Caracterização da Unidade Curricular / Characterization of the Curricular Unit

Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Segurança em IoT / IoT Security
Área científica da UC / CU Scientific Area: Ciências Informáticas / Computer Science
Semestre / Semester: 2º
Número de créditos ECTS / Number of ECTS credits: 6
Carga horária por tipologia de horas / Workload by type of hours: TP: 22,5; PL: 22,5; OT: 6; O: 9
Carga letiva semanal / Weekly letive charge: 3h

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

- Conhecer e tipificar as especificidades das ameaças e vulnerabilidades nas redes IoT.
- Estudo e teste das ferramentas de auditoria à segurança.
- Estudo da estratégia de implementação de políticas de segurança na organização.

Intended learning outcomes (knowledge, skills and competences to be developed by the students):

- Know and typify the specifics of threats and vulnerabilities in IoT networks.
- Study and test of security audit tools.
- Study of the implementation strategy of Security Policies in the organization.

Conteúdos programáticos:

1. Modelos de dados em sistemas IoT

1.1. Ecossistema no IoT
1.2. Arquitetura de sensores, atuadores, dispositivos e Gateway
1.3. Protocolos de comunicação
1.4. Edge driven distributed IoT versus vs Cloud driven central IoT
1.5. Camadas de gestão em sistemas IoT
1.6. Soluções AWS, Microsoft Azure e outras
1.7. Protocolos populares: Zigbee / NB-IoT / 5G / LORA / Witespec

2. Risco e Segurança em sistemas IoT

2.1. Implementação ao nível do firmware
2.2. Segurança ao nível dos protocolos de comunicação da camada de transporte: NB-IoT, 4G, 5G, LORA, Zigbee etc.
2.3. Segurança ao nível dos protocolos da camada aplicacional: MQTT, Web Socket etc.
2.4. Estudo das vulnerabilidades:

2.4.1. API end points;
2.4.2. Gateway e Serviços;
2.4.3. Sensores;
2.4.4. Serviços de Cloud;
2.4.5. Camada de Aplicação;
2.4.6. Gestão da autenticação.

3. Casos de estudo de ataques à segurança do IoT

4. Estratégias para a implementação de uma politica de segurança da IoT numa organização

Syllabus:

1. Data models in IoT systems

1.1. Ecosystem in the IoT
1.2. Architecture of sensors, actuators, devices and Gateway
1.3. Communication protocols
1.4. Edge driven distributed IoT versus vs Cloud driven central IoT
1.5. Management layers in IoT systems
1.6. AWS, Microsoft Azure and others
1.7. Popular protocols: Zigbee / NB-IoT / 5G / LORA / Witespec

2. Risk and Security in IoT systems

2.1. Implementation at the firmware level
2.2. Security at the level of transport layer communication protocols: NB-IoT, 4G, 5G, LORA, Zigbee etc.
2.3. Security at the level of the application layer protococci: MQTT, Web Socket etc.
2.4. Study of vulnerabilities:
2.4.1. API end points;
2.4.2. Gateway and Services;
2.4.3. Sensors;
2.4.4. Cloud services;
2.4.5. Application layer;
2.4.6. Authentication management.

3. IoT security attack case studies

4. Strategies for implementing an IoT security policy in an organization