SEGURIDAD EN WIRELESS

Estas notas de apoyo tienen como objetivo suplementar las transparencias y facilitar la comprensión de los contenidos vistos en clase. Son, por tanto, un complemento y no un sustituto de estas.

1 INTRODUCCIÓN

Si bien el escenario que se describe en la transparencia de introducción está basado en las capacidades de los coches de hace unos años, todavía es más relevante para los vehículos más actuales que han incorporado enormes capacidades de control remoto.

En definitiva, se analizan algunas de las vías de ataque posibles, en especial aquellas con carácter remoto como los accesos mediante bluetooth o internet con conexión directa al sistema electrónico de control del vehículo. De esta forma se podría llegar a un escenario (que ya existe en cierta medida) en el que se tiene un catálogo de vehículos con acceso remoto y que se puede permitir su robo a cualquiera que pague lo suficiente. Evidentemente, este tipo de ataques no se limita al robo del vehículo, ya que se podría utilizar los mecanismos de control activo (dirección, aceleración, frenado, etc.) para realizar otro tipo de ataques posiblemente más peligrosos.

Es importante destacar que los sistemas de comunicación inalámbrica proporcionan una cantidad enorme de ventajas, mejorando la productividad y la economía y llegando a ser indispensables en muchos casos. No obstante, como todos los sistemas de información, tienen vulnerabilidades y son objetivo de ataques que, además, son especialmente peligrosos dada la naturaleza no conectada de los mismos. Como aspecto positivo, y debido a su importancia, la seguridad de estos sistemas inalámbricos ha mejorado de forma significativa en los últimos años.

2 BLUETOOTH

La tecnología bluetooth proviene de la compañía sueca Ericsson y se diseñó inicialmente en 1994, si bien ha sufrido numerosas revisiones desde entonces. Hay multitud de dispositivos compatibles con bluetooth, generalmente asociados a control remoto y audio, pero también a otros campos como dispositivos médicos que requieran de cierto control exterior (lo que requiere extremar las medidas de seguridad).

Hay dos topologías básicas: *piconet* en la que cada dispositivo secundario se conecta a un único maestro o primario y *scatternet* en la que un dispositivo secundario puede estar conectado simultáneamente a varios primarios o maestros.

Al igual que otras tecnologías inalámbricas, la seguridad de bluetooth ha ido mejorando de forma significativa con el tiempo. No obstante, hay dos clases de ataques básicos asociados a bluetooth:

- *Bluejacking*, que consiste en el envío de información o mensajes no deseados a través de esta tecnología y que ha sido utilizado durante algún tiempo por anunciantes o comercios con el objetivo de atraer clientes e incrementar las ventas.
- Bluesnarfing, que consiste en exfiltrar información de un dispositivo a través de conexiones *bluetooth*. En muchos casos se pueden emplear antenas y amplificadores específicos para lograr explotar alguna vulnerabilidad o error de configuración desde mucha distancia y extraer información comprometedora, mensajes, fotografías, vídeos, etc., del dispositivo.

3 ATAQUES WIFI

A lo largo de los años, se ha ido mejorando de forma significativa, tanto en seguridad como en rendimiento, la propuesta inicial de redes locales inalámbricas IEEE 802.11.

Es importante considerar que las transmisiones *wireless* no están sujetas a los mismos límites que las conexiones cableadas y, en muchas ocasiones, nos puede sorprender su alcance. Es esencial, por ello, implementar medidas de seguridad adecuadas y no depender en que los atacantes no tengan el alcance suficiente.

Los atacantes pueden capturar las transmisiones e interpretar la información de forma muy sencilla, identificando los diferentes paquetes y accediendo o modificando cualquier información que no esté cifrada. El cifrado en una comunicación inalámbrica debe ser considerado obligatorio. Otra posibilidad consiste en que los atacantes puedan emitir en el mismo espectro de radiofrecuencia logrando la inhibición de la comunicación y, de hecho, una denegación de servicio (DoS).

3.1 DESCUBRIMIENTO

Las especificaciones de las redes WiFi implican la transmisión de unos paquetes pequeños de identificación (*beaconing*) con una frecuencia determinada, lo que permite a usuarios y atacantes identificar y catalogar las redes WiFi que estén accesibles.

Por ello, existe el concepto de *war driving*, que consiste en ir apuntando en un mapa todas las redes inalámbricas, así como sus características (nombre, intensidad, seguridad, etc.), que vamos encontrando al ir en movimiento mediante un vehículo o a pie. Antiguamente, este proceso requería de herramientas específicas muy concretas; en la actualidad, se puede realizar con muchos dispositivos móviles comunes. No obstante, es muy frecuente emplear antenas y dispositivos especiales para lograr un mayor alcance o efectividad a la hora de catalogar redes.

Evidentemente, entre otras muchas cosas, disponer de esta información puede servir tanto para realizar ataques (explotando configuraciones indebidas) o detectar y corregir problemas existentes en redes bajo nuestro control.

3.2 ESPECTRO RF

Mediante el mero acceso a la frecuencia que se utilice para las transmisiones WiFi (en general 2.4 o 5GHz) se pueden lograr ataques pasivos (análisis) o activos (interferencia):

- *Análisis de protocolo*. Se puede analizar el tráfico simplemente mediante una antena sintonizada a la frecuencia adecuada. Para lograr este tipo de acceso, es frecuente utilizar un interfaz inalámbrico que permita su uso en modo monitor (análogo al modo promiscuo de las redes cableadas) con el objetivo de capturar paquetes sin estar asociado a un punto de acceso concreto.
- *Interferencia.* Existe la posibilidad de interferencias tanto de forma intencionada como accidental. Muchos dispositivos emiten en las mismas frecuencias que se utilizan para WiFi: microondas, fotocopiadoras, teléfonos inalámbricos, el propio bluetooth, etc. No obstante, un atacante puede provocar interferencias con un dispositivo específico que evite la comunicación entre dispositivos; la inhibición de frecuencias es ilegal en muchos países.

3.3 PUNTOS DE ACCESO

En los ataques mediante puntos de acceso, hay dos casos muy frecuentes:

- *Punto de acceso no autorizado*. Esto ocurre cuando alguien instala un punto de acceso por conveniencia y lo hace sin autorización ni ningún tipo de control. En muchos casos, estos puntos de acceso no están configurados de forma adecuada y permiten el acceso a la red local desde el exterior para cualquier atacante que consiga conectar con este punto de acceso.
- *Gemelo maligno*. Este ataque consiste en emular un punto de acceso legítimo, de forma que los dispositivos intenten conectarse a este punto de acceso maligno y proporcionen información valiosa, etc.

3.4 VULNERABILIDADES 802.11

El filtrado de MAC consiste en bloquear (lista negra) o limitar el acceso a ciertas direcciones MAC legítimas (lista blanca). No se debe confiar en este mecanismo para garantizar puesto que un atacante es perfectamente capaz de descubrir las direcciones que se utilizan y cambiar su dirección para lograr acceso. En un sistema útil en ciertas situaciones, pero con un nivel de efectividad bajo frente a atacantes con conocimientos.

Si bien existe la posibilidad de *ocultar el SSID* (nombre de la red inalámbrica), es relativamente sencillo para atacantes y dispositivos identificar las redes incluso si están ocultando su SSID. En algunos casos, la ocultación del SSID es contraproducente, puesto que puede permitir ciertos ataques por la forma en la que tienen de elegir punto de acceso ciertos sistemas operativos, dando preferencia a aquellos puntos de acceso que no ocultan la SSID.

3.5 WEP

El protocolo WEP (Wired Equivalent Privacy) fue la primera propuesta generalizada para dotar de seguridad a las redes inalámbricas. No obstante, tiene muchos problemas de seguridad y no se debería utilizar en la actualidad en ningún caso.

El principal problema consiste en que cifra cada paquete con una clave fija y un IV variable de 24 bit. En el momento en el que se repite el IV (lo que puede ocurrir en minutos si hay suficiente tráfico) tenemos dos paquetes distintos cifrados con la misma secuencia cifrante, lo que permite eliminar el cifrado realizando el XOR entre ambos paquetes. Si bien se emplea RC4 para el cifrado, que no está recomendado en la actualidad al haberse encontrado problemas, este problema es independiente del cifrador empleado, es propio del protocolo en sí.

4 SOLUCIONES DE SEGURIDAD WIRELESS

4.1 WPA

El protocolo WPA (WiFi Protected Access), es una mejora significativa sobre WEP. Entre otras cosas, el sistema de cifrado ya no tiene el problema de repetición de secuencia cifrante propio de WEP, si bien sigue empleando RC4 como cifrador por motivos de compatibilidad hardware.

Las principales vulnerabilidades de WPA tienen que ver con la gestión de las claves y la elección de contraseñas precompartidas débiles.

4.2 WPA2

La mejora de WPA, WPA2 mejora los esquemas de autentificación y el sistema de cifrado de las propuestas anteriores. Ya no se utiliza RC4 como cifrador, se emplea AES en modo CTR que es mucho más seguro, pero requiere soporte hardware específico para funcionar en tiempo real.

Cabe destacar que ya está disponible la especificación de WPA3 (2018), si bien no se ha implementado de forma significativa todavía.

4.3 OTROS FACTORES

Entre los múltiples factores a considerar a la hora de implementar redes de comunicación WiFi seguras, podemos destacar:

- *Disposición de antenas*. Es importante colocar las antenas de forma que se minimicen las interferencias y el acceso externo a la señal, pero maximizando la cobertura en las zonas deseadas.
- *Control de potencia*. Para lograr el objetivo anterior, puede ser necesario realizar ajustes manuales de la potencia de cada dispositivo para tener un mayor control de la cobertura de señal.
- *Descubrimiento*. En instalaciones empresariales y comerciales es esencial realizar un control continuo y riguroso para evitar la instalación de puntos de acceso no autorizados y otros errores de configuración.
- *Segmentación*. Puede ser útil el empleo de técnicas de segmentación de redes locales (VLANs) para optimizar la seguridad en un entorno concreto. Si bien, antaño, esto requería hardware costoso, en la actualidad muchos dispositivos incorporan la posibilidad de definir múltiples redes para distintos propósitos de forma barata y sencilla.

5 AMPLIACIÓN

Existen muchos materiales en O'Reilly Safari (acceso gratuito con la cuenta de la UA) para ampliar, entre otros:

- Curso "Certified Wireless Security Professional"
- Libro "Wireless Communications Security"
- Libro "Seven Deadliest Wireless Technologies Attacks"
- Topic "Wireless Technology"