TRABALLO TUTELADO
CIBERSEGURIDADE EN CONTORNAS INDUSTRIAIS
MÁSTER INTERUNIVERSITARIO EN CIBERSEGURIDADE

Ciberseguridade en contornas aeroportuarias

Estudante: Mauro A. de los Santos Nodar

A Coruña, abril de 2022.

Índice Xeral

Capítulo 1
Introdución

Os aeroportos son considerados hoxe en día infraestruturas críticas, xa non só polos 8 millóns de persoas que viaxan a diario a través deles [1], senon tamén pola importancia que teñen na sociedade globalizada actual o transporte inmediato e a mobilidade en xeral. Por outra banda, neles atopámonos con auténticas cidades comprimidas nunha pequena superficie e *macro-tecnoloxizadas*, con todo o bo e malo que isto conleva. Relacionando isto co concepto de ciberseguridade, vemos como mesturar dúas características como son a importancia dun sistema crítico xunto ca diversidade de ameazas presentes en cidades *ultra-tecnoloxizadas*, da lugar a unha combinación perigosa que pode ser moi interesante de cara aos ollos de dito campo. Dado que o tema é realmente amplo, imos dividir o traballo de igual forma que poderiamos dividir un aeroporto, segundo as partes máis importantes que o conforman, ocupándonos así dos diferentes vectores de ataque que podemos atopar neste tipo de infraestruturas. En primeiro lugar, falaremos do que respecta ás **persoas**, onde intentaremos aproveitar este conxunto de caracterísiticas comentadas para atacar e defender algo tan importante como son os habitantes de ditas cidades aeroportuarias. Respecto a isto, a experiencia dinos que o eslabón máis débil da cadea sempre adoita ser o humano, polo que as persoas terán que ser sempre contempladas coma un potente vector de ataque, e quizais coma o primeiro paso ou punto de entrada de ataques máis elaborados, sen deixar de lado o propio dano que se lles pode ocasionar ás mesmas. En segundo lugar, falaremos da propia **infraestrutura aeroportuaria**: os aeroportos están cheos dunha infinidade de tecnoloxías, máquinas e sistemas, polo que atacalos, a veces pode ser igual de efectivo ou máis que atacar calquera outra parte dos mesmos. E por último, abordaremos a temática dos **vehículos** destas contornas, que aínda que poidan ser, de igual forma que no anterior caso, de múltiples tipos (por exemplo helicópteros, drons, autobuses ou vehículos de transporte), ocuparémonos do máis principal e protagonista: os avións comerciais.

Vemos entón esta división estrutural en tres partes que van seguir tamén as respectivas seccións do traballo. Onde, primeiro, faremos un repaso das tecnoloxías máis empregadas e comúns nestas contornas, definíndoas brevemente e vendo a grandes rasgos como funcionan, que aplicacións teñen e o seu impacto na seguridade, para saber así despois que estamos a explotar e como poder optimizar ditos ataques. Tras isto, comentaremos diversos casos prácticos, máis en concreto, mínimo dous de cada un dos tres apartados mencionados, que se aproveiten todos eles das vulnerabilidades asociadas ás tecnoloxías expostas e intenten causar o maior dano posible, vendo tamén para cada caso, posibles solucións a tomar para evitalos. Recalcar por último antes de comezar co capítulo referente ás tecnoloxías, que por motivo da complexidade de obter a posibilidade de facer probas nuha contorna aeroportuaria real, unha gran parte do apartado práctico estará baseado en estudios e ataques realizados por terceiros, concretamente, a base fundamental serán as charlas *DEF-CON* atopadas na canle de *Youtube* de **Aerospace Village** [2]. De igual maneira, levaranse tamén a cabo demostracións empíricas nunha serie dos casos prácticos, implementando para este traballo os escenarios amosados. Buscarase por tanto facer un balance da aplicabilidade e realismo da parte práctica, xunto ca complexidade e dificultade de certos ataques, para darlle así un carácter máis heteroxéneo e completo ao traballo.

Capítulo 2

Tecnoloxías: definición, aplicacións e impacto na seguridade

A continuación falaremos das tecnoloxías máis habituais e empregadas nos tres subapartados deste traballo. Faremos especial fincapé naquelas referentes á parte dos vehículos, ao seren estas máis descoñecidas e moito máis complexas. Consistirán en tecnoloxías usadas fundamentalmente por avións comerciais nas súas comunicacións, sendo todas elas atacadas ou empregadas na parte práctica da memoria. En canto ás tecnoloxías referentes ás outras dúas partes, persoas e infraestrutura, trataranse de protocolos máis coñecidos e habituais, algúns deles comentados en profundidade incluso na asignatura e no máster, coma poden ser WiFi ou IoT, polo que non os abordaremos en tanto detalle. De igual maneira, destacaremos todos aqueles que sexan empregados na parte práctica. Vemos entón de forma breve ditas tecnoloxías divididas nas tres seccións comentadas.

2.1 Persoas

2.1.1 WiFi

Sen dúbida, o primeiro que debería vir a mente de calquera experto en ciberseguridade ao mencionar a posibilidade de atacar ás persoas dun aeroporto, debería ser a tecnoloxía WiFi. Os aeroportos basean, tanto a nivel público como privado, gran parte do seu funcionamento nesta tecnoloxía, indo por exemplo dende as propias compañías aéreas para a organización nos mostradores de embarque ou o acceso do persoal a certos servizos, ata aos viaxeiros que requiren de conexión a Internet mentras esperan polo seu voo. Máis que detallar os fundamentos tecnolóxicos do WiFi, que como ben dixemos antes, xa se abordan na asignatura e no máster en xeral, imos comentar nesta subsección unha das partes da tecnoloxía que pode ser máis útil para posibles ataques: **o portal cautivo**.

Portal cautivo

Os portais cautivos WiFi son un tipo de páxinas web que automaticamente ao conectarse a unha rede WiFi se abren nun navegador para, dunha ou outra forma, demostrar que se dispón da autorización requerida para empregar dita rede [3].

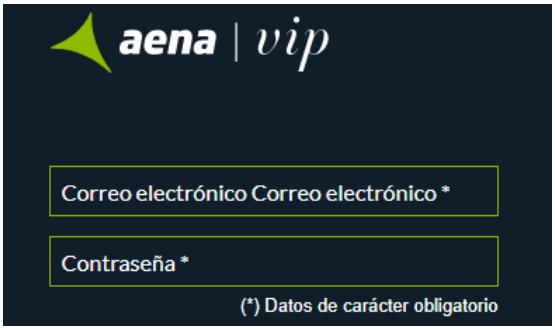

Figura 2.1: Exemplo de portal cautivo WiFi dun aeroporto.

Dita tecnoloxía aporta aplicacións e beneficios obvios como poden ser protexer o uso ilegal do acceso a Internet, controlar a conexión ou filtrar o tráfico, pero tamén leva implícitas unha serie de vulnerabilidades que poden ser explotadas por un atacante, como por exemplo a falta de mecanismos de demostración de autenticidade ou a sinxeleza da implementación dos mesmos. No caso dos aeroportos, é tipico que existan unha ou máis redes WiFi abertas, sen contrasinal, que ao conectarse a elas fagan uso desta tecnoloxía para garantir ou non a conectividade a Internet, polo que dentro de WiFi, este será o principal vector de entrada que utilicemos para atacar ás persoas dun aeroporto. Nin que mencionar cabe a importancia hoxe en día de ter en todo momento conexión a Internet por parte da xente, polo que esa necesidade, mesturada cas vulnerabilidades comentadas e un bo uso de enxeñería social [4], pode traer consecuencias moi graves na ciberseguridade das persoas dun aeroporto.

2.1.2 PDF417

Outra das formas para atacar ás persoas pode ser explotando as súas tarxetas de embarque. É certo que esta tecnoloxía pode pertencer a outras seccións, pero debido á compoñente humana que teñen as tarxetas de embarque, imos comentala neste apartado. **PDF417** é un formato de código de barras, é dicir, de información codificada nunha dimensión, amplamente utilizado en variedade de aplicacións, sobretodo en transporte e inventario. PDF significa *Portable Data File* e o número 417 significa que cada patrón no código consiste en 4 barras e espacios, e que cada patrón é 17 unidades de largo [5].

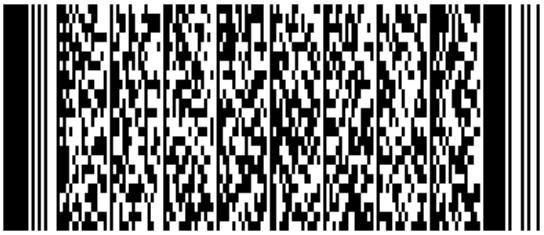

Figura 2.2: Exemplo de código PDF417.

Neste traballo resultará moi útil dita tecnoloxía porque é a empregada polas tarxetas de embarque impresas de todas as aeroliñas de todos os aeroportos do mundo, segundo dicta o estándar da IATA [6], o cal comentaremos na sección práctica.

2.2 Infraestrutura aeroportuaria

Nesta sección ocuparémonos das tecnoloxías propiamente relacionadas ca infraestrutura física dos aeroportos. Todas elas son comúns a outras contornas e teñen especial similitude cas contornas industriais, polo que é unha temática moi relacionada ca asignatura. Mencionamos a continuación algunhas das máis importantes.

2.2.1 Acceso físico

Pode parecer unha obviedade, pero a veces simplemente tendo a facilidade dun acceso físico a tomas ou dispositivos *hardware* que non se debera, conséguese sen case esforzo, un gran dano. Exemplo disto son os accesos a cables para desconectar pantallas, ordenadores, cámaras de seguridade, etcétera. Aínda que pode parecer unha temática non relacionada, a seguridade física dos dispositivos electrónicos tamén é un subconxunto da ciberseguridade, e se como vemos na seguinte Figura 2.3, temos acceso a desactivar unha pantalla con información crítica de voos para os pasaxeiros, unha cámara ou un sensor de seguridade que vixía un terminal crítico, incluso a veces simplemente acceso a un porto USB ou Ethernet, podemos conseguir inflinxir un gran dano e saltarnos unha enorme serie de medidas de seguridade, que dunha forma lóxica, requerirían de complexos e longos ataques, para finalmente acabar causando disrrupción ou simplemente dando un primeiro paso no caso de ataques moi elaborados, como veremos na parte práctica. A continuación vemos o caso real dunha pantalla FIDS dun aeroporto, á cal temos acceso físico nun lugar externo e sen cámaras de seguridade, onde poderiamos desconectala ou acceder libremente a varias tomas USB, así como a un cable Ethernet conectado (aínda que non se poidan apreciar ben), accións que podrían dar lugar a graves incidentes de ciberseguridade.

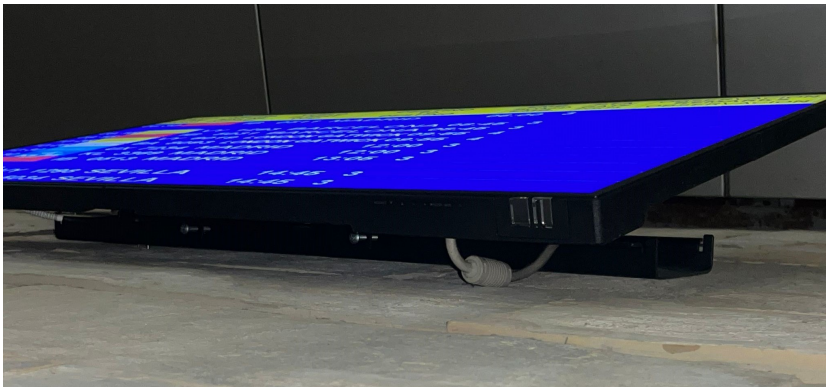

Figura 2.3: Acceso físico a unha pantalla FIDS dun aeroporto.

2.2.2 CCTV

CCTV fai referencia a *Circuito cerrado de televisión*, e non é máis que a tecnoloxía de videovixiancia para supervisar diferentes actividades ou recintos [7], neste caso, aeroportos. Estes sistemas cobran moita importancia nos ciberataques contra a infraestrutura porque hoxe en día, a maioría deles usan tecnoloxías sen fíos e cámaras IP con WiFi ou conexión a Internet para transmitir, así como páxinas web vulnerables para acceder ao que está sendo transmitido. De feito, como xa se viu na asignatura, empregando a ferramenta Shodan [8], cunhas búsquedas concretas e aproveitando a funcionalidade de mapa xeográfico da mesma [9], podemos explotar e ver con dous *clicks*, vulnerabilidades e portais de *login* dos circuitos de videovixiancia abertos de calquera aeroporto do mundo. Todo isto, sen olvidarnos da comentada seguridade física do propio CCTV.

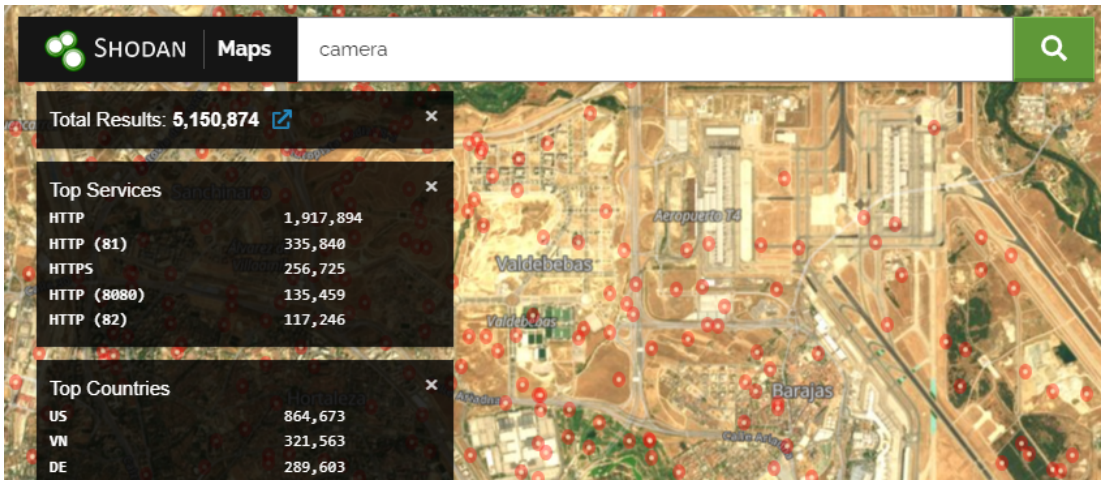

Figura 2.4: CCTV dun aeroporto dende Shodan.

2.2.3 FIDS e GIDS

Para acabar cas tecnoloxías da infraestrutura aeroportuaria, relacionados cos puntos anteriores temos os FIDS e GIDS. **FIDS** é o acrónimo de *Flight Information Display System*, o cal consiste en sistemas baseados en computador para mostrar nos aeroportos a información referente aos voos do mesmo, onde de forma centralizada, un ordenador administra ás pantallas distribuidas polo aeroporto a información de chegadas e saídas de voos en cada momento. Normalmente amosan información como o *ICAO*, identificador único dos voos (i.e., IB123), cidade de orixe ou destino, estado e hora prevista. Por outra banda, **GIDS** é o acrónimo de *Gate Information Display System*, subtipo en moitos casos do FIDS, cuxa función é amosar a información referente ás portas de embargue dos voos dun aeroporto.

Figura 2.5: Pantalla co FIDS dun aeroporto.

Ambas tecnoloxías teñen un gran impacto nun aeroporto, xa que a interrupción do seu funcionamento pode desatar o caos nos pasaxeiros, como xa temos comprobado en ataques pasados amosados en [10] ou [11]. En canto á definición da tecnoloxía de xeito máis técnico, tenden de forma normal a organizarse de xeito centralizado, onde normalmente un equipo central, o servidor, comunica ás diferentes terminais a información de voos e portas de cada momento. Por outra banda, en cada terminal adoita haber un sistema operativo lixeiro embebido, normalmente tipo UNIX, o cal só conta (ou debería) cas funcións necesarias para recibir a información de voos e portas, *parseala*, e mostrala no formato axeitado na pantalla á que está conectada. Unha tecnoloxía moi empregada é Zabbix [12], sistema de monitorización para rexistrar os estados de servizos de rede, servidores e *hardware*. Emprega normalmente bases de datos relacionales por debaixo, estilo MySQL ou SQLite, e segue o modelo de múltiples axentes recibindo ou enviando información dun só servidor. Por último, en canto esta tecnoloxía, debemos facer mención a que adoitan ser implementacións propietarias, dispoñibles no mercado por diferentes precios e que inclúen diferentes funcionalidades, polo que o seu impacto na seguridade así como os ataques ás mesmas, poden variar moito dun modelo de produto a outro. Destacamos por exemplo os ofertados por *Indra* [13] ou *Amadeus* [14].

2.3 Vehículos

Nesta última sección do capítulo imos encargarnos de falar daquelas tecnoloxías das contornas aeroportuarias referentes aos vehículos, e máis en concreto, aos avións comerciais presentes neles. Consistirán principalmente en protocolos de comunicación destes. Será necesario ter un mínimo coñecemento delas para saber despois na parte práctica que estamos a atacar, así mesmo, debido á súa complexidade e extensión, así coma polos tempos dispostos para o traballo, non sei vai afondar nelas, senon que máis ben, a seguinte sección consistirá nunha enumeración e resumo a grandes rasgos de cómo funcionan e para qué se usan, é dicir, falar da súa definición e aplicacións, xunto co impacto a nivel de seguridade que pode supor atacalas.

2.3.1 TCAS

O *Traffic Collision Avoidance System* ou *Traffic Alert and Collision Avoidance System* [15] é o sistema empregado para evitar a colisión de aeronaves. Proporciona axudas visuais e auditivas aos pilotos, amosando información do resto de tráfico aéreo de aeronaves cercanas. Estas mensaxes poden estar en dúas *burbullas*, como ben vemos na seguinte Figura 2.6: a *TA* e a *RA*. A zona **TA**, en laranxa, non supón unha zona de ameaza inmediata e as mensaxes enviadas serán *Traffic Advisory*. Cando se entra na zona rosa, a **RA**, envíanse mensaxes *Resolution Advisory*, as cales indican ao piloto que ten que tomar accións inmediatas para evitar a colisión. Estes *RAs* obligarán ben a ascender ou descender ca finalidade de evitar a colisión, nunca movéndose en vertical. Teñen prioridade fronte a calquera outro tipo de mensaxe de control. As aeronaves interróganse varias veces por segundo entre elas con estas mensaxes, e adoitan comunicarse en frecuencias que oscilan os 1030 a 1090 MHZ. Por outro lado, existe o chamado ADS-B (*Automatic Dependent Surveillance-Broadcast Protocol*) [16], tecnoloxía para determinar a posición dunha aeronave via navegación satélite e outros sensores que emiten a direccións *broadcast*, para que dita información sexa *trackeada* e *parseada*. Certas naves poden ter un modo híbrido, mesturando ambas tecnoloxías TCAS e ADS-B, o que normalmente altera o funcionamento de TCAS ralentizando o procesado das mensaxes TCAS e facendo ao sistema en xeral, máis propenso a ataques ao gozar unha maior superficie a atacar. Todo isto verémolo no apartado práctico.

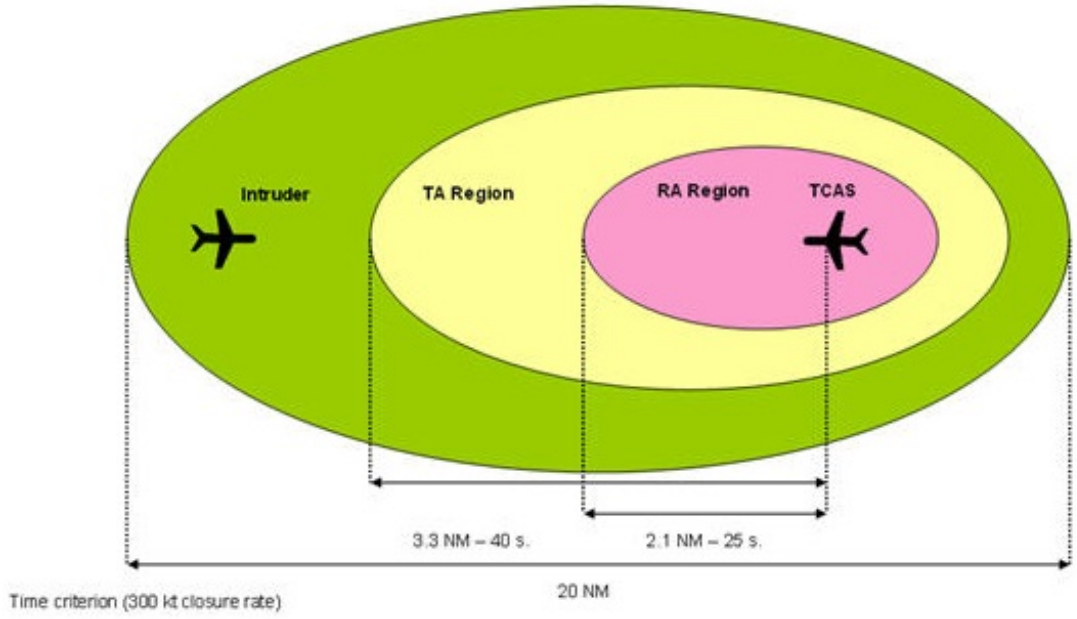

Figura 2.6: TCAS.

2.3.2 ILS

Estas siglas fan referencia a *Instrument landing system* [17]. Este protocolo brinda un guíado lateral e vertical aos pilotos cando se pretende aterrar. É tipicamente usado en malas condiciones temporais aínda que pode ser empregado en calquera momento. A súa finalidade é asegurar que a aeronave esta aliñada ca pista de aterraxe. Como vemos na seguinte Figura 2.7, o seu funcionamento consiste na existencia de dous lóbulos, onde, en cada pista utilizaran unhas frecuencias concretas. O *glide slope* será o encargado do posicionamento vertical, mentras que o *localizer* encargarase do horizontal. O funcionamento será o mesmo en ambas partes: para detectar que a aeronave está correctamente aliñada, polo posicionamento destes dous lóbulos con sinais en frecuencias diferentes, sábese que nos puntos centrais a potencia de ambas debe ser a mesma, polo que as aeronaves compararán os valores que reciben de ambos lóbulos, en ambos ángulos, lateral e vertical, para coñecer cal é o seu posicionamento e buscar o aliñamento total tendendo a igualar o valor da potencia de ambas.

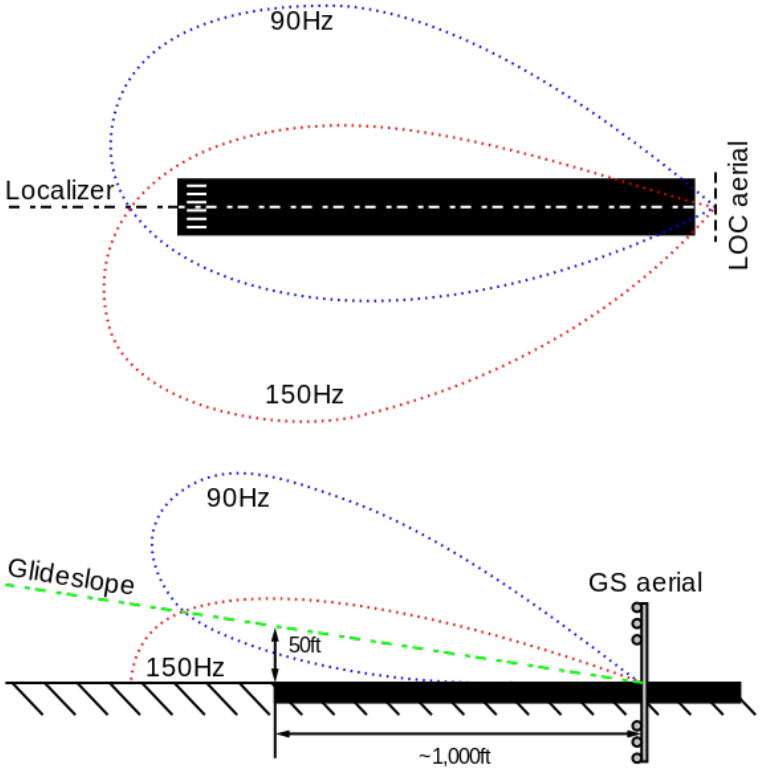

Figura 2.7: ILS.

2.3.3 CPDLC

Siglas referentes a *Controller–pilot data link communications* [18]. Protocolo que nace para substituír ao ATC (*Air Traffic Control*), o cal está baseado en mensaxes de voz, con transmisión directa entre terra e aire e cun baixo ancha de banda. CPDLC compartirá características con el, pero tratará de solucionar a habitual conxestión do ATC, para elo, substituirá o tráfico de control de voz, por texto. Reducirá por tanto tamén a ambigüidade, acortando as comunicacións e reducindo a saturación, brindando tamén a posibilidade de automatizar certas mensaxes. Ademais, permite transmitir información dun xeito máis fiable á tripulación, coma por exemplo información xeográfica. En canto á seguridade, destacar que se centra na integridade e dispoñibilidade, incorporando *checksums* para reducir o ruido, pero non garantindo a confidencialidade ao tranmsitir en texto plano e recaendo a autenticididade na confianza nas autoridades humanas.

Figura 2.8: CPDLC.

Capítulo 3

Casos prácticos: explotando vulnerabilidades

Neste capítulo faremos de novo a mesma división, intentando abordar a maior parte de puntos que no vídeo da *DEF CON* [19] se enumeran como vectores de entrada e potenciais ataques a estes tipos de infraestruturas. Intentaremos realizar, como mínimo, dous casos prácticos por ámbito, expoñendo en todo caso as vulnerabilidades explotadas e posibles medidas de mitigación.

3.1 Persoas

Como ben explicamos, este ámbito refírese a atacar ás persoas de todo tipo que se atopen nos aeroportos: persoal do mesmo, de aeroliñas, pasaxeiros, etcétera. Neste caso, o máis útil ou práctico será atacar á rede WiFi do aeroporto, xa que como detallamos na anterior sección, é o vector de entrada máis sinxelo e amplo, común ademais a todos os tipos de persoas do aeroporto. Por outro lado, aínda que non pertenza de forma tan clara a esta subdivisión, atacaremos tamén as tarxetas de embarque dos pasaxeiros (entre eles incluirémonos tamén a nos mesmos), onde poderemos explotalas ben por beneficio económico, ou simplemente por diversión.

3.1.1 Creando un Fake Evil Twin con portal cautivo

Para non solapar contidos coa práctica dous da asignatura, así como para coidar a extensión do traballo, non imos detallar e eximplificar dende 0 este ataque, debido a que xa o fixemos para a asignatura. Concretaremos por tanto que cambios facerlle para adaptalo e dirixilo ao máximo a este caso. Teremos entón que ca *suite Airgeddon*, atacar a WiFi aberta e pública do aeroporto, a cal conta por defecto cun portal cautivo, para facerlle un *jamming*, e levantar un *Fake AP* co mesmo nome, ao que se conectará a xente tras o fallo do punto

de acceso auténtico. O éxito do ataque recaerá no elaborado que sexa o portal cautivo *fake* que deseñemos para introducir no noso portal cautivo e capturar o maior volume de datos sensibles das persoas posibles. Mesturaremos por tanto este ataque técnico, con técnicas de enxeñaría social, para eminentemente, conseguir un ataque de *phishing*. A idea que se propón para conseguilo consistiría en, ir ao aeroporto en cuestión previamente, conseguir o código HTML de dito portal cautivo, para despois introducilo en *Airgeddon* da maneira exposta na P2 da asignatura e conseguir quedarnos cos datos que queremos. Por exemplo, unha opción sería clonar o *login* de correo e contrasinal de *Aena VIP*, para conseguir ditos datos con gran facilidade. Mostramos a continuación un exemplo de como se vería dito ataque nun móbil, estando o procedemento práctico relatado como ben dixemos, na P2 da asignatura.

Figura 3.1: Portal cautivo fake dun aeroporto nun iPhone 8.

3.1.2 Explotando as tarxetas de embarque

Este apartado vai estar baseado na charla *DEF CON* [20]. Nela, a cal recomendo encarecidamente, vemos como se trata de explotar de diferentes formas as tarxetas de embarque

nos aeroportos. Antes de nada, temos que comentar que estas tarxetas seguirán todas elas o estándar **IATA Resolution 792**, que podemos atopar en [6] e que actualmente está na súa séptima versión dende xuño de 2018. Nela, atopámonos un documento de 56 páxinas onde se concreta o protocolo a seguir nas tarxetas de embarque. Botándolle unha ollada podemos extraer unha serie de rápidas conclusións:

- Temos 4 formas diferentes de mostrar unha tarxeta de embarque:
  1. Papel: con **PDF417**, tecnoloxía explicada no anterior Capítulo 2.
  2. Móbil:
     - **Códigos QR**, amplamente coñecidos.
     - **Códigos Azteca**, tecnoloxía moi similar aos QR [21].
     - **Data Matrix**, tecnoloxía tamén moi semellante aos dous anteriores [22].
- Temos unha serie de **campos** definidos, uns deles **obligatorios** (60 caracteres), e outros **opcionais**. Onde a seguridade recae unicamente nos opcionais, polo que é moi probable que na maioría de tarxetas de embarque non estén securizadas.
- Normalmente **non hai cifrado**, é información codificada, polo que amosar a nosa tarxeta de embarque publicamente pode ser perigoso.
- En USA estase a comezar a facer obligatorio o uso de certa seguridade nelas, usando o campo 18, de ***Pre Check***.
- Só **media carilla** das 56 páxinas do estándar é adicada á seguridade das tarxetas de embarque.
- Hai 2 conceptos que axudan a entender mellor o funcionamento. Unha reserva dará lugar a varios:
  1. **PNR**: *Passenger Name Records*. Estrutura de datos que contén información sobre o pasaxeiro.
  2. **CRS**: *Computer Reservation Systems*. Sistemas de procesado das reservas de voos. Non só existe un, se non que coexisten varios de diferentes implementacións e as compañías difiren no seu uso.
  3. Destes conceptos hai que recalcar que non todos os organismos (aeroportos, aeroliñas, etc.) teñen acceso a todos eles, e a gran disparidade de tipos e accesos facilita os enganos e ataques a esta tecnoloxía.

Polo tanto, tras ler este documento e ver o vídeo mencionado, comezamos co caso práctico. Primeiro de todo, accedo a unha das miñas últimas tarxetas de embarque, e procedo a leela con calquera escáner PDF417 que podemos atopar *online* de forma gratuita en Internet. Obteño o seguinte:

Figura 3.2: PDF417 cunha tarxeta de embarque real.

```
M1DELOSSANTOSNODAR/MAUEZ94THV LCGBCNVY 1291 233Y023E0120 100
```

Figura 3.3: Contido decodificado da tarxeta de embarque.

O primeiro que vemos é como a tarxeta só conta cos 60 caracteres obligatorios, polo tanto sabemos que non hai ningún mecanismo de seguridade implementado. Por outro lado, se analizamos o estándar e o contido, podemos saber o significado de todos e cada un dos caracteres, como o identificador de pasaxeiro, voo, asento ou clase na que se viaxa. Imos entón agora, facendo uso dun simple programa que atopamos nun repositorio público, xerar códigos PDF417 de tarxetas de embarque falsas, tras copiar a información da nosa tarxeta e cambiar por exemplo a clase na que viaxamos, á cal fai referencia o **caracter Y**, *item* con número 71, referente ao *Compartment Code*, onde o **Y** soe facer referencia a *Economy*, e nos queremos xerar o **caracter C**, referente a *First Class*. Co resto, sabemos que unicamente con que o *Flight Number* e a data (*Date*) coincidan, os lectores non van dalo como erróneo, polo que poderiamos cambiar tamén, por exemplo, o noso asento, *item* 104, chamado *Seat Number*, conxunto de 4 caracteres, no noso caso concreto **023E**, por calquera outro, por exemplo **001A**, e ter a maiores do embarque prioritario por ir en primeira clase, o primeiro asento en *business*. Facendo todos estes cambios e axustando manualmente ca ferramenta e a referencia orixinal os campos restantes, acabamos xerando unha tarxeta de embarque **falsa, pero válida** para calquer lector do aeroporto e incluso da aeroliña, da seguinte forma:

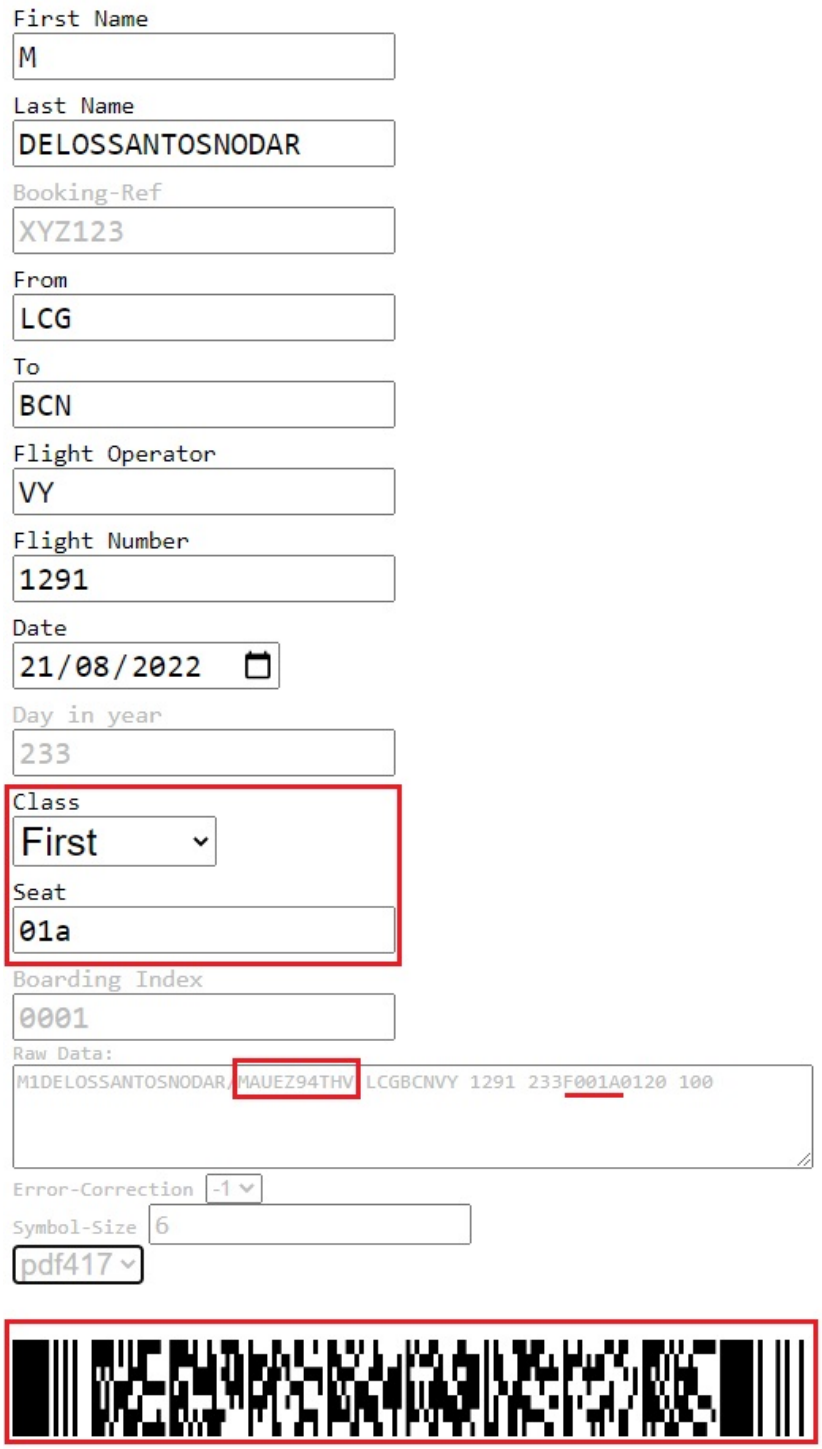

Figura 3.4: Tarxeta de embarque hackeada en primeira clase.

3.2 Infraestrutura aeroportuaria

Ocuparémonos nesta sección dos ataques á propia infraestrutura aeroporturarias. Realmente o traballo podería contar só con esta sección, ao seren os aeroportos practicamente cidades, cunha infraestrutura e equipamento xigantes. Aínda así, eliximos os seguintes ataques debido a que consultando diferentes fontes, como por exemplo [19], vemos que en relación sinxeleza-impacto, poden ser os máis rentables.

3.2.1 Atacando ás pantallas do aeroporto

Primeiro de todo, como ataque máis obvio temos o físico. Cando a seguridade física non está implementada, e por exemplo como viamos na Figura 2.3, os cables das pantallas están expostos e sen securizar, o ataque máis sinxelo e efectivo consistiría en desconectar ou incluso cortar ou danar de calquera forma ditos cables que alimentan as pantallas FIDS. Por outra banda, para facer algo máis técnico e elaborado, como tamén sabemos que temos acceso ás tomas USB de ditas pantallas, imos realizar o seguinte modelo de ataque:

1. Compraremos un controlador remoto de pantallas, como pode ser un Chromecast e, tras acceder ás instalacións do aeroporto e poder ver a marca das pantallas empregadas para o FIDS, compraremos tamén un mando universal compatible, por exemplo, no caso de ser *Samsung* poderianos valer este de AliExpress. Actualmente moitos pantallas son compatibles para o control remoto dende *smartphones*, polo que poderiamos probar tamén con aplicacións do estilo.

2. Accedemos físicamente ás pantallas FIDS do aeroporto e conectamos o *Chromecast* ao non teren seguridade física.

3. Nun dispositivo móbbil propio, temos unha imaxe *fake* FIDS, da complexidade que escollamos: ou collida directamente dende Internet, como é o caso, ou de forma máis elaborada, editando con ferramentas estilo *Photoshop* unha imaxe para facela case indistinguible ao caso concreto de cada aeroporto.

4. Subimos a *Google Photos* dita imaxe, co mando universal cambiamos o *source* das pantallas se fixera falta (a veces de forma automática ao conectar o *Chromecast* isto xa ocurre), e seleccionariamos no noso teléfono a opción de compartir imaxe no *Chromecast*.

5. Teriamos entón, como vemos na seguinte Figura 3.5, unha apariencia FIDS na pantalla que escollamos cos datos totalmente falsificados por nós, o que podería dar lugar a un caos total nun aeroporto real ao alterar as portas de embarque, horarios, etcétera.

Figura 3.5: Superpoñendo unha imaxe FIDS fake nunha TV persoal.

3.2.2 Atacando ao CCTV

De novo, neste apartado o primeiro e máis sinxelo dos ataques consistiría na desconexión das cámaras, se coma no caso anterior, non existira seguridade física. Elaborando máis os ataques, poderiamos usar *Shodan*, para filtrando xeográficamente como vimos no capítulo anterior, acceder ás cámaras web abertas públicamente e intentar explotalas, facerlles un denegación de servicio ou calquera posibilidade que se nos ocurra. Vimos esto na primeira práctica da asignatura. Outra opción, consistiría en se son cámaras web IP que transmiten por WiFi, utilizar de novo a *suite Airgeddon* para facerlles un *deauth jamming* básico e deixalas inoperativas, como abordamos na segunda das prácticas. E por último, se quixeramos aínda un maior nivel de sofisticación, podemos probar a realizar algún dos ataques expostos no amplo estado da arte sobre o tema, ou por exemplo, no interesante *post* de [23], empregando:

- **Hikvision Exploit Tool**, explotando a vulnerabilidade de marzo de 2017 se non está parcheada.
- **Bruteforce** de contrasinais con *hydra*.

3.3 Vehículos

Trataremos nesta última sección do capítulo práctico de explotar vulnerabilidades e atacar aos propios vehículos que podemos atopar nestas contornas. As consecuencias destes ataques teñen un gran impacto, pero tamén constan dunha enorme complexidade comparándoos cos anteriores casos. A parte práctica desta sección estará baseada en ataques realizados por terceiros, debido á complexidade dos mesmos e á dificultade de acceder a ditas contornas reais. En concreto, a fonte principal de información serán as charlas *DEF CON* de *Aerospace Village* [2].

3.3.1 Atacando aos propios vehículos

Aínda que sobre esta temática nos atopamos cunha gran literatura, paga a pena mencionar as seguintes referencias de charlas *DEF CON*: primeiro de todo, a charla 747-400 Walk through From a Hacker's Perspective, ideal punto de partida para esta sección, onde se fai un repaso total de todas as partes *Hardware* e incluso *Software* que podemos atopar nun avión comercial modelo *Boeing 747*. A continuación, outra moi interesante charla sería a What I Learned Trying to Hack a 737, onde se procede a intentar explotar as diferentes partes amosadas na referencia anterior. Por último, se quixeramos afondar máis, poderíamos ver algo máis técnico ca charla de Evaluating Wireless Attacks on Real World Avionics Hardware, onde se faran probas prácticas moi concretas sobre equipos reais para intentar levar a cabo varios ataques. No noso caso, imos falar con algo máis de detalle da charla referente aos ataques ao *IFEC Hardware Lgeacy* que atopamos en [24].

IFEC Legacy in 747s

Neste ataque realizado por Alex Lomas e Phil Eveleigh, daráselles acceso a ambos a un modelo de *Boeing 747* ca finalidade de que auditen o *hardware IFEC* do mesmo. Este concepto fai referencia ás pantallas das que dispoñen os pasaxeiros ubicadas na parte traseira dos asentos do pasaxeiro que teñen en fronte. Para elo, o primeiro que fan é intentar acceder ás mesmas. Realizarán dous casos prácticos diferentes, onde resumimos a continuación un deles e recomendamos encarecidamente a visualización do vídeo para entender mellor o exposto.

- No propio avión, o primeiro que buscarán serán acceder de forma física a algunha toma ou porto que os conecte cas pantallas IFEC. Aínda que no primeiro dos casos atópano de forma doada, no segundo deles e que aquí expoñemos, a única posibilidade recaería en conectarse cun porto RJ45 dispoñible debaixo dos asentos dunha das filas centrais, situación pouco útil para pasar desapercibido no mundo real.

- Danse conta tamén, de que o *software* detrás das pantallas IFEC é relativamente moderno, tendo cada unha das pantallas un *Ubuntu Box* e estando interconectadas entre elas mediante WiFi, polo que de novo, será o vector de entrada idóneo a explotar.
- O acceso á rede interna pódese realizar doadamente de forma física ao estar na cabina de azafatos, ao carón dos servicios, un router exposto cun folio onde aparecían expostas en texto claro as credenciais da rede WiFi interna do avión.
- Unha vez dentro e con aceso ás pantallas IFEC, analizan os protocolos de comunicación, os cales parecen estar en texto plano.
- O maior dano que poden conseguir é o control das pantallas, cambiándoas de modo, alterando o seu contido, pero realmente nada máis aló que se vaia de poser chegar irritar aos pasaxeiros ou facer un dano reputacional.
- Comentar rapidamente que o outro ataque levouse a cabo a través de novo dun porto *Ethernet* exposto nun lateral do avión, onde conectándose a el se obtiña acceso directo a un *Windows NT4*, sistema totalmente *deprecated* e o cal a través de *exploits* públicos se conseguía infectar. De novo, o impacto e consecuencias eran similares, aínda que non puideron acabar o caso práctico por problemas ca aeroliña, pero poderia ter dado lugar a máis ataques e incluso saltos a redes e protocolos moito máis críticos, como por exemplo os referentes aos pilotos e navegación.

Figura 3.6: Porto Ethernet exposto nun Boeing 747.

Figura 3.7: Atacando o sistema IFEC dun Boeing 747.

3.3.2 Atacando as comunicacións dos vehículos

Falaremos agora de ataques ás comunicacións dos vehículos destas contornas. De novo, e agora quizais aínda en maior medida, o contido desta temática e enormemente amplo e podería dar lugar para unha tese el só. Polo que, voltamos recomendar unha serie de charlas *DEF CON* para afondar máis nel como poden ser primeiro, a charla de Simulated Satellite Communications on Raspberry Pi para aprender a emular estas comunicacións de vehículos nun entorno de probas, a referente tamén a Attacking Flight Management Systems, amosando diversos ataques xenéricos a todos os niveis dos protocolos de xestión de voo, e por último, atacando aos protocolos A2G (*Air To Ground*), ca charla técnica de Hacking Airplane, A2G Systems. De igual forma que no caso anterior, nós imos afondar máis en detalle en dous vídeos, máis breves, pero de igual xeito dun carácter eminentemente práctico. Podemos atopalos en [25] e [26], e farán referencia a ataques aos protocolos explicados no Capítulo 2 de tecnoloxías.

TCAS

Neste vídeo [25], Alex Lomas tratará de crear un escenario o máis real posible para atacar este protocolo explicado anteriormente, principalmente mediante técnicas de *spoofing* de mensaxes TCAS simulando a presencia de outras aeronaves cerca. Para elo, non usará un

avión comercial real, senon un simulador dun *Airbus A320*. O ataque relatado consistirá en *spoofear* mensaxes **RAs** do protocolo TCAS dun suposto conxunto vertical de aeronaves, para que con estas mensaxes, que como sabemos teñen prioridade ante calquera outro tipo de mensaxe de control, facer que a aeronave descenda obligatoriamente. A importancia deste ataque recae en que a aeronave, automaticamente tomará o control de si mesma para descender sen intervención do piloto, intentando chegar á altura marcada en verde no panel da esquerda que vemos nas seguintes imaxes, para intentar esquivar o tráfico de aeronaves falso que vemos no radar da pantalla da dereita. Para acabar, citar as referencias dos ataques aos modelos híbridos con ADS-B comentados na sección de tecnoloxías: [27] e [28].

Figura 3.8: Spoofeando tráfico TCAS nun Airbus 320.

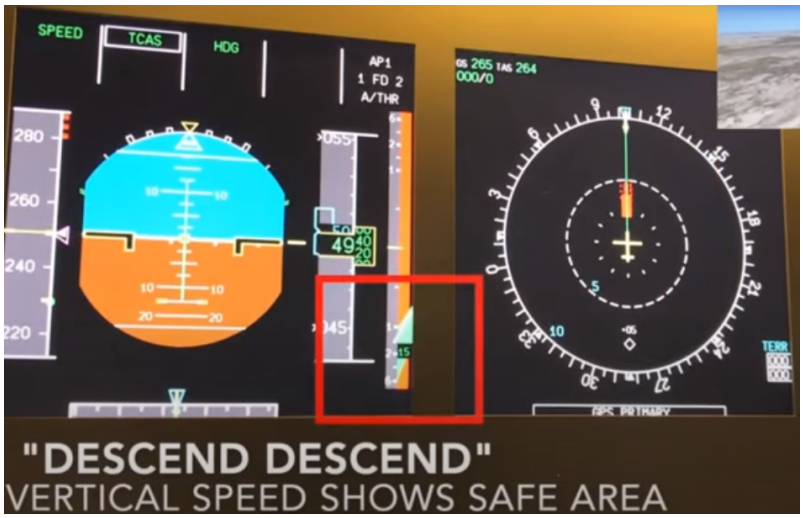

Figura 3.9: Airbus A320 descendendo automaticamente tras TCAS Spoofing.

ILS

Na segunda parte do vídeo anterior [25], Alex Lomas atacará agora ao protocolo ILS, tamén explicado previamente no Capítulo 2. Para elo, o escenario necesario deberá contar co entorno do aeroporto de San Francisco simulado (*KSFO 28R*), coa sinal ILS *spoofeada* na pista *27L* e simulando unhas condicións temporais con nubes (*Cat III*), sen visibilidade até unha altura duns *300 feet*, o que son uns 91 metros, é dicir, moi preto do chan, para intentar causar o maior dano no aterraxe posible reducindo o tempo de reacción para contrarrestar os efectos do mesmo. Isto, para ser aplicable nun entorno real, Alex Lomas comenta que se requiriía dunha antena moi cercana á pista de aterraxe e cun enorme alcance para conseguir *spoofear* esas dúas sinais en forma de lóbulos de ILS, así como a maiores, ao ser o protocolo sensible ao tempo de voo, necesitariamos unha aeronave falsa que levara o mesmo tempo de voo exacto que a aeronave á que imos atacar, polo que complica en maior medida o ataque, por exemplo comparándoo co caso de TCAS. Nas seguintes figuras vemos, primeiro, na Figura 3.10, a pantalla de control que indica o aliñamento ILS, na parte esquerda, onde o azul e o laranxa están balanceados, indicando a igualdade de potencia de ambas sinais dos lóbulos ILS e polo tanto un aliñamento tanto lateral como vertical da aeronave ca pista de aterraxe. A maiores, vemos a situación no exterior que ve o piloto abaixo á dereita, que é todo nubes.

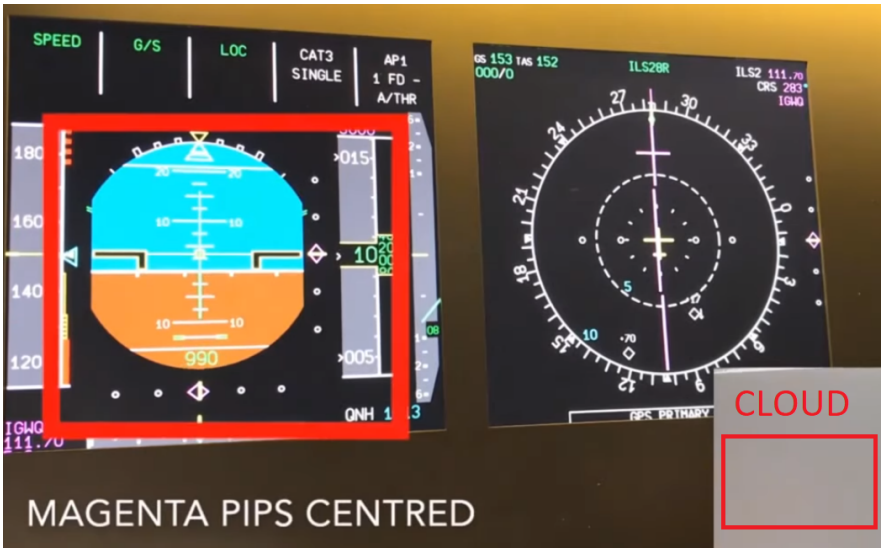

Figura 3.10: Pantalla de control ILS e exterior con nubes.

Agora, tras a realización do ataque, veremos como a pantalla de control ILS segue a indicar ese aliñamento ca pista, pero no momento de baixar dos *300 feet* (91 metros) e ser capaces de ver o exterior, vemos como o piloto vería a pista de aterraxe moito máis a dereita do que debería, imposibilitando o aterraxe e deixándoo con poucos segundos para a toma de decisións.

Figura 3.11: Situación lonxe da pista a pesar das indicacións ILS de aliñamento coa mesma.

CPDCL

Para este ataque, basearémonos na charla [26] impartida por Joshua Smailes onde tratará de realizar ataques MitM ao protocolo explicado de CPDCL. Para elo, será necesario un escenario onde o atacante conste dunha SDR (*Software Defined Radio*) que poida transmitir na banda VHF, unha antena VHF e un amplificador. Así como deberá ter un decodificador e un codificador CPDLC, sendo o primeiro deles doado de conseguir ao haber varias aproximacións *Open Source*, por exemplo o dumpvdl2, e o segundo máis complexo, tendo que implementar o propio atacante un, baseándose na especificación pública e aberta do protocolo.

O primeiro ataque dos amosados, que será no que nos centremos, será unha inxección básica de mensaxes no protocolo. Para elo, non haberá máis que codificar co noso codificador a mensaxe amosada, ca mesma sintaxe, e emitila ca nosa antena na banda VHF concreta, para ver como o noso decodificador, por exemplo, correndo nunha *Raspberri*, procedería a decodificar a resposta da aeronave: *WILCO*. Isto, aínda que poida parecer moi básico, pode ser o comezo para ataques máis sofisticados, coma os que él proba, referentes a *Jamming* de mensaxes, e combinación destes dous para acabar realizando un *MitM* no protocolo. Polo momento comentamos o primeiro, cuxo modelo se pode ver na Figura 3.12, así como tamén observamos o resultado de decodificar tráfico CPDCL recollido pola nosa antena e decodificador na *Raspberri*, no seu caso concreto no aeroporto de Zürich, na Figura 3.13.

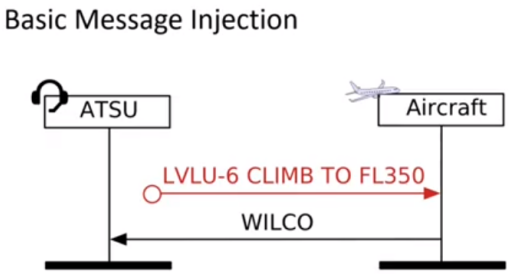

Figura 3.12: Esquema do ataque de inxección de mensaxes CPDCL.

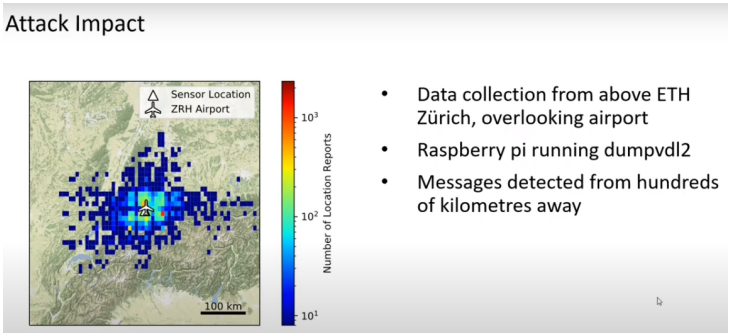

Figura 3.13: Tráfico CPDCL recollido polo dumpvdl2.

3.4 Shodan

Por último, e para acabar ca parte práctica do traballo, hai que mencionar de forma moi breve a opción de **Shodan**. Tanto como se ningún dos casos anteriores tivo éxito, como se queremos ir máis aló, ou descubrir novos vectores de entrada, sempre podemos acudir a Shodan, e buscando xeograficamente, sen ningún filtro, situarnos enriba do aeroporto obxectivo para ver que dispositivos accesibles ten e comezar a intrusión en calquera deles.

Figura 3.14: Dispositivos públicos nun aeroporto dende Shodan.

Capítulo 4
Conclusións

Tras rematar o traballo exposto e poder comprobar o estado da ciberseguridade nas contornas aeroportuarias, obtivemos as seguintes conclusións a nivel de contramedidas para securizar o atacado e dende un punto de vista global.

Mitigación e securización

- A nivel dos ataques a **persoas**, a mitigación pasará polo **lado da vítima** na maioría dos ataques, ao depender o éxito de todos eles no feito de caer ou non nas técnicas de enxeñaría social. Un exemplo máis técnico, por exemplo para evitar os ataques de tipo portal cautivo, sería facer un mellor uso das tecnoloxías 802. á hora de securizar na medida do posible a tecnoloxía WiFi.
- En canto ás tarxetas de embarque, a securización das mesmas pasará simplemente por usar os mecanismos xa creados para elas nos **campos opcionais**.
- A nivel de **infraestrutura**, a **protección física** de pantallas e cámaras, e a **securización da rede interna** serán chaves para evitar as consecuencias dos ataques.
- A nivel de **vehículos**, vemos como haberá que evitar de novo os portos ou **accesos físicos** libres, así como o uso de tecnoloxías ***Legacy***. Por outro lado, nos casos concretos dos protocolos, as solucións irán máis orientadas á implementación de funcionalidades de **confidencialidade, autenticidade e integridade** nos mesmos, onde priman as solucións en texto plano cuxa seguridade recae na confianza no lado humano.

Conclusións xerais

- Debido ao gran tamaño destas contornas, as posibilidades de ataque e defensa son enormes, polo que sumado á criticidade dos mesmos, a idea do **necesaria que debería ser a ciberseguridade** neste tipo de contornas debería estar aínda máis presente.

- Podemos atacar de forma moi elaborada ás partes destas contornas, todas elas moi diferentes, para rematar inflinxindo **dano a prácticamente todos os niveis**: sociais, económicos, físicos, etcétera.
- A propia **seguridade física dos dispositivos** é crucial. Adoita ser a vía de entrada menos securizada e a máis sinxela para o inicio de todo tipo de ataques.
- Empréganse, en practicamente todos os niveis, **tecnoloxías moi antigas** e onde en xeral, a **ciberseguridade** non é un concepto que pareza ter demasiado peso.
- A **proporción de ciberseguridade fronte a seguridade clásica**, por exemplo antiterrorista, nestas contornas é moi baixa.

Vemos por tanto como de novo, a ciberseguridade, tamén neste tipo de contornas, supón un elemento chave á vez que está moi lonxe de estar nunha situación óptima, polo que a adicación de recursos á mesma debería de ser esencial para o futuro próspero deste tipo de infraestruturas. Por outra banda, en lugar do clásico medo polo mero feito de voar, quizais deberia existir unha maior preocupación por todas as *ciberconsecuencias* que isto pode conlevar.

Bibliografía

[1] ICIT, "Hacking our nations airports," 2019, consultado o 2022-04-29. [En liña]. Dispoñible en: https://icitech.org/wp-content/uploads/2019/05/ICIT-Brief-Hacking-Our-Nations-Airports-1.pdf

[2] "Aerospace village," consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.youtube.com/channel/UC0NxjsvnBmhiCy2P8LHsXpw

[3] Wikipedia, "Captive portal," consultado o 2022-04-29. [En liña]. Dispoñible en: https://en.wikipedia.org/wiki/Captive_portal

[4] ——, "Social engineering," consultado o 2022-04-29. [En liña]. Dispoñible en: https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

[5] ——, "Pdf417," consultado o 2022-04-29. [En liña]. Dispoñible en: https://es.wikipedia.org/wiki/PDF417

[6] IATA, "Bar coded boarding pass (bcbp) - implementation guide," consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.iata.org/contentassets/1dccc9ed041b4f3bbdcf8ee8682e75c4/2021_03_02-bcbp-implementation-guide-version-7-.pdf

[7] Wikipedia, "Cctv," consultado o 2022-04-29. [En liña]. Dispoñible en: https://es.wikipedia.org/wiki/Circuito_cerrado_de_televisi%C3%B3n

[8] "Shodan," consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.shodan.io/

[9] "Shodan.maps," consultado o 2022-04-29. [En liña]. Dispoñible en: https://maps.shodan.io/

[10] BBC, "Cyber attack led to bristol airport blank screens," consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.bbc.com/news/uk-england-bristol-45539841

[11] CBS, “Cleveland hopkins airport recovers from computer malware attack; fbi investigates,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.cbsnews.com/news/cleveland-hopkins-international-airport-computer-systems-malware-attack-hack-fbi-investigating/

[12] “Zabbix,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://es.wikipedia.org/wiki/Zabbix

[13] Indra.Company, “Indra fids,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.indracompany.com/sites/default/files/Indra_airports_FIDS_2010.pdf

[14] DCS.aero, “Amadeus fids,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://dcs.aero/product/amadeus-flight-information-display-system-fids/

[15] Wikipedia, “Traffic collision avoidance system,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://en.wikipedia.org/wiki/Traffic_collision_avoidance_system

[16] ——, “Automatic dependent surveillance–broadcast,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://en.wikipedia.org/wiki/Automatic_Dependent_Surveillance%E2%80%93Broadcast

[17] ——, “Instrument landing system,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://en.wikipedia.org/wiki/Instrument_landing_system

[18] ——, “Controller–pilot data link communications,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://en.wikipedia.org/wiki/Controller%E2%80%93pilot_data_link_communications

[19] L. Wharton, “Airport hacking choose your own adventure,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.youtube.com/watch?v=86u_aYpEma0

[20] P. Jaroszewski, “Hacking boarding passes for fun and profit,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.youtube.com/watch?v=qnq0UfOUTlM

[21] Wikipedia, “Aztec codes,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://es.wikipedia.org/wiki/C%C3%B3digo_Aztec

[22] ——, “Data matrix,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://es.wikipedia.org/wiki/Matriz_de_datos

[23] “How to hack cctv camera (for education purpose),” consultado o 2022-04-29. [En liña]. Dispoñible en: https://learncctv.com/how-to-hack-cctv-camera//

[24] Aerospace.Village, “Hacking legacy ifec in old 747s,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.youtube.com/watch?v=p0A03vVHXnw

[25] ——, “Tcas and ils spoofing demonstration,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.youtube.com/watch?v=VbCzABE6jec

[26] ——, “Cpdlc man in the middle attacks and how to defend against them,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.youtube.com/watch?v=cl_56FUk8ps

[27] A. F. Andrei Costin, “Ghost in the air(traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.euroga.org/system/1/user_files/files/000/039/455/39455/bf9548c8f/original/BH_US_12_Costin_Ghosts_In_Air_WP.pdf

[28] I. M. Martin Strohmeier, Vincent Lenders, “On the security of the automatic dependent surveillance-broadcast protocol,” consultado o 2022-04-29. [En liña]. Dispoñible en: https://www.euroga.org/system/1/user_files/files/000/039/456/39456/2ca88c951/original/1307.3664.pdf