Corso Professionalizzante e di Specializzazione

Sicurezza nelle Reti di Sensori Wireless / *Wireless Sensor Networks Security*

Destinatari: Studenti dei corsi di laurea magistrale in Ingegneria delle Telecomunicazioni, Ingegneria Informatica e Automatica, Ingegneria Elettronica, 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 corso è adatto anche per gli studenti del corso di dottorato in Ingegneria e Scienze dell'Informazione.

Durata: 28 ore (4 ore al giorno per 7 giorni)

Docente: Dott. Ing. Marco Pugliese

Programma del Corso / *Course Program*

Parte I. Generalità sulla Sicurezza nelle Reti Radio di Sensori (Sicurezza WSN) (8 ore) / *Part I. Generalities on Wireless Sensor Network Security (WSN Security) (8 hours)*

Giorno 1. Lezione 1.1. Architetture WSN e Scenari Applicativi (4 ore/ hours): descrizione delle peculiarità delle Reti Radio di Sensori (WSN), dei vincoli progettuali, degli scenari applicativi e delle architetture standard. Viene introdotto il modello di riferimento della sicurezza e vengono definiti i requisiti di sicurezza per classe di applicazioni.
Day 1. Lecture 1.1. WSN Architectures and Application Scenarios (4 hours)*: description of Wireless Sensor Networks (WSN) features, design constraints, application scenarios and current standard architectures. The reference security model is introduced and the security requirements per application class are defined.*
Argomenti trattati / *Specific Topics:*

1.1.1 Generalità sulle WSN / *Generalities on WSN*
1.1.2 Vincoli Progettuali / *Design Constraints*
1.1.3 Architetture di Riferimento / *Reference Architectures*
1.1.4 Modello di Riferimento della Sicurezza: Sicurezza Passiva e Attiva / *Reference Security Model: Passive vs. Active Security*

Giorno 2. Lezione 1.2. Attacchi "Cyber" (4 ore): viene presentata la classificazione degli attaccanti "cyber" e la descrizione dei principali attacchi alle WSN.
Day 2. Lecture 1.2. Cyber Attacks (4 hours)*: classification of cyber attackers and the description of the most common and known cyber attacks against a WSN are presented.*
Argomenti trattati / *Specific Topics:*

1.2.1 Attaccanti "Cyber" / *Cyber Attackers*
1.2.2 Attacchi "Cyber" / *Cyber Attacks*

Parte II. Tecniche di Sicurezza nelle WSN (16 ore) / Part II. Techniques for WSN Security (16 hours)

Giorno 3. Lezione 2.1. Funzioni di Sicurezza Passiva (4 ore): vengono introdotte le funzioni di sicurezza passiva, ovvero quelle tecniche di sicurezza esclusivamente difensive che non restituiscono informazioni di riscontro utili per applicare contromisure o su diagnostica di sistema. Tipicamente sono funzioni riconducibili a schemi crittografici e di autenticazione dati.

Day 3. Lecture 2.1. Passive Security Functions (4 hours)*: passive security functions, i.e. purely defensive techniques which do not return any feedback information for the application of countermeasures and system diagnostics, are introduced. Typically such security functions deal with cryptography and data authentication.*

Argomenti trattati / *SpecificTopics:*

2.1.1 Elementi di Formalismo Matematico / *Mathematical background*

2.1.2 Tecniche di Sicurezza Passiva / *Passive Security Techniques*

Giorno 4. Lezione 2.2. Il Progetto WINSOME: lo Schema TAKS (4 ore): il progetto interno al Centro di Eccellenza DEWS e denominato "WINSOME" (*Wireless Sensor Network Secure System for Structural Integrity Monitoring and Alerting*) viene descritto nelle sue linee funzionali: questa piattaforma integra le primitive di sicurezza verso le applicazioni attraverso specifici "middleware". Attualmente la piattaforma "WINSOME" implementa lo schema TAKS (*Topology Authenticated Key Scheme*), tecnica di sicurezza passiva sviluppata presso i laboratori DEWS. E' prevista una sessione sperimentale di applicazione dello schema TAKS su rete IEEE 802.15.4.

Day 4. Lecture 2.2. The WINSOME Project: the TAKS scheme (4 hours): *the DEWS "WINSOME" project (Wireless Sensor Network Secure System for Structural Integrity Monitoring and Alerting) is described: the related platform embeds security functions to be provided at the application layer through a specific middleware. Currently the "WINSOME" platform implements TAKS (Topology Authenticated Key Scheme), the passive security technique developed at DEWS labs. An experimental session dealing with TAKS over IEEE 802.15.4 networks is included.*

Argomenti trattati / *SpecificTopics:*

2.2.1 Lo Schema TAKS / *TAKS scheme*

2.2.2 Sessione Sperimentale di TAKS su rete IEEE 802.1.5.4 / *Experimental Session of TAKS over IEEE 802.15.4 WPANs*

Giorno 5. Lezione 2.3. Funzioni di Sicurezza Attiva (4 ore): vengono introdotte le funzioni di sicurezza attiva che, contrariamente alle tecniche passive, restituiscono informazioni di riscontro utili per applicare contromisure o su diagnostica di sistema. Tipicamente sono funzioni riconducibili a stimatori del comportamento di sistemi dinamici e rivelatori di anomalie.

Day 5. Lecture 2.3. Active Security Functions (4 hours)*: active security functions, i.e. security techniques which return feedback information that are useful for the application of countermeasures and system diagnostics, are introduced. Typically such security functions deal with system behavior estimators and anomaly detectors.*

Argomenti trattati / *SpecificTopics:*

2.3.1 Elementi di Formalismo Matematico / *Mathematical background*

2.3.2 Tecniche di Sicurezza Attiva / *Active Security Techniques*

Giorno 6. Lezione 2.4. Il Progetto WINSOME: lo Schema WIDS (4 ore): attualmente la piattaforma "WINSOME" implementa lo schema WIDS (*WPM-based Intrusion Detection Scheme*), tecnica di sicurezza attiva sviluppata presso i laboratori DEWS. E' prevista una sessione sperimentale di applicazione dello schema WIDS su rete IEEE 802.15.4.

Day 6. Lecture 2.4. The WINSOME Project: the WIDS scheme (4 hours): *Currently the "WINSOME" platform implements WIDS (WPM-based Intrusion Detection Scheme), the active security technique developed at DEWS labs. An experimental session dealing with WIDS over IEEE 802.15.4 networks is included.*

Argomenti trattati / *SpecificTopics:*

2.4.1 Lo Schema WIDS / *WIDS Scheme*

2.4.2 Sessione Sperimentale di WIDS su rete IEEE 802.1.5.4 / *Experimental Session of WIDS over IEEE 802.15.4 WPANs*

Parte III. Attività di Ricerca sulla Sicurezza nelle WSN (4 ore) / *Part III. Research Activity on WSN Security (4 hours)*

Giorno 7. Lezione 3.1. Avanzamenti presso il Centro d'Eccellenza DEWS (4 ore): vengono presentati i recenti avanzamenti nel campo della ricerca sulla Sicurezza WSN raggiunti presso i laboratori de Centro DEWS.
Day 7. Lecture 3.1. Recent Achievements at the Center of Excellence DEWS (4 hours): *recent research issues on WSN Security achieved at DEWS labs are presented.*
Argomenti trattati / *SpecificTopics:*

3.1.1 Estensioni dello Schema TAKS: TAKS2/ECTAKS / *Extensions of TAKS: TAKS2/ECTAKS*

3.1.2 Rivelazione di Anomalie in Applicazioni di Monitoraggio su WSN: MVET (*Mean-Variance Estimation Technique*) / *Anomaly Detection for Monitoring Applications over WSN: MVET (Mean-Variance Estimation Technique)*

Calendario e Sede: Il corso avrà luogo tra fine Giugno e Settembre 2016 in date da definire, tenendo anche conto delle esigenze degli studenti interessati, presso le aule del Dipartimento DISIM nel Polo di Coppito.

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

Iscrizioni: Gli studenti interessati possono inviare domanda di iscrizione a partire dal 13-06-2016 ed entro il 20-06-2016 all'Ing. Marco Pugliese, tramite e-mail all'indirizzo marco.pugliese@ieee.org, indicando come oggetto "Corso Professionalizzante e di Specializzazione su Sicurezza nelle WSN", con nome e cognome, numero di matricola, corso di laurea, anno di iscrizione, CFU acquisiti, indirizzo e-mail e numero di cellulare.