Un canal encubierto de red en el protocolo IEEE 802.11

Leandro F. Meiners[1,2]

[1] Universidad de Buenos Aires, FCEyN, Departamento de Computación,
lmeiners@dc.uba.ar
[2] CORE Security Technologies,
leandro.meiners@coresecurity.com

Resumen El presente trabajo presenta un canal encubierto de red en el protocolo **IEEE 802.11**, utilizando las extensiones provistas por el mismo para soportar el protocolo de confidencialidad **WEP**, cuyo tráfico resulta "indistinguible" del tráfico normal de la red.
Se muestran dos implementaciones distintas del canal encubierto propuesto: una mediante la modificación de un controlador de red para plataformas **Linux** y otra que inyecta tramas **IEEE 802.11** en el aire directamente.
La idea fundamental del trabajo es la utilización de valores pseudoaleatorios existentes dentro de un protocolo para el envío de datos pertenecientes a un canal encubierto.
Adicionalmente, se analiza la posibilidad de extrapolar el canal encubierto a redes **IEEE 802.11** protegidas por **WPA/WPA2**.

Keywords: canal encubierto, IEEE 802.11, WEP

1. Introducción

Los canales encubiertos son comúnmente utilizados para poder enviar y recibir información de forma anónima (difícil detección del origen) y mediante un canal confidencial[3] (difícil detección de la existencia). En el caso particular de un canal encubierto de red, la difícil detección de existencia se traduce en que no es posible distinguir el uso, o el no uso, del mismo.

El protocolo de redes inalámbricas para redes de área local más utilizado actualmente es el protocolo **802.11** estandarizado por **IEEE** ([12]). La primera versión del estándar ([12]) data de 1997 y define al protocolo **WEP** (Wired Equivalent Privacy) para ser utilizado en redes que requieren confidencialidad. En la actualidad la seguridad (confidencialidad, integridad y disponibilidad) de los datos, comunicaciones y sistemas es una necesidad de las organizaciones y crecientemente también de los individuos.

El protocolo **WEP** se basa en el uso del algoritmo criptográfico **ARC4**[18], para el cual se detectaron debilidades en el algoritmo de generación de sub-claves

[3] Cabe aclarar que confidencial refiere al canal en sí mismo y no al carácter de los datos enviados por el mismo ni si los mismos se encuentran cifrados.

([30]). En el año 2002 se publicó un trabajo que explicaba como utilizar las debilidades del algoritmo criptográfico **ARC4** para recuperar la clave **WEP** de una red protegida, efectivamente anulando la protección brindada por el algoritmo. Poco tiempo después surgieron herramientas públicas ([23]) que implementaban los ataques. Como respuesta a este problema de **WEP**, la asociación **Wi-Fi Alliance** (compuesta por las empresas más importantes de la industria de redes inalámbricas) publicó el estándar **WPA** (Wi-Fi Protected Access) ([1]) que sigue utilizando el algoritmo criptográfico **ARC4** pero imposibilita los ataques de **WEP**. Posteriormente, **IEEE** publicó el anexo **IEEE 802.11i** ([11]) al estándar **IEEE 802.11** ([12]) que incorpora **TKIP** (comercialmente conocido como **WPA**) y también agrega otro protocolo de confidencialidad que utiliza el algoritmo de cifrado **AES** ([9]) en modo **CCMP**, comercialmente conocido bajo el nombre **WPA2**.

A pesar de la existencia de herramientas públicas ([32]) para atacar redes **WEP**, sigue habiendo investigación en el tema ([33]) dada la popularidad del protocolo; principalmente relacionada con la gran cantidad de hardware instalado que únicamente soporta dicho protocolo[4] y los costos en recursos y tiempos que implican una migración. Cabe resaltar que la última versión del estándar **IEEE 802.11** ([12]) que data del 2007 indica que el protocolo **WEP** se encuentra obsoleto y **TKIP** o **AES-CCMP** deben ser utilizados en su lugar.

La popularidad del protocolo **WEP** lo demuestran diversos estudios; un estudio ([33]) conducido en Alemania en el año 2007 indica que más del 45 % de las redes todavía utilizan **WEP**, estudios similares enfocados a cadenas de minoristas conducidos en Nueva York (en el 2008) indica que el 29 % de los locales lo utilizan ([15]) y en las ciudades Atlanta, Boston, Chicago, Los Ángeles, Nueva York, San Francisco, Londres y París (realizado a fines del 2007) indica que el 25 % de los locales lo utilizan ([14]). Estudios similares conducidos en la zona céntrica de la ciudad de Buenos Aires en los años 2005, 2006, 2007, 2008 y 2009 ([24], [25], [26], [27], [28]) indica que el porcentaje de redes que utilizan el método de cifrado mencionado ha aumentado junto con la cantidad de redes presentes, de un 27 % hasta el 33 % que se mantuvo hasta el año 2009, decendiendo ligeramente en el mismo.

Los ataques al protocolo **WEP** conocidos atacan la confidencialidad provista por el protocolo ([30], [5], [7], [2], [34], [33]). Los mismos pueden ser divididos en dos clases: aquellos que permiten recuperar la clave de cifrado utilizada y aquellos que permiten recuperar parte del flujo pseudoaleatorio (*keystream*) utilizado para cifrar. La primera clase de ataques vulnera completamente la confidencialidad brindada por **WEP** mientras que la segunda permite enviar información y leer únicamente una pequeña parte del tráfico. Sin embargo, la primera clase de ataques suele ser más fácil de detectar por sistemas de detección de intrusiones para redes inalámbricas, por ejemplo las herramientas de AirDefense ([13]), AirTight ([17]) o AirMagnet ([16]), ya que son ataques activos que requieren

[4] A pesar de que TKIP fue diseñado para funcionar en el mismo hardware que WEP no todos los fabricantes proveen actualizaciones para utilizarlo, siendo necesario adquirir nuevo hardware.

enviar cientos o miles de tramas con propiedades particulares; de forma tal que se pueden construir "*signatures*" que los sistemas de detección de intrusiones son capaces de detectar.

En este trabajo se muestra la implementación de un canal encubierto de red sobre el protocolo **IEEE 802.11** (en todas sus versiones ya que la especificación de **WEP** no ha sufrido ningún cambio significativo) utilizando las extensiones provistas en el mismo para soportar **WEP**. Este tipo de problemas se ha analizado parcialmente en el protocolo **IEEE 802.11** ([6]), y adicionalmente, en ([10]) y ([31]) se estudian posibles canales encubiertos utilizando las extensiones provistas para **WEP**. Sin embargo, los canales encubiertos propuestos resultan ser triviales de detectar ya que no cumplen con la especificación del protcolo.

El objetivo de implementar un canal encubierto de red que resulte indistinguible, es que permite demostrar que **WEP** no sólo no cumple su objetivo primario (proveer confidencialidad equivalente a la provista por una red cableada), ya demostrado por numerosos estudios, sino que además agrega nuevos problemas de seguridad. Esto aumenta el riesgo de utilizar **WEP**, ya que un atacante podría no sólo obtener acceso a una red protegida por **WEP** (mediante los ataques conocidos) sino que utilizar el canal encubierto para enviar información sin ser detectado. Al no registrarse actividades sospechosas, el atacante podría mantener el control del sistema por más tiempo.

El presente trabajo se organiza de la siguiente manera: en la sección siguiente (Sección 2) se introducen los canales encubiertos y se presentan los requisitos para lograr un canal encubierto de red "indistinguible". En la tercera sección (Sección 3) se presenta una descripción del canal encubierto propuesto y se describe las implementaciones realizadas del canal encubierto propuesto (tanto mediante la modificación a un controlador de red para plataformas **Linux** y la inyección de tramas **IEEE 802.11** en el aire). La cuarta sección (Sección 4) compara, principalmente desde un punto de vista de posibilidad de detección, el canal encubierto propuesto con los trabajos relacionados así como las distintas implementaciones desarrolladas. Por último, la quinta sección (Sección 5) finaliza el presente trabajo, reflexionando sobre posibles problemas o áreas interesantes que quedan por explorar. Adicionalmente, se cierra con un análisis de su posible implementación de un canal encubierto similar en redes inalámbricas protegidas por los estándares **WPA** y **WPA2**.

2. Canales encubiertos

La seguridad informática está compuesta por tres pilares: la confidencialidad, la integridad y la disponibilidad ([4]). La confidencialidad, el aspecto que nos interesa, se puede definir como "la ocultación de información o recursos" ([4]). Habitualmente este objetivo de la seguridad informática se logra a través del uso de criptografía. Sin embargo, existen otras técnicas para ocultar información como la esteganografía ([22]) o los canales encubiertos.

Las técnicas de ocultación de información pueden ser rastreadas hasta civilizaciones antiguas ([22]). Los canales encubiertos fueron definidos en la era digital

como "aquellos no intencionados para la transferencia de información" por B. W. Lapmson ([19]) y posteriormente definidos como "cualquier canal de comunicación que puede ser explotado por un proceso para transferir información en violación de la política de seguridad del sistema" ([21]), por el Departamento de Defensa de Estados Unidos.

Los canales encubiertos utilizan recursos compartidos como vía de comunicación ([4]). Los recursos compartidos en un sistema informático son el espacio o el tiempo; esto nos lleva a las siguientes dos clases de canales encubiertos ([4]):

- almacenamiento: utilizan un atributo de un recurso compartido.
- temporales: utilizan una relación temporal o de orden respecto al uso de un recurso compartido.

En lo que respecta a canales encubiertos en redes de comunicaciones, la definición genérica anterior puede ser especializada a "una manipulación de un protocolo de comunicación para transferir información de forma no prevista por la especificación del protocolo" ([29]). Los mismos pueden ser o bien de almacenamiento, utilizando el contenido de las tramas o paquetes del protocolo en sí, para codificar la información del canal, o bien temporales, utilizando el tiempo de envío o el orden de envío de las tramas o paquetes para codificar la información del canal.

El otro aspecto que permite clasificar a los canales encubiertos, ortogonal al anterior, distingue entre un canal al cuál únicamente el emisor y receptor tienen acceso (utilizando un recurso compartido únicamente por ellos) y otro en el que terceras partes también tienen acceso (utilizando un recurso compartido por ellos y por al menos un tercero que no participa del canal). Los primeros se llaman canales encubiertos "sin ruido" mientras que los segundos se llaman canales encubiertos "ruidosos" ([4]).

Por último, cabe destacar que una de las propiedades clave de un canal encubierto es su ancho de banda y es uno de los parámetros más críticos utilizados a la hora de comparar canales encubiertos. Otros criterios de evaluación son:

- Probabilidad de detección
- Grado de anonimidad
- Facilidad de implementación
- Alcance (en el caso particular de canales encubiertos de red)

2.1. Requisitos de un canal encubierto

A continuación se detallan los puntos que se definieron como los requisitos que el canal encubierto debía cumplir, con el objetivo de obtener un canal encubierto robusto y de difícil detección.

1. Respete el estándar del protocolo, lo que implica respetar:
   - El formato de las tramas (y sus reglas de construcción)
   - Las secuencias de intercambio de tramas permitidas

2. Tener un ancho de banda estrictamente mayor que cero (el canal debe permitir enviar información).
3. Una trama que pertenece al canal encubierto debe ser "indistinguible"[1] de una trama que no pertenece al mismo.[2]
4. La implementación del protocolo que contenga el canal encubierto debe ser interoperable con implementaciones que no lo contengan.
5. De comprometerse la existencia del canal encubierto, ésta no debe comprometer el contenido del mismo.

Si bien a primera vista no resulta evidente la necesidad de respetar el estándar del protocolo, basta con tener en cuenta que si el canal encubierto no respeta el mismo se presentará una anomalía que podría conducir a la detección del canal encubierto.

3. Canal encubierto propuesto

Para poder cumplir con los requisitos detallados en 2.1, se ideó un canal encubierto de red que hace "uso y abuso" de las extensiones provistas por el protocolo **IEEE 802.11** para soportar **WEP**, con el objetivo de utilizarlas para enviar información de una forma no prevista por el protocolo pero compatible con el mismo.

El estándar **WEP**, agrega los siguientes campos a una trama de datos **IEEE 802.11**:

- *IV*: Compuesto por el vector de inicialización (de 24 bits), 6 bits de relleno (que deben estar en cero según el estándar [12]) y 2 bits para indicar la clave de cifrado en uso.
- *ICV* (Integrity Checksum Value): un *CRC-32* del los datos de la trama computado previo al cifrado.

La generación del vector de inicialización no se encuentra especificada en el estándar, por lo tanto cualquier esquema de generación es válido. Sin embargo, en la práctica se comienza con un valor o bien fijo (comúnmente cero), o un valor aleatorio o se retoma el último valor utilizado, y se continúa generando los valores subsiguientes de alguno de los siguientes modos:

- Se incremente el valor actual en modo *little-endian.*
- Se incremente el valor actual en modo *big-endian.*
- Se elige otro valor de forma aleatoria.

[1] Con indistinguible se hace referencia a que la trama se encuentre bien formada (su construcción respete el estándar) y que respete la secuencia de intercambios de tramas a la que pertenece.

[2] La idea detrás del requisito de "indistinguibilidad" proviene de un intento de formalizar el requisito de "difícil detección", es decir debe ser "difícil" detectar la existencia del canal encubierto observando el tráfico generado.

También se han observado implementaciones que alternan entre dos valores ([30]). Sin embargo, este tipo de implementaciones es muy poco común.

La idea del canal encubierto propuesto es utilizar el vector de inicialización para transmitir datos. Se eligió este campo ya que su comportamiento no se encuentra especificado, por lo tanto independientemente de los valores que tome este campo al ser utilizado para implementar el canal encubierto, cumplirá con el estándar; siendo ínter-operable la implementación con el canal encubierto con otras implementaciones del protocolo.

La pregunta que queda pendiente es cómo utilizar el valor del vector de inicialización para enviar datos. La respuesta es simple; se codifica el valor que se desea enviar en el vector de inicialización y se construye la trama según el proceso estándar de **WEP**, utilizando el valor resultante de la codificación como el vector de inicialización. La trama construida de esta forma resulta una trama **WEP** válida, que puede ser interpretada por el resto de las estaciones pertenecientes a la red.

Desde el punto de vista del receptor de los datos transmitidos a través del canal encubierto resulta que, debido a que el vector de inicialización se envía como parte del campo *IV* de la trama, el receptor puede identificar, debido a la codificación, que es una trama que contiene parte de los datos enviados a través del canal encubierto, y decodificar el valor codificado en el vector de inicialización; obteniendo el dato enviado a través del canal encubierto.

Por último, resta la descripción del proceso de codificación empleado. Dados los mecanismos de funcionamiento del canal encubierto, resulta necesario que el proceso de codificación le permita al receptor identificar que una trama es parte de la comunicación del canal encubierto. Además, uno de los requisitos impuestos es que de detectarse el canal encubierto no se comprometa los datos enviados a través del mismo. Para cumplir con este requisito se recurrió a la criptografía; los datos codificados en el vector de inicialización estarán cifrados.

Con el objetivo de implementar un mecanismo de codificación que dificulte la detección del canal encubierto, se ideo una forma de señalización, que llamaremos *encapsulada*, la cual consiste en agregar una capa de control (encapsulado en el campo *IV*) mediante la cuál el receptor puede distinguir si la trama pertenece al canal encubierto. De esta forma ningún valor tiene un significado especial; es decir, que son todos equiprobables. Sin embargo, al descifrar un *IV*, de tener la estructura correcta (asegurada mediante un código de detección de errores, por ejemplo un **CRC**) será considerada una trama de datos perteneciente al canal.

3.1. Implementación mediante la modificación de un controlador de red

La presente sección describe como se modificó la pila ("stack") del protocolo **IEEE 802.11** incluido en el núcleo *Linux* desde la versión *2.6.22*, para implementar el canal propuesto. La pila del protocolo **IEEE 802.11** llamada *mac80211*[5] (incluida desde la versión *2.6.22*) es utilizada por diferentes con-

[5] *mac80211* reemplaza a la pila anterior llamada *ieee80211*.

troladores, por ejemplo por el controlador incluido en el núcleo *Linux* desde la versión *2.6.25* para las placas **Zydas ZD1211**.

Se decidió implementar un controlador que utilice el mecanismo de señalización encapsulada, sobre un controlador que incrementa el IV de forma aleatoria. Se definió el siguiente formato para el campo IV:

- Primer byte: valor aleatorio utilizado como vector de inicialización para cifrar, mediante un cifrador de flujo, los datos del canal encubierto.
- Segundo byte: dato del canal encubierto (cifrado).
- Tercer byte: código de detección de errores (cifrado), basado en *CRC8-SMBUS*[6].

Cabe resaltar que la elección de *CRC8-SMBUS* fue arbitraría pudiéndose utilizar cualquier otro código de detección de errores de un byte.

En la señalización encapsulada implementada, la verificación de la pertenencia de una trama al canal encubierto se realizará de la siguiente manera:

1. Se concatena al valor del primer byte la contraseña que protegerá las comunicaciones del canal encubierto, para construir la clave utilizada para cifrar los datos del canal y el *CRC8-SMBUS*.
2. Se descifran el segundo y tercer byte del campo IV, utilizando la clave construida en el paso anterior y el algoritmo de cifrado de flujo *ARC4*.
3. Se calcula el valor *CRC8-SMBUS* del segundo byte descifrado.
4. Se compara el valor calculado con el valor del tercer byte descifrado, de coincidir la trama pertenece al canal encubierto.

Debido a la presencia del *CRC8-SMBUS*, es posible para el que conoce la clave del canal encubierto verificar la pertenencia de un IV al canal encubierto, ya que los datos poseen una estructura interna. La probabilidad de que un IV aleatorio sea reconocido como del canal es: 1/256 (ya que cada dato enviado tiene un único *CRC8-SMBUS*).

Se decidió utilizar un vector de inicialización para cifrar ya que de esta forma es posible sincronizar al emisor y receptor y permitir que el cifrado del mismo dato del canal encubierto resulte en un campo IV distinto, siempre y cuando el vector de inicialización elegido haya variado (razón por la cuál se lo elige aleatoriamente). De esta forma nos aseguramos que la distribución de la fuente que está generando los datos del canal encubierto no se traduzca en una distribución análoga del campo IV. Esto se debe a que si se cifrase con la misma clave todos los datos, valores iguales resultarían en el mismo valor cifrado; resultando en una mera traslación del sesgo de la fuente emisora.

3.2. Implementación mediante la inyección de tráfico

En la presente sección se describe el diseño de la herramienta desarrollada para implementar el canal encubierto mediante la inyección de tramas **IEEE**

[6] Ver `http://smbus.org/faq/crc8Applet.htm` para la descripción técnica del código de detección de errores.

802.11; ya que de ésta forma no es necesario modificar el controlador de red. La solución se programó en **Python** utilizando la biblioteca **Scapy**[3] para el manejo del envío de tramas.

A la hora de implementar la herramienta surgió el siguiente problema: ¿qué datos enviar en las tramas cifradas? En el caso de la implementación modificando el controlador, este problema no se presentó ya que se enviaban en las tramas del canal encubierto los datos indicados por el sistema operativo.

Se analizaron las siguientes alternativas al problema:

- Enviar paquetes de datos vacíos[7].
- Enviar datos inválidos.
- Enviar datos válidos.

Con respecto a la primer alternativa, cabe recordar que el estándar **IEEE 802.11** posee una trama especial que es una trama de datos vacía, por ende no se puede utilizar la trama de datos habitual y enviarla vacía. Tampoco se puede utilizar la trama especial de datos vacíos ya que no posee la encapsulación provista por **WEP** y por ende no posee un campo de vector de inicialización. Ésto se debe a que al no tener datos, no hay nada que cifrar, por ende no tiene los campos adicionales que tiene una trama cifrada.

Por otro lado, la segunda alternativa es viable, pero presenta dos variantes: o bien los datos basura se cifran de forma correcta para que la estación receptora los envié a la pila de red y sean descartados por la misma (por ser datos basura) o no se cifran correctamente y son descartados por la pila **IEEE 802.11** (dado que el **ICV** va a ser incorrecto). En el primer caso es difícil prever si se presentará un problema en la estación receptora y en el segundo caso será fácil detectar que hay un problema, ya que una estación generará más tramas malformadas que lo usual[8]; conduciendo a la posible detección del canal encubierto.

Por lo mencionado anteriormente, se decidió implementar la tercera opción: enviar datos válidos. Ya que no presenta ninguno de los problema exhibidos anteriormente. A la hora de definir qué datos enviar se decidió enviar paquetes pertenecientes a un protocolo de capa superior que no tuviese estado para evitar cualquier conflicto en la red (producto de no cumplir con la secuencia de estados impuesta por el protocolo de capa superior). Se analizaron varias alternativas: paquetes *ICMP*, paquetes *ARP* y paquetes *UDP*. Se optó por enviar un *gratuitous ARP* ya que este paquete no produce una respuesta por parte de la estación receptora y tampoco generará conflictos en la red. Cabe resaltar que el envío reiterado de cualquier tipo de trama puede resultar sospechoso y conducir a la detección del canal encubierto, aunque nuestro análisis toma como restricción realizar solamente un análisis de la trama en sí misma y no de su contenido.

[7] Normalmente sólo son utilizados por los controladores de red para indicar el inicio de modo de ahorro de energía por parte de la estación o si se está utilizando el modo de operación **PCF**.

[8] Al descifrar las tramas el *ICV* no será correcto.

El análisis de factibilidad de detección que se realizó asumía que las tramas del canal encubierto eran indistinguibles de las tramas que no pertenecían al mismo. Este supuesto es cierto para el caso de las implementaciones que modifican el controlador, ya que lo único que se modifica es el algoritmo de elección de *IV*. Por el contrario, ésto no es cierto para el caso de la implementación que inyecta tramas, ya que la misma no respeta la asignación de números de secuencia (el número de secuencia es un campo que se incrementa linealmente y está presente en todas las tramas de datos). Dado que el mismo debe ser incrementado de a uno no es posible hacer que las tramas del canal encubierto sean indistinguibles de las tramas legítimas.

Para evitar que se pueda detectar por el incremento no lineal del número de secuencia a una trama del canal encubierto, la primera implementación (llamada "inject_ivs.py") que se realizó emula una estación que se conecta a la red (se autentica y asocia) y envía las tramas incrementando el número de secuencia linealmente; en lugar de enviar las tramas como si fuese una estación que ya se encontraba utilizando la red.

La segunda implementación (llamada "reinject_ivs.py"), que emula una estación que ya pertenece a la red (copiando su dirección MAC), utiliza en cada trama el último número de secuencia utilizado por la estación real, pero indicando que es una retransmisión (así la estación receptora ignora la trama). De esta forma se logra emular una estación que ya pertenece a la red y respetar el incremento lineal del número de secuencia.

Sin embargo, aún se presentaba un problema a resolver al implementar la segunda versión, a saber: qué datos cifrar. Si se cifran datos distintos, se puede producir un error en el receptor y además, si son de distinta longitud ésta diferencia podrá ser percibida por un sistema de detección de intrusiones; la retransmisión de la trama anterior no puede ser de distinta longitud, ya que justamente es una retransmisión de la misma trama. Por este motivo, se optó por utilizar los mismos datos contenidos en la trama, lo que implica descifrar la trama y volverla a cifrar con el valor de *IV* a utilizar para el canal encubierto.

4. Comparación entre las implementaciones

En la presente sección se resumen las diferencias entre las implementaciones desarrolladas.

Comenzaremos por analizar la facilidad de instalación del canal encubierto. Ambos tipos de implementaciones requieren privilegios de administrador para funcionar; ya que una requiere modificar el controlador de red, mientras que la otra requiere enviar tramas en modo *raw* a la interfaz de red. Por otro lado, los requisitos de software y hardware para ambas implementaciones son diferentes. Las implementaciones que modifican el controlador requieren que se esté utilizando un controlador que utilice la pila **IEEE 802.11** llamada *mac80211*. Este requisito no está presente en la versión que inyecta, sin embargo ésta tiene como requisito que el sistema tenga instalado *Python*.

Desde el punto de vista de la factibilidad de detección, hemos visto que la implementación que modifica el controlador lo hace de forma tal que las tramas pertenecientes al canal son "indistinguibles" de las tramas que no pertenecen. Esto se debe a que en ambos casos se envía un valor aleatorio como valor del campo IV; si no pertenece al canal se genera un valor aleatorio, y si pertenece al canal se envía un valor cifrado que lo es por propiedades del algoritmo de cifrado.

Como se explicó anteriormente, este análisis es suficiente para las implementaciones que modifican el controlador, pero no es lo es para las versiones que inyectan tramas. Para esta clase de implementaciones la siguiente tabla resume las conclusiones, para dos casos: cuando el controlador de red de la estación es incremental (independientemente del modo que incremente) o cuando es aleatorio.

Implementación	Controlador Incremental	Controlador Aleatorio
Emula una estación nueva que se une a la red (inject_ivs.py)	Detección en base a los números de secuencia	
Emula una estación existente en la red (reinject_ivs.py)	Detección en base al IV	Indetectable

Cuadro 1. Análisis de detectabilidad para implementaciones que inyectan tramas

En el caso "indetectable", el único comportamiento anómalo que se podría detectar es que el controlador debe retransmitir tramas periódicamente; cuestión que ocurre usualmente en redes inalámbricas debido al uso de un medio "ruidoso" como es el aire.

Con respecto a la confiabilidad de las solución propuesta, y debido a que el canal como está planteado no es bidireccional, no existe ningún mecanismo que garantice que el receptor recibió los datos. De implementarse un canal bidireccional, por ejemplo, utilizando el mismo canal encubierto en el sentido inverso o un canal alternativo, es posible implementar un protocolo que utilice como medio de transporte al canal encubierto y que garantice el envío de los datos. Además, cabe mencionar que se puede incorrectamente catalogar tramas como pertenecientes al canal que en realidad no lo son (aunque con muy baja probabilidad). Esto se podría solucionar utilizando un protocolo superior que ayude a detectar este tipo de errores.

Por último, resta analizar si la solución propuesta es un canal encubierto con o sin "ruido". En la Sección 2 se definió lo que se entiende por canal encubierto con y sin "ruido": un canal sin ruido es aquel que utiliza un recurso disponible únicamente a los usuarios del canal, mientras que un canal con ruido utiliza un recurso que también está disponible a terceros que no participan del canal. En el caso particular de nuestra propuesta, nos encontramos ante un canal sin "ruido"

ya que si bien los datos (cifrados) enviados a través del canal encubierto pueden ser leídos por cualquiera dentro del rango de alcance de la señal inalámbrica, el campo *IV* utilizado como medio para enviar los datos del canal sólo puede ser "escrito" por el emisor del canal.

En cuanto al ancho de banda del canal encubierto, definido como la cantidad de datos (bytes) del canal que se pueden enviar en cada trama del protocolo, es trivial notar que por cada trama de datos enviada es posible enviar un byte de datos pertenecientes al canal encubierto en cualquiera de las implementanciones desarrolladas.

4.1. Comparación con otras implementaciones de canales encubiertos sobre IEEE 802.11

A continuación se presenta un análisis de cualquier implementación que utilice mensajes de gestión y/o de control para enviar los datos del canal encubierto, como es el caso de la implementación previa de canales encubiertos sobre redes **IEEE 802.11** ([6]) de la cuál se dispone de código fuente. Del mismo, se deduce que las implementaciones que utilicen mensajes de gestión y/o de control no cumplen con los requisitos explicitados anteriormente, justificando la decisión de idear e implementar una solución que sí cumpla con los mismos.

En 2.1, se definieron ciertos puntos que un canal encubierto de red "ideal" debería cumplir, por ende la comparación con implementaciones (que utilicen mensajes de gestión y/o de control) se hará con respecto a los mismos. El primer punto enunciado indicaba que se debe respetar el estándar del protocolo, lo cual implicar respetar no sólo el formato de las tramas y sus reglas de construcción, sino que también las secuencias de intercambio de tramas permitidas por el estándar. Si se considera cada tipo de trama, se verá que las únicas viables para implementar un canal encubierto que cumpla con los requisitos impuestos, es utilizar las tramas *ACK* o *Probe request*. Si se analiza en detalle la estructura de cada una de dicha tramas se nota que todos los campos que la componen se encuentran especificados y por ende no es posible enviar datos del canal encubierto sin violar las reglas de construcción de las mismas.

Es importante resaltar que en las tramas *Probe request* se podría enviar datos en el campo "Last (Vendor Specific) Information Element", pero dado que su uso no es habitual y su contenido no se encuentra especificado en el estándar, llamaría rápidamente la atención; potencialmente revelando la existencia del canal encubierto.

En ([10]) se proponen dos canal encubiertos: uno que utiliza el vector de inicialización para el envío de datos, y el otro los números de secuencia de las tramas de datos. El uso de los números de secuencia viola el requisito que indica respetar el estándar del protocolo ya que el número de secuencia debe ser incrementado linealmente. El uso del vector de inicialización propuesto es similar al implementado en la versión que inyecta datos, pero a diferencia de ésta, no respeta las secuencias de intercambios de tramas del estándar, utiliza el campo *Key ID* que según el estándar debe permanecer en cero, y tampoco cifra los datos enviados (aunque menciona que esta posibilidad existe).

Adicionalmente, en ([31]) también se propone utilizar el vector de inicialización para implementar un canal encubierto en conjunto con las direcciones MAC (para lograr un mayor ancho de banda); violando el requisito que indica respetar el estándar del protocolo, ya que se enviarán tramas a direcciones MAC que no se corresponden a estaciones asociadas a la red (para las cuales nunca se reciben tramas de confirmaciones). También se propone enviar datos en tramas corruptas (cuyo CRC-32 falle), cuestión que claramente viola el requisito que indica respetar el estándar del protocolo y facilitará la detección del canal encubierto ya que se generaran más fallas de CRC-32 que lo habitual.

5. Trabajo futuro y comentarios finales

La conclusión fundamental del presente trabajo es que es posible construir un canal encubierto sobre el protocolo **IEEE 802.11** (utilizando las extensiones provistas en el mismo para soportar **WEP**), que cumple con los requisitos planteados en la Sección 2.1, que esencialmente definen un canal encubierto cuyo uso es "indistinguible" de su no uso.

La existencia de canales encubiertos en un protocolo de red es un problema de seguridad ya que aumenta el riesgo de utilizar el mismo. Esto se debe a que utilizar el protocolo introduce un mecanismo oculto de comunicación que puede ser aprovechado por un atacante con resultados perjudiciales para quien emplea el protocolo.

Uno de los objetivos del presente trabajo era mostrar que **WEP** no sólo no cumple su objetivo primario, proveer confidencialidad (ya demostrado por numerosos estudios), sino que además agrega otros problemas de seguridad a una red que supuestamente protege. El mismo se cumplió al demostrar que **WEP** permite implementar un canal encubierto de muy difícil detección que no es posible implementar en redes sin protección ni en redes con **WPA/WPA2**. Esto se debe a que a la hora de diseñar **WPA/WPA2** se buscó un mecanismo que permitiese prevenir contra ataques de repetición ("replay attacks" [9]).

En el caso de **WPA** o **TKIP** (nombre no comercial utilizado en el estándar), que sigue utilizando el algoritmo **ARC4** para el cifrado, el vector de inicialización se construye a partir de un contador que es incrementado en uno por cada trama enviada. Por lo tanto el valor del vector de inicialización no puede ser aleatorio como en el caso de **WEP** sino que está perfectamente definido, por ende no pudiendo ser utilizado para implementar un canal encubierto.

En el caso de **WPA2** o **CCMP** (nombre no comercial utilizado en el estándar), se presenta una situación similar. A diferencia de **WPA** se utiliza el algoritmo de cifrado **AES**, sin embargo, de forma similar el vector de inicialización utilizado es un contador que debe ser incrementado en uno por cada trama enviada.

Es posible extender las ideas presentadas en este trabajo en diferentes formas. A continuación se presentan las líneas de acción que consideramos más interesantes y fructuosas:

[9] Los protocolos vulnerables a este ataque son aquellos donde es posible reenviar una trama, sin modificación, y la misma sigue siendo válida.

- Extender el concepto de utilizar un valor pseudoaleatorio de un protocolo de comunicación para implementar un canal encubierto a otros protocolos de red.
- Mejorar la implementación del canal encubierto para que sea bidireccional, con el objetivo de crear una interfaz de red virtual que permita utilizar protocolos como *TCP/IP* a través del canal encubierto.
- Estudiar otras alternativas para implementar un canal encubierto en redes inalámbricas protegidas por **WPA/WPA2**, ya que no es posible extrapolar la idea presentada a éste tipo de redes.
- Estudiar la viabilidad de implementar un canal encubierto similar al propuesto en el presente trabajo, basado en las particularidades del manejo de tramas *Probe Request* por parte de las estaciones *Windows XP* [8] [20]. Debido a que las estaciones *Windows XP* envían datos aleatorios en el campo *SSID* periódicamente, es posible extrapolar el concepto presentado en este trabajo, potencialmente obteniendo un canal encubierto "indistinguible".

Referencias

[1] Wi-Fi Alliance. *Wi-Fi Protected Access (WPA)*. URL http://www.wi-fi.org.

[2] William A. Arbaugh, Narendar Shankar, and Y. C. Justin Wan. Your 802.11 wireless network has no clothes, May 15 2001. URL http://citeseer.ist.psu.edu/472552.html;http://www.drizzle.com/~aboba/IEEE/wireless.pdf.

[3] Philippe Biondi. Scapy. URL http://www.secdev.org/projects/scapy/.

[4] M. Bishop. *Computer Security: Art and Science*. Addison-Wesley, Boston, USA, 2003.

[5] Andrea Bittau, Mark Handley, and Joshua Lackey. The final nail in WEP's coffin. In *IEEE Symposium on Security and Privacy*, pages 386–400. IEEE Computer Society, 2006. ISBN 0-7695-2574-1. URL http://doi.ieeecomputersociety.org/10.1109/SP.2006.40.

[6] L. Butti and F. Veysset. Wi-fi advanced stealth. Black Hat Briefings USA, 2006. URL http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Veyssett.pdf.

[7] Rafik Chaabouni. Break wep faster with statistical analysis. Technical report, EPFL, LASEC, June 2006.

[8] Shane A. Macaulay Dino A. Dai Zovi. Attacking automatic wireless network selection, 2005. URL http://www.theta44.org/karma/aawns.pdf.

[9] FIPS. *Advanced Encryption Standard (AES)*. National Institute for Standards and Technology, pub-NIST:adr, November 2001. URL http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[10] L. Frikha and Z. Trabelsi. A new covert channel in wifi networks. In *Risks and Security of Internet and Systems, 2008. CRiSIS '08. Third International Conference on*, pages 255 –260, 28-30 2008. doi: 10.1109/CRISIS.2008.4757487.

[11] IEEE. *IEEE Std 802.11i, Amendment to IEEE Std 802.11 - Amendment 6: Medium Access Control (MAC) Security Enhancements*. IEEE, 2004.

[12] IEEE. *IEEE Std 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE, Edition 2007. URL http://standards.ieee.org/getieee802/download/802.11-2007.pdf.

[13] AirDefense Inc. Motorola airdefense - security and compliance solutions, . URL http://www.airdefense.net/products/servicesplatform/securitycompliance/index.php.

[14] AirDefense Inc. Airdefense's comprehensive survey of 3,000 retail stores finds many wireless data security vulnerabilities as holiday shopping season nears, . URL http://www.airdefense.net/newsandpress/11_15_07.php.

[15] AirDefense Inc. Airdefense's survey of retailers across new york city discovers wireless security vulnerabilities in brooklyn, the bronx, man-

hattan, queens and staten island, . URL http://www.airdefense.net/newsandpress/01_14_08.php.
[16] AirMagnet Inc. Airmagnet enterprise, . URL http://www.airmagnet.com/products/enterprise/.
[17] AirTight Networks Inc. Spectraguard enterprise, . URL http://www.airtightnetworks.com/home/solutions/wireless-intrusion-prevention.html.
[18] K.Kaukonen and R.Thayer. A stream cipher encryption algorithm "arcfour", 1999.
[19] B. W. Lampson. A note on the confinement problem. *ACM*, 16(10):613–615, October 1973.
[20] Microsoft. Description of the wireless client update for windows xp with service pack 2, 2007. URL http://support.microsoft.com/kb/917021.
[21] Department of Defense Standard. *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.
[22] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. Information hiding – a survey. *Proceedings of the IEEE (USA)*, 87(7):1062–1078, July 1999.
[23] Anton T. Rager. Wepcrack. URL http://wepcrack.sourceforge.net.
[24] Cybsec S.A. Wardriving buenos aires 2005, . URL http://www.cybsec.com/upload/TadeoCwierz_Buenos_Aires_Wardriving2005_1.pdf.
[25] Cybsec S.A. Wardriving buenos aires 2006, . URL http://www.cybsec.com/upload/Tendencias06_WardrivingBsAs2006.pdf.
[26] Cybsec S.A. Wardriving buenos aires 2007, . URL http://www.cybsec.com/upload/cybsec_Tendencias07_Wardriving_BsAs2007.pdf.
[27] Cybsec S.A. Wardriving buenos aires 2008, . URL http://www.cybsec.com/upload/Estadisticas_WarDriving_Wireless.pdf.
[28] Cybsec S.A. Tendencias en seguridad de la información, . URL http://www.cybsec.com/upload/tendencias_Arg_2009_v1_Pmilano.pdf.
[29] R. Sbrusch. Network covert channels: Subversive secrecy. Technical report, SANS Institute, October 2006. URL http://www.sans.org/reading_room/whitepapers/covert/1660.php.
[30] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. Using the fluhrer, mantin, and shamir attack to break WEP. In *NDSS*. The Internet Society, 2002. ISBN 1-891562-14-2; 1-891562-13-4. URL http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf.
[31] Krzysztof Szczypiorski. Hiccups: Hidden communication system for corrupted networks. In *In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, October 22-24, 2003 Mie;dzyzdroje*, pages 31–40, 2003.
[32] The Aircrack-NG team. Aircrack-ng suite. URL http://www.aircrack-ng.org.
[33] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. Cryptology ePrint Archive, Report 2007/120, 2007. URL http://eprint.iacr.org/2007/120.pdf.
[34] Y.C.J. Wav W.A. Arbaugh, N. Shankar. An inductive chosen plaintext attack against wep/wep2, 2001.