Seminario Professionalizzante e di Specializzazione

su:

**Seminario Professionalizzante**
**" Sicurezza nelle Reti Radio di Sensori e Veicolari"**
"Wireless Sensor and Vehicular Networks Security"

**10ª edizione**

**A.A. 2025-26**

**Destinatari:** i potenziali destinatari sono gli studenti dei corsi di laurea magistrale e gli studenti dei corsi di laurea triennale regolarmente iscritti al terzo anno di corso in Ingegneria delle Telecomunicazioni, Ingegneria Informatica, Ingegneria dei Sistemi di Controllo e dell'Automazione, Informatica. La partecipazione al corso ed il conseguimento dell'idoneità consentono di acquisire 3 CFU nella tipologia F. Si ammetteranno fino ad un massimo di 30 partecipanti, selezionati sulla base del numero di crediti acquisiti. Per impostazione e contenuti il seminario è adatto anche per gli studenti del corso di dottorato in Ingegneria e Scienze dell'Informazione. Sono ammessi anche uditori esterni.

*Recipients: potential recipients are students of the "laurea magistrale" as well well as students of the "laurea triennale" master's degree courses regularly enrolled in the third year of the course, in Telecommunications Engineering, Computer Engineering, Control Systems and Automation Engineering, Computer Science . Participation in the course and the achievement of eligibility allow you to acquire 3 CFU in type F. Up to a maximum of 30 participants will be admitted, selected on the basis of the number of credits acquired. The seminar is also suitable for students of the PhD course in Engineering and Information Sciences. External auditors are also allowed.*

**Durata**: 28 ore (lezioni di 4 ore al giorno per 7 giornate)
***Duration**: 28 hours (lessons of 4 hours a day for 7 days)*

**Docente / *Lecturer***: Ing. Marco Pugliese, Ph. D., Sr. IEEE Member, Sr. Security Manager UNI 10459:2017

**Calendario e modalità di erogazione**: Il seminario avrà luogo tra il **24 Aprile e il 11 Giugno 2026 in modalità on-line via TEAMS**.

***Schedule and delivery:** The seminar will take place between 24$^{th}$ April and 11$^{st}$ June 2026 on-line via TEAMS.*

**Programma del Seminario /** *Course Program*

**Part I. Security Analysis applied to WSN and VANET (12 hours)**

**Day 1-2. Lecture I.1 The Framework of Security Management (6h):** ISO 31000 Risk Management and NIST Cyber Security frameworks are briefly introduced. The path from risk to security management process is delineated and the techniques for Cyber Risk Quantification (CRQ) are presented. The Reference Security Model is then produced. Security levels and criteria for metrics definition are introduced. The concepts of "Required Security Level" and Offered Security Level" are introduced and defined per class of application. A simple guide line (primer) for leading a Security Management Process is introduced.

*TOPICS: The framework of Security Management. From Risk to Security Management. Security Management Process, Models and Techniques for Cyber Risk Evaluation: FTA/ETA/CVSS. Reference Security Model: Security Metrics, Timing constraints, the "Required Security Level" vs. the "Offered Security Level".* Guide lines to manage a *Cyber Security Management Process.*

**Day 2-3. Lecture I.2 The case of WSN and VANET (4h)**: ad hoc networks, taxonomy, definition of WSN and VANET. Characterization of WSN, design constraints, application scenarios and current standard architectures. WSN security requirements are introduced and defined per application class. Characterization of VANET, communication models (V2V, V2I), smart vehicles, application scenarios and current standard architectures are introduced.

*TOPICS: Wireless ad-hoc networks. WSN vs. mobile ad-hoc networks (MANET). MANET vs. vehicular ad-hoc networks (VANET). Design constraints for WSN. WSN Architecture: MAC and routing functions for WSN. WSN standardization roadmap: IEEE 802.15.4, ZigBee. The operating system for WSN: TinyOS. Security Requirements for WSN layer functions and applications. Security Management Plane. Definition of VANET, VANET vs. MANET, VANET applications, vehicular communications system, Communication models (V2V, V2I), inter-vehicle and intra-vehicle communications, broadcast techniques.*

**Day 3. Lecture I.3 Threats and Attacks against WSN and VANET (2h)**: the classification of cyber attackers and review of the most significant cyber attacks against WSNs and VANETs, the correspondent strategies of countermeasures are presented.

*TOPICS: Classification of Cyber Attackers and Cyber Attacks. Attacks to physical layer, data link layer, network layer, transport layer and application layer. Review of attacks against WSN. Review of attacks against VANET.*

**Part II. Mitigation Measures: Security Techniques applied to WSN and VANET (16 hours)**

**Day 4. Lecture II.1 Passive Security Functions (4h)**: passive security functions, i.e. purely defensive techniques without feedbacks for countermeasures, are introduced (cryptographic functions such data encryption and authentication). Key metrics and quantitative criteria to measure the "Offered Security Level" from information theory are represented. A brief mathematical introduction is presented. The main techniques are introduced.

*TOPICS: The Shannon's lessons. Hints on Modular Arithmetic, Generating Prime Numbers, Generating Pseudo-Random Numbers, Factoring Problem, Elliptic Curve Algebra, Pairings on Elliptic Curves. Passive Security Functions: Ciphering, Hash Functions, Message Authentication Codes, Digital Signatures. Key Establishment Protocols (KEP): Symmetric KEP, Asymmetric KEP, Id-based Encryption and Signature schemes, Hybrid KEP. Key Management Protocols (KMP): TinySEC, TinyECC. Passive security techniques for: IEEE 802.15.4 MAC, Routing, ZigBee.*

**Day. 5. Lecture II.2 Active Security Functions (4h)**: active security functions, i.e. security techniques with feedbacks for countermeasures, are introduced (system behavior estimators and anomaly detectors). Key metrics and quantitative criteria to measure the "Offered Security Level" are represented. A brief mathematical introduction is presented. The main techniques are introduced.

*TOPICS: Dynamic Systems. Discrete Event Dynamic Systems (DEDS). The Canonical Problems of Dynamic Systems. The Intrusion Detection Problem: System Modeling (Petri Nets), Mapping into a Finite State Machine (Finite Automata, Stochastic Finite Automata or Discrete Time Markov Chains, Weighted Finite Automata), Identification of the Hidden State Machine (Hidden Markov Models, Weak Process Models), Hidden State Sequence Estimation (Viterbi Algorithm, Highest Score Method). Behavior Classifier. Information Theoretic Model of an Intrusion Detection System. Anomaly Detection System: Audit data, Classification Model, Representation Model. Representation Techniques: Supervised vs. Unsupervised Approach, Parametric vs. Non-parametric Techniques.*

**Day 6. Lecture II.3 Security Functions made in Univaq. TAKS/ECTAKS/WIDS/MVET schemes (4h):** the cryptographic encryption/decryption and signature scheme TAKS (Topology Authenticated Key Scheme) and its ECC (Elliptic Curve Cryptography) extension is presented. TAKS has been embedded into WINSOME platform: WINSOME Project (Wireless Sensor Network Secure System for Structural Integrity Monitoring and Alerting) is briefly introduced. The intrusion detection system WIDS (WPM-based Intrusion Detection Scheme) and the behaviour estimator MVET (Mean-Variance Estimation Technique) are presented. WIDS has been implemented over embedded into WINSOME platform.

*TOPICS: TAKS / ECTAKS Schemes. TAKS driving ideas & main features, Authenticated Network Topology, TAKS definition, EC-based TAKS (ECTAKS) pwECTAKS, cwECTAKS and xwECTAKS, ECTAKS Encryption / Decryption Scheme, ECTAKS Signature Scheme, ECTAKS SignEncryption Scheme, NIST Standard ECC. xTAKS in WINSOME Project. WIDS / MVET Schemes. Weak process model IDS (WIDS) Reference Architecture: WIDS Technique, Basic Network Threats, Examples of Anomaly Rules, WPM-based Threats Models, Aggregated Threats Models, Security Analysis. WIDS in WINSOME Project. MVET driving ideas & main features, Reference Architecture, the estimation technique and performance analysis.*

**Day 7. Lecture II.4 VANET Privacy Functions (2h):** security and privacy requirements, adversary model, specific threat classification, security architectures and techniques are introduced.

*TOPICS: Security and privacy requirements, analysis, architecture, guidelines to secure a VANET, privacy preserving solutions for inter-vehicle communications. Security techniques for intra-vehicle communications.*


**Esame finale**: Sulla base delle nozioni apprese durante il seminario, verrà richiesto agli studenti di redigere una relazione di approfondimento tecnico su un argomento del seminario, preferibilmente in lingua inglese. La relazione proposta dallo studente potrà essere oggetto di un'eventuale discussione orale **in modalità on-line via TEAMS**. Il conseguimento dell'idoneità permette l'acquisizione di 3 CFU di tipologia F.

*Final exam: On the basis of the notions learned during the seminar, students will be asked to write a technical in-depth report on a topic of the seminar, preferably in English. The report proposed by the student may be the subject of an oral discussion **on-line via TEAMS**. The achievement of the eligibility allows the acquisition of 3 CFU of type F.*


**Iscrizioni**: Gli studenti interessati possono inviare domanda di iscrizione fino al **22 Aprile 2026** all'Ing. Marco Pugliese, tramite e-mail all'indirizzo **marco.pugliese@univaq.it,** indicando come oggetto "Seminario Professionalizzante e di Specializzazione su Sicurezza nelle WSN e nelle VANET", con nome e cognome, numero di matricola, corso di laurea, anno di iscrizione, CFU acquisiti, indirizzo e-mail.

*Registration: Interested students can send an application for registration until 22nd April 2026 to ing. Marco Pugliese, by e-mail to **marco.pugliese@univaq.it**, indicating as subject "Seminario Professionalizzante e di Specializzazione su Sicurezza nelle WSN e nelle VANET", with name and surname, matriculation number, degree course , year of enrollment, earned credits, e-mail address.*