

Monográfico

Sistemas Aéreos No Tripulados

Ciberseguridad en el ámbito de los RPAS. Hackeando un Dron

¿Es posible secuestrar un dron?, ¿cuáles son las vulnerabilidades cibernéticas que tienen los RPAS?, ¿afectan a cualquier tipo de plataforma?, ¿qué conocimientos se requieren para explotar una vulnerabilidad?

Las vulnerabilidades de los drones no sólo son achacables al sistema de comunicaciones, al enlace radio, y aunque a ojos de un ingeniero de telecomunicación pudiera ser lo más evidente, existen otros riesgos que también deben ser revisados, de diferente naturaleza y concernientes a otras partes del producto. Por otro lado, y aunque aquí trataremos las plataformas comerciales, aquellas pertenecientes al segmento de “juguetes”, no están exentas de riesgo aquellas plataformas y RPAS del ámbito profesional, incluido aquellas tecnologías fuertemente vinculadas a los ámbitos de seguridad y defensa.

Un dron = una cosa

El RPAS es un dispositivo “conectado”. De cara a cuál es el tratamiento que se le debe dar a un dron, en el mundo del ciberespacio y de la ciberseguridad, la consideración más acertada es la de “cosa” y, por lo tanto, debe ser tratada como un elemento más de esa gran bolsa que representa el IoT (*Internet Of Things*), con sus retos y desafíos tecnológicos. Elementos que se conectan a la gran red IP, y que, al igual que muchas *SmartTVs* o *SmartToys* existentes en el mercado, carecen de la seguridad necesaria para garantizar, por un lado, la privacidad de los ciudadanos y por otro lado, el más grave, para brindar opciones al crimen organizado, a los colectivos



Samuel Álvarez González

Grupo de Trabajo de Defensa y Seguridad (GTDS) del COIT
Director General del Grupo In-Nova

✉ salvarez@in-nova.org



Esther Álvarez González

Presidente de la Fundación In-Nova

✉ ealvarez@in-nova.org

terroristas o a los ciberdelicuentes en general, para fines ilegales y con consecuencias peligrosas.

5 desafíos o medidas útiles sobre la ciberseguridad en el *Internet Of Things* (IoT)

Desde el punto de vista de la conectividad, el tipo de información que produce y utiliza para su navegación, así como el tipo y formato de la información que comparte y cómo se comparte, los retos y desafíos de la ciberseguridad que actualmente impactan en vulnerabilidades que son explotadas por los ciberdelincuentes son los siguientes:

- ▶ Mejora de la seguridad del software y firmware de los IoT desde fábrica. Mejora del diseño de la seguridad de los productos y dispositivos que están bajo el paraguas del IoT, desde fábrica. No sólo los drones, que claramente y como se argumenta posteriormente son vulnerables a este error de diseño, sino dispositivos que hoy en día suponen un serio riesgo para la privacidad y seguridad no sólo de organismos públicos o empresas, sino hogares, como son elementos domóticos (termostatos, reguladores de luz, cerraduras controladas por apps, etc.), televisiones inteligentes, juguetes para niños, etc. Incluso los coches, cada vez con mayor capacidad de conectividad, por ejemplo, a través de su centralita de mantenimiento, donde ya se han publicado graves lagunas de seguridad en diferentes proyectos de hackeo de un vehículo, con éxito en al menos dos marcas muy conocidas.
- ▶ Uso de comunicaciones cifradas con la suficiente robustez para complicar su ruptura mediante las



técnicas y potencia de cálculo de los ordenadores actuales. Necesidad de cifrado sea cual sea la tecnología inalámbrica utilizada (wifi, bluetooth, infrarrojos...)

- ▶ Leer y comprender políticas de uso y privacidad que aceptamos cuando compramos un dron o un elemento IoT. En muchos casos con la adquisición del propio producto se acompaña una documentación donde, además de explicar el funcionamiento del mismo, su mantenimiento, etc., se abordan cuestiones que pueden afectar a la privacidad de los consumidores. Como muestra este ejemplo de un fabricante muy conocido en el sector comercial, que debería llevar a la reflexión a todos los consumidores.

RECOPIACIÓN LEGAL DE DATOS DE TERCEROS

"Al utilizar el servicio, usted otorga a DroneDeploy un servicio no exclusivo, irrevocable, totalmente pagado y libre de regalías, transferible, sublicenciable, licencia mundial para usar, copiar, reproducir, procesar, adaptar, modificar, publicar, transmitir, mostrar y distribuir su contenido de usuario".

Las dos preguntas obligadas en este punto son: ¿Somos conscientes que todo lo que se hace con estos drones, este fabricante puede estar monitorizándolo y haciendo uso comercial de ello? Si soy un cuerpo o fuerza de seguridad de estado, que ha comprado este tipo de plataformas para sus operaciones, ¿cómo se asegura que toda la información de las mismas no está circulando libremente por internet o la DeepWeb? Sin duda, preocupante.

- ▶ Creación de mayor normalización y calidad de los estándares de la industria en estos sistemas para garantizar que cumplen unos mínimos requisitos en materia de ciberseguridad. Esta normalización o legislación debería condicionar el mercado CE o no de estos productos en Europa.
- ▶ Mayor sensibilización y formación a la sociedad, al cliente y al usuario final. Como eje transversal a cualquier medida de las anteriores y, dada la complejidad que requiere la comprensión de la vulnerabilidad a la que un usuario final se enfrenta por adquirir uno de estos productos, se necesita un mayor esfuerzo en comunicación, divulgación y alerta temprana respecto a las conductas, consejos y riesgos que suponen la compra y uso de estas tecnologías.

Subsistemas y elementos vulnerables de un dron

Para poder caracterizar el tipo de ataques que puede sufrir un dron es necesario antes preguntarse, ¿cuáles son las vulnerabilidades cibernéticas que tiene un dron?, ¿sobre qué elementos o subsistemas puede haber interés en comprometer, alterar o interceptar para *exfiltrar* información (extraer información sin que la fuente de la misma sea consciente de esa fuga de datos y que son de utilidad para quien los extrae)? Para ofrecer una respuesta global y representativa a estas cuestiones es importante plantear adicionalmente otras preguntas, que ayudarán a su determinación y sobre qué tipo de parte del RPA concierne a cada problema o amenaza:

- ▶ ¿Dónde están los datos que almacena o gestiona/transmite un RPAS?
- ▶ ¿Qué información se guarda y cómo se guarda?, ¿está encriptada?
- ▶ ¿Dónde se encuentra el dron en reposo o guardado? ¿Quién tiene acceso físico al dron?
- ▶ ¿Qué licencia o términos de condiciones hemos aceptado al comprar el producto y en qué pueden afectar a nuestros derechos de privacidad o al desarrollo de nuestras misiones?
- ▶ ¿Qué tipo de tecnología inalámbrica y protocolos de comunicación utiliza el RPAS y cómo de vulnerables son?

Analizando las partes, componentes y subsistemas que conforman un RPA, desde los drones más comerciales y sencillos, hasta los más complejos y de uso militar, todos ellos tienen unas partes comunes: subsistemas conectados, electrónica y software, comunicaciones embarcadas y comunicaciones remotas, sensores y actuadores para la auto-navegación, etc. Al final, para cualquier dron, las propias vulnerabilidades que puede tener cada subsistema generan un escenario de vulnerabilidad a nivel sistema. Por lo tanto, en función de las intenciones de ataque y vulnerabilidad que explotará un hacker, podrá provocar:

- ▶ Una simple caída por fallo de la plataforma (actuando sobre cualquiera de sus subsistemas críticos para la navegación y sustentación en el aire).
- ▶ Una acción más quirúrgica, precisa y compleja, como es lograr que el dron realice una misión diferente a la programación predefinida de misión del dueño del dron.



- Simplemente una interceptación de comunicaciones “transparente del dron” (sin que el propietario sea consciente de ello), para *exfiltrar* información sobre las misiones que realiza el dron, tanto de los itinerarios y planes de vuelo que realiza, como de los parámetros e información que capten sus diferentes sensores.

Los elementos que deben analizarse, desde un punto de vista aislado y como sistema, para identificar las vulnerabilidades primero y luego, garantizar la ciberseguridad integral en un RPA después, son los siguientes:

- **Microprocesador principal.** Responsable de procesar la información entre los sensores y actuadores para garantizar una navegación correcta. La mayoría de los sistemas utilizan Linux.
- **Magnetómetro.** Sensor para medir la dirección.
- **Sensor GPS.** Para determinar la posición global de la plataforma.
- **Sensor de velocidad del aire y altímetro.** Para medir la velocidad relativa del aire y la altitud (fundamentales para una navegación correcta).
- **Comunicaciones inalámbricas.** Responsable de comunicar la plataforma a otras plataformas o la estación de tierra. Canal de monitorización y control del dron.
- **Sistema de potencia** (variador / gestor de energía).

- **Sensores inerciales (IMU).** Elemento que mide e interpreta el movimiento de la plataforma.
- **Actuadores** (servomotores, etc.). Elementos que reciben las órdenes del procesador principal para actuar sobre las superficies de control de la aeronave.
- **Sistema de control de piloto manual.** Subsistema que permite dar control directamente desde la estación de tierra a la plataforma, anulando el piloto automático.
- **Estación de tierra.** Normalmente ordenador convencional.
- **Link de comunicación satelital.** Opcional.
- **Sistema de entrada de datos para configuración de misión.** Elemento para permitir la carga de misión dentro del procesador principal.

Tipos de ataque y escenarios específicos de ataque sobre un RPA

Con la información anterior, respecto a qué tipo de consecuencias pueden lograrse atacando un dron y los elementos disponibles y subsistemas para lograrlo, existen tres tipos de ataque a un RPAS. Son:

Ataque al hardware: representa el conjunto acciones para la explotación de vulnerabilidades directamente sobre los elementos del autopiloto del RPAS. La forma más común de implementar estos ataques es teniendo





acceso físico a los componentes de la plataforma. Algunas de las acciones contempladas bajo este tipo de ataque son:

- ▶ Se pueden corromper datos almacenados a bordo.
- ▶ Se pueden reprogramar elementos y subsistemas de la plataforma.
- ▶ Adulteración de componentes electrónicos.
- ▶ Modificación de firmware de subsistemas.
- ▶ Manipulación de tarjetas de memoria utilizadas en la plataforma (por ejemplo, memoria tipo SD).
- ▶ Explotación de vulnerabilidades aprovechando puertas traseras existentes y creadas en la fase de diseño del producto.

Ataque inalámbrico: conjunto de acciones para la explotación de vulnerabilidades a través de los canales de comunicación inalámbrica principalmente que utiliza el RPAS.

- ▶ El peor escenario es cuando el atacante logra romper el cifrado del canal de comunicación.
- ▶ Otro escenario es que el atacante logre crear un desbordamiento de *buffer* en las comunicaciones, que corrompa datos o reinicie algún evento que ponga en peligro la navegación o estabilidad del sistema.

Algunas preguntas obligadas en una prueba de *pentesting* (la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de

seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas) sobre este tipo de ataque son: ¿cuál es el tipo de tecnología inalámbrica utilizada? Y, ¿qué cifrado utiliza y si es posible romperlo con facilidad?

Ataque a los sensores. Spoofing. Conjunto de acciones para la generación de datos falsos para ser captados por los sensores del dron y el sistema actúe en consecuencia de éstos. Por ejemplo, inyección de datos sobre los receptores de GPS, o sistemas de visión, radar, sonar, lidar, sensores térmicos, etc. Dado que el sistema de navegación depende en gran medida de los datos captados por los sensores, abordar este tipo de ataque puede poner en serio riesgo la estabilidad del vuelo.

Hackeando un dron: ¿Un juego de niños?

¿Realmente se requieren conocimientos profundos para *hackear* un dron comercial? La realidad es que no. Internet ya se encarga de publicar guías prácticas para hacerlo. Multitud de videotutoriales, en todos los idiomas imaginables para demostrar que, con un ordenador, algo de tiempo, unos pocos conocimientos de Linux y algún que otro *gadget* al alcance de la mano por pocos euros, cualquier persona es capaz de convertir, por ejemplo, una simple vulnerabilidad de un juguete que vuela, en un arma mortal que poder arrojar a una multitud.

A continuación, y como resultado del presente artículo, se explica de forma general, cómo es posible hacerse con un dron que está en vuelo, mediante un patrón de ataque basado en la interceptación de sus comunicaciones y suplantación de la estación de control.

Casi todos los drones al alcance de la sociedad civil, como los que se pueden encontrar en cualquier gran superficie comercial, utilizan, para su enlace de comunicaciones, la tecnología WIFI (en 2,4 o 5,8 GHz), tanto para recibir la telemetría del RPAS, como recibir en tiempo real lo que captan sus sensores (imágenes y video principalmente). Los pasos a seguir son los siguientes:

1. Identificar la SSID. Un SSID (Identificador de Conjunto de Servicios) es el nombre que identifica la red inalámbrica particular a la que te conectas. Cada red inalámbrica en tu rango tiene su propio nombre único o SSID. Algunos de los drones analizados tienen pública la SSID que establece la comunicación entre la plataforma y la estación de tierra, generando así el link de Mando y Control (C2: *Command and Control*). En caso de que la SSID esté oculta, utilizando un analizador de redes es inmediata su identificación. También es



posible ver las redes ocultas utilizando un SmartPhone con Android, con aplicaciones como HiddenSSID Enabler.

2. **Levantar un Punto de Acceso Fake** (falso) con la misma SSID oculta. Realizar este paso es sencillo. Algunos ordenadores permiten realizar esta acción con facilidad desde el entorno gráfico, pero puede utilizarse un punto de acceso externo (adquirido a un coste de unos 20 euros o utilizando alguno de los módem-routers de los equipos de ADSL que prácticamente todas las familias españolas tienen en casa).
3. **Lograr des-autenticar (deauthenticate) o romper el enlace establecido** entre el dron y la estación de tierra original, para que el dron se conecte a la red fake levantada en el punto anterior. Forzar esta des-autenticación es sencillo, basta con buscar en internet cómo se puede hacer en función de los medios que cada uno tiene más a mano. Para aquellas personas más familiarizadas con herramientas de pentesting y hacking, por ejemplo, las que están a disposición en la distribución Kali Linux: *Penetration Testing Tools*, una de las más utilizadas es *Aircrack-ng*, mediante un ataque de inyección de datos para reinicio y restablecimiento del link.
4. **Intervenir el dron.** Una vez el sistema de Mando y Control del dron ha sido capturado, interceptado, ahora sólo se trata de conocer el protocolo, tramas y mensajes que el dron entiende para ser comandado. En la mayoría de los drones comerciales esta información está accesible en internet. Ya sea utilizando el protocolo MAVLINK u otro. En este estado es fácil lograr:
 - Pintar sobre un mapa las posiciones geolocalizadas de la operación que el dron está ejecutando. Así como la descarga y acceso a toda la información de los logs de misiones sobre la información que esté a bordo.

- Es posible enviar comandos hacia el controlador de vuelo (procesador a bordo del dron), utilizando por ejemplo ser2net (mediante un conversor serie a network). Es posible modificar las posiciones de “retorno a casa”, cambiar el plan de vuelo o descargar las imágenes del sensor principal a través de un servidor web embebido donde las credenciales de acceso vía SSH están también publicadas en internet.

```
** Rcv from port 0x08, seq 0, cmd 0x04,
subcmd 0x00, error 0, payload len 0
0x0400: server says hello!
** Sent to port 0x0a, seq 3, cmd 0x53,
subcmd 0x00, error 0, payload len 0
** Rcv from port 0x0a, seq 2, cmd 0x49,
subcmd 0x00, error 0, payload len 52
[0x49]: Seq 2, GPS sats 4, home
[+39.862979,-4.013394] loc [+39.860377,
-3.950969],
accel xyz [+00, +00, +00], ag +1.2 meter,
compass roll/pitch/heading [180, 180, 093],
batt 12065mV (74%), unknown 6
[0x53]: Seq 3, battery <5200mA, 5440mA>,
current level <12090mV,
4619mA>, unknown 6e fc 63 54 1e 03 00
```

Envío de comunicaciones al Controlador de Vuelo (Flight Control) utilizando Ser2Net .
Cambiando posición “home” del dron.

Como conclusión, la mejor solución para mejorar la ciberseguridad de los RPAS requiere, en las fases de diseño y fabricación, comprender el dron como un sistema, compuesto a su vez de diferentes subsistemas sobre los que hay que cuidar la ciberseguridad; con diferentes tecnologías y protocolos de comunicación (Linux, ROS, CAN, I2C, PWM, MAVLINK, etc.), que deben entenderse entre sí y que deben coordinarse entre sí, tanto en relación a los valores espe-





rados de comunicación entre ellos, así como la comprensión de los valores anómalos o no esperados en función de la situación de cada misión. Es decir, la aplicación del concepto de Ingeniería de Sistemas resulta crucial para dar solución integral a un problema de integración de sistemas. Indudablemente aún queda mucho, y la brecha es, si cabe, mucho más grande para aquellas soluciones comerciales que se venden por decenas de miles en el mundo.

Bibliografía

1. National Telecommunications & Information Administration (NTIA). United States Department of Commerce. Jun 2016: "Multistakeholder Process: Unmanned Aircraft Systems".
2. BITAG Publishes Report: Internet of Things (IoT) Security and Privacy Recommendations Report explores the technical aspects of the security and privacy of networked consumer devices. Nov 2016.
3. USENIX LISA 2016 Congress. Dic 2016: UAVs, IoT, and Cybersecurity by David Kovar.
4. "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles" by Alan Kim, Brandon Wampler, James Goppert and Inseok Hwang (from Purdue University, Indiana) and Hal Aldridge (from Sypris Electronics, Tampa, Florida). Jun 2012.
5. Integriography BLOG: A Journal of Broken Locks, Ethics, and Computer Forensics.

Cyber security in the realm of RPAS: Hacking a drone

There are a series of weaknesses in drones that are not solely attributable to the communications system or radio connection. To improve

cyber security of RPAS, it is required, during the design and manufacturing stages, to understand how the drone is a system comprised

of different subsystems for which cyber security must be safeguarded (with different technologies and communication protocols).