Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Università degli Studi dell'Aquila

Seminario Professionalizzante e di Specializzazione

A.A. 2020-21

su:

Sicurezza nelle Reti Radio di Sensori e Veicolari

Wireless Sensor and Vehicular Networks Security

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., Senior Security Manager UNI 10459:2017

Calendario e modalità di erogazione: Il seminario avrà luogo tra il **7 Maggio e il 18 Giugno 2021 in modalità on-line via TEAMS**.

***Schedule and delivery:** The seminar will take place between 7 May and 18 June 2021 on-line via TEAMS.*

Programma del Seminario / *Course Program*

Part I. Generalities on WSN and VANET Security (12 hours)

Day 1. Lecture I.1 WSN Architectures and Application Scenarios (4h): the position of WSN within wireless networks: ad-hoc networks (MANET, VANET) vs. WSN. Characterization of WSN, design constraints, application scenarios and current standard architectures. WSN security requirements are introduced and defined per application class.

***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.*

Day. 2 Lecture I.2 VANET Architectures and Application Scenarios (4h): the position of VANET within wireless networks, characterization of VANET, communication models (V2V, V2I), smart vehicles, application scenarios and current standard architectures are introduced.

***TOPICS**: 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 The Framework of Security Management (1h): the standard ISO 31000 Risk Management framework is briefly introduced. The path from risk to security management is delineated and the Reference Security Model is 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.

TOPICS*:. The framework of Security Management. From Risk to Security Management. Reference Security Model: Security Metrics, Timing constraints, the "Required Security Level" vs. the "Offered Security Level". Reference technical standards.*

Day 3. Lecture I.4 Cyber Attacks (3h): 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. Techniques for WSN and VANET Security (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 WSN Security. TAKS/ECTAKS scheme (2h): 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.

***TOPICS**: The TAKS / ECTAKS Scheme. 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.*

Day 6. Lecture II.4 WSN Security. WIDS/MVET scheme (2h): 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**: 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.5 VANET Security and Privacy (4h): security and privacy requirements, adversary model, specific threat classification, security architectures and techniques are introduced.

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