ipt Instituto Politécnico de Tomar

Escola Superior de Tecnologia de Tomar **Ano Letivo** 2017/2018

Mestrado em Engenharia Informática - Internet das Coisas

Mestrado, 2º Ciclo

Plano: Despacho n.º 7043/2016 - 27/05/2016

Ficha da Unidade Curricular: Segurança Aplicada à Internet das Coisas

ECTS: 7.5; Horas - Totais: 203.0, Contacto e Tipologia, TP:30.0; PL:30.0; OT:15.0; O:10.0;
Ano|Semestre: 1|S2; Ramo: Tronco comum;
Tipo: Obrigatória; Interação: ; Código: 39096
Área Científica: Engenharia de Software e Sistemas de Informação

Docente Responsável
Luís Miguel Lopes de Oliveira

Docente e horas de contacto
Luís Miguel Lopes de Oliveira
Professor Adjunto, TP: 30; PL: 30; OT: 15;

Objetivos de Aprendizagem

- Conhecer as principais ameaças à segurança das redes de sensores
- Conhecer os mecanismos de segurança mais adequados às redes de sensores.
- Conceber soluções de segurança para redes de sensores de acordo com o serviço a suportar
- Detectar e prevenir ataques de segurança
- Identificar os problemas éticos, sociais e legais relativos à utilização das redes de sensores

Conteúdos Programáticos

- Identificação das principais ameaças aos dados e aos sistemas em redes de sensores
- Primitivas de segurança baseadas em criptografia de chave simétrica e assimétrica
- A gestão de chaves criptográficas em redes de sensores
- Mecanismos de segurança para cada uma das camadas da pilha protocolar
- Agregação segura de dados
- Mecanismos de controlo de acesso e de detecção de intrusões
- Identificação dos problemas de segurança relativos aos aspectos sociais, éticos e legais

Metodologias de avaliação

A avaliação é composta por duas componentes: i) prática e ii) teórica. A componente prática é composta pela avaliação de trabalhos práticos realizados ao longo do semestre individualmente ou em grupo com o peso de 40%. A componente teórica é composta pela realização e defesa oral de um projecto, realizado maioritariamente fora das horas de

contacto, com o peso de 60%. As duas componentes têm a nota mínima de 9,5 valores. São obrigatórias todas as componentes de avaliação, assim como a defesa oral do projecto.

Software utilizado em aula
Cooja e Foren6.

Estágio
Não aplicável.

Bibliografia recomendada

1) L. Oliveira, J. Rodrigues, A. de Sousa, Lloret J, "Denial of service mitigation approach for IPv6-enabled smart object networks", Concurrency and Computation: Practice and Experience, vol. 25, no. 1, 2013, pp. 129–142.
2) X. Du, H. Chen, "Security in wireless sensor networks", IEEE Wirel. Commun. vol. 15, 2008, pp. 60–66.
3) Y. Yu, K. Li, W. Zhou, P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures". Journal of Network and Computer Applications, vol. 35, no 3, 2012, pp. 867-880.
4) T. Kavitha, D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey", J. Inf.Assur. Secur, vol. 5, 2010, pp. 31–44.
5) K. Pelechrinis, M. Iliofotou, V. Krishnamurthy, "Denial of service attacks in wireless networks: The Case of Jammers", IEEE Commun. Surv. Tut., vol 13, 2011, pp. 245–257.
6) J. Lee, K. Kapitanova, S. H. Son, "The price of security in wireless sensor networks. *Computer Networks*, vol. 54, no 17, 2010, pp. 2967-2978.

Língua de ensino
Português

Pré requisitos
Não aplicável.

Observações

Docente Responsável

Diretor de Curso, Comissão de Curso

Conselho Técnico-Científico