MUniCS

Ciberseguridad en aeropuertos

Ismael Verde Costas

Curso 2022/2023

Universidade Vigo

UNIVERSIDADE DA CORUÑA

Ciberseguridad en aeropuertos
Seguridad en entornos industriales. Curso 2022/2023

Máster Inter-Universitario en Ciberseguridade
Universidade da Coruña
Facultade de Informática
Campus de Elviña s/n
15071, A Coruña

Índice general

1 Introducción

La ciberseguridad en los aeropuertos es un tema crítico y cada vez más importante en la actualidad. Los aeropuertos son lugares altamente conectados, en donde se maneja gran cantidad de información y se utilizan sistemas informáticos variados, lo que los convierte en un objetivo interesante para los ciberdelincuentes. Al mismo tiempo, el transporte es considerado un servicio esencial, siendo el transporte aéreo una gran parte de este. Un ciberataque en un aeropuerto puede tener graves consecuencias, desde la interrupción del tráfico aéreo hasta la exposición de información personal y sensible de los pasajeros. Por lo tanto, es crucial que los aeropuertos implementen medidas de seguridad efectivas y estén preparados para hacer frente a posibles ciberataques.

En este trabajo se explorarán distintos puntos clave en la seguridad de un aeropuerto y del transporte aéreo y se comprobará el nivel de seguridad que tienen. Para comenzar, se investigará acerca de los billetes de avión y su seguridad. Lo siguiente será comprobar el nivel de seguridad de los sistemas IT de un aeropuerto. Por último, se indagará acerca de los nodos de comunicación y posicionamiento que usan los aviones.

2 Ciberseguridad en los billetes de avión

La seguridad en los billetes de avión es esencial para garantizar la integridad y privacidad de la información del pasajero, así como para prevenir el fraude y la falsificación. Los billetes de avión contienen una gran cantidad de información personal y sensible. Entre esta información se suele encontrar: el nombre completo del pasajero, la fecha y hora de salida y llegada, el número de asiento, el número de vuelo y el precio pagado por el billete. En ocasiones, es posible encontrar también información relacionada con la tarjeta de crédito, que también es información sensible. Por todo esto, la seguridad en los billetes de avión es importante para garantizar que solo las personas autorizadas tengan acceso a esta información, evitando así posibles robos de identidad o fraude.

2.1 Investigación sobre los billetes

Para investigar la seguridad de los billetes de avión se han recogido distintos billetes usados de diferentes compañías de vuelo que operan en España. Para mostrar el contenido, se cambiará la información sensible del pasajero por una inventada. Aquí podemos ver un par de ejemplos de 3 billetes de Ryanair, 2 obtenidos en una misma compra para un mismo vuelo y 1 de otro vuelo diferente:

Billete 1: M1AP1 AP2/NOMBRE KYF7TZ VLCBGYFR 4632 038Y002F0146 148>5182W 2037BFR 00000000000002A0000000000000 0 N

Billete 2: M1AP1 AP2/NOMBRE KYF7TZ VLCBGYFR 4632 038Y021F0147 148>5182W 2037BFR 00000000000002A0000000000000 0 N

Billete 3: M1AP1 AP2/NOMBRE NGHTWG SCQBVAFR 2718 342Y007F0166 148>5182W 2341BFR 00000000000002A0000000000000 0 N

Aquí un ejemplo de como se ve el billete para un cliente de ryanair:

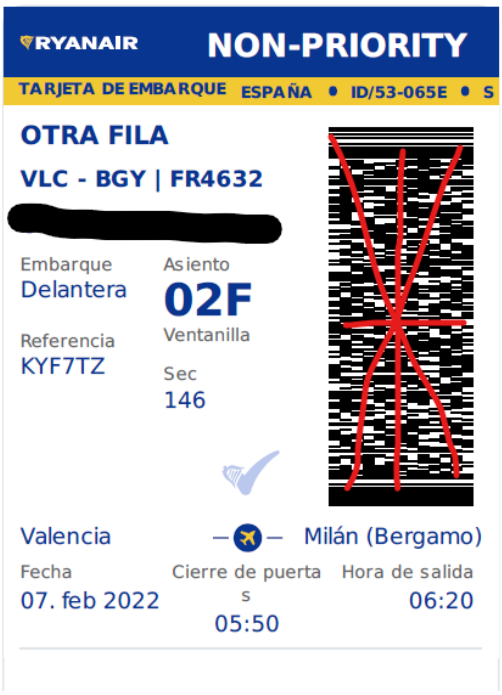

Fig. 2.1: Ejemplo de billete de Ryanair

A partir de comparar los billetes escaneados, se puede sacar la siguiente información:

- El contenido del billete al escanear el QR se puede leer en claro.
- Se puede sacar, en orden, la siguiente información:
  - M1: código del formato del billete
  - AP1 AP2/NOMBRE: apellidos y nombre (en caso de no ser muy largos)
  - KYF7TZ: la referencia de compra
  - VLCBGYFR: salida y destino junto a un identificador de la compañía de vuelo, en este caso, Valencia Bergamo en Ryanair que tiene el identificador FR.
  - 4632: el número de vuelo
  - 038: la fecha juliana
  - Y: clase económica, también puede ser una F de primera clase o una J para business.
  - 02F: Asiento

– 0146: Número de secuencia

– Relleno que es igual para cada vuelo y en su mayoría en todos los vuelos.

Este mismo patrón se puede encontrar en billetes de otras compañías [sha23]. Ahora se ve un ejemplo de Vueling:

Billete: M1AP1 AP2/NOMBRE JHWG9Q SCQPMIVY 3981 061Y023F0108 148>5180 3061BVY 00000000000002A0000000000000 0 N

Fig. 2.2: Ejemplo de billete de Vueling

A partir de esta comparativa se pueden sacar la conclusión de que los códigos QR del billete varían según la compañía, pero la información que contienen siempre sigue el mismo formato.

Estos son algunos de los formatos QR que se usan en los billetes de avión:

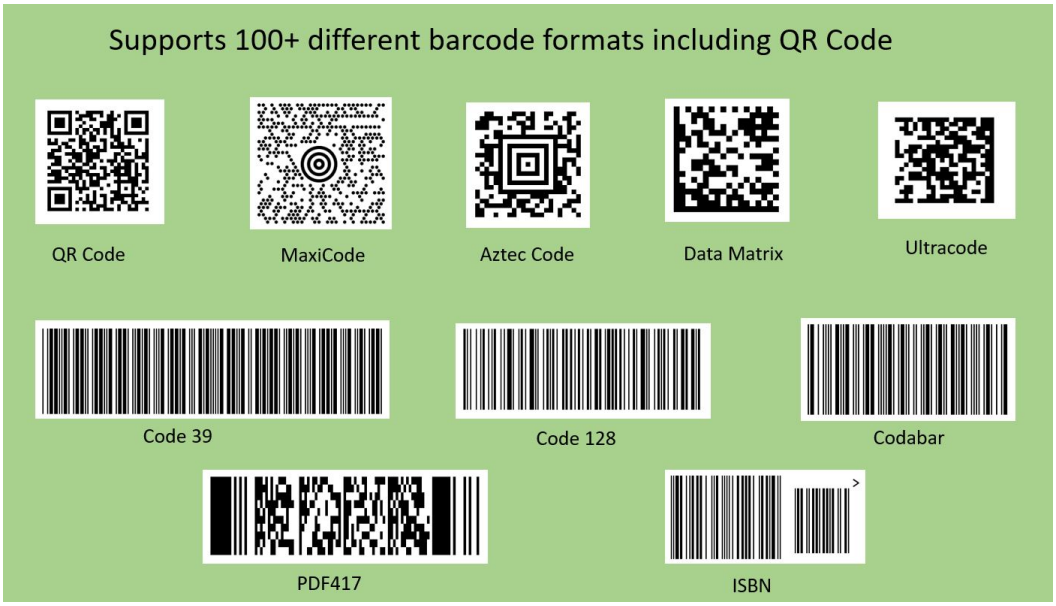

Fig. 2.3: Formatos de QR

2.2 Posibles ataques

Ahora que sabemos que la información se almacena en claro y qué significa cada parámetro del billete, es posible pensar en vulnerabilidades de este sistema.

Los códigos QR son fáciles de escanear y pueden ser leídos por cualquier persona con un teléfono inteligente o un escáner adecuado. Si la información del billete de avión, como el nombre del pasajero, la fecha del vuelo, el número de asiento y otros, se almacena en claro dentro del código QR, esta información podría ser fácilmente interceptada y leída por alguien malintencionado. La interceptación podría darse mediante ingeniería social o simplemente escaneando un billete físico de una persona despistada.

Esto podría llevar a una serie de problemas de seguridad, como la suplantación de identidad, la cancelación del vuelo, la alteración de los datos del pasajero o incluso el acceso no autorizado a los sistemas de la aerolínea. Para esto último la persona maliciosa tendría que pasar antes que el pasajero legítimo por los sistemas de control o falsificar o clonar el billete obtenido para crear uno nuevo a partir del verdadero.

En cuanto a falsificar y clonar billetes, se debe profundizar en como se hace y como se podría impedir. Si el contenido del mismo se encuentra en claro en un QR, es sencillo crear un nuevo QR que contenga datos sobre un vuelo si se conocen los

parámetros que identifican al mismo. Para conocer algunos de estos parámetros, como el número de vuelo, el número de secuencia o la referencia de compra, es necesario tener un billete real para poder incorporar los datos reales al billete.

Sin embargo, todo depende de las comprobaciones que hagan internamente los sistemas de control de acceso. A continuación se describen algunas comprobaciones que deberían realizarse:

- Comprobar que un mismo billete no puede pasar 2 veces por mismo sistema de control de acceso: si no se hace, una persona podría comprar 1 solo billete y compartirlo con más personas para viajar todos.
- Comprobar si un billete es íntegro y no ha sido modificado: si no se hace, una persona podría modificar si billete y falsificar otros a partir del mismo, bastaría con cambiar el número de secuencia y el asiento. Como el overbooking (venta de más plazas de las disponibles) es un problema real, en caso de coincidir en asiento con otro pasajero, se podría usar como excusa.
- Comprobar si el número de secuencia corresponde a un billete comprado y si este coincide: si no se hace, podrían crearse billetes falsos con números de secuencia aleatorios.

2.3 Posibles soluciones

La mejor solución para evitar el clonado o falsificación de billetes es cifrar el contenido del código QR del billete. Una vez escaneado el QR, el sistema internamente se encargaría de descifrar el texto leído y mostrar la información en claro para cualquier sistema de control de acceso que lo precise.

Además, deberían implementarse los sistemas de comprobación de integridad mencionados anteriormente en los controles de acceso. De esta forma, se aseguraría de manera casi segura que no se realiza una clonación o falsificación de billetes.

3 Ciberseguridad en los sistemas IT de un aeropuerto

Los sistemas de Tecnología de la Información (IT) son fundamentales para el correcto funcionamiento de un aeropuerto en la actualidad. Estos abarcan desde los sistemas de información para pasajeros, hasta los sistemas de seguridad y control de tráfico aéreo. Los sistemas IT permiten la gestión de una gran parte de los procesos y operaciones en el aeropuerto, lo que hace que sean un componente crítico. Debido a esto, es esencial que los sistemas IT del aeropuerto sean seguros, eficientes y fiables. En este apartado se mencionarán algunos de los sistemas IT más importantes de un aeropuerto y posibles ataques que podrían sufrir.

3.1 Los diferentes sistemas IT de un aeropuerto

Para listar los diferentes sistemas IT, se ha tomado como referencia las soluciones IT que ofrece AERTEC en su página web [AER23]. Otras compañías ofrecen productos similares, por lo que los ataques listados en un futuro también serían parecidos.

Algunos sistemas IT interesantes son:

- ATIKA (Airport Touchscreen Information Kiosk Assistant): consiste en un sistema multi-plataforma y multi-dispositivo orientado a brindar, de forma interactiva y en tiempo real, información útil a pasajeros, aeropuertos y concesionarias. Su objetivo es gestionar de una forma más eficaz los servicios aeroportuarios a la vez que mejora sensiblemente la experiencia del pasajero.
- AERTASK / Sistema móvil de gestión de tareas: permite gestionar las tareas relacionadas con el aeropuerto, tales como: pasarelas, limpieza, mantenimiento, asistencia a PMR, control de calidad, etc. Además, proporciona a las concesionarias de terceros las herramientas que necesitan para cumplir el ANS del aeropuerto con dispositivos móviles.
- Sistema de supervisión del flujo de pasajeros: sistema de supervisión en tiempo real del flujo de pasajeros con tecnología Bluetooth. Permite escalar los recursos

del aeropuerto estimando la duración de las colas en los filtros de seguridad, con el objetivo de mejorar la experiencia de los pasajeros.

3.2 Posibles ataques

A continuación se listarán una serie de ataques posibles hacia las tecnologías anteriormente descritas. Sin embargo, es posible orientar estos ataques a otros dispositivos similares que se pueden encontrar en cualquier aeropuerto.

Algunos de los ataques posibles son:

- DDoS: los ataques de denegación de servicio distribuidos (DDoS) son un tipo de ataque que puede afectar a los sistemas IT del aeropuerto, impidiendo que los sistemas de la aerolínea y del propio aeropuerto estén disponibles para los usuarios legítimos.

- Acceso no autorizado: los sistemas IT del aeropuerto pueden ser vulnerables a ataques de acceso no autorizado, ya sea por una vulnerabilidad u obteniendo el acceso mediante ingeniería social, los atacantes consiguen acceso no autorizado a los sistemas de la aerolínea y del propio aeropuerto.

- Malware: la inyección de malware a los sistemas informáticos de un aeropuerto puede dañar los datos y sistemas de la aerolínea y del propio aeropuerto.

- Ataques por Bluetooth: pese a que bluetooth es una tecnología cómoda de usar, es altamente vulnerable a distintos ataques. Algunos de los sistemas IT de los aeropuertos usan bluetooth y permiten ser controlados desde un móvil y, por lo tanto, podrían ser vulnerables a ataques como Bluesnarfing, Bluebugging, Jamming o Man in the Middle.

- Ingeniería social: los atacantes tratarían de engañar a los usuarios para que divulguen información confidencial o realicen acciones maliciosas. Los empleados del aeropuerto y los pasajeros son susceptibles a los ataques de ingeniería social. Para este ataque en concreto, se ha preparado un ejemplo para demostrar como un atacante, mediante ingeniería social, puede engañar a un cliente:

  En este caso, el atacante se hace pasar por un punto de acceso WiFi legítimo. La víctima en busca de una red WiFi a la que conectarse, entra en la red del ciberdelincuente y se encuentra con la siguiente pantalla:

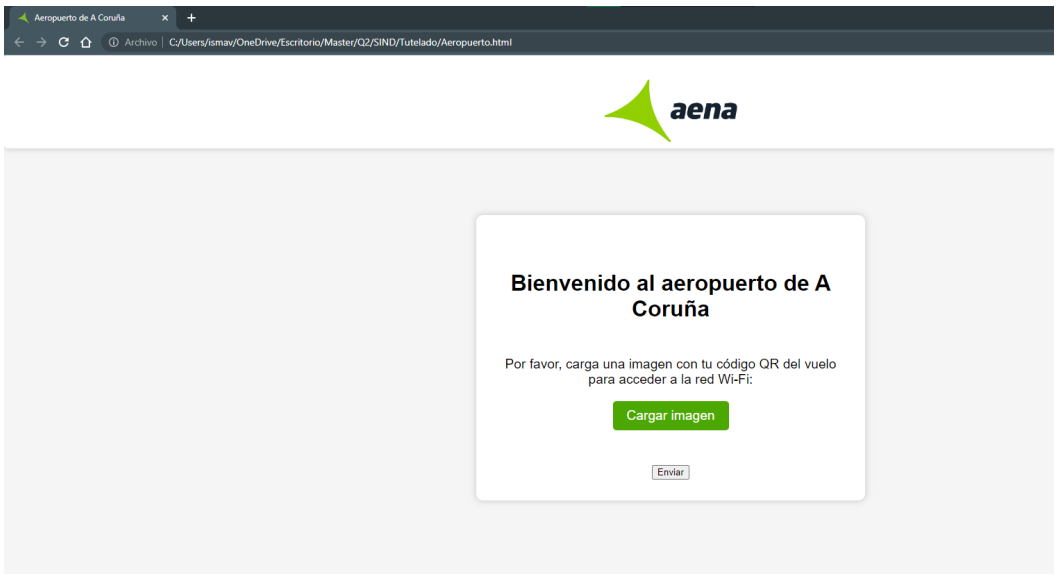

Fig. 3.1: Visualización del portal cautivo en un PC

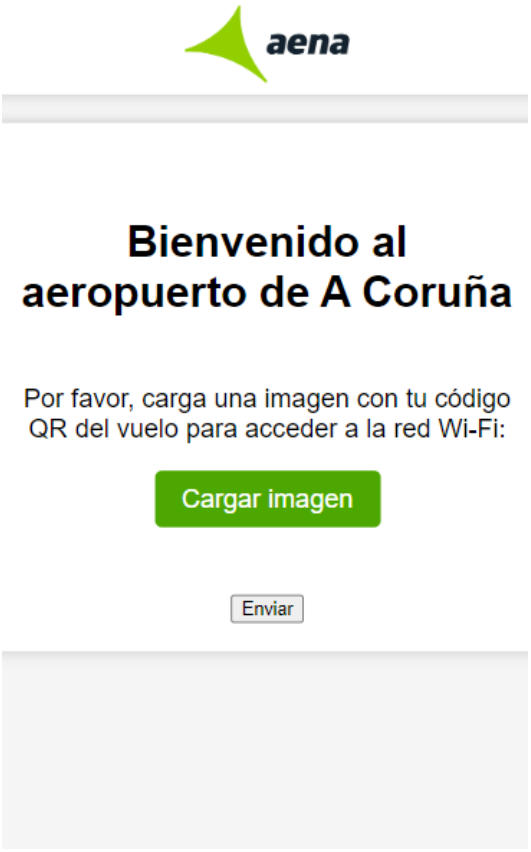

Fig. 3.2: Visualización del portal cautivo en un móvil

El atacante ha creado un portal cautivo para que las víctimas del mismo le entreguen sus billetes de vuelo. Con ellos, podrá hacer un clonado y falsificación de los mismos como se veía en el anterior capítulo 2. Este ataque se centra en los clientes, sin embargo, métodos similares pueden ser empleados para engañar a personal del aeropuerto en busca de credenciales de sistemas IT.

3.3 Posibles soluciones

Proteger los sistemas IT de un aeropuerto no es tarea sencilla, puesto que los ciberataques mencionados son muy variados y evolucionan con el tiempo. Para asegurar la protección de estos sistemas, los aeropuertos deberían seguir una serie de pautas:

- Mantener el software actualizado: esto ayuda a proteger el sistema contra vulnerabilidades conocidas y reduce la posibilidad de que los atacantes exploten estas debilidades.
- Evitar usar Bluetooth para el control de sistemas IT: pese a ser una tecnología cómoda de usar, esta cuenta con múltiples vulnerabilidades y no sería recomendable usarla en un sistema de un ámbito tan crítico como el transporte aéreo.
- Fortificar el control de acceso: se deberían establecer políticas de control de acceso para limitar quiénes pueden acceder a los sistemas IT. Se deberían también implementar controles de autenticación sólidos, como el uso de contraseñas seguras, autenticación de dos factores y sistemas de reconocimiento biométrico.
- Formar al personal y concienciar a los clientes: impartiendo programas de formación y campañas de concienciación para educar a los usuarios sobre las buenas prácticas de seguridad cibernética, se podrían reducir los riesgos de los ataques de ingeniería social.
- Monitorizar los dispositivos: establecer un sistema de monitorización para detectar posibles amenazas en tiempo real permitiría una respuesta rápida y efectiva a los ataques, aumentando la capacidad del aeropuerto para proteger sus sistemas IT.

4 Ciberseguridad en los nodos de comunicación y posicionamiento

Los sistemas de comunicación y posicionamiento son esenciales para garantizar la seguridad y eficiencia del transporte aéreo. Sin embargo, estos sistemas también son vulnerables a los ciberataques, que pueden dar lugar a consecuencias catastróficas. Por lo tanto, es fundamental que se implementen medidas de seguridad adecuadas para proteger estos nodos.

En Internet existen diversas webs que muestran información sobre el tráfico aéreo del planeta en tiempo real, véase planefinder.net [Pla23]. La fuente de datos principal de estos sitios web y la clave de estos sistemas, es ADS-B.

ADS-B (Automatic Dependent Surveillance Broadcast), es una tecnología de vigilancia cooperativa en la que un avión determina su posición a través de la navegación por satélite y la emite periódicamente, lo que permite realizar su seguimiento. Contiene información útil como el ID del avión, la altitud, la posición en lat/lon o la velocidad. Es práctico especialmente en zonas muertas para radares como regiones montañosas u océanos. Tiene 2 modos:

- ADS-B Out: en este modo, el sistema transmite toda la información mencionada anteriormente. El envío de información es automático. Usa las frecuencias 1090Mhz para aviones comerciales y 978Mhz para aviones más pequeños.
- ADS-B In: en este modo, el sistema es capaz de recibir la información enviada por otro ADS-B. Esto se usa en aviones para recibir información útil de otros aviones y en sistemas en tierra.

4.1 Posibles ataques

A la hora de hablar de ADS-B, en términos de ciberseguridad, lo más interesante sobre este protocolo es que ADS-B no está cifrado ni usa autenticación. Cualquier

persona puede escuchar en la frecuencia 1090Mhz y decodificar las transmisiones de un avión en tiempo real. Esto da lugar a diferentes amenazas:

- Escuchar a escondidas las transmisiones: es sencillo capturar en texto claro los datos del tráfico aéreo.
- Inyectar datos en el tráfico aéreo: es posible crear vuelos fantasmas en los sistemas de tráfico aéreo sabiendo como se distribuye la información y en qué frecuencia.
- Crear el caos: a raíz del punto anterior, sería posible crear muchos vuelos fantasma en lugares y momentos clave como en vacaciones, destinos populares o eventos masivos como en la sede del mundial de fútbol o las olimpiadas, por ejemplo.
- Crear vuelos fantasma regulares para engañar al sistema: de nuevo, gracias a los vuelos fantasma se puede causar confusión en el tráfico aéreo. En una Defcon, se mostró como una persona era capaz de generar un vuelo fantasma a través de la información de un juego de simulación de vuelo. De esta forma, si posición virtual en el juego, aparecía en los radares en el mundo real [Man12]
- Jamming: se puede interferir en las señales de ADS-B y provocar fallos en la comunicación.
- Jamming a GPS: es posible bloquear los GPS de los aviones con interferencias, con lo que se pierden todas las ventajas de ADS-B. Este método lo usa Corea de Norte sobre sus fronteras.
- Inyectar datos en los ADS-B In: se pueden inyectar datos confusos, imposibles o que causen pánico en los sistemas de recepción.
- GPS spoofing: se podría introducir una señal manipulada para generar información falsa como la localización del avión.

4.2 Posibles soluciones

En vista de lo peligrosas que son las amenazas vistas en el apartado anterior, es necesario que se trabaje en soluciones para mitigarlas. La Administración Federal de Aviación respondió ante críticas surgidas por estos posibles ataques diciendo que eran conscientes de los riesgos en su seguridad, pero no enseñó ninguna técnica de mitigación debido a que esta información estaba clasificada. Una posible mitigación

es la multilateración, que es una técnica para determinar la posición de un vehículo basada en la medición de los tiempos de llegada (TOA) de ondas de energía (radio, acústica, sísmica, etc.) que tienen una forma de onda y una velocidad conocidas cuando se propaga desde (navegación) o hacia (vigilancia) múltiples estaciones del sistema. Sin embargo, este sistema prácticamente no es usado en la aviación.

Conclusión

5

A partir de lo visto en este trabajo, se puede afirmar que la ciberseguridad en los aeropuertos es fundamental para garantizar la seguridad de los pasajeros, la protección de la información personal y la integridad de los sistemas de las aerolíneas. Sin embargo, a pesar de los esfuerzos y las medidas de seguridad implementadas, actualmente los aeropuertos y el tráfico aéreo no son todo lo seguros que podrían ser.

A lo largo del trabajo, también se han visto distintas soluciones ante las vulnerabilidades presentadas. Es importante que los aeropuertos continúen invirtiendo en medidas de seguridad nuevas y efectivas, así como la educación y concienciación de los usuarios y personal sobre los riesgos y buenas prácticas de seguridad cibernética.

En conclusión, los aeropuertos y el sistema de transporte aéreo no son todo lo seguros que deberían y es necesario invertir más en la ciberseguridad de los mismos.

Bibliografía

[AER23] AERTEC. *Soluciones IT AERTEC*. 2023. URL: https://aertecsolutions.com/aviation/soluciones-it/ (vid. pág. 11).

[Man12] Render Man. *Spoofing ADS-B*. 2012. URL: https://www.youtube.com/watch?v=NSLqRXyxiBo (vid. pág. 16).

[Pla23] PlaneFinder. *Flight Tracker - Live Flight Tracking*. 2023. URL: https://planefinder.net/ (vid. pág. 15).

[sha23] shamooo. *Have a safe flight*. 2023. URL: https://infosecwriteups.com/have-a-safe-flight-hacking-the-boarding-pass-6016a2a6ff59 (vid. pág. 7).