACTIVITY (code): NETWORK INFRASTRUCTURES (1027171)
FORMATIVE AIMS: This course presents the basic concepts, protocols and architectures of the current network infrastructures. Specific attention is given to the broadband access, the optical backbone and the next-generation wireless networks. Furthermore, main technologies leading to the QoS support in a network infrastructure are described. Expected learning results At the end of the course the students will have competences in technologies and network infrastructures presented in the course like: xDSL, PON, LTE, 5G, SDH, OTN, SDN. Moreover, they will be able to configure and analyze an IP based network by using the Netkit tool. Specific projects carried out during the course will allow the students to apply their knowledge to innovative network scenarios and applications.
COURSE CONTENTS: 1. Review on TCP/IP networks, LAN/MAN technologies 2. Review on fundamentals of Digital Communications 3. Telephone networks (Architecture and context, digital channels, switching hierarchies, SS7 signaling) 4. Access network • Copper based broadband access networks • ADSL and VDSL, networking solutions • Fiber based: PON and relevant extensions • Metro Ethernet/Gigabit Ethernet • Multihop/3G/4G wireless data • Wi-xx family (WiGi, WiMax and mesh networks) • 4G cellular systems: LTE, LTE-A 5. Core network • Optical networking concepts • Optical link layers (SONET, WDM) • Optical Transport Network based on DWDM: single link characterization, optical components and devices, systems and networks • Network control and management (Software Defined Networks and OpenFlow) 6. The 5G network: architectural models and enabling technologies
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

3 FORMATIVE ACTIVITY (code): CRYPTOGRAPHY (1047622)
FORMATIVE AIMS: General Objectives The goal of the course is to hand down the foundations of cryptography, which is at the heart of security in nowadays digital applications. Specific Objectives The students will learn the methodology of provable security, which allows to prove security of modern cryptosystems in a mathematically sound way. Knowledge and Understanding -) Knowledge of the mathematical foundations of modern cryptography. -) Knowledge of the main hardness assumptions, on which the security of cryptographic constructions is based. -) Knowledge of the cryptographic schemes currently used in real life. Understanding of their (practical and theoretical) properties. Applying knowledge and understanding: -) How to select the right cryptographic scheme for a given application. -) How to analyze the security of a given cryptographic scheme. Autonomy of Judgement The students will be able to judge whether a given cryptographic scheme is secure or not. Communication Skills How to describe the security of a cryptographic construction in the language of provable security. Next Study Abilities The students

interested in research will learn what are the main open challenges in the area, and will obtain the necessary background for a deeper study of the subjects.
COURSE CONTENTS:
ASSESSMENT METHODS:
TEACHING METHODS:

4 FORMATIVE ACTIVITY (code): Computer systems and programming (1054960)
FORMATIVE AIMS: General Objectives Main objective of the course is to provide the basics of system programming. Specific Objectives Students will be able to autonomously develop programs able to interact with the operating system and exploit its services. Knowledge and Understanding -) Knowledge of the C programming language and of the tools normally available in the development environment (compiler, preprocessor, debugger, make, etc.). -) Knowledge of the main functions of an operating system and its fundamental components (Scheduler, Virtual Memory Manager, Filesystem ..) -) Knowledge of the most important primitives and interfaces in order to create and synchronize processes and threads, exchange messages and signals. -) Knowledge of the socket framework and its API. Applying knowledge and understanding: -) How invoke system primitives and correctly integrate system calls in applications -) How select the most appropriate frameworks and paradigms, depending on application requirements and runtime characteristics. Autonomy of Judgement Students will be able to assess the complexity and the implementation criteria of specific applications Communication Skills Students will be able to describe how their applications use the system call API and explain the reasons behind their choices. Next Study Abilities Students will be able to further develop their skills examining, with more details, the architecture and the programming interface of the operating system.
COURSE CONTENTS: Programming environment: compiler, make & makefiles, gdb debugger Recap of the C programming language: variables, costants, operators, expressions, control instructions, functions, pointers, arrays, structures & unions, preprocessor directives Operating system basics (Linux): processes, filesystem, inter-process communication primitives (signals, pipes, semaphores, shared memory) Thread programming: pthread management, mutual exclusion, synchronization Network programming: sockets, raw sockets, sniffers Software vulnerabilities: buffer overflows, arc injection, file infection
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

5 FORMATIVE ACTIVITY (code): Distributed Systems (1022807)
FORMATIVE AIMS: Computing systems are at the heart of any information systems today. This course aims to provide students with a clear characterization of concurrency in a distributed system considering its characteristics like failures, variable latencies and the absence of a global clock. The course will analyze the main system models and abstractions for basic communications and synchronization. Finally, we will provide the concepts related to distributed consensus and an introduction to distributed ledgers. Knowledge and understanding The student will be able to design systems and distributed algorithms on top of different system models such as synchronous, asynchronous and partially synchronous, while understanding impossibilities and limitations in performance. Students will also have the ability to abstract systems and platforms using models that are easier to treat.
COURSE CONTENTS: - Introduction to Distributed Systems - Basic Abstractions (Distributed Computations, Abstracting Processes, Abstracting Communications, Timing Assumptions, Abstracting Time) - Clock Synchronisation - Broadcast (Best Effort Broadcast, Reliable Broadcast, Uniform Reliable Broadcast, Probabilistic Broadcast) - Consensus (Regular Consensus, FLP Impossibility Result, Uniform Consensus, Paxos Algorithm) - Ordered Communications - Shared Memories - Software Replication - CAP Theorem and its Applications - Byzantine Fault Tolerance - Distributed ledgers
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

6 FORMATIVE ACTIVITY (code): Practical Network Defense (10589555)
FORMATIVE AIMS: General objectives The course explains the fundamentals of the methods and tools for the protection of computer networks. Particular attention is paid to the practical application of the concepts learned. Knowledge and understanding List commonly-seen threats arising from the use of particular protocols in networked computer systems. Explain mechanisms commonly used by intruders and designers of malware in order to compromise a computer system's security. Explain the basic mechanisms used for the detection of intrusion attempts in computer systems. Application of knowledge and understanding At the end of the course students will be able to monitor traffic in networks, apply a security policy, perform a network scan and search for vulnerabilities in a computer network. Students will develop the ability to select the appropriate firewall rules to protect a network, select the most appropriate mechanisms to protect a networked computer system and to make the most appropriate design choices to implement a "defense in depth" strategy, using isolated networks and dedicated tools (VPN, proxy and firewall). Judgment skills Students will develop the analytical skills necessary to evaluate different alternatives during the design process of a computer network, with particular reference to the evaluation of the architectural choices and related risks and to the security objectives that the system wants to pursue. Communication capacity

Students will learn how to document their choices, also through the use of automated reporting tools. They will also have acquired the ability to prepare presentations related to specific scientific topics. Ability to continue learning in an autonomous way The concepts acquired during the course will provide students with a solid knowledge base in order to further deepen the more technical aspects, explore the alternatives not dealt with for time reasons and to autonomously keep themselves informed on the continuous developments and updates of network security and protection.
COURSE CONTENTS:
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

7 FORMATIVE ACTIVITY (code): Cyber and Computer Law (1055055)
FORMATIVE AIMS: General Objective The aim of the course is to deepen on the main issues of legal regulation of computer activities, in companies and in public administration, with reference to the issues of computer security and Cybercrime, regulation on the development and processing of personal data and on e-commerce and intellectual property in computer matters. The course is structured in modules also with examination of practical cases. Knowledge and Understanding At the end of the course, the student is able to identify and develop the main legal knowledge in the field of data processing and therefore to operate effectively within public administrations in the relationship with judicial or police offices. It is also able to participate effectively in working groups or joint investigation teams having clear the essential notions and legal responsibilities. The course allows the student to connect technology skills with organizational, economic and legal skills regarding the use of computer science tools in business and public sector. Application of Knowledge and Understanding For the realization of the training objectives, the didactic activities are articulated in thematic study modules, for the definition and the intervention in specific contexts or in particular situations of risk or emergency and to understand the needs of operators, there will also be joint initiatives with other courses of study on the issues of security, resilience and methodology for the acquisition of traces and evidences of cyber crime also in the international environment.
COURSE CONTENTS:
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

8 FORMATIVE ACTIVITY (code): ETHICAL HACKING (1055682)
FORMATIVE AIMS: General objectives Ethical hackers are a category of professionals increasingly in demand by companies and governments aware of the need to effectively protect their infrastructure from possible cyberattacks. The course deals with the fundamentals of ethical hacking. In particular, it starts from the systematic study of the methodologies and tools used by hackers to carry out the various attacks in the cyberspace. Next, it illustrates how the professional of ethical hacking can carry out a series of legal and useful activities by subjecting the computer systems to vulnerability tests. These tests are intended to evaluate and prove the cybersecurity of an organization and to help owners and managers to become aware of, and solve their cybersecurity problems. Particular attention is paid to the practical application of the concepts learnt. Specific objectives The course explains in detail what hackers are doing, how hacking activities occur, how hackers illegally manage to enter a computer system protected by security measures, and how to defend against them. Knowledge and understanding Understanding the Ethical Hacking concepts and scope. Namelly, Casing the Establishment: the hacking techniques used to enumerate the targets completely. Endpoint and Server Hacking: the ultimate goals of any hacker including Advanced Persistent Threats. Infrastructure hacking: the way hackers attack the equipments our systems connect to. Application and Data Hacking: attacks to web/databases world as well as mobile hacking techniques. The countermeasures that can be used to hinder hackers' activities on the subsystems considered. Penetration testing execution standards. Application of knowledge and understanding At the end of the course, students will have the ability to analyze complex cybersystems and gain a better understanding of the target organization's vulnerabilities. Produce report in a manner that provides the most value to the target organization executives. Wisdom of judgement Students develop the ability to plan ethical hacking activities in a way that do not violate current applicable law. Ability to follow a code of ethical conduct and provide assurance of good intentions in conducting systems penetration testing activities. Communicative Capabilities Students will learn how to document their choices, including through the use of automated reporting tools. They will also have acquired the ability to prepare presentations on scientific subjects. Ability to pursue learning independently The notions acquired during the course will provide students with a solid knowledge in order to further investigate the most technical aspects, and to keep themselves informed about the continuous developments and updates of the ethical hacking sector.
COURSE CONTENTS: This course aim at the understanding the Ethical Hacking concepts and scope. Namelly, Casing the Establishment: the hacking techniques used to enumerate the targets completely. Endpoint and Server Hacking: the ultimate goals of any hacker including Advanced Persistent Threats. Infrastructure hacking: the way hackers attack the equipments our systems connect to. Application and Data Hacking: attacks to web/databases world as well as mobile hacking techniques. This course presents the countermeasures that can be used to hinder hackers' activities on the subsystems considered, and the Penetration testing execution standards.

ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

9 FORMATIVE ACTIVITY (code): WEB SECURITY AND PRIVACY (1044404)
FORMATIVE AIMS: The course aims at providing the fundamentals on Web-application security, and on privacy in the electronic society. Concerning the security of Web application a classification of the threats and of the main techniques of attack, and of the targets and goals of the attackers. The course also focuses on the basic design strategies and the main resources that are available to support designers and developers to reach the goal of "security by design". Particular emphasis will be devoted the e-mail security and to privacy preserving, studying the threats, the basic fixes and pros/cons of anonymity as a tool for aiming at privacy preserving. The course also provides the knowledge for the protection of privacy. Techniques and tools designed to violate privacy and anonymity in economic transitions, in the release of statisitical data, and in social networks. Economic issues and psychological aspects of the use and release of sensitive data will be considered and regulatory issues for the protection of sensible data.
COURSE CONTENTS:
ASSESSMENT METHODS:
TEACHING METHODS:

10 FORMATIVE ACTIVITY (code): Security Governance (1055061)
FORMATIVE AIMS: The main objective of the course is to provide an introduction to all issues related to the cybersecurity management. In particular, the course will highlight that cybersecurity is a vertical problem with respect to the company organisation. Consequently, its management impacts different levels. Aspects related to international and national regulations and standards will be analysed. Then, it will be discussed how, from the methodological point of view, these aspects are taken in to account and implemented by defining cybersecurity frameworks. Finally, another fundamental aspect of the course will be to present methods and open problems to carry out auditing, verification, compliance and certification activities considering specific techniques and tools that can be used for this purpose.
COURSE CONTENTS: Information Security Governance Models and Methodologies SG Best Practices and Guidelines • CSF NIST • ISO 27000 Family Risk Management and Cyber Risks • ISO 31000 • A Methodology for establishing a Risk Management Process • Case Study Threat Modelling • Data Flow Diagrams • STRIDE • Attack Trees and Attack Libraries • Attack Graphs • Case Study Intrusion Detection • IDS and IPS • Port Scan Detection Incident Management, SOC and CERT Seminars
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

11 FORMATIVE ACTIVITY (code): Risk management (1055050)
FORMATIVE AIMS: General objectives The course deals with the evaluation of cyber risks that can damage an enterprise information system, the methodologies to mitigate these risks and the necessary countermeasures to be applied with the aim of making the company or public institution secure from the IT point of view. Specific objectives The course deals with the relationships between the operating mechanisms of information systems and computer networks and the computer threats to which they may be subject, the mechanisms for identifying and opposing attacks and their implementation through the application of specific countermeasures to reduce cyber risk. Particular attention is paid to the practical application of the notions learned through the analysis of case studies and exercises. The basic reference for the Risk Management course is the ISO 27005 standard, complemented by the NIST SP 800-30 framework. Knowledge and understanding Analyze the most common and dangerous threats, relating them to the vulnerabilities of systems and networks on which threats can have an impact. Assess the business risks associated with this impact and recommend the implementation of appropriate countermeasures; alternatively, suggest criteria for accepting the risks identified. Explain the basic mechanisms used to identify intrusion attempts into computers and networks. Determine and establish continuous improvement processes. Application of knowledge and understanding At the end of the course, students will be able to identify and assess the risks that can affect the functioning and security of an information system and their impacts. Based on the risk analysis and management methodologies learned in the course, the students will develop the ability to identify and select the appropriate countermeasures to protect the information system, from a technical, administrative, and cost point of view, determining the best governance profile of the security process. Judgment skills Students will develop the analytical skills necessary to evaluate different alternatives during the process of identifying the security risks of an Information System, with particular reference to the assessment of the architectural choices and the risks that they may involve and the security objectives imposed on the system in relation to the level of sensitivity of the information it manages. Communicative skills Students will learn how to document their choices, including through the use of automated reporting tools. They will also have acquired the ability to prepare presentations on topics related to risk management. Ability to continue learning in an autonomous way The notions acquired during the course will provide students with a basic knowledge in order to further deepen the more technical aspects, and to keep themselves informed about the continuous developments and updates of the assessment of cybersecurity risks of systems and networks.

COURSE CONTENTS:
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

12 FORMATIVE ACTIVITY (code): BIOMETRIC SYSTEMS (1041792)
FORMATIVE AIMS: General goals: To be able to design and evaluate a biometric or multibiometric system. Specific goals: To know the features and basic techniques related to physical biometric identifiers, such as face, fingerprint, iris, etc., and behavioral, such as gait, signature (dynamic), voice, typing mode, etc. Architecture of a biometric system: unimodal systems and multibiometric architectures. To be able to evaluate the performance of a biometric system according to the adopted modality: verification and identification. To be able to evaluate/assure the robustness of a biometric system against spoofing attacks (identity theft). Knowledge and understanding: Fundamentals of design of a biometric system and of the techniques to extract/match the specific characteristics for the main biometric traits. Applying knowledge and understanding: To be able to design and implement an application for biometric recognition for at least one biometric trait. Critical and judgmental capabilities: To be able to assess the performance and robustness of a biometric system to presentation attacks. To be able to transfer techniques and protocols in different contexts. Communication skills: To be able to communicate/share the requirements of a biometric system, the most suited modalities for a certain application, and the performance measures of a system. Capability of autonomous learning: To be able to autonomously get a deeper insight on the course topics, in relation to either specific/complex techniques and methods, or to biometric traits not covered in the course.
COURSE CONTENTS: Introduction to biometric systems (5 hours) Evaluation of a biometric system (10 hours) Performance evaluation Reliability of recognition results Main biometric traits (30 hours) Face detection Face recognition 2D and 3D Ear recognition Iris recognition Basics on fingerprints recognition Other biometrics Multibiometric systems (15 hours) Course web page: https://sites.google.com/a/di.uniroma1.it/biometric-systems/
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

13 FORMATIVE ACTIVITY (code): Cyber Security Seminars (AAF1803)
FORMATIVE AIMS: Organizations today are facing an increasing sophistication, stealth and persistence of cyber-attacks – from nation-states, organised crime, hacktivists, as well as threats from within the organisation. The goal of the course is to describe the main critical challenges of protecting information systems and assets – financial information, customer data, intellectual property – and the implications of failing to do so.
COURSE CONTENTS: The list of speakers and seminars covered changes from year to year on the basis of the evolution of the cybersecurity sector.
ASSESSMENT METHODS: Idoneità
TEACHING METHODS: 0

14 FORMATIVE ACTIVITY (code): MALWARE ANALYSIS AND INCIDENT FORENSICS (1055681)
FORMATIVE AIMS: Today's cyber security scenario shows a relentless growth of malicious software used to perpetrate cyber attacks. This course aims to provide students with the knowledge, methods and basic tools to analyze, identify, categorize and understand the behavior of different classes of malicious software. The course will adopt a practical approach, with frequent application of the learned methods to real-world cases. Expected learning results Students will be able to analyze, both manually and through the use of automated tools, malicious software of different nature to identify all its salient features. They will be able to extract these characteristics and relate them with existing knowledge bases. Finally, students will be able to contextualize these activities as part of an overall process of threat intelligence and incident management caused by such malicious software.
COURSE CONTENTS: Introduction to cybersecurity (2h) Recap on ASM x86 (6h) Threat models and attack kill chain (2h) The internal structure of a malware (2h) Basic malware analysis (6h) Static analysis (12h) Dynamic analysis (12h) Obfuscation and evasion techniques (6h) Threat intelligence (25h)
ASSESSMENT METHODS: Attestato di profitto
TEACHING METHODS: 30

15 FORMATIVE ACTIVITY (code): Final exam (AAF1028)
FORMATIVE AIMS: The final exam consists in the discussion of a master thesis, composed of a document written in English, which presents the results of an original study conducted on a problem of an applicative, experimental or research nature. The preparation of the thesis takes place under the direction of a teacher in the second year of the course. The final exam assesses the ability to apply the knowledge learnt to a specific problem, the ability to make autonomous decisions and to communicate the methodological and technical aspects of the work carried out.
COURSE CONTENTS:
ASSESSMENT METHODS:
TEACHING METHODS: