ESPECIAL

"Radio Security"

DE Tecnología & Sentido Común

ESPECIAL

AGOSTO 2024

ESPECIAL

"Radio Security"

DE Tecnología & Sentido Común

EQUIPO TYSC
Javier Peris - El Gobernauta
Manuel Serrat - Futuro y Seguridad
Nacho Alamillo - Tecnoregulación en Prospectiva
Miguel Angel Arroyo - Hack & News
Juan Carlos Muria - Diario de una Tortuga Ninja
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Marcos Navarro - Ai Robot
Víctor Almonacid - La Nueva Administracion
Jesús López Peláz - Consejo de Amigo
Renato Aquilino - Marcos y Normas
Alex Aliaga - Radio Security
Marta Martín - Mentes Divergentes

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
soluciones@businessandcompany.com

EDITA
Business, Technology & Best Practices, S.L.
Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://tecnologiaysentidocomun.com
soluciones@businessandcompany.com

Alex Aliaga

Profesional Especializado en la Gestión de la seguridad, tanto desde el punto de vista tecnológico como desde el punto de vista estratégico. Con más de 20 años de experiencia en el sector, ha trabajado tanto en España como en otros países ayudando a las empresas en la gestión, y mitigación de los riesgos TIC, aplicando siempre las mejores prácticas y controles para aportar siempre la protección adecuada. Es colaborador habitual en diversos congresos de seguridad, así como, medios de comunicación, radio y prensa escrita, a nivel internacional donde sus publicaciones técnicas y estratégicas son muy apreciadas. Puede hablarte de ciberseguridad en 3 idiomas

ISSN 2951-8180

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Sesión de Formación y Certificación en:

Sistema de Gestión de la Inteligencia Artificial

Director Académico:

Javier Peris

- Duración 5 horas
- Sesión única
- Miércoles de 16:00 a 21:00 horas
- En Directo y en Remoto
- Basado en la norma ISO 42001:2023
- Examen de Certificación Incluido
- Certificación ISO 42001 Leader
- Plazas limitadas

MPPM® MGEIT® eGob®

Miércoles 10 de Abril

+ 34 96 109 44 44
campus@escueladegobierno.es

ESPECIAL AGOSTO 2024

índice

DE CONTENIDOS

https://tecnologiaysentidocomun.com

índice

#TYSC

Premios recibidos

Premio 2016 a la Difusión de los Valores de la Gestión y Gobierno TI

El Foro de Profesionales de la Gestión del Servicio en España itSMF otorga a «Tecnología y Sentido Común» el Galardón 2016 a la Difusión de los Valores de la Gestión y Gobierno de Tecnologías de la Información.

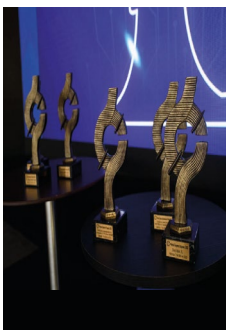
itSMF ESPAÑA

Premio Medio de Comunicación 2018 de la Asociación Profesional Española de Privacidad

La Junta Directiva de la Asociación Profesional Española de Privacidad durante su VI Congreso Nacional de Privacidad APEP celebrado en Madrid otorga el Premio Medio de Comunicación 2018 a Tecnología y Sentido Común #TYSC

apep

Tecnología y Sentido Común "Premio Sapiens" Medio de Comunicación 2022



El Colegio Oficial de Ingeniería Informática de la Comunidad Valenciana entregó el Premio Sapiens Medio de Comunicación 2022 a nuestra Revista "Tecnología y Sentido Común #TYC". El Colegio Oficial de Ingeniería Informática de la Comuni- dad Valenciana COIICV alabó tanto la gran labor de difusión que viene realización Tecnología y Sentido Común desde hace siete temporadas como su capacidad de adaptación y resiliencia adaptándose a nuevos formatos con los que continuar en su labor de evangelización en Buenas Prácticas al conjunto de los profesionales a pesar de la alerta sanitaria con nuevos formatos que partiendo de un programa de Radio y Podcast han permitido seguir llevando su mensajes a través de la Revista Mensual, o el informativo televisivo "El Semanal" de Tecnología y Sentido Común.

COLEGIO OFICIAL DE INGENIERÍA INFORMÁTICA DE LA COMUNITAT VALENCIANA

Premio 2022 ESET al Periodismo y Divulgación eb Seguridad Informática

VI Premios ESET Periodis- mo y Divulgación: Tecnología y Sentido Común Premiada en la Categoría Blogs por el Articulo de Ricard Martínez "Seguridad en el Smartphone".
Los Premios ESET apuestan por la educación y la concienciación de la sociedad en materia de ciberseguridad, y los medios de comunicación son esenciales en este cometido.
Los periodistas y divulgadores son fundamentales para difundir el conocimiento necesario que permita a los usuarios disfrutar de la tecnología de una manera más segura.
Estos VI Premios ESET pretenden fomentar la divulgación de la ciberseguridad.

eset

Agradecimiento de la Asociación Valenciana de Informática Sanitaria AVISA

La Asociación Valenciana de Informática Sanitaria AVISA durante las XIV Jornadas Técnicas que bajo el título "20 Años Implantando TIC en Sanidad" se celebraron en Benidorm en febrero de 2024 hizo entrega de su agradecimiento a Tecnología y Sentido Común por su apoyo y visibilidad a la profesión.

AVIS@ ASOCIACIÓN VALENCIANA DE INFORMÁTICA SANITARIA

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión Documental y Gestión del Conocimiento

ISO 30301:2021
ISO 30401:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 30300 Leader
- Certificación ISO 30401 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

Seguridad de las comunicaciones inalámbricas

Hoy en día, vivimos en un mundo cada vez más interconectado donde, las tecnologías inalámbricas empiezan a cobrar un gran protagonismo respecto al uso de comunicaciones cableadas. Cada vez, podemos ver más protocolos de comunicaciones inalámbricas, y prácticamente, siempre que sea posible, huimos de los cables para hacernos la vida más sencilla.

Estos nuevos escenarios tecnológicos, entre otras cosas, conllevan muchos riesgos y amenazas que deben gestionarse para evitar un impacto negativo en las infraestructuras que cuentan con este tipo de tecnologías. Por esta razón, gestionar adecuadamente la ciberseguridad de las comunicaciones inalámbricas se ha convertido en uno de los pilares fundamentales en todo proceso dentro de una organización.

SEGURIDAD DE LAS COMUNICACIONES INALÁMBRICAS EN LA EMPRESA

En el entorno empresarial, cuando hablamos de seguridad de las comunicaciones inalámbricas, directamente pensamos en tecnologías como Wireless y/o Bluetooth, quizás en alguna otra, pero principalmente en los sistemas Wifi.
De lo que no somos conscientes es que, hoy en día, un atacante no necesita hacer una gran inversión económica para poder llevar a cabo ataques sobre los sistemas inalámbricos. Pensamos que este tipo de ataques son complejos, y que no existen los conocimientos suficientes para atacar esos sistemas.

Nada más lejos de la realidad, hablemos por ejemplo de un dispositivo que ha capturado la atención de los TAs (Threat Actors), entusiastas de la seguridad y curiosos de las tecnologías; hablamos del **Flipper Zero**.

Este dispositivo viene a demostrar lo que comentábamos anteriormente, con una inversión limitada, tenemos acceso a un dispositivo capaz de analizar y emular diferentes protocolos inalámbricos.

Entre las muchas características que posee este dispositivo está su capacidad para analizar y auditar redes inalámbricas, capturar y decodificar señales Wi-Fi, decodificación de señales infrarrojas (IR), permite detectar y analizar señales de radio, puede emular y clonar tarjetas inteligentes, incluso dispone de la capacidad para manipular sistemas electrónicos como cerraduras, sistemas de alarmas, controles remotos; incluso puede interactuar con protocolos de comunicación utilizados en sistemas de control industrial como **Modbus, DNP3 y OPC.**

Como se puede observar, sus características lo convierten en una herramienta capaz de poner a prueba muchos de los sistemas de comunicaciones inalámbricos que podemos encontrar a nuestro alrededor.

CONTINÚA EN PRÓXIMA PÁGINA

Tanto es así, que ya se han llevado a cabo ataques a infraestructuras críticas, donde con el uso de esta herramienta han conseguido. Pero no sólo eso, las autoridades de diferentes países están dando la voz de alarma ante las acciones que se están llevando a cabo con este dispositivo para sustraer vehículos.

Con estos pequeños ejemplos damos comienzo esta nueva sección donde abordaremos este tipo de ataques, en los cuales las comunicaciones inalámbricas serán las protagonistas. A lo largo de esta temporada, iremos conociendo diversos protocolos de comunicaciones, cuáles son los vectores de ataque que se están usando para explotar vulnerabilidades en las estos sistemas, y cómo debemos proteger los sistemas.

Como se ha visto, ya no estamos hablando de ciencia-ficción, o de películas de Hollywood donde roban coches con sistemas inalámbricos, atacan infraestructuras críticas o, por ejemplo se lleva a cabo el hackeo de un satélite. Todo esto está ocurriendo hoy en día, y en esta sección vamos a ir desgranando cuáles son esos ataques, pero sobre todo, vamos a intentar concienciar a los decisores de la importancia de proteger estos sistemas de comunicaciones inalámbricas.

Pero después de comentar y hacer una introducción a esta nueva sección que abordamos en la revista en esta nueva temporada, quizás ha llegado el momento de que conozcas un poco más sobre mí, me presentaré. # ¿Quién es Alejandro Aliaga?

Con más de 20 años de experiencia profesional en el sector de las Tecnologías de la Información, a lo largo de mi carrera profesional he pasado por organizaciones internacionales, donde he participado en proyectos de transformación tecnológica relevantes, en diversos sectores como banca, administración pública, entre otros muchos.

A lo largo de mi carrera profesional he tratado de especializarme en la gestión de la seguridad, tanto desde el punto de vista tecnológico, como desde el punto de vista estratégico. En las empresas donde he ejercido como responsable, he tratado de ayudar en el análisis, gestión y mitigación de riesgos TIC, aplicando siempre los mejores estándares, las mejores prácticas y controles para aportar siempre una protección adecuada a la información, servicios y sistemas de la organización.

Con la incorporación a la revista, pretendo mostrar un punto de vista diferente, donde la seguridad de los sistemas inalámbricos (RF) serán el foco de todos los artículos. Unos sistemas de comunicaciones que, a menudo, no se protegen de la forma adecuada, o no se les presta la atención debida, y pueden suponer un riesgo para las infraestructuras de las organizaciones.

Siempre pensamos en la seguridad, como la seguridad de las comunicaciones TCP/IP, y las redes conectadas. Pero como hemos visto hoy, en esta pequeña introducción, ya es posible vulnerar sistemas de comunicaciones que pueden poner en peligro nuestra infraestructura o, lo que es peor, convertirse en una puerta de entrada a nuestros sistemas donde no hemos puesto la debida protección, y por tanto estaremos “ciegos” ante cualquier ataque que se produzca a través de estos protocolos de comunicaciones.

Mi intención será aportar mi pequeño granito de arena, para impulsar la ciberseguridad de estos sistemas, desarrollando nuevos contenidos, generando nuevas guías y divulgando las mejores prácticas en esta disciplina.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Inteligencia Estratégica y Gestión de la Innovación

ISO 56002:2019
ISO 56006:2021

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Basado en las Últimas Normas ISO
- Exámenes de Certificación Incluidos
- Certificación ISO 56002 Leader
- Certificación ISO 56006 Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Septiembre

Solicita tu admisión en:

+ 34 96 109 44 44
campus@escueladegobierno.es


RENFE
28

Seguridad en los sistemas ferroviarios (Parte I)

Vivimos en un mundo interconectado, con multitud de sistemas de comunicación, donde cada vez más, las tecnologías inalámbricas se hacen más presentes. Es cierto que este tipo de tecnologías tiene una serie de ventajas y comodidades frente a otro tipo de tecnologías, pero su despliegue y su uso no está exento de riesgos.

Hace muy poco tiempo saltaba en todos los medios la noticia que los ferrocarriles polacos habían sufrido un ataque; muchos medios lo llamaron ataque cibernético, pero realmente fue un ataque utilizando como vector de ataque las radiocomunicaciones y que podría haber tenido consecuencias dramáticas. # Sistemas de comunicaciones ferroviarios

Cuando hablamos de transformación digital en el sector ferroviario, la tendencia es irse a pensar en los sistemas de billetes electrónicos, compra por internet y conectividad a bordo. Sin embargo, dejamos de lado algunos avances que se están produciendo con la futura incorporación de tecnologías como el 5G asociada a las comunicaciones de los trenes, sin olvidar los sistemas ya implantados como el sistema **"tren-tierra" o GSM-R** que pueden ser vulnerables a ataques, tal y como veremos en esta serie de artículos que vamos a publicar.

RIESGOS ASOCIADOS

Antes de entrar a comentar el ataque a los sistemas ferroviarios polacos, es importante resaltar que todos los sistemas de información de transporte ferroviario están sujetos a altos niveles de exigencia para garantizar siempre su disponibilidad, accesibilidad y por último seguridad ("safety" que no, "security").

Hoy en día, los sistemas de control y asistencia al conductor cuentan con conexión y comunicación; a lo largo de estos artículos veremos algunos de ellos. Que dichos sistemas cuenten con comunicación hace que se presenten nuevas superficies de exposición, que quizás no se tengan en cuenta a la hora de hacer un modelado de amenazas.

Y es que, como iremos viendo en esta sección, los sistemas inalámbricos más allá del wifi y del bluetooth raramente se tienen en consideración a la hora de hacer un modelado de amenazas; aprovechar estas vulnerabilidades y/o debilidades en estos sistemas puede suponer consecuencias muy graves como la capacidad interactuar con los sistemas de un tren, ¿nos suena verdad? se parece mucho a lo ocurrido en Polonia.

Cuando se produce un ciberataque en el sector transporte, en especial, en el sector ferroviario, pueden producirse rápidamente consecuencias totalmente dramáticas, incluso en vidas humanas

El caso del incidente en el sistema ferroviario polaco

Hace muy poco saltaba a la luz la noticia que la policía polaca había arrestado a dos hombres sospechosos de comprometer la seguridad de la red de comunicaciones del ferrocarril nacional, lo que condujo a un problema que logró alterar el normal funcionamiento del tráfico en algunas áreas del país durante un fin de semana.

Lo curioso de esta noticia, y lo que nos lleva a este artículo, es que la policía confiscó a estos presuntos delincuentes unos dispositivos radio con los que supuestamente se había llevado el ataque.

CONTINÚA EN PRÓXIMA PÁGINA

Aunque nos puede parecer sorprendente, no es el primer ataque que se produce, ya en el 2008 un joven de 14 años con un simple mando a distancia modificado provocó el descarrilamiento de cuatro trenes, produciendo 12 heridos.
Para entender cómo se produjo el ataque, es necesario comprender cómo son los sistemas de comunicación del sector ferroviario, y cómo están evolucionando. Donde su evolución depende mucho de cada país.

Sistemas ferroviarios
Sin entrar en tecnicismos, no es complicado llegar a entender, que los sistemas que puedan ir embarcados en algunas unidades puedan estar ligeramente obsoletos o que no se hayan actualizado.
Ya estoy viendo a muchos llevarse las manos a la cabeza, pero no es tan sencillo actualizar esos sistemas como pudiéramos pensar. Aquí, como en otros entornos similares (sector aviación y automovilístico) debemos entender conceptos como "safety" vs "security".
Cuando se concibieron los sistemas de comunicación ferroviarios, en muchas ocasiones, se hicieron con protocolos propietarios que no fueron diseñados para proporcionar seguridad a los datos que transportan, sino que estaban diseñados para garantizar que la información se podia transmitir y que llegaba a su receptor.
Partiendo de esa base, podemos encontrarnos con sistemas de comunicaciones radio como el sistema "tren-tierra" o con sistemas más avanzados como el GSM-R.

¿CÓMO SE LLEVÓ A CABO EL ATAQUE?

En este primer artículo no profundizaremos en los sistemas de comunicaciones para entender cómo se llevó a cabo el ataque, eso lo dejamos para la siguiente edición. Pero si daremos algunas pinceladas para poder entender cómo de sencillo o complicado puede llegar a ser este tipo de amenazas.
En Polonia el sistema de radiocomunicaciones que todavía está en vigor está compuesto por un sistema analógico que se integra en equipos tanto en "tierra", como en "tren", así como en "equipos portátiles". Dicho sistema permite comunicaciones de voz simplex y el uso de señales de operación ("tonos") para realizar acciones. Además, el sistema cuenta con una función llamada "radiostop"
El sistema al que hacemos mención, se llama sistema "tren-tierra", y es el que fue explotado por los atacantes para llevar a cabo sus acciones. Dicho sistema analógico no dispone de protecciones que verifiquen la identidad del emisor, esto les permitió a los atacantes emitir los "tonos" adecuados a través de un sistema radio, para que enviar órdenes al tren.
No podemos considerar que sea extremadamente sencillo replicar este ataque, ya que requiere conocer

muy bien cómo funciona el sistema "tren-tierra" y además requiere de conocimientos de radio, para hacer que el equipo de transmisión transmita esos tonos que son interpretados por el tren como una orden.
Pero lo que, si pone de relevancia, es lo que en esta sección queremos destacar, la importancia de las radiocomunicaciones, y lo olvidadas que las tenemos cuando modelamos las amenazas. Como hemos repetido muchas ocasiones, hay más luz fuera del Wifi y del bluetooth, y estas comunicaciones si no se protegen adecuadamente pueden ser un vector de entrada, y causar graves daños.
En el siguiente artículo profundizaremos en cómo funciona el sistema "tren-tierra" en los posibles pasos que pudo llevar a cabo el atacante para producir este ataque.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno del Tiempo y Gestión de la Productividad

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación TSG4® Yellow Belt
- Certificación UNE 71404 Executive
- Módulo 1: MasterGEIT®
- Módulo 1: MasterPPM®

MPPM® MGEIT® eGob®

Del 15 al 23 de marzo

+ 34 96 109 44 44
campus@escueladegobierno.es

Seguridad en los sistemas ferroviarios (Parte II)

En el artículo anterior abordábamos el ataque que se producía contra los ferrocarriles polacos. En esta segunda parte, nos centraremos en conocer, evaluar y determinar las consecuencias que un ataque EM pudiera tener contra una infraestructura ferroviaria.

EL PROYECTO SECRET EU

El proyecto **SECRET EU**, es un proyecto ya cerrado, que nació en 2012 con el objetivo de evaluar los riesgos y consecuencias de los ataques electromagnéticos a la infraestructura ferroviaria. Durante su desarrollo, se trabaja en determinar medidas preventivas y de recuperación, así como de desarrollar soluciones de protección para garantizar la seguridad de la red ferroviaria.
Con una dotación de 3M€ y durante 3 años, se evaluaron los escenarios críticos donde pudieran tener lugar ataques EM y se evaluaron sus consecuencias mediante metodología de análisis de riesgos y la experimentación de supuestos ataques que surgieron de un modelado de amenazas previo.

ENISA

Pero esta iniciativa, no es la única. La comisión Europea publicó en octubre de 2019 un informe en el que se establece una primera evaluación sobre los enfoques elegidos para cumplir la directiva NIS desarrollando un enfoque especial en el sector ferroviario.
Tanto es así, que en 2020 **ENISA** en noviembre de 2020, publicó un informe que recogía más información de cómo se debe afrontar la ciberseguridad en este sector.
Lo que queda demostrado con estos esfuerzos, es que existe una preocupación por la ciberseguridad. Aunque en la realidad, y como se ha podido demostrar a lo largo de los años, no ha sido posible avanzar tanto como le hubiese gustado a los stakeholders, y se han dado casos que han trascendido como el reciente ocurrido en los ferrocarriles polacos. ## Escenarios más comunes

Uno de los escenarios analizados por diversos informes, ha sido el caso en el que los atacantes usan sistemas para hacer “jamming” a las comunicaciones del sistema ferroviario.
En caso de interferencia intencionada, el principal objetivo del atacante será provocar el frenado de emergencia del tren (como sucedió en el incidente del tren en Polonia). Un frenado de emergencia induce a consecuencias significativas en el tráfico ferroviario y requiere de un proceso de reinicialización del tren para su puesta en marcha.
En el caso de una interferencia intencionada (jamming), los distintos factores que influyen y que determinan el nivel de riesgo sobre el sistema ferroviario son los siguientes:

•**Ubicación del tren:** en función de dónde se encuentre el tren, su proximidad o lejanía de los sistemas radiantes (RF) pueden determinar el éxito o fracaso de dicho ataque.

•**Potencia de la fuente emisora de la interferencia y localización de la misma:** en función de la potencia de la fuente emisora de la interferencia (jammer) de sus características técnicas y su ubicación pueden suponer mayor o menor riesgo

CONTINÚA EN PRÓXIMA PÁGINA

Existen otros escenarios más complejos donde pueden darse ataques a las infraestructuras, pero por motivos de seguridad, no consideramos que sea apropiada la publicación de los mismos para no dar "pistas" a los malos. ## Los sistemas de comunicaciones

Como vimos en el anterior artículo, todavía quedan se usa el sistema de comunicaciones tren-tierra. El sistema **tren-tierra,** es un sistema de comunicaciones analógico de radiotelefonía que se utiliza para comunicarse entre trenes, estaciones y puestos de mando, permitiendo el intercambio bidireccional de mensajes codificados mediante tonos o incluso voz.
Y, aunque en muchas líneas de alta velocidad está implementado el sistema GSM-R, todavía quedan muchas líneas con sistemas analógicos como tren-tierra. Todos estos sistemas no están exentos de vulnerabilidades y de poder sufrir ataque vía sistemas RF.

En breve comenzaremos a ver **pilotos** dde 5G para entornos ferroviarios como el que se está trabajando desde **5gbarcelona** que consiste en el despliegue de cobertura 5G en un tramo de la red FGC.

La introducción de este tipo de tecnologías, por supuesto, tendrá que ser estudiada y evaluada para incorporar desde el diseño la ciberseguridad y la capacidad de resiliencia frente a ataques basados en sistemas RF.

CONCLUSIONES

Tras el análisis del proyecto **SECRET EU** y otras publicaciones relacionadas, y con el reciente incidente ocurrido en Polonia no podemos mirar a otro lado y pensar que un escenario de ataque utilizando técnicas EM no sería posible llevarlo a cabo hoy en día, y más aún sabiendo que el acceso a la tecnología SDR se ha abaratado muchísimo.
Para conseguir avanzar en materia de ciberseguridad en este sector hay que salvar ciertas barreras y conseguir retos complejos como:

•Mejorar la concienciación digital y de ciberseguridad en el sector ferrovario
•Concienciar ambos dos mundos como son "safety" y "cybersecurity"
•Conseguir impulsar la transformación digital en el core ferroviario
•Equilibrar adecuadamente la seguridad, la competitividad y la eficiencia operativa
•Mejorar aspectos normativos relacionados con la ciberseguridad en el sector

Iniciativas como el proyecto **SECRET EU**, documentos como los mostrados en este artículo de ENISA y otros, han contribuido a evaluar los riesgos reales, identificando ámbitos para reforzar la seguridad ferroviaria. Es cierto que, para que las medidas propuestas, se hagan efectivas hace falta mucha inversión, recursos profesionales y tiempo.

METADATA

Referencias Internas
•[[20.12.01.01 - Railroad Cybersecurity]]
  –[[20.12.01.01 - Railroad Cybersecurity#Security of railways against EM attacks|PDF - Security of railways against EM attacks]]
  –[[20.12.01.01 - Railroad Cybersecurity#Cyber Security Risk Management for Connected Railroads|PDF - Cyber Security Risk Management for Connected Railroads]]
•[[30.05.03 - Seguridad en los sistemas ferroviarios (Parte I)]]
•[[El sistema Tren-Tierra en España]]

Referencias externas
•PDF- Security of Railways against Electromagnetic attacks deliverable D 8.3 (01/08/2012)
•PDF- Security of railways agains electromagnetic attacks November 2015
•5G Railway

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Análisis de Negocio y Gestión por Procesos

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BPA Leader
- Certificación BPM Executive
- Módulo 2: MasterGEIT®
- Módulo 2 MasterPPM®

MPPM® MGEIT® eGob®

Del 5 al 13 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Seguridad en los sistemas TETRA

El sistema de comunicaciones trunking digital TETRA (Terrestrial Trunked Radio) es un estándar abierto de comunicaciones digital desarrollado en Europa en la década de 1990 por la ETSI (Instituto Europeo de Normas de Telecomunicaciones) y expertos de cuerpos y fuerzas de seguridad de varios países.

Su objetivo inicial, fue desarrollar un sistema de comunicación estándar para garantizar que los dispositivos TETRA ya sean portátiles, de mano, instalados en vehículos o en otras ubicaciones, proporcionasen servicios de comunicaciones de voz y datos seguras, fiables e instantáneas en entornos de misión crítica.

En su diseño se tuvo en cuenta que permitiese tener una arquitectura escalable que permita despliegues de red económicos desde cobertura monoemplazamiento, a coberturas multiemplazamientos. De entre todas sus características podemos destacar:
•Establecimiento rápido de llamada (< 0,3s)
•Funcionamiento en modo directo (DMO), sin necesidad de hacer uso de la infraestructura
•Calidad y claridad de la voz
•Diversos métodos de cifrado (TEA1, TEA2, etc.)
•Llamadas de emergencia
•Llamadas de voz en formato full dúplex
•Capacidad de integración telefónica (PABX y PSTN)

En la actualidad, los sistemas de comunicaciones TETRA son usados en más de cien países a lo largo de todo el mundo. Esta elevada expansión de este sistema es debido a su interoperabilidad y a las funcionalidades que ofrece dicho protocolo. Es más, en muchos países el órgano competente, tienen reservas de frecuencias destinadas a la utilización de este tipo de estándar.

Vulnerabilidades encontradas

El pasado verano, un equipo de investigadores de Países Bajos, formado por Carlo Meijer, Wouter Bokslag, y Jos Wetzels hacían pública una investigación donde daba a conocer cinco vulnerabilidades en el estándar de comunicaciones TETRA:

•**CVE-2022-24401, crítico:** permite ataques de oráculo de descifrado que conducen a una pérdida de confidencialidad y autenticidad.
•**CVE-2022-24402, crítico:** una puerta trasera en el algoritmo de cifrado TEA1 permite ataques triviales de fuerza bruta sobre las claves que conducen a una pérdida de confidencialidad y autenticidad.
•**CVE-2022-24404, alto:** la falta de autenticación en AIE permite ataques de maleabilidad que conducen a una pérdida de autenticación.
•**CVE-2022-24403, alto:** débil ofuscación en las identidades de radio permitiendo la desanonimización del usuario.
•**CVE-2022-24400, alto:** un fallo en el algoritmo de autenticación puede provocar una pérdida de autenticidad y una pérdida parcial de confidencialidad.
Una de las vulnerabilidades más destacadas residía en uno de los algoritmos de cifrado (TEA1) que puede ser empleado por los equipos de comunicaciones. Esta vulnerabilidad podría permitir a un atacante acceder a las comunicaciones de voz y datos, así como al envío de información falsa, o a la suplantación de la identidad del subscriptor.

Divulgación de las vulnerabilidades

Aunque las vulnerabilidades se descubrieron durante el transcurso de 2020, se decidió posponer la divulgación pública hasta julio de 2023 para que los servicios de emergencia y los proveedores pudiesen parchear los equipos.

Análisis del estándar de cifrado

Para la ingeniería inversa, se utilizó una radio comercial modelo Motorola MTM-5400 que dispone de COTS (Commercial off-the-self). Aunque los equipos comerciales disponen de controles de seguridad para proteger los algoritmos de cifrado y la carga de firmware en sus equipos, los investigadores usando otra serie de vulnerabilidades pudieron ejecutar código arbitrario en el núcleo ARM, pero para ello, previamente tuvieron que explotar otra serie de vulnerabilidades conocidas, utilizando el el interface AT como vector de ataque.
Una vez se realizó la ingeniería inversa al software, los investigadores pudieron realizar ya una investigación en profundidad, donde descubrieron las cinco vulnerabilidades arriba mencionadas.

¿A qué ataques se exponen las comunicaciones TETRA?

Aunque este año se detectaron estas vulnerabilidades, hoy en día, con la facilidad de acceso a tecnologías

CONTINÚA EN PRÓXIMA PÁGINA


ICOM
WATERPROOF
DIAL
DUAL
SCAN
LOCK
H/L
IC-M71
ICOM
IC-M6
1
ORANGE:CHARGE
GREEN:FULL
2

SDR, los ataques de «eavesdropping» al interface aire se han popularizado, y esto es debido a que todavía muchas redes de comunicaciones no hacen uso de protocolos de cifrado.
Por otro lado, en este tipo de redes, si se dispone de acceso al interface aire, también se pueden producir ataques de «replay», donde un posible atacante podría reenviar mensajes antiguos y confundir al destinatario. Tampoco podemos olvidar que existen otros posibles escenarios de ataque como:
•Jamming
•Ataques a la infraestructura IP
•Denegación de Servicio (DoS)
•Vandalismo, sabotaje…
•Monitorización del tráfico y obtención de inteligencia a partir de las escuchas.

¿Cómo abordar estas amenazas en las redes TETRA?

Las redes TETRA disponen de mecanismos de seguridad para tratar de minimizar estas amenazas. Vamos a abordar muy brevemente y, a muy alto nivel, los controles de seguridad que se pueden aplicar siguiendo los cinco principios de seguridad puesto que dejaremos para otro artículo el profundizar en estos controles.

Autenticación:
•Para el acceso a la red, tetra dispone de mecanismos para la autenticación de los terminales de radio
•También es posible autenticar en las consolas de dispatcher a los usuarios que van a hacer uso de estos aplicativos.

Autorización
•Una vez autenticados los usuarios de la red TETRA, estos pueden tener diferentes niveles de autorización para el acceso a diferentes servicios (grupos, aplicaciones, etc.)
•Con los permisos de autorización se pueden otorgar diferentes privilegios para establecer una comunicación, para añadir o retirar privilegios de comunicación o membresía a usuarios de un grupo de conversación (talkgroup).

Confidencialidad:
•Para evitar las escuchas TETRA dispone de sistemas de cifrado del interface aire-aire (entre el terminal y la estación base)
•Además para garantizar la confidencialidad de extremo a extremo, la tecnología TETRA provee mecanismos para garantizar que los mensajes irán cifrados de un terminal a otro, garantizando que la infraestructura no es capaz de descifrar el mensaje, protegiendo así también los canales de comunicación de la infraestructura: canales IP, radioenlaces…

Integridad:
Para garantizar la integridad de la información transmitida a través de las redes TETRA se pueden implementar un gran abanico de controles de seguridad como:
•En la parte de backend de la red TETRA se deberán implementar medidas para que la información esté debidamente protegida, en especial se deberá dotar de mecanismos de recuperación a la información almacenada en las bases de datos
•Se deberán implementar mecanismos para evitar el uso no autorizado de software de dispatcher o para otras funcionalidades que pueda afectar a la seguridad de la red.
•Además se deberán implementar controles, para monitorizar el estado de los terminales así como la información transmitida por los canales de control.
•Se deberán implementar medidas de monitorización, para llevar un control de los dispositivos que se registren en la red.

Disponibilidad:
Para garantizar la disponibilidad en las redes TETRA se pueden implementar los siguientes controles
•Disponer de un plan de recuperación (DRP)
•Procedimientos para el remplazo de las unidades que puedan fallar y por tanto afectar a la disponibilidad de la red
•Monitorización de los enlaces para modificar los caminos empleados y re-enrutar la información mediante el uso de otros enlaces.
•Definir claramente los usuarios que dispondrán de un acceso garantizado a la infraestructura en caso de congestión o de degradación de la red.
•Monitorizar la carga de los enlaces para tomar acciones preventivas ante un posible colapso o saturación de la red
•Despliegue de procedimientos de «fall-back» y capacidad de operar en modo DMO (Direct Mode Operation)

No-repudio:
•Definir controles que permitan la grabación de todo el tráfico de la red
•Monitorización y logging de las llamadas one-to-one de los subscriptores
•Monitorización y logging de los accesos a las consolas de dispatching
•Implementar controles que garanticen la trazabilidad de todas las acciones
•Implementación de sistemas CDR
•etc.

Conclusión

Evidentemente estas medidas se encuentran a muy alto nivel, pero no era el objetivo de este artículo profundizar en exceso en los detalles técnicos de la implantación de medidas de protección frente a ataques en las redes TETRA. El objetivo de este artículo es arrojar un poco de luz sobre los controles que se deben implantar en las redes TETRA frente al aumento de las amenazas y ataques consecuencia de la popularidad que han adoptado los sistemas SDR. No olvidemos que podemos encontrar este tipo de redes de comunicaciones en infraestructuras críticas y, en muchos casos, conectando dispositivos SCADA que podrían ser accionados de forma remota.

Por lo tanto y, siguiendo con los artículos de esta sección, queremos crear consciencia de que las comunicaciones inalámbricas pueden ser una amenaza, y suelen ser las más olvidadas a la hora de protegerlas.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Proyectos

OpenPM² (PjM) + ISO 21502

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PjM) Executive
- Certificación ISO 21502 Leader
- Módulo 3: MasterGEIT®
- Módulo 3 MasterPPM®

MPPM® MGEIT® eGob®

Del 19 al 27 de abril

+ 34 96 109 44 44
campus@escueladegobierno.es

Seguridad en el entorno marítimo

El ámbito marítimo es uno de los sectores críticos que también está experimentando una importante transformación digital. Hace años que la Organización Marítima internacional instó a la comunidad marítima a introducir la gestión de riesgos cibernéticos en sus planes. Con este gesto, se demuestra la importancia de la gestión de riesgos en este entorno. A lo largo de este artículo vamos a profundizar en los riesgos y amenazas a los que se enfrenta uno de los sistemas embarcados.

Dado que es un tema muy extenso, nos centraremos sólo en la navegación marítima donde, como es evidente, se ha identificado que la tecnología esencial empleada a bordo de buques, tales como los sistemas de navegación GPS, AIS (Automatic Identification System) y ECDIS (Electronic Chart Display and Information System), son especialmente vulnerables a posibles ciberataques, al no contener mecanismos propios de encriptación de datos o de autenticación. Como es de esperar, las potenciales consecuencias de estos ataques para la seguridad marítima, la infraestructura portuaria y el comercio internacional son devastadoras. Ser consciente de estas amenazas, supone también un reto para el sector. Por ello, en respuesta a estos retos, la "Mesa Redonda de Asociaciones Marítimas" que agrupa al sector naviero internacional, comenzó a publicar unas directrices sobre ciberseguridad abordo de buques, para tratar de ayudar a navieros y operadores marítimos a evaluar sus riesgos, establecer los procedimientos y adoptar las medidas necesarias para garantizar la seguridad de los sistemas informáticos y de comunicaciones a bordo de sus buques. # Sistemas embarcados

Automatic System Identification (AIS)
El sistema de identificación automática (AIS) es un sistema que se utiliza para mejorar la seguridad marítima al proporcionar información en tiempo real, como seguimiento y monitorización de barcos. Desde su creación, allá por el año 2002, se ha instalado en mucho más de 300.000 barcos en todo el mundo, consiguiendo monitorizar el tráfico marítimo y evitando colisiones en embarcaciones. De igual forma, se ha demostrado que el uso de esta tecnología es útil para la investigación de accidentes y para operaciones de búsqueda y rescate (SAR -Search & Rescue).

CONTINÚA EN PRÓXIMA PÁGINA

Como ya hemos dicho, **AIS** es el acrónimo para "**AUTOMATIC IDENTIFICATION SYSTEM**" y es un sistema para ver la posición, el rumbo y la velocidad de una embarcación (identificación automática), pero vamos a tratar de ver cómo funciona para poder entender cuáles son las amenazas a las que se enfrenta.

El sistema AIS transmite a través de un sistema RF (en la banda de VHF) la posición, rumbo y velocidad de la embarcación. Sin profundizar en detalle sobre el protocolo, diremos que la información transmitida por el sistema AIS puede ser de cuatro tipos:

•**Datos estáticos:** Nombre y distintivo de llamada, número IMO, eslora, manga y, tipo de buque
•**Datos dinámicos:** esta información es actualizada automáticamente por los sensores del buque conectados al sistema AIS y transmite datos como posición, hora en formato UTC, rumbo, velocidad, proa, etc.
•**Datos relacionados con la travesía:** en este apartado se incluyen datos de calado, carga potencialmente peligrosa, destino y hora estimada de llegada, plan de navegación.
•Mensajes: mensajes de texto breve y formato libre que se introducen manualmente

Principales ataques contra el sistema AIS
Los problemas de seguridad de los sistemas AIS pueden aparecer por dos vías, una de ella sería la del propio software (que no vamos a tratar en este artículo) y a la que sí vamos a analizar, las amenazas que puede provenir de los sistemas RF (señales de radio).

Como ya hemos descrito anteriormente, el protocolo AIS no incorpora medidas de protección y seguridad, lo cual lo hace vulnerable a múltiples ataques. Y aunque existe una versión mejorada (EAIS) que incorpora cifrado su uso es residual. A continuación vamos a ver algunos de ellos:
•**AtoN spoofing:** es el método por el cual se pueden inferir vía señales de radio para colocar boyas falsas en canales angostos para engañar a los buques hacia zonas de bajos fondos y dejarlos encayados.
•**SAR Spoofing:** este ataque suplantaría la identidad de una baliza de "hombre al algua" en una posición concreta. Al ser obligatoria la asistencia por cualquier buque que se encuentre cercano a esta posición, puede ser usado por la piratería para acercar buques a una zona concreta para, después proceder a abordarlo.
•**AIS Hijacking:** este ataque consiste en la alteración de la información del buque como la posición, velocidad o tipo de cargamento. Si este ataque se hace junto a una estación receptora de la señal AIS y esta a su vez inyecta los datos recibidos mediante RF a una web de seguimiento de barcos en internet podemos llegar a visualizar este ataque en internet.

Otra de las amenazas, quizás más rocambolescas, sería usar el protocolo AIS como canal encubierto para el intercambio de información de tipo C&C (mando y control), evadiendo así, los controles de seguridad de los sistemas conectados a internet. Puede parecer que es muy complicado usar este sistema para este cometido y desde aquí no queremos dar pistas a los "malos" pero múltiples estudios dan viabilidad técnica a esta capacidad.

¿Cómo protegerse de estas amenazas?
Tanto los ataque que se pueden realizar en la parte software como, los que en este artículo destacamos, más enfocados a la parte RF, muestran la importancia de tomarse en serio la seguridad de este protocolo. Ya que, un ataque como los descritos anteriormente pueden tener consecuencias desastrosas.
Tanto es así, que la exploración de todas las amenazas posibles en este entorno, ha llevado a diversos investigadores a la conclusión de que se deben añadir capas adicionales de seguridad al protocolo AIS. Entre ellas se destacan:

•**Detección de anomalías:** a la hora de validar los mensajes que provienen de este sistema, se deben aplicar técnicas de identifiquen patrones anómalos, tales como rutas de las embarcaciones, o la información estática proporcionada por los sistemas AIS de estos. Si bien este control de seguridad puede ser muy valioso no está exento de otros ataques como el jamming o spoofing de las señales RF
•**Infraestructura de clave pública:** otra de las medidas de seguridad que se podrían adoptar para mejorar la seguridad de estos sistemas, es la adopción de un esquema PKI en las comunicaciones del protocolo AIS. De este modo, se conseguiría autenticar los mensajes intercambiados por las estaciones.
Si bien, se está avanzando mucho en el ámbito de la ciberseguridad con nuevos estándares como OneNet, aún queda un largo camino por recorrer. Al igual que en otros sectores como el aéreo, las medidas de seguridad (safety) que se deben cumplir, hacen muy compleja la adopción de nuevos estándares en un corto espacio de tiempo. Esta tarea, por su complejidad, debería involucrar a reguladores, fabricantes, integradores y usuarios.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gestión de Programas

OpenPM² (PgM) + ISO 21503

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación OpenPM² (PgM) Executive
- Certificación ISO 21503 Leader
- Módulo 4: MasterGEIT®
- Módulo 4 MasterPPM®

MPPM® MGEIT® eGob®

Del 3 al 11 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Evento de Cierre de Temporada 2024 de las Revistas Tecnología y Sentido Común y Stakeholders.news

El 19 de julio de 2024, las revistas Tecnología y Sentido Común y Stakeholders.News celebraron el Cierre de su novena y tercera temporada respectivamente con un interesante evento en la sede de UNE Asociación Española de Normalización, en Madrid.

En una tradición que se inició el pasado año 2023, las revistas Tecnología y Sentido Común y Stakeholders.News prepararon un cierre de temporada a la altura tanto de la calidad de sus contenidos como del nivel de sus colaboradores. Con la inestimable colaboración de UNE Asociación Española de Normalización, el día 19 de julio de 2024 se reunió en Madrid un granado grupo de profesionales, entre los que estaban algunos de los colaboradores de nuestras revistas.

El evento comenzó con una bienvenida a cargo de Paloma García, Directora de Programas de Normalización y Grupos de Interés de UNE, y de Javier Peris, Director de las revistas Tecnología y Sentido Común y Stakeholders.News, en el que agradecieron a los presentes su asistencia, sobre todo a aquellos afectados por el incidente global en sistemas de información de grandes compañías de todo tipo que se dio en esa fecha.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Tras la bienvenida, se dio paso al ponente principal del evento, Ramsés Gallego, primer español (y tercer europeo) en ser nombrado para el "Hall of Fame" de ISACA internacional, evento que tuvo lugar en este 2024. Renombrado conferenciante, deleitó al público asistente con su charla "De Gestionar a Gobernar …. con 'G' de Ganar", en la que glosó las bondades de dar ese salto hacia el gobierno de las Tecnologías de la Información, sobre todo en los aspectos relacionados con la ciberseguridad. Ciertamente, un lujo contar con él para el evento.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

El siguiente acto fue la mesa redonda con cinco de los autores que colaboran con la revista Tecnología y Sentido Común en el que participaron: Alejandro Aliaga líder de la seccion “Radio Security”, Renato Aquilino líder de la sección “Marcos y Normas”, Marlon Molina líder de la seccion “Es Tendencia”, Marcos Navarro líder de la seccion Ai Robot” que a partir de la proxima temporada pasará a llamarse “Ai Futuro” y Manuel Serrat líder de la seccion “Futuro y Seguridad”.

Durante la mesa redonda de Tecnologia y Sentido Común, estos cinco representantes respondieron a las preguntas del presentador y director de la revista, Javier Peris, acerca de los contenidos de la temporada que terminaba, y de qué se podía esperar de sus secciones en cuanto a contenidos y novedades en la décima temporada de la revista.

Alejandro Aliaga centró su intervención en recordad que el objetivo de su sección “Radio Security” es concienciar a los lectores de que existen vectores de ataque no convencionales asociados con las comunicaciones inalámbricas, y que, por la evolución tecnológica, es difícil que éstos se reduzcan.

Por su parte, Renato Aquilino, en su sección “Marcos y Normas” ha centrado sus contenidos en poner de manifiesto el gap existente entre las normas y quienes las escriben, frente a quienes las han de convertir en realidad en las organizaciones, algo que resulta extremadamente complejo en algunos casos.

Por lo que respecta a Marlon Molina, con su sección “Es Tendencia”, ha tratado de contar a los lectores en esta temporada que termina los temas que, mes a mes, han atraído la atención del sector por diferentes motivos.

Marcos Navarro anunció que su sección, a partir de la décima temporada, cambiaba de enfoque y de nombre, para explicar cómo es la vida en 2024, sólo dentro de diez años, gracias a tecnologías como la Inteligencia Artificial y la Robótica.

En cuanto a Manuel Serrat, explicó que con su sección “Futuro y Seguridad” ha tratado de poner el foco en aquellos aspectos de la evolución tecnológica que pueden suponer algún tipo de riesgo, y concienciar a los lectores para evitarlos.

CONTINÚA EN PRÓXIMA PÁGINA

Evento Protagonista

Finalizada esta mesa redonda, se llevó a cabo la segunda Mesa Redonda, que contó con cuatro de los colaboradores de la revista Stakeholders.News: Juan Manuel Domínguez líder de la Seccion "Organizaciones Resilientes", Luis Morán líder de la sección "Personas y Procesos", José Antonio Puentes líder de la seccion "Tendiendo Puentes" y Juan Jesús Urbizu líder de la seccion "Tecno-transformación".

Dada la temática de la revista, fundamentalmente dirigida a aquellos profesionales de la gestión de proyectos, programas y portfolios y áreas conexas, las preguntas para los participantes en la mesa redonda se centraron en poner de relieve la necesaria aplicación de estándares y buenas prácticas en cada uno de los ámbitos que tratan las diferentes secciones de la revista.

Juan Manuel Domínguez, a través de su sección "Organizaciones Resilientes", expuso aspectos tales como que, en Japón, con aproximadamente 120 millones de habitantes, hay 45.000 empresas centenarias, frente a las poco más de 5.000 que existen en España con 48 millones de habitantes.

Luis Moran comentó algunos de los temas que había tratado durante esta tercera temporada en su sección "Personas y Procesos", y avanzó alguna de las cuestiones que va a tratar en la cuarta temporada de la revista.

José Antonio Puentes (sección "Tendiendo Puentes") compartió con los presentes algunas vivencias personales, relacionadas con las dificultades que la gestión de proyectos enfrenta en determinadas organizaciones.

Por último, Juan Jesús Urbizu, que estas temporadas ha escrito en su sección "Tecno Transformación", apuntó algunas de las cuestiones más relevantes a las que se enfrenta el gestor de proyectos, programas y portfolios en relación con la digitalización de las organizaciones, y más desde la irrupción para el gran público de los sistemas de inteligencia artificial.

CONTINÚA EN PRÓXIMA PÁGINA

Tras las dos mesas redondas, Javier Peris anunció el nombramiento de los tres embajadores de la revista Stakeholders.News en Hispanoamérica más concretamente en Puerto Rico, Uruguay y El Salvador.
En Puerto Rico contaremos cada mes con la participacion de Nesty Delgado en Uruguay contaremos con Daniel Sorokins y en el pais de la eterna sonrisa "El Salvador contaremos con Luis Guardado quienes fueron nombrados y serán a partir de ahora Embajadores de Stakeholders.news.

Los actos de cierre de temporada terminaron con la entrega de los premios Tecnología y Sentido Común y Stakeholders. News, en esta ocasión en su edición de 2024.

El "Premio Tecnología y Sentido Común 2024" recayó en el Consejo General de Colegios Profesionales de Ingeniería Informática (CCII), por su aportación al progreso de la sociedad de la información, el impulso al desarrollo ético de los avances tecnológicos y la defensa y promoción de la ingeniería en informática. El premio fue recogido por José García Fanjul, secretario del CCII y vicedecano del Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Por otro lado, el "Premio Stakeholders.News 2024" fue otorgado a la Agencia para la Administración Digital de la Comunidad de Madrid, por haberse convertido en referente en la innovación y digitalización de la administración pública y por su compromiso con el cumplimiento y la excelencia del servicio al ciudadano. Este premio fue recogido por Zaida Sampedro Préstamo, subdirectora general de Transformación y Gestión del Cambio de la Agencia para la Administración Digital de la Comunidad de Madrid.

Al terminar el acto, todos los presentes pudieron disfrutar de un magnífico networking alrededor de un espectacular catering que se sirvió en las mismas instalaciones de UNE, con lo que se dio por cerrada la temporada de ambas revistas. ¡Nos vemos en septiembre!

Hace mucho tiempo que hablas.

¿Pero hace cuánto no dialogas?

Somos una organización global de beneficio para la comunidad cuya misión es crear normas para contribuir a la construcción de un mundo más seguro, sostenible y competitivo.

Creamos espacios de colaboración neutrales e inspiradores en los que compartir conocimiento para desarrollar, a través del diálogo y el consenso, normas que sirvan a los intereses de toda la sociedad y que movilicen a los que apuestan decididamente por la excelencia empresarial y la conciencia social.

UNE Normalización Española

Progreso compartido

une.org

Seguridad en las comunicaciones móviles

Hoy en día los teléfonos móviles se han convertido en una herramienta de comunicación imprescindible en nuestra rutina. Los dispositivos móviles constituyen uno de los principales, sino el principal, medio de comunicación que utilizamos en la actualidad.

Cada vez son más utilizados, y por más personas, y cada vez se emplean para más cometidos, desde el ocio hasta acceso a información corporativa, con datos, en muchas ocasiones sensibles.

Por desgracia los teléfonos móviles no fueron diseñados con la premisa de garantizar privacidad y la seguridad de las comunicaciones. Estos dispositivos al realizar múltiples funciones, más cercanas a las de un ordenador, si no se toman las medidas adecuadas nos exponen a un nuevo tipo de amenazas.

•Pérdida o robo del dispositivo
•Infecciones por virus o Malware vía email u otros medios
•Robo de Información
•Suplantación de identidad
•Acceso a datos confidenciales: conversaciones, imágenes, o vídeos.
•Etc.

AMENAZAS MÁS COMUNES: ROGUE BTS

¿Rogue BTS?

Al igual que en las comunicaciones inalámbricas (Wireless) se pueden crear **rogue AP** dentro de las comunicaciones móviles también se pueden crear estaciones base falsas con el objetivo de que el dispositivo objetivo caiga en una red controlada por el atacante.
Es bien sabido, que las agencias de inteligencia utilizan dispositivos profesionales capaces de crear una estación base falsa, con el objetivo de ayudar a localizar y hacer el seguimiento de posibles sospechosos. Para conseguir este objetivo se despliegan equipos profesionales capaces de recoger información y datos del objetivo a investigar.

Estos dispositivos profesionales son públicamente conocidos con muchos nombres:
•IMSI-Catchers
•Interceptores
•Stingrays
•Etc.

¿Por qué deben preocuparnos estos dispositivos?

Se ha podido comprobar, que con la llegada de los SDR, y con dispositivos como BladeRF, HackRF o USRP un atacante, sin necesidad de invertir una gran cantidad de dinero podría desplegar una estación base falsa de forma muy sencilla y en relativamente poco tiempo.
De forma muy resumida; en caso de que se levantase una estación base falsa, y fuésemos el objetivo de ataque, nuestro dispositivo se conectaría a esta estación base sin que el usuario detectase nada anormal.
Una vez conectado, los riesgos son muy elevados. Ya que un atacante podría conocer y/o grabar las comunicaciones establecidas por el dispositivos móvil; esto es más grave en el mundo empresarial, ya que se podrían ver comprometidas conversaciones e información confidencial de nuestra empresa. Lo que está claro, es que la privacidad del objetivo se vería comprometida.

¿Cómo podemos defendernos?

Existen multitud de aplicaciones para Android que permiten detectar ciertas anomalías, y por tanto nos ayudan a disponer de indicios de que pudiéramos estar sufriendo un ataque de Rogue BTS. Si bien estas aplicaciones son útiles, su uso queda restringido a móviles Android (no todos los modelos) y que estos deben ser “rooteados”.
Lo ideal sería disponer de un equipo independiente del terminal móvil que permita caracterizar el entorno y detectar anomalías.Este dispositivo debería monitorizar ciertos parámetros que se envían desde las estaciones base como:
•ARFCN
•MCC
•MNC

CONTINÚA EN PRÓXIMA PÁGINA

•Cell ID
•LAC
•TxP
•Celdas vecinas
•Intensidad de la señal

Detectando Rogue BTS.

Para poder detectar anomalías, primero debemos caracterizar el entorno, es decir, crear una baseline que nos permita conocer cómo se encuentran dispuestas las BTS a nuestro alrededor.
Una vez creada esa "baseline", cualquier cambio que sufra nuestro entorno, debe desencadenar una alerta y está deberá ser estudiada por el equipo de seguridad.

¿Qué tipo de anomalías debemos detectar?

Por ejemplo, si de repente aparece una nueva estación base que antes no teníamos inventariada, eso debería generar una alerta, si además la BTS estuviese transmitiendo con una potencia más elevada que el resto se podría considerar como sospechosa.

Siguiendo con los ejemplos, si de repente una estación base conocida cambia de frecuencia y/o de potencia este cambio debería generar una alerta que, al igual que la anterior, tendría que ser estudiada por el equipo de seguridad.

Otro claro ejemplo sería, si aparece una estación base con un LAC extraño o que carezca del mismo. Existen muchas casuísticas, aquí sólo hemos mostrado algunos ejemplos de cómo se podrían detectar Rogue BTS´s.

Interceptación de las comunicaciones IMSI-Catching

IMSI-Catching es una técnica que permite la escucha y/o monitorización del tráfico generado por teléfonos móviles.
El dispositivo simula ser una estación base, de forma que los teléfonos que están alrededor, al recibir una señal más potente que la estación base "real" tratarán de conectarse a esa estación.

¿Qué es el IMSI?

El IMSI (International Mobile Subscriber Number) es el número que identifica a los usuarios de la red móvil

IMSI Catching, ¿En qué consiste?.

Un ataque de IMSI Catching consiste, básicamente en la captura no autorizada de IMSIs. Este ataque es realmente peligroso ya que con la captura del IMSI podemos determinar que un usuario X tiene presencia en una zona determinada.
Para llevar a cabo un ataque de este tipo, bastará con desplegar una estación base falsa que permitiese mantener una conversación con el "objetivo".
El dispositivo "objetivo" de repente, detecta una nueva estación base, con más potencia que a la que está conectada, y solicita hacer un cambio a dicha "antena". Aquí vemos cómo sería una conversación entre el móvil "objetivo" y la estación base falsa:
En el contexto de las BTS falsas, existen proyectos que son capaces de emular diferentes elementos de una red GSM. Estamos hablando de proyectos como: OpenBSC y OpenBTS.
Utilizando este Software es relativamente sencillo desplegar una BTS, que usando Asterisk (software para VoIP) permite enrutar las llamadas a la PSTN. Además, con la popularidad de los equipos SDR y su potencia, cada vez es más sencillo emular una BTS con estos equipos SDR. Pero eso lo dejaremos para otro artículo.

Conclusión

A la vista de lo expuesto en este artículo, no podemos descuidar la seguridad de nuestros dispositivos móviles. Y, aunque hoy en día, existe mayor concienciación de los riesgos, en los departamentos de seguridad de muchas empresas no conocen más que los ataques más populares tras el escándalo de Snowden.
Como cierre del artículo, quisiera dejar una reflexión, o más bien, una mirada hacia el futuro. Es importante combinar todas las medidas de seguridad y correlar todas las alertas que se reciben en diversos escenarios. En un futuro no muy lejano, espero, que lo que actualmente conocemos como Security Operations Center (SOC), se puedan convertir en centros de monitorización y resiliencia que incluyan capacidad de monitorización que van más allá de las redes IP y los ataques por internet porque, aunque en este artículo por sus limitaciones no se ha podido profundizar en detalle, se pueden combinar ataques a la infraestructura IP con ataques a las comunicaciones móviles para conseguir materializar intrusiones, u obtener información valiosa para conseguir ataques más complejos.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Service Management FitSM + ISO 20000

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación FitSM Executive
- Certificación ISO 20000 Leader
- Módulo 5 MasterGEIT®
- Módulo 5 MasterPPM®

MPPM® MGEIT® eGob®

Del 17 al 25 de mayo

+ 34 96 109 44 44
campus@escueladegobierno.es

Drones ¿una amenaza para la ciberseguridad?

Hace muy poco que la Agencia de Seguridad de infraestructura y Ciberseguridad (CISA) emitía un nuevo informe con directrices para abordar los riesgos de seguridad derivados del uso de sistemas aéreos no tripulados. En concreto alertaban sobre el uso de estos dispositivos cuya fabricación sea china. Y no solo esto, durante el conflicto entre Ucrania y Rusia, se ha podido constatar el papel fundamental que están jugando los drones. Esta guerra se considera como la primera "guerra híbrida a gran escala", guerra que combina la guerra tradicional con la ciberseguridad.
En nuestro caso, no vamos a tratar la seguridad de los drones en sí misma, sino que, vamos a tratar de entender a qué riesgos nos enfrentamos, desde el punto de vista de la ciberseguridad y los sistemas de RF (radiofrecuencia).

Desafíos derivados del uso de estas tecnologías

A lo largo de todos los artículos de esta sección, hemos visto como han evolucionado los desafíos a los que se enfrentan las organizaciones a la hora de proteger sus activos, su infraestructura y su personal en un panorama cada vez más complejo.
El panorama de las amenazas es altamente cambiante, y se presentan de muchas formas, observándose en los últimos tiempos un aumento considerable de los ataques híbridos, que pueden combinar vectores de ataque físico y cibernético. Por lo tanto, las medidas de seguridad tradicionales, por sí solas, pueden no ser suficientes para mitigar las amenazas actuales.

Principales amenazas

Cuando hablamos de drones, habitualmente nos viene a la mente la imagen de su uso recreativo. Si bien, este uso es el más extendido, no podemos dejar de pensar en otros posibles usos maliciosos. Usos que suponen amenazas para algunas ubicaciones tales como organizaciones, infraestructuras críticas o edificios singulares.
Desde el punto de vista del atacante, siempre se trata de buscar la manera de saltarse los controles de seguridad que una organización pueda disponer. Es por eso, que cuando pensamos estrategias de defensa en profundidad, debemos contemplar escenarios de ataques híbridos aunque, por desgracia, lo más común sea sólo pensar en ataques cibernéticos.

El uso de drones para realizar ciberataques, por suerte, no está muy extendido pero si han existido casos en los que se ha podido demostrar su capacidad para poder perpetrar ciberataques. Veremos a continuación algún ejemplo que muestra su capacidad y los riesgos que implican.

CONTINÚA EN PRÓXIMA PÁGINA


SPARK

En general, los drones pueden ser utilizados para realizar ataques tales como:

•**Vigilancia física:** se pueden utilizar drones equipados con cámaras de alta precisión para poder observar a distancia cambios de turnos, recopilar información sobre protocolos de seguridad, observar las pantallas de los empleados, grabar las pulsaciones del teclado mientras hacen login en las aplicaciones, para planificar ataques futuros.

•**Ataques de Denegación de Servicio (DoS):** los drones pueden transportar dispositivos capaces de realizar de-autenticación masivos, también pueden bloquear mediante ataques de jamming redes wifi u otros protocolos inalámbricos (comunicaciones radio, etc.) impidiendo que estos funcionen con normalidad.

•**Rastreo y suplantación de redes:** en esta sección, nos centraremos sobre todo en este aspecto. Los atacantes, como veremos en el siguiente ejemplo, pueden equipar a los drones con equipos tales como raspberry pi o similares para detectar información sobre redes wireless que desde fuera de la organización no es posible. Desde el aire, pueden recopilar direcciones MAC, mapear los SSIDs para luego más tarde llevar a cabo ataque de "de-authentication" a los usuarios, ataques mediante "fake APs" o similares. Todos desde una distancia prudencial y sin ser detectados.

Además, los drones están evolucionando rápidamente para volverse más silenciosos y rápidos, son capaces de volar más lejos de sus operadores, rastrear objetivos en movimiento, y tomar fotografías o vídeos de mayor resolución. Y, aunque pueda parecer que los drones son un problema de seguridad física, como veremos en el siguiente ejemplo, debemos empezar a pensar en seguridad como un concepto más amplio sin diferenciar física de cibernética y, donde los centros de operaciones de seguridad (SOC) deben contemplar aspectos de seguridad fuera de la dimensión ciber.

Aunque no es el objetivo de este artículo, hoy en día, ya es posible integrar los sistemas de vigilancia físicos y sistemas anti-drones con los sistemas de seguridad y correlación de alertas de un SOC. Creando un nuevo nivel de centro de monitorización y respuesta frente a incidentes de seguridad, lo que bien podríamos llamar "Cyber Resillience Center".

Un ciberataque con drones

En el año 2022, el investigador Greg Linares explicaba el ciberataque sufrido por una empresa y que fue llevado a cabo gracias a los drones No han trascendido muchos detalles de este ataque, se supo que era una empresa especializada en inversiones privadas. Todo saltó cuando el equipo de seguridad detectó una actividad inusual en sus sistema de documentación "Confluence", lo que no sabían es que el ataque se llevó a cabo desde un dron que se posó en la azotea de su edificio y que, a través de su conexión wireless, logró entrar en la red interna de la organización sin ser detectado.

Los equipos de investigación ante incidentes, detectaron una dirección MAC no conocida, y rastreando la señal de donde provenía la conexión wireless llegaron hasta la azotea del edificio, allí se encontraron con dos drones de la marca DJi modificados, viendo que uno de ellos llevaba como "carga de pago" un dispositivo wireless conocido como "pinapple" que falsificaba la red wireless a la que normalmente se conectaban los empleados.
Sin entrar en detalles muy técnicos, el ataque se llevó a cabo, suplantando la identidad de uno de los puntos de acceso, hasta conseguir que uno de los empleados se conectara a dicho "fake AP" obteniendo datos suficientes para robar credenciales, y realizar inicio de sesión en uno de sus sistemas.

El segundo de los drones, llevaba una raspberry pi con un moódem 4G y otro dispositivo wifi. Según las investigaciones se pudo concluir que este segundo drone era el encargado de realizar el ataque contra la red de la organización y que era gestionado a través de esa conexión 4G que ofrecía el módem que llevaba enganchado.

¿Ciberataques desde el cielo? ¿es esto normal?

El uso de drones para realizar ciberataques, ya se teorizó mucho antes de que se produjese esta noticia en el 2022. Podemos remontarnos hasta 2015, donde la empresa Aerial Assault enseñó un drone modificado en el congreso DEF CON (Las Vegas) que contenía una raspberry pi con aplicaciones para poder realizar ataques contra sistemas wireless. O también, podemos remontarnos a la demostración que hizo el investigador Samy Kamkar que creó un drone llamado "SkyJack" que sirvió para tomar el control de otros drones en vuelo en tiempo real.

Esta presentación, junto con el ataque sufrido por esta organización en 2022 nos hace pensar que no es ciencia ficción. Ahora bien, la tecnología ha ido avanzando mucho, y ahora mismo con un dispositivo mucho más pequeño se pueden realizar una gran cantidad de ataques; ¿qué sucedería si ahora en vez de llevar como carga de pago un pineapple, llevase un "flipper zero"?.

Conclusiones

A la hora de hacer un modelado de amenazas, no podemos dejar de pensar en lo que me gusta denominar "ataques no convencionales", atraques que, por su naturaleza, pueden llevarse a cabo, pero para los que quizás no hayamos pensado. Ataques en donde el factor de las comunicaciones inalámbricas tienen un papel fundamental.

Evidentemente, no podemos profundizar mucho más, pero este tema daría para comentar mucho más en detalle, todos los estudios que se están llevando a cabo para analizar las vulnerabilidades de los protocolos de comunicaciones de los drones, sus firmware alternativos y cómo los "malos" se saltan las protecciones que ponen los fabricantes, asi que, quizás lo dejemos para otro artículo.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Seguridad de la Información

CSX + ISO 27001

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación CSX Executive
- Certificación ISO 27001 Leader
- Módulo 6: MasterGEIT®

MGEIT® eGob®

Del 7 al 15 de junio

+ 34 96 109 44 44
campus@escueladegobierno.es

¿Cuidamos de nuestros secretos cuándo hablamos?

En esta sección siempre hemos tratado de ver la seguridad de nuestros activos desde un punto de vista diverso, y nada convencional, haciendo hincapié siempre en la seguridad de las comunicaciones inalámbricas. En el artículo de hoy, para entender mejor el riesgo al que nos enfrentamos, vamos a ponernos en el supuesto de una gran empresa que celebra anualmente una reunión de todas sus oficinas para hablar de I+D, donde presenta su roadmap y cuentan sus estrategias.

Este evento que, inicialmente, puede parecer inofensivo para la seguridad de la compañía se volverá un problema para su equipo de seguridad como veremos a lo largo del artículo.

Contexto empresarial
La empresa, a la que llamaremos **BIGCOMPANY** es una multinacional de gran éxito, que tiene muchos proyectos a nivel internacional y que, además, tiene un gran peso en la economía nacional de su país de origen. A nivel cyber, sufren constantemente ataques de grupos **APT** (Advanced Persistent Threats) para intentar conseguir información relevante de su estrategia y de sus proyectos, información muy valiosa para los ciberdelincuentes

Por tanto, no es una empresa que invierta poco en medidas de seguridad, pero como venimos adelantando en esta sección, cuando hacemos un "modelado de amenazas" casi siempre nos dejamos de lado, las que tienen que ver con los entornos inalámbricos, y en este caso a **BIGCOMPANY** le salió muy caro no tener en cuenta ciertos aspectos técnicos.

Contexto técnico
La sala de conferencias donde se celebra el evento está ubicada en un conocido hotel de lujo de la ciudad, allí la empresa **BIGCOMPANY** ha alquilado una sala y ha contratado a un equipo de sonido para colocar pantallas, y equipos de sonido para que pueda escucharse perfectamente desde todas partes. Como es una presentación de proyectos, utilizarán proyectos, y diversos medios audiovisuales.
La empresa, ha decidido utilizar micrófonos inalámbricos para aquellas personas que van a explicar ante el público proyectos o avances en I+D, para ello van a utilizar micrófonos de diadema con una "petaca wireless" que llevará el sonido desde el micrófono hasta el centro de control de sonido ubicado al final de la sala.

Los ingenieros de sonido ya estuvieron el día anterior, revisando la sala y ubicando correctamente las antenas direccionales para que pudiesen recibir la señal de las "petacas" perfectamente, sin importar la ubicación del ponente. Además, al encontrarse en un entorno urbano, usaron el software que acompaña a la macar de micrófonos para seleccionar aquellos canales con menos ruido.

Tras un día duro de trabajo, todo el equipamiento audiovisual ya estaba listo, y sólo quedaban hacer las pruebas oportunas y algún que otro ensayo.

Preparando el ataque
Sin embargo, algo que no se esperaban, es que el grupo de ciberdelincuentes **APT9999XC,** conocedor de esta reunión, buscó una ubicación cercana a la sala en el mismo hotel, se alojaron en el mismo hotel previamente para poder estudiar todas las estancias y localizar la que mejores probabilidades tenía para llevar a cabo su ataque. Recordemos que **BIGCOMPANY** es una gran empresa internacional que hace proyectos de I+D muy punteros y su tecnología es codiciada por muchas potencias.

Horas antes de la celebración del evento, se hicieron pasar por trabajadores del hotel, para posicionar un equipo **SDR** camuflado en una ubicación cercana a la sala donde se iba a celebrar el evento. Dicho equipo SDR, también estaba equipado con un sistema de comunicaciones inalámbrico que será el encargado de transmitir todo aquello que recibe a través de una comunicación 4G a los ciberdelincuentes que se encuentran en su "guarida" con todo su equipamiento técnico.

Como querían garantizar su éxito, también buscaron ubicaciones desde las que pudieran apuntar antenas direccionales hacia la ubicación

de la sala; sala que, por desgracia, tenía ventanas. Unas ventanas que daban a la calle, con lo que desde la acera de enfrente se podían ver las ventanas de la sala alquilada por **BIGCOMPANY**.

Recapitulemos, en estos momentos, **APT9999XC** tiene ubicado un dispositivo cerca de la sala, y está ubicado en una posición estratégica enfrente de la sala del hotel desde la que se vislumbra la ventana.

La tarea no es sencilla, ya que no existe un "estandar" de frecuencias y/o modulaciones para poder ubicar fácilmente los micrófonos inalámbricos. En este caso, los atacantes hicieron previamente una labor de investigación y revisaron el CNAF (Cuadro Nacional de Asignación de Frecuencias) para intentar ver, dónde se podrían ubicar según la legislación de vigente en ese país. Con dicha investigación, se encontraron con diversos rangos.

Durante los ensayos, los atacantes, estuvieron analizando todo el espectro en las bandas donde se podrían ubicar los micrófonos. Los sistemas que habían posicionado, les permitieron hacer un "sensado" del espectro, para conocer aquellas frecuencias activas y que tuviesen como origen la sala donde se realizaba el ensayo.

CONTINÚA EN PRÓXIMA PÁGINA

El día "D" momento de llevar a cabo el ataque

Llegó el día "D", tras el desayuno, todos los integrantes de la empresa **BIGCOMPANY** fueron acudiendo a la sala donde estaban citados; nadie sospechaba que ese día iba a marcar un antes y un después en la seguridad de la empresa.

APT9999XC ya estaba preparado, sus equipos listos, y el congreso a punto de comenzar. Todo transcurrió con normalidad, las charlas, los asistentes, etc. Pero nadie sabía que, tras las paredes de esa sala, existían sistemas de captura de RF que estaban decodificando en tiempo real el audio que se transmitía por los micrófonos inalámbricos.

Finalizó el día, y **APT9999XC** volvía a casa, con unas grabaciones muy "suculentas" donde tenía de primera mano, la información y detalle de la estrategia de I+D, así como de los proyectos que se llevarían a cabo en **BIGCOMPANY**.

Meses después, apareció un prototipo muy similar al de un proyecto de **BIGCOMPANY** en el país **CHINTAJISTANZ**, a través de una compañía que había sido identificada como competencia directa de **BIGCOMPANY** en aquel país.

Conclusiones

Cuando hablamos de comunicaciones inalámbricas, casi siempre pensamos en wireless y bluetooth, protocolos ampliamente conocidos por el público en general y que, muchos responsables de seguridad intentan proteger con herramientas y controles adecuados para no ser vulnerados. Pero hoy en día, los ataques que sufren las grandes organizaciones son mucho más complejos, y no siempre tienen como vector de entrada Internet.

En esta historia de hoy, hemos hablado de cómo, se ha vulnerado la seguridad de la empresa, sin necesitar acceder a ningún servidor, sin necesidad de atacar ninguna infraestructura. Si bien, es un ataque muy complejo que no todos los ciberdelincuentes usarán, sirva de ejemplo para conocer los riesgos a los que nos enfrentamos.

Para evitar dar más detalles, se ha reducido al mínimo la complejidad del ataque, y no se han dado detalles de herramientas ni sistemas que podrían haberse utilizado para materializar este ataque. Ahora, por un momento, pensemos en la combinación de este ataque, junto con otros de caracter cyber, o incluso con la combinación de ataques RF (escucha de micrófonos inalámbricos, fake AP en el mismo hotel, fake BTS, etc.) junto con un ataque cyber a las infraestructuras de **BIGCOMPANY**.

Sirva este artículo, como reflexión de cómo debemos realizar nuestro modelado de amenazas, y cómo debemos pensar siempre que sea posible "fuera de la caja" para intentar tener el mayor número de variables controladas.

Realmente, ¿sabemos quién nos escucha?, ahí dejo la reflexión. Espero que os haya gustado el artículo, y nos vemos en la próxima edición.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Continuidad de Negocio

BCI + ISO 22301

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación BCI Executive
- Certificación ISO 22301 Leader
- Módulo 7: MasterGEIT®

MGEIT® eGob®

Del 5 al 13 de julio

+ 34 96 109 44 44
campus@escueladegobierno.es

Jamming GPS y el aumento de los incidentes de seguridad en el tráfico aéreo

Hoy en día, son muchos los sectores, servicios e infraestructuras que dependen de información de posición, navegación y tiempo (PNT). Es el caso de la gestión del tráfico aéreo, que debatiremos a lo largo de este artículo.

Las capacidades **PNT** descansan sobre los sistemas globales de navegación por satélite, también llamados GNSS (Global Navigation Satellite System) que emplean constelaciones de satélites de cobertura global y proporcionan a los usuarios información precisa sobre posición (coordenadas y altura), navegación (rumbo, velocidad) y tiempo (hora y sincronización), en cualquier parte del mundo y de forma permanente.

El Sistema de posicionamiento más conocido, que no el único, es el **GPS** (siglas de Global Positioning System) compuesto por satélites orbitando alrededor de la Tierra, que proporcionan señales radio que son recibidas por los receptores para calcular posicionamiento; entre los sistemas actuales podemos encontrar el americano **(GPS)**, el europeo **(GALILEO)**, el ruso **(GLONASS)**, así como el chino **(BeiDou).**

Los métodos usados para generar interferencias (jamming) o suplantación (spoofing) cambian a medida que aparecen nuevas tecnologías. Por tanto, es de vital importancia, evaluar constantemente las potenciales amenazas para evitar que estas puedan afectar a los sistemas que hacen uso de las señales GNSS, sistemas que, en muchas ocasiones, son infraestructuras críticas o, como comentábamos anteriormente, sistemas para la gestión del espacio aéreo.

Un reciente informe de la OTAN indicaba que, la seguridad del sistema **GPS,** ha sido reconocida como una de las amenazas de seguridad más seria de los últimos años, debido al uso intensivo y grado de dependencia, que hoy en día, se hace de este sistema de posicionamiento.

El acceso al sistema GPS y sus capacidades han crecido tan rápido y se ha convertido en algo tan normal y cotidiano que, no ha dado tiempo a que la gente se plantee la seguridad de este sistema, los vectores de ataque posibles y, por supuesto, las implicaciones que pudiera tener la explotación de vulnerabilidades.

CONTINÚA EN PRÓXIMA PÁGINA


CEBU PACIFIC AIR.COM

Aumento de las amenazas e incidentes debido a los recientes conflictos bélicos

Desde el inicio del conflicto entre Rusia y Ucrania, se han detectado de forma contínua interferencias en los sistemas GPS, lo mismo sucede también, en el reciente conflicto en Israel. El uso de sistemas para interferir las señales GPS se ha intensificado debido al uso de sistemas de guerra electrónica (EW) y. como consecuencia de ello, está provocando serios problemas al tráfico aéreo.

Para luchar contra este tipo de incidentes de seguridad, muchos expertos se reúnen de forma periódica para poder evaluar los sistemas y tratar de buscar soluciones que hagan que los receptores sean más resilientes a este tipo de perturbaciones. Si bien es cierto que ya existen medidas para combatir estas interferencias, su uso no está extendido todavía.

Afectación al tráfico aéreo

Con tanta actividad de sistemas de guerra electrónica (EW) tratando de interferir las señales de los sistemas GNSS en los actuales conflictos, el tráfico aéreo se ha visto afectado.

Muestra de ello, es que la mayor parte del tráfico de aviones comerciales que vuelan al aeropuerto internacional Ben Gurion se ven afectados por estas interferencias, ya que los vuelos cruzan desde el Mediterráneo por encima de la costa.

Para continuar con las operaciones aéreas y garantizar la seguridad (safety) de los aviones y sus tripulantes, son necesarias rutas de vuelo más largas hacia el sureste de Israel; esto cuesta tiempo y combustible.

No solo destaca el caso de vuelos alrededor de Israel, en toda Europa, en medio de este inestable escenario con varios conflictos bélicos en curso, cada día más aeronaves comerciales reportan haber recibido interferencias en sus sistemas de navegación. Tanto es así que, la compañía aérea australiana Qantas ha emitido una carta a sus pilotos informando de estos hechos.

Los sistemas de geoposicionamiento GPS son herramientas esenciales para la navegación aérea. De ellos depende, en buena parte, que el avión siga la ruta preestablecida a través de las aerovías para garantizar la seguridad de todo el pasaje y la tripulación.

El **jamming** es una de las técnicas usadas para generar interferencias malintencionadas que consisten en la emisión de señales de radiofrecuencia on unas características concretas y con una potencia superior, generando una disrupción en los sistemas de recepción de estas señales. Esto se hace, con el fin de bloquear total o parcialmente la recepción de las señales radio transmitidas desde el satélite.

Medidas para combatir este tipo de interferencias

En Europa, las autoridades competentes, han acordado intercambiar información sobre este tipo de incidentes a través del programa Data4Safty de la EASA (Agencia Europea de Seguridad Aérea). Dado que se trata de un problema mundial, es importante, para una mejor y completa comprensión, juntar toda la información disponible mediante la conexión de bases de datos.

Mapa de interferencias de FlightRadar24

Debido a la proliferación de estos ataques, y las noticias que aparecen todos los días en los medios, la conocida web FlightRadar24 anunciaba hace muy poco en su blog una nueva herramienta: “un mapa de interferencias GPS”. Este mapa permite a los usuarios ver áreas donde se han detectado interferencias en las señales GPS en un formato visual muy fácil de entender. Más allá de mostrar la información este nuevo mapa, es también una herramienta de concienciación para hacer ver a todos los usuarios la gravedad que este tipo de amenazas supone para el tráfico aéreo.

Ojalá con herramientas como estas, aumente más la concienciación sobre estas interferencias deliberadas que plantean importantes desafíos para sectores como el de la aviación que, como hemos abordado a lo largo del artículo, dependen de estos sistemas de localización y tiempo (PNT).

Conclusiones

Ahora que ya conocemos un poco la naturaleza de estas amenazas, es importante recalcar que, todas las autoridades que regulan la seguridad de la navegación aérea, clasifican estas amenazas en el ámbito de la ciberseguridad.

Y es que, este tipo de incidentes nos debe hacer reflexionar sobre la importancia de la seguridad de las comunicaciones RF. Ya que muchas veces, cuando hablamos de seguridad, sólo lo aplicamos a las comunicaciones TCP/IP, wireless o bluetooth, pero debemos ser conscientes que otros sistemas de telecomunicaciones pueden verse atacados y que las consecuencias pueden ser, en algunos casos, muy relevantes.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de
Doble Certificación

Gobierno de I&T

COBIT + ISO 38500

Director Académico:

Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COBIT Executive
- Certificación ISO 38500 Leader
- Módulo 8: MasterGEIT®

MGEIT® eGob®

Del 6 al 14 de septiembre

+ 34 96 109 44 44
campus@escueladegobierno.es

El gran hermano te vigila - apaga tus dispositivos inalámbricos -

Vivimos desde hace mucho tiempo en un mundo hiperconectado, rodeados de dispositivos que requieren de conexión a internet y, en la gran mayoría de los casos, a través de protocolos inalámbricos. Uno de los estándares más populares y que seguro que todos conocemos es el protocolo **IEEE 802.11** ampliamente usado en las redes wireless.

Sin duda alguna, esta conectividad trae grandes ventajas y beneficios para los usuarios que hacen uso de esta tecnología a diario. Si nos ponemos a contabilizar cuántos dispositivos inalámbricos llevamos encima seguro que nos salen más de dos o tres. Pero ¿supone un riesgo para nuestra seguridad personal disponer de tantos dispositivos que transmiten información al aire? ## Obtención de inteligencia mediante la captación de señales RF

Normalmente para realizar la localización de un objeto o persona, se hace de forma activa, es decir, disponemos de un dispositivo que es capaz de transmitir su posición a través de una tecnología de comunicaciones: GSM, SIGFOX, etc. Pero ¿qué sucede si somos capaces de seguir y localizar a una persona de forma pasiva sin que esta necesite disponer de ningún objeto adicional?; veamos cómo.

Para obtener inteligencia a través de las señales de radio, es necesario hacer servir distintos sensores que, ubicados en puntos estratégicos, nos permitan poder hacer un mapa de dónde se están produciendo las comunicaciones en un entorno determinado y, con esta información, identificar objetos y/o personas.

Para ver cómo se puede obtener inteligencia, abordaremos el caso de las ciudades. Seguro que los habrás visto, pero igual no conoces cuál es la función de muchos de los sensores que existen en nuestras ciudades. Por ejemplo, muchas de las ciudades más modernas, disponen de sistemas de control de aforos aplicadas normalmente a la medición de parámetros de tráfico y movilidad. Para ello se despliegan estaciones permanentes en puntos concretos de la ciudad, que proporcionan datos sobre la intensidad de vehículos, bicicletas y peatones.

No sólo existen este tipo de sensores, en una ciudad podemos encontrar muchos más; veamos, a continuación, los distintos tipos de sensores, y las tecnologías que usan:

Cámaras con capacidad de identificar obejtos

Muchas de las cámaras de gestión de tráfico que vemos en las ciudades, ya disponen de tecnología avanzada, como para diferenciar objetos (peatones, bicicletas, vehículos, etc), además con el software apropiado son capaces, incluso de leer matrículas, y comprobar en bases de datos la información que reciben.

Aforador radar

Dispositivo que dispone de un pequeño radar, normalmente ubicado en un poste junto a una vía, que opera en la banda de microondas. Al mismo tiempo, el sensor proporciona conteo de vehículos por carril, ocupación, velocidad y clasificación en hasta 12 zonas de detección definidas por el usuario

Aforador Bluetooth y/o wifi

Esta estación detecta y mide las señales wifi y bluetooth recibidas desde los dispositivos a su alcance. Con la información recopilada, clasifica las señales y las almacena de forma individual con un identificador único. Con varias estaciones de este tipo, es posible detectar el mismo dispositivo a lo largo de una ruta.

Para nuestro artículo, este sensor es el más interesante, y a continuación veremos por qué. Pero empecemos a unir piezas, imaginemos que somos capaces de combinar la información recibida por el sensor, con la matrícula del vehículo, tendríamos una forma inequívoca de identificar a un individuo y poder saber en todo momento por donde ha pasado, cuál ha sido su rutina de viaje, y muchos datos más.

Otros dispositivos

Pero no sólo en el exterior, en las ciudades, también existen otros dispositivos que permiten trackear a las personas escuchando solamente las comunicaciones que emiten sus dispositivos inalámbricos. Por ejemplo, los usados en los centros comerciales, supermercados, etc. Todos ellos, utilizan los "beacons" que transmiten nuestros dispositivos móviles para tratar de identificar de forma única a los individuos con fines comerciales y/o de marketing. Información que les permite saber cuál es el recorrido que hacen las personas en un centro comercial, qué lineales se visitan más en un supermercado, etc.

CONTINÚA EN PRÓXIMA PÁGINA

ESTADOS UNIDOS: UN CASO DE ESTUDIO

Si fuésemos capaces de combinar toda esta información y usarla en un entorno como una ciudad, tendríamos algo parecido al "Gran Hermano" capaz de identificar personas. Pues algo así parece estar sucediendo en algunos condados de EEUU.

Los registros de contratación de varios gobiernos locales de EEUU, muestran informaciones de la adquisición de tecnología capaz obtener "inteligencia" a través de las comunicaciones que realizan los teléfonos móviles, smartwatches, auriculares inalámbricos o sistemas de "infoentertainment" de los vehículos.

Según indica un informe de un medio de comunicación de EEUU, el gobierno de Texas ha comprado un producto llamado "TraffiCatch" que es capaz de recopilar información de las señales de protocolos como Wireless, BLE y Bluetooth, entre otros. Según versa la descripción del producto: "TraffiCatch es capaz de detectar señales inalámbricas en vehículos, y fusionarlas con los datos de la matrícula de este." Tanto "TraffiCatch" como otros sistemas similares, aprovechan que los dispositivos necesitan comunicarse de forma inalámbrica entre sí, para analizar esas comunicaciones radio para tratar de identificar a un individuo.

Supuesto caso de obtención de inteligencia a través de las señales de radio

Dejando de lado la noticia de EEUU, supongamos por un momento que, disponemos de acceso a diversos sensores, como los anteriormente citados, a lo largo y ancho de una ciudad. Y que, dicha red de sensores está desplegada por toda la ciudad, cubriendo esta en su totalidad.

Vamos a ponernos en un supuesto caso práctico, imaginemos a un individuo al que llamaremos "Bob" que conduce su vehículo por la ciudad desde el punto A (su casa) al punto B (trabajo), y luego desde B (trabajo) a un punto A (su casa). Dentro de su rutina diaria de lunes a viernes, Bob se mueve desde A a B, y de B a A en un margen de horas más o menos predecible.

Al realizar su trayecto, Bob pasaría por diversos sensores en la ciudad, que detectarían sus dispositivos inalámbricos como su teléfono, su smartwatch, el bluetooth de su vehículo, etc. Como Alicia en el País de las maravillas iría dejando un rastro desde el punto A al punto B, que quedaría registrado en un sistema informático. Si esa información la combinamos con la matrícula de su vehículo, podríamos tener identificado a Bob con nombres y apellidos.

Este es un ejemplo muy sencillo, pero partiendo de esta premisa, podríamos hacer mucho más complejo el ejemplo y evolucionarlo con muchos más sensores. Dejó al lector alguna pista para que pueda indagar por su cuenta. Partiendo del caso anterior expuesto, podemos añadir sensores pasivos como puedan ser la recepción de sensores como **TPMS** (Tire-Pressuere Monitoring System) que, junto con las cámaras de tráfico, y los sensores Wireless, Bluetooth y BLE pueden detectar de forma unequívoca a un individuo. # Conclusiones

Tal y como venimos reflejando en esta sección desde su inicio, muchas veces no somos conscientes de que las comunicaciones inalámbricas suponen un riesgo para nuestra seguridad y privacidad. Aunque poco a poco, se van implementando nuevos controles de seguridad a los protocolos inalámbricos, todavía siguen existiendo ataques que pueden atentar contra nuestra seguridad y privacidad.

Como nota final, dejaremos una vía a explorar y que ampliaremos en siguientes artículos. Y es que, estas técnicas de inteligencia de señales también pueden ser utilizadas para defender nuestra infraestructura con aplicaciones muy diversas como la monitorización de espacios e intrusiones físicas, etc.

Escuela de Gobierno
eGob®
https://escueladegobierno.es

LIVE STREAMING

Curso de
Doble Certificación

Gobierno Corporativo COSO + ISO 37000

Director Académico:
Javier Peris

- Duración 20 horas
- Cuatro sesiones de cinco horas
- Horario Ejecutivo
- Viernes tardes y sábados mañanas
- Curso en Directo y en Remoto
- Certificación COSO Executive
- Certificación ISO 37000 Executive
- Módulo 10: MasterGEIT®
- Módulo 1:0 MasterPPM®

MPPM® MGEIT® eGob®

Del 22 al 30 de noviembre

+ 34 96 109 44 44
campus@escueladegobierno.es

La nueva amenaza en el cielo: “ataques con drones que pueden sembrar el caos”

INTRODUCCIÓN

El auge de los drones de consumo ha transformado fundamentalmente la aviación, introduciendo nuevos desafíos de seguridad y protección frente a estos pequeños dispositivos. Ante esta realidad, las Autoridades de Aviación Civil de todo el mundo han impulsado la adopción de protocolos y reglas de Identificación Remota **(RemoteID)** para drones de consumo. Estos reglamentos exigen que los drones transmitan periódicamente su información, permitiendo a entidades de terceros, como las FFCCSE, identificar y localizar drones y sus operadores.

Las regulaciones de RID surgieron en respuesta a las características peculiares de los drones: su pequeño tamaño, baja detectabilidad por radar, ruido casi imperceptible a distancias largas, capacidad de vuelo a altitudes extremadamente bajas y maniobrabilidad que les permite volar bajo árboles y entre edificios. Estos atributos dificultan el seguimiento fiable de drones mediante tecnologías de monitorización del espacio aéreo existentes, como los sistemas de radar y visión. Los estándares de RID buscan aumentar la seguridad para los operadores de drones y las operaciones en el espacio aéreo, minimizando riesgos en zonas críticas como aeropuertos y bases militares.

EL PROTOCOLO OPEN DRONE ID (ODID)

El protocolo **Open Drone ID** (ODID) es una solución de código abierto diseñada para cumplir con las especificaciones de RID en diversas regiones del mundo. Este protocolo define métodos de comunicación y formatos de mensajes que permiten a los drones transmitir información esencial a estaciones receptoras en tierra. La estructura del mensaje ODID incluye datos como la ubicación del dron, la altitud, la velocidad y la identificación del operador.

El ODID utiliza tecnologías, como **Wi-Fi y Bluetooth**, para transmitir datos de identificación y telemetría. La principal ventaja de este enfoque es que no requiere una conexión a internet o infraestructura en la nube para funcionar, haciendo que los datos estén disponibles para cualquier receptor cercano.

VULNERABILIDADES EN LOS PROTOCOLOS

A pesar de los beneficios de los protocolos RID (RemoteID), la implementación actual de estos sistemas presenta serias vulnerabilidades de seguridad. La falta de cifrado, autenticación y verificaciones de integridad en los datos implica que la información transmitida no puede ser considerada confiable.

Por ejemplo, un atacante podría recrear el impacto de drones en zonas de exclusión de vuelo, sin necesidad de un dron real, simplemente inyectando datos RID falsos en un canal inalámbrico. **Este tipo de ataque podría provocar interrupciones significativas en infraestructuras críticas**, como aeropuertos, con consecuencias económicas y de seguridad graves.

El protocolo Drone ID, desarrollado por DJI, presenta vulnerabilidades críticas que comprometen la integridad y seguridad del sistema de Identificación Remota (RID). En primer lugar, la transmisión de datos carece de cifrado, lo que permite que los datos puedan ser interceptados fácilmente por actores malintencionados. Esta deficiencia en la protección de la información significa que los datos transmitidos desde el dron a las estaciones receptoras pueden ser capturados y manipulados sin ninguna dificultad.

Además, el protocolo Drone ID no implementa mecanismos de autenticación ni verificaciones de integridad para los datos transmitidos. Esta falta de medidas de seguridad permite que un atacante inyecte datos falsos en los canales de comunicación. Como resultado, es posible simular la presencia de drones en ubicaciones específicas sin necesidad de utilizar un dron físico. Esta capacidad de inyectar datos falsos es particularmente preocupante en contextos donde la precisión y autenticidad de la información de vuelo son cruciales para la seguridad, como en aeropuertos y zonas de exclusión aérea.

CONTINÚA EN PRÓXIMA PÁGINA

Por último, la tecnología de radiofrecuencia propietaria de DJI, conocida como OcuSync, también adolece de la ausencia de mecanismos robustos para asegurar la confidencialidad de los datos.
Esta debilidad facilita la realización de ataques de replay, en los cuales los datos de telemetría previamente capturados son retransmitidos para crear trayectorias de vuelo falsas. Esta vulnerabilidad permite que las estaciones receptoras en tierra, como el dispositivo Aeroscope de DJI (usado por FFCCSE para la identificación y control de drones maliciosos), sean incapaces de diferenciar entre datos legítimos y falsificados. En consecuencia, la eficacia del sistema RID se ve comprometida, poniendo en riesgo la seguridad del espacio aéreo y la integridad de las operaciones que dependen de información precisa y confiable.

ESCENARIOS DE ATAQUE

El análisis de las vulnerabilidades de los protocolos, han permitido identificar diversos escenarios de ataque que explotan las debilidades intrínsecas en estos sistemas de Identificación Remota (RID). Cada uno de estos escenarios demuestra cómo un atacante puede manipular la información telemétrica y comprometer la seguridad del espacio aéreo.

Escenario 1:
Falsificación de un solo Dron

En este escenario, un atacante utiliza la inyección de datos falsos para simular la presencia de un único dron en una ubicación específica. El atacante puede transmitir mensajes que contienen coordenadas GPS, altitud y otros datos telemétricos falsificados, creando la ilusión de que un dron está operando en un área restringida. Esta falsificación puede desencadenar una respuesta de seguridad innecesaria, como el cierre temporal de un aeropuerto o la movilización de fuerzas del orden, causando interrupciones significativas en la operación normal de la infraestructura crítica.

Escenario 2:
Falsificación de múltiples Drones

Este escenario amplía el ataque anterior al simular la presencia de múltiples drones en una zona restringida. El atacante puede inyectar varios conjuntos de datos falsos, cada uno representando un dron diferente. Esta técnica de saturación puede sobrecargar los sistemas de monitorización y complicar la respuesta de las fuerzas del orden, ya que tendrán que diferenciar entre múltiples amenazas potenciales. Además, la presencia simulada de varios drones puede desviar recursos críticos y crear un estado de caos y confusión en el área afectada.

Escenario 3:
Nube de Drones

Un atacante puede crear una "nube de drones" mediante la inyección continua de datos RID falsos desde múltiples ubicaciones. Utilizando radios definidas por software (SDR) como el HackRF, el atacante puede transmitir datos telemétricos falsificados que simulan una gran cantidad de drones operando simultáneamente en una amplia zona geográfica. Este ataque puede engañar a los sistemas para que perciban una actividad de dron mucho mayor de la que realmente existe, desbordando los recursos de respuesta y afectando gravemente la seguridad del espacio aéreo. Este tipo de ataque es especialmente peligroso en eventos públicos grandes o cerca de infraestructuras críticas, donde una respuesta rápida y coordinada es esencial.

Escenario 4:
Timer de DroneScout (CVE-2023-29156)

Este escenario explota una vulnerabilidad específica en el temporizador del DroneScout. El atacante puede manipular el temporizador del dispositivo mediante técnicas de "**spoofing**" o **modificación de firmware**. Al alterar la secuencia de recepción de datos, el atacante puede causar que los datos válidos sean ignorados o malinterpretados por el sistema. Esta vulnerabilidad puede ser utilizada para crear lagunas en la monitorización, permitiendo que drones no autorizados operen sin ser detectados durante periodos críticos.

Escenario 5:
Canales Adyacentes del DroneScout (CVE-2023-31191)

En este escenario, el atacante explota la vulnerabilidad de los canales adyacentes del DroneScout. Al manipular las frecuencias de transmisión, el atacante puede interferir con la recepción de datos válidos, perturbando el funcionamiento normal del sistema RID (RemoteID).
Esto se logra mediante la transmisión de señales de alta potencia en frecuencias cercanas a las utilizadas por el DroneScout, causando que el receptor no pueda recibir correctamente la señal. Este ataque puede ser particularmente efectivo en áreas con alta densidad de drones, donde la interferencia en un solo canal puede afectar a múltiples dispositivos simultáneamente.

CONCLUSIÓN

El despliegue global de los protocolos de Identificación Remota (RID) de drones, como el ODID y el DroneID de DJI, son fundamentales para la seguridad y la gestión del espacio aéreo. Sin embargo, las vulnerabilidades actuales en estos sistemas presentan riesgos significativos que deben ser abordados. La falta de mecanismos robustos de seguridad, como el cifrado y la autenticación, deja a los sistemas RID abiertos a un amplio espectro de ataques, que pueden simular la presencia de drones y causar interrupciones en infraestructuras críticas con consecuencias desastrosas.

Una vez más, la seguridad de las comunicaciones radio debe ponerse en valor, ya que como venimos explicando en esta sección, deben formar parte de nuestra estrategia de seguridad.

Escuela de Gobierno

eGob®

https://escueladegobierno.es

Curso de Doble Certificación en:

Gestión de Beneficios y Gestión de Portafolios

P4MGO!® BfM Leader
P4MGO!® PfM Leader

Dirección Académica:
Javier Peris

- Dos formatos para tu comodidad
- Opción A: Remoto en Directo
- Opción B: Virtual con Tutoría
- Metodología P4MGO!®
- Exámenes de Certificación Incluidos
- Certificación P4MGO!® BfM Leader
- Certificación P4MGO!® PfM Leader
- Solicita tu admisión

MPPM® MGEIT® eGob®

Próxima Convocatoria en Directo
Octubre 2024

Solicita tu admisión en:

+ 34 96 109 44 44
admisiones@escueladegobierno.es

P4MGO!

NUEVOS MASTERS

Escuela de Gobierno eGob®
admisiones@escueladegobierno.es
https://escueladegobierno.es