FICHA DE ASIGNATURA

Título: Entornos Ubicuos (SCADA, móviles) e IICC

Descripción:

En esta asignatura, el alumnado aprenderá nociones relacionadas con la computación ubicua, sistemas empotrados y formas de comunicación y almacenamiento, los riesgos asociados al uso de tecnologías y comunicaciones móviles, por la naturaleza de los datos y el uso que actualmente hacen los usuarios, y la metodología básica para recopilar, tratar y obtener datos de estos dispositivos móviles. También se darán a conocer los protocolos y componentes de los sistemas industriales, así como la convergencia entre IT y OT. Es importante también, la parte del temario centrada en la descripción y uso de los entornos SCADA, los riesgos asociados alrededor del IoT / IoE así como una introducción a las Smart Cities y sus retos de seguridad.

Carácter*:* Obligatoria

Créditos ECTS: 6

Contextualización:

Con la aparición de los smartphones la sociedad ha modificado sus hábitos con la finalidad de emplear los dispositivos móviles para todo menos para casi lo que realmente fueron diseñados, que es realizar llamadas. Debido a la cantidad de información, tanto personal como de negocio, que pueden almacenar dichos dispositivos se transforman en un activo en el que, la seguridad debe tenerse en consideración.

Durante el módulo se pretenderá mostrar cómo enfocar la seguridad a emplear sobre estos dispositivos, así como las amenazas a las que estamos expuestos en el día a día. Por otro lado, también se revisará cómo proceder frente a otro tipo de entornos poco comunes como son los sistemas industriales. Conoceremos los equipos que nos encontraremos en estos entornos, veremos cuáles son los protocolos de comunicaciones exclusivos de los fabricantes, y sus vectores de ataque ya que, cada vez más, estos entornos son un blanco para el ataque a infraestructuras críticas.

Modalidad*:* Online

Temario:

- Entornos ubicuos: definiciones, características y vulnerabilidades
- Comunicaciones y almacenamiento en computación ubicua: protocolos y encriptación, aplicaciones a IoT (Internet de las cosas) y Smart Cities
- Seguridad en dispositivos móviles: consideraciones de seguridad en redes 4G/5G, SMS y bluetooth
- Entornos industriales: protección de entornos empotrados (SCADA), seguridad en Industria 4.0
- Infraestructuras críticas en la Estrategia Nacional de Ciberseguridad: securización, gestión de riesgos y aplicación de la normativa nacional (PIC -Protección de las Infraestructuras Críticas)

Competencias Específicas:

CE8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.

CE10 - Identificar componentes y protocolos propios de la computación ubicua, sistemas empotrados y las formas de comunicación utilizados en entornos industriales e infraestructuras críticas.

CE11 - Aplicar las directrices generales en materia de Ciberseguridad en España derivadas de la Estrategia Nacional de Ciberseguridad y normativas implicadas.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	30	100%
Desarrollo de actividades del portafolio	24	0
Trabajo autónomo del alumno	96	0

Metodologías docentes

- Clases síncronas

- Vídeos con píldoras de conceptos teóricos

- Caso práctico

- Soporte a consultas

Sistema de Evaluación

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Examen	40%	60%
Trabajo individual	40%	60%

Normativa específica:

Bibliografía:

1. "Internet of Things (IoT) Broadband Internet Technical Advisory Group, Broadband Internet Technical Advisory Group, Nov 2016.

2. "IoT Security Guidance," Open Web Application Security Project (OWASP), May 2016.

3. "Strategic Principles for Securing the Internet of Things (IoT)," US Department of Homeland Security, Nov 2016.

4. "Security," OneM2M Technical Specification, Aug 2016.

5. "Security Solutions," OneM2M Technical Specification, Aug 2016.

6. "IoT Security Guidelines Overview Document," GSM Alliance, Feb 2016.

7. "IoT Security Guidelines for Service Ecosystems," GSM Alliance, Feb 2016.

8. "IoT Security Guidelines for Endpoint Ecosystems," GSM Alliance, Feb 2016.

9. "IoT Security Guidelines for Network Operators," GSM Alliance, Feb 2016.

10. "Establishing Principles for Internet of Things Security," IoT Security Foundation, undated.

11. "IoT Design Manifesto," www.iotmanifesto.com, May 2015.

12. "NYC Guidelines for the Internet of Things," City of New York, undated.

13. "IoT Security Compliance Framework," IoT Security Foundation, 2016.

14. "Principles, Practices and a Prescription for Responsible IoT and Embedded Systems Development," IoT IAP, Nov 2016.

15. "IoT Trust Framework," Online Trust Alliance, Jan 2017.

16. "Five Star Automotive Cyber Safety Framework," I am the Cavalry, Feb 2015.

17. "Hippocratic Oath for Connected Medical Devices," I am the Cavalry, Jan 2016.

18. "Industrial Internet of Things Volume G4: Security Framework," Industrial Internet Consortium, 2016.

19. "Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products," Cloud Security Alliance, 2016.

20. Mobile Application Security Testing Initiative “June 2016” - https://downloads.cloudsecurityalliance.org/assets/research/mobile/MAST_White_Paper.pdf

21. Damn Vulnerable iOS Application (DVIA). A vulnerable app to test your iOS Penetration Testing Skills http://damnvulnerableiosapp.com

22. Jordan Golson. Apples app store now has over 2 million apps. News article, June 2016. Retrieved December 2, 2016 from

http://www.theverge.com/2016/6/13/11922926/apple-apps-2-million-wwdc- 2016

23. Apple Inc. iOS security: White Paper, May 2016. Retrieved December 8, 2016 from https://www.apple.com/business/docs/iOS-Security-Guide.pdf.

24. Daniel A. Mayer and Drew Suarez. Faux disk encryption: realities of secure storage on mobile devices. White Paper, August 2015. Retrieved September 2, 2016 from https://www.blackhat.com/docs/us-15/materials/us-15-Mayer-Faux-Disk-Encryption-Realities-Of-Secure-Storage-On-Mobile-Devices-wp.pdf