19-20

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y CONTROL INDUSTRIAL

GUÍA DE ESTUDIO PÚBLICA



SEGURIDAD EN REDES INDUSTRIALES

CÓDIGO 28803241

UNED

19-20

SEGURIDAD EN REDES INDUSTRIALES

CÓDIGO 28803241

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

EQUIPO DOCENTE

HORARIO DE ATENCIÓN AL ESTUDIANTE

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

RESULTADOS DE APRENDIZAJE

CONTENIDOS

METODOLOGÍA

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

BIBLIOGRAFÍA COMPLEMENTARIA

RECURSOS DE APOYO Y WEBGRAFÍA

ADENDA AL SISTEMA DE EVALUACIÓN CON MOTIVO DE LA PANDEMIA COVID 19

Nombre de la asignatura	SEGURIDAD EN REDES INDUSTRIALES
Código	28803241
Curso académico	2019/2020
Título en que se imparte	MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y CONTROL INDUSTRIAL
Tipo	CONTENIDOS
Nº ETCS	5
Horas	125.0
Periodo	ANUAL
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Las redes industriales son, por un lado, vitales y, por otro, vulnerables, con consecuencias potencialmente devastadoras en el caso de un incidente exitoso de ciberseguridad. Los ataques están evolucionando rápidamente, haciéndose más inteligentes y adaptables, difíciles de detectar y muy persistentes. Se habla ya de sabotajes industriales y de problemas en infraestructuras críticas. La tendencia es muy preocupante e implica la necesidad de profesionales mejor preparados, tanto desde el punto de vista puramente industrial como desde el punto de vista de la seguridad en redes y sistemas

Siguiendo este razonamiento, se puede expresar como objetivo general de esta asignatura el ubicar correctamente la seguridad informática como uno de los puntos clave a tener en cuenta en cualquier proceso de análisis, diseño, desarrollo y mantenimiento de sistemas de comunicación industrial, enseñando a valorar la importancia que debe tener y qué consecuencias, siempre negativas, podría tener el no hacerlo así.

Se trata de conseguir que los estudiantes obtengan el conocimiento de los principales problemas de seguridad informática relacionados con las redes industriales, tanto los de naturaleza física como los de naturaleza lógica. Asimismo se busca que los estudiantes obtengan el conocimiento de las principales soluciones técnicas y organizativas que se utilizan hoy en día en la industria para tratar de minimizar los riesgos asociados a tales problemas de seguridad. Este conocimiento debe además estar especialmente orientado a aspectos prácticos, por lo que se debe plantear al estudiante aspectos prácticos ligados a los conocimientos citados.

Es muy importante señalar desde el principio la necesidad previa de conocimientos de redes de comunicación, tanto industriales como (especialmente) de redes IP, así como unos conocimientos básicos de los ataques más habituales a la seguridad de sistemas y redes IP, y de las principales soluciones a estos problemas. Los alumnos que carezcan de estos requisitos previos DEBEN cursar previamente la asignatura "Aplicaciones Industriales de las comunicaciones" (código 28803256) del mismo itinerario de "Ingeniería Telemática" del Máster

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Es muy importante señalar desde el principio la necesidad previa de conocimientos de redes de comunicación, tanto industriales como (especialmente) de redes IP, así como unos conocimientos básicos de los ataques más habituales a la seguridad de sistemas y redes IP, y de las principales soluciones a estos problemas. Los alumnos que carezcan de estos requisitos previos DEBEN cursar previamente la asignatura "Aplicaciones Industriales de las comunicaciones" (código 28803256) del mismo itinerario de "Ingeniería Telemática" del Máster.
Además, es necesario tener un buen conocimiento de inglés técnico que le permita leer y comprender la parte de la bibliografía que está en ese idioma.

EQUIPO DOCENTE

Nombre y Apellidos	GABRIEL DIAZ ORUETA (Coordinador de asignatura)
Correo Electrónico	gdiaz@ieec.uned.es
Teléfono	91398-8255
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA

Nombre y Apellidos	SERGIO MARTIN GUTIERREZ
Correo Electrónico	smartin@ieec.uned.es
Teléfono	91398-7623
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA

Nombre y Apellidos	ELIO SAN CRISTOBAL RUIZ
Correo Electrónico	elio@ieec.uned.es
Teléfono	91398-9381
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	INGENIERÍA ELÉCTRICA, ELECTRÓNICA, CONTROL, TELEMÁTICA Y QUÍMICA APLICADA A LA INGENIERÍA

HORARIO DE ATENCIÓN AL ESTUDIANTE

La tutorización de los alumnos se llevará a cabo:
1- A través de la plataforma de e-Learning aLF
2- Por correo electrónico con el equipo docente:
Gabriel Díaz Orueta - gdiaz@ieec.uned.es
Sergio Martín Gutiérrez - smartin@ieec.uned.es
Manuel Castro Gil - mcastro@ieec.uned.es
3- En el horario de guardia, los martes de 14:00 a 18:00 en el Telf 91-3988255

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

Competencias Básicas:

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias Generales:

CG3 - Ser capaz de comunicar de forma oral y escrita de conocimientos en español como lengua propia

CG4 - Ser capaz de comunicar de forma oral y escrita de conocimientos en inglés como lengua extranjera

CG5 - Ser capaz de tomar decisiones

CG6 - Saber aplicar los conocimientos adquiridos

CG7 - Adquirir habilidades en investigación

CG8 - Adquirir habilidades para la creatividad

CG9 - Ser capar de realizar razonamientos críticos

CG10 - Adquirir la capacidad de comunicación

Competencias Específicas:

CE2 - Ser capaz de analizar la información científica y técnica

CE3 - Conocer los métodos y técnicas de investigación científica y desarrollo tecnológico

CE4 - Adquirir destrezas en la aplicación de técnicas de investigación científica y desarrollo tecnológico

CE5 - Adquirir destrezas en la búsqueda y gestión bibliográfica y documental

CE6 - Ser capaz de planificar actividades de investigación

CE7 - Ser capar de realizar razonamientos críticos en el ámbito científico y tecnológico

CE8 - Adquirir habilidades para la elaboración y exposición de informes científicos

RESULTADOS DE APRENDIZAJE

Los resultados del aprendizaje que debe alcanzar el estudiante son:

- Identificar los diferentes tipos de ataques a redes, sistemas y datos en una organización, así como las soluciones más habituales empleadas para tratar de soslayarlos. Estudiar los diferentes protocolos de uso posible en las redes de comunicación estudiadas.
- Identificar las herramientas de seguridad más habituales como cortafuegos, sistemas de detección de intrusiones (IDS) o aplicaciones de análisis de vulnerabilidades. Entender para qué se deben aplicar y en qué casos.
- Entender, desde un punto de vista práctico, las diferentes aplicaciones de la criptografía a la seguridad informática, tanto en protocolos como en sistemas criptográficos, de manera que se comprenda cómo usar la firma digital o cómo se configura una red privada virtual.
- Identificar cuáles son los principales problemas de seguridad en redes industriales (DCS, SCADA, etc.)
- Ser capaz de asesorar sobre qué soluciones de seguridad dar a problemas concretos de seguridad en redes industriales
- Ser capaz de explicar las principales motivaciones de los ataques a redes industriales, así como las consecuencias de los mismos
- Ser capaz de hacer un análisis de riesgos en un sistema de comunicaciones industriales
- Identificar, y entender cómo funcionan, las soluciones más habituales a los problemas de seguridad en redes industriales: zonas, segmentaciones, conduits, etc.
- Ser capaz de aplicar una política de monitorización de la seguridad en redes industriales.

CONTENIDOS

TEMA 1. Revisión de aspectos importantes generales de seguridad de redes IP

Se trata en este capítulo de hacer una revisión general de los aspectos más significativos de seguridad en los elementos típicos existentes en cualquier red IP actual, tanto los físicos como los lógicos. También se estudiará una taxonomía común de tipos de ataques, su importancia y qué defensas son las más habituales. Finalmente es muy importante fijar la relevancia de las políticas de seguridad como verdadero “cerebro” que marca cómo fijar todas las defensas. En este sentido es fundamental conocer, al menos a nivel básico, los estándares y la legislación relacionados con la seguridad.

Contenido:

1.1 Seguridad en elementos físicos y software

1.2 Métodos de ataque a equipos y redes

1.3 Defensas básicas antes ataques

1.4 Política de seguridad y aspectos relacionados

TEMA 2. Revisión de herramientas de seguridad no criptográficas

Se hará una revisión de las principales herramientas de seguridad en redes que no hacen uso, como parte primordial de su trabajo, de la criptografía. En este sentido se estudiarán los cortafuegos, sus puntos fuertes y débiles y alguno de los más utilizados. Igualmente debe conocerse en qué consiste el trabajo de los sistemas de detección de intrusiones (IDS en sus siglas en inglés) y en qué pueden ayudar dentro de una política de seguridad correcta. Finalmente se debe conocer los posibles usos de los analizadores de vulnerabilidades de seguridad.

Contenido:

2.1 Cortafuegos

2.2 Sistemas de detección de intrusiones

2.3 Analizadores de vulnerabilidades

TEMA 3. Revisión de criptografía aplicada

Existe la opinión generalizada de que la criptografía es una disciplina realmente difícil, sólo al alcance de personas con muchos conocimientos matemáticos. En realidad para su uso en seguridad informática no es tan necesario conocer al detalle el funcionamiento de cada uno de los algoritmos criptográficos más potentes como conocer para qué sirven y cómo podemos usarlos. Este es el objetivo esencial de este tema.

Para conseguir la competencia general de poder hacer un análisis de la seguridad de datos, sistemas y comunicaciones, y poder proponer soluciones básicas criptográficas, consistentes con una política de seguridad correcta y que cumpla la legislación pertinente, se debe alcanzar un conocimiento de cuáles son los principales problemas de seguridad en los que la criptografía puede ayudar (confidencialidad, integridad, autenticación y no repudio) y cuáles son los principales tipos de algoritmos criptográficos que se utilizan para conseguirlo (criptografía simétrica, asimétrica y funciones hash), describiendo alguno de los más significativos: DES (Data Encryption Standard), SHA (Secure Hash Algorithm) y RSA (Rivest Shamir Addleman).

Se debe entender también cómo este tipo de algoritmos permiten crear los sistemas de firma digital, qué son los certificados digitales X.509, las autoridades de certificación y qué papel juegan en el cada vez más relevante asunto de la autenticación.

Se estudiará también cuáles son y cómo se utilizan los principales protocolos criptográficos construidos sobre los anteriores (SSL, PGP y el conjunto de protocolos IPSec) así como las arquitecturas de seguridad de comercio electrónico construidas sobre ellos.

Contenido:

3.1 Algoritmos, protocolos y sistemas criptográficos
3.2 Sistemas de clave privada, de clave pública y funciones hash
3.3 Certificación digital, PKI y firma digital
3.4 Protocolos más habituales: SSL, IPSec y PGP

TEMA 4. Introducción a los problemas de seguridad en redes industriales

En este capítulo se definirá la terminología del resto de la asignatura, aclarando términos como ICS, DCS, SCADA, red industrial, protocolos industriales, zonas, etc. Se discutirá el alcance de las recomendaciones de seguridad industrial más comunes, cómo se han alcanzado y qué éxito han tenido hasta ahora.
Igualmente se discutirá algunos de los casos más peligrosos sucedidos hasta ahora, analizando cómo han ido evolucionando las amenazas y cuál es la situación actual.
Contenido:
4.1 Terminología de seguridad en redes industriales
4.2 Sistemas DCS, SCADA y protocolos y redes industriales
4.3 Recomendaciones habituales de seguridad industrial
4.4 Ideas asumidas falsas sobre seguridad en redes industriales
4.5 La importancia de la seguridad en redes industriales
4.6 Evolución de las amenazas informáticas en redes industriales

TEMA 5. Diseño, arquitectura de red y protocolos en redes industriales

En una primera parte se estudiará los activos del sistema, qué se debe conocer de cómo funcionan los sistemas de control industrial y también cuáles son las principales operaciones de sistema.
Se debe estudiar, con cierto detalle, cuáles son las topologías y esquemas de segmentación más comunes en las redes industriales, cómo se integran las redes inalámbricas y el acceso remoto. Se debe conocer también las particularidades de rendimiento de las redes industriales, como el tratamiento de la latencia y el jitter.
Igualmente se debe conocer, dentro del contexto de esta asignatura, las principales características de algunos de los protocolos más típicos de este entorno.
Contenido:
5.1 Los activos de sistema y las operaciones de sistema en redes industriales
5.2 Aspectos generales de diseño y arquitectura de red
5.3 Consideraciones de rendimiento y de seguridad
5.4 Protocolos Fieldbus, protocolos backend y simuladores de protocolos

TEMA 6. Principales problemas de seguridad en sistemas de control industrial

Se presentan primero las principales motivaciones y las posibles consecuencias de estos incidentes de seguridad. Se muestran cuáles son los objetivos de ataque más comunes, así como los métodos de ataque más comunes, para acabar analizando con detalle algunos de los incidentes más graves sucedidos.
Contenido:
6.1 Motivaciones y consecuencias
6.2 Los objetivos industriales más comunes
6.3 Métodos de ataque más comunes
6.4 Ejemplos de amenazas reales que tuvieron éxito

TEMA 7. Evaluaciones de vulnerabilidades y riesgos

Después de establecer las razones por las que la gestión de riesgos es la base para una buena ciberseguridad, se presentan las principales metodologías de evaluación de riesgos en el sector industrial.
A continuación se identifican las amenazas principales, así como las vulnerabilidades más típicas, para acabar con una clasificación general de los riesgos.

Contenido:
7.1 Gestión de riesgos y metodologías de evaluación en sistemas de control industrial
7.2 Identificación de amenazas
7.3 Identificación de vulnerabilidades
7.4 Clasificación de riesgos

TEMA 8. Introducción a las defensas básicas en redes industriales

Se presenta en este tema la definición de zonas de seguridad y conduits, ayudando a entender cómo clasificarlas y separarlas en redes industriales.Igualmente se muestra cómo segmentar redes para implantar controles de seguridad de redes, de host y de acceso. Finalmente se hace una introducción a la detección de anomalías y amenazas.
Contenido:
8.1 Zonas y conduits de seguridad
8.2 Separaciones recomendadas de zonas
8.3 Segmentación de redes
8.4 Implantación de controles de seguridad de acceso, de host y de red
8.5 Detección de anomalías y de amenazas

TEMA 9. Monitorización de la seguridad en redes industriales

Se empieza por analizar qué es necesario monitorizar. Se presentan procedimientos para monitorizar zonas de seguridad con éxito. Igualmente se muestra como hacer una gestión segura de la información obtenida, así como de los logs.
Contenido:
9.1 Determinación de activos y eventos a monitorizar
9.2 Monitorización de zonas de seguridad
9.3 Gestión de la información y de logs

METODOLOGÍA

Conforme al espíritu del Espacio Europeo de Educación Superior (EEES), el trabajo en la asignatura y el proceso de evaluación es continuo a lo largo del curso y está de acuerdo con la carga de trabajo y organización del contenido dado en los apartados anteriores.
El estudio y preparación de los contenidos debe ser continuo desde el inicio del curso y, como se ha indicado, se debe seguir el orden dado a los temas. La orientación de la carga de trabajo que le debe suponer cada tema, que aparece en la Guía de Estudio en el curso virtual, le permitirá distribuir el estudio a lo largo del curso entre los meses de octubre y mayo.
El estudiante deberá realizar una serie de ejercicios que se propondrán durante el curso y participar en los debates que se propongan. Deberá realizar asimismo un trabajo final sobre una serie de temas que se propondrán en el curso virtual.
Esta asignatura NO tiene Prueba Presencial asociada, estando la evaluación completamente basada en los procedimientos comentados.

SISTEMA DE EVALUACIÓN

TIPO DE PRIMERA PRUEBA PRESENCIAL

Tipo de examen: No hay prueba presencial

TIPO DE SEGUNDA PRUEBA PRESENCIAL

Tipo de examen2: No hay prueba presencial

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad: No

Descripción

Es un **Trabajo final** de la asignatura, en el que el estudiante deberá seleccionar entre una serie de temas (o proponer uno propio) y darle formato de trabajo de investigación. El equipo docente fijará las bases mínimas del mismo.

Criterios de evaluación

Se evaluará la capacidad de exposición, estructuración, sintesis, investigación, en un tema relacionado directamente con las últimas aproximaciones de alguna de las materias de la asignatura

Ponderación de la prueba presencial y/o los trabajos en la nota final	NO hay prueba presencial. El trabajo Final pondera como el 50% de la nota final de la asignatura
Fecha aproximada de entrega	Hacia mediados de junio
Comentarios y observaciones	

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	Si,PEC no presencial

Descripción

Serán dos ejercicios breves de realización de cuestiones prácticas relacionadas con el análisis de seguridad en redes industriales. Tendrán una parte de exposición y otra de análisis

Criterios de evaluación

Se evaluarán de 0 a 10 y, entre las dos, tendrán un peso del 35% de la nota final de la asignatura

Ponderación de la PEC en la nota final	35% entre las dos
Fecha aproximada de entrega	La primera a finales de enero, la segunda a finales de marzo
Comentarios y observaciones	

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?	Si,no presencial

Descripción

Se organizarán al menos dos **debates en foros** ad-hoc para aclarar una serie de conceptos y prácticas importantes de la asignatura

Criterios de evaluación

Participación e interés mostrado

Ponderación en la nota final	15% de la nota final
Fecha aproximada de entrega	Principios de diciembre, principios de febrero
Comentarios y observaciones	

¿CÓMO SE OBTIENE LA NOTA FINAL?

La nota final de la asignatura se compone de la siguiente forma:

- un 35% de los ejercicios propuestos,

- un 15% por la participación en los debates y, en general, en los foros y

- un 50% asociado a la nota del trabajo final.

En cualquier caso, para aprobar la asignatura el estudiante deberá realizar correctamente al menos un ejercicio, participar suficientemente en los debates y aprobar el trabajo final

BIBLIOGRAFÍA BÁSICA

ISBN(13):9780124201149
Título:INDUSTRIAL NETWORK SECURITY (Segunda)
Autor/es:Joel Thomas Langill ; Eric D. Knapp ;
Editorial:SYNGRESS

ISBN(13):9788436267167
Título:PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES (2013)
Autor/es:Castro Gil, Manuel Alonso ; Ignacio Alzórriz ; San Cristóbal Ruiz, Elio ; Díaz Orueta, Gabriel ;
Editorial:UN.E.D.

Para preparar y estudiar el contenido de cada uno de los temas, le indicamosla bibliografía que debe utilizar.
Esta bibliografía básica es la que usted debe conseguir y consultar para el estudio de cada tema, ya que es a partir de ella sobre la que hemos diseñado y desarrollado esta asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

"*The Code Book, the Secret History of Codes and Code Breaking*", S. Singh, 2000, version interactiva disponible desde el curso virtual de la asignatura.
Es un gran clásico como introducción a la criptografía aplicada. Con un lenguaje sencillo y muchos ejemplos prácticos presenta al lector desde la historia de la criptografía hasta los últimos avances en criptografía cuántica. Desde hace ya varios años Singh permite distribuir, sólo con intenciones didácticas, la versión interactiva de la que se dispone en el curso virtual. Es importante señalar, no obstante, que este libro cubriría un curso entero de 8 meses sólo dedicado a criptografía.
Además el estudiante dispondrá de artículos y trabajos varios sobre los diferentes contenidos de seguridad en redes industriales, que intentaremos ir haciendo accesibles en el curso virtual de la asignatura.

RECURSOS DE APOYO Y WEBGRAFÍA

Curso Virtual
La plataforma aLF de e-Learning de la UNED proporcionará el adecuado interfaz de interacción entre el alumno y sus profesores. aLF es una plataforma de e-Learning y colaboración que permite impartir y recibir formación, gestionar y compartir documentos, crear y participar en comunidades temáticas, así como realizar proyectos online. Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como los estudiantes, encuentren la manera de compaginar tanto el trabajo individual como el aprendizaje cooperativo.

Videoconferencia

La videoconferencia se contempla como una posibilidad de comunicación bidireccional síncrona con los estudiantes, tal y como se recoge en el modelo metodológico de educación distancia propio de la UNED. La realización de videoconferencias se anunciara a los estudiantes con antelación suficiente en el curso virtual de la asignatura.

ADENDA AL SISTEMA DE EVALUACIÓN CON MOTIVO DE LA PANDEMIA COVID 19

https://app.uned.es/evacaldos/asignatura/adendasig/28803241

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.