



Unidad 12: Seguridad en Redes Inalámbricas

Autor: Alberto Escudero Pascual, LaNeta, IT +46

Traducción de LaNeta

Tabla de contenido

1. Sobre este documento.....	2
1.1 Información sobre propiedad intelectual.....	2
1.2 Pre-requisitos.....	2
1.3 Grado de dificultad.....	2
1.4 Información sobre los iconos.....	2
2. Introducción.....	2
3. Definiendo seguridad inalámbrica.....	3
4. ¿Qué es seguridad de la información?.....	3
4.1 Confidencialidad.....	4
4.2 Autenticación.....	4
4.3 Integridad.....	4
4.4 Disponibilidad.....	4
4.5 No repudiación (rendición de cuentas).....	5
5. Seguridad de información y las WLAN.....	5
6. Implementando los atributos de seguridad.....	6
6.1 Comentarios generales acerca del cifrado en el nivel de enlace.....	6
7. Confidencialidad en redes inalámbricas.....	7
7.1 WEP o no WEP.....	7
7.2 WEP muere, nacen WPA y WPA2.....	8
8. Autenticación en Redes inalámbricas.....	9
8.1 Detener la difusión de la SSID como medida de seguridad.....	10
8.2 Usando el filtrado de direcciones MAC como medida de seguridad.....	11
8.3 Portales cautivos para redes inalámbricas.....	11
9. Integridad de datos en redes inalámbricas.....	12
9.1 Nota sobre seguridad acerca de WPA.....	13
10. Disponibilidad en redes inalámbricas.....	14
11. No repudiación en redes inalámbricas (rendición de cuentas).....	15
12. Amenazas de seguridad en redes inalámbricas	15
13. Conclusiones.....	16
14. Declaración de Derechos de Propiedad Intelectual.....	17

1. Sobre este documento

Este material es parte del paquete de materiales del proyecto TRICALCAR. Para información sobre TRICALCAR consulte el módulo de introducción de estos materiales, o www.wilac.net/tricalcar/. Este material fue traducido del inglés de los materiales desarrollados para el proyecto "Capacity Building for Community Wireless Connectivity in Africa" de APC <<http://www.apc.org/wireless/>>. El material fue actualizado y adaptado para el contexto de América Latina.

1.1 Información sobre propiedad intelectual

Esta unidad temática se ha hecho disponible bajo los términos de la licencia **Atribución-No Comercial-Licenciamiento Recíproco 3.0 Genérica**. Para ver los términos completos de esta licencia: http://creativecommons.org/licenses/by-nc-sa/3.0/deed.es_MX

1.2 Pre-requisitos






Se recomienda leer primero la unidad "Redes avanzadas".

1.3 Grado de dificultad

El grado de dificultad de esta unidad es Avanzado.

1.4 Información sobre los iconos

En los contenidos encontraremos 5 tipos de iconos, cuyo significado se describe a continuación:

Concepto teórico clave	Recomendación práctica importante	Ejercicio	Propiedad intelectual	Propiedad intelectual
				

2. Introducción

Esta guía inicia brindando una breve introducción al modelo de referencia OSI, y conceptos claves de seguridad, antes de introducir las ideas de seguridad inalámbrica en el contexto de IEEE 802.11 o WLAN.

Se aborda la seguridad en el contexto de la seguridad de información y se describen y evalúan cinco atributos de seguridad (confidencialidad, autenticación, integridad, no-repudio y disponibilidad). La unidad finaliza con la presentación de algunas amenazas de seguridad importantes que deben ser consideradas en cualquier diseño de red inalámbrica.

La unidad se enfoca en dar una imagen de la seguridad inalámbrica dentro de un contexto amplio de seguridad de la información. Busca lograr un entendimiento acerca de dónde construir la seguridad en cada capa de la pila de protocolos OSI/TCP/IP. Además, considera elementos claves de seguridad que deben ser abordados en la fase de diseño de una red inalámbrica.

3. Definiendo seguridad inalámbrica

La definición de seguridad es en gran medida específica al contexto; la palabra seguridad abarca un rango amplio de campos dentro y fuera del ámbito de la computación. Hablamos de seguridad cuando describimos medidas de seguridad en la carretera o cuando describimos una nueva plataforma de cómputo que es segura contra virus. Se han desarrollado varias disciplinas para abordar cada aspecto de seguridad.

Con esto en mente, hemos intentado enmarcar el término “seguridad inalámbrica” en el contexto de seguridad de información. Cuando hablamos de “seguridad inalámbrica” de hecho estamos hablando de “seguridad de información en redes inalámbricas”.

4. ¿Qué es seguridad de la información?

Para entender el significado de Seguridad Informática es necesario entender la manera en que el término ha evolucionado en el tiempo. Hasta fines de los 70's, esta área de seguridad fue referida como Seguridad de comunicaciones. Seguridad de Comunicaciones o COMSEC, por un acrónimo en inglés, fue definido por la U.S. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) como:



“Medidas y controles que se toman para negar el acceso no autorizado de personas a información derivada de las telecomunicaciones y asegurar la autenticidad de tales telecomunicaciones”.U

Se incluyeron cuatro áreas como partes las actividades de seguridad de COMSEC: Criptoseguridad, Seguridad de Transmisiones, Seguridad de Emisiones y Seguridad física. La seguridad en COMSEC incluyó dos atributos relacionadas con esta unidad: **Confidencialidad y Autenticación.**

4.1 Confidencialidad

Asegurar que la información no es divulgada a personas no autorizadas, procesos o dispositivos. (Protección contra divulgación no autorizada).

4.2 Autenticación

Medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información (Verificación de emisor).

En los 80's con el crecimiento de las computadoras personales se inició una nueva era: Computación personal, y la seguridad aplicada a este campo (COMPUSEC). COMPUSEC fue definido por NSTISSI como:



“Medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de sistemas de información incluyendo hardware, software, firmware e información que está siendo procesada, almacenada y comunicada”.

COMPUSEC introdujo dos atributos de seguridad adicionales, relacionados con esta unidad: **Integridad y Disponibilidad.**

4.3 Integridad



La calidad de un sistema de información refleja el correcto funcionamiento y confiabilidad de sistema operativo, la coherencia del hardware y software que implementan los sistemas de protección y la consistencia de las estructuras de datos de la información almacenada.

4.4 Disponibilidad



Acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.

Finalmente en los 90's, las dos eras de la información, COMSEC y COMPUSEC, fueron integradas para formar Seguridad en Sistemas de Información (INFOSEC). INFOSEC incluyó los cuatro atributos: Confidencialidad, Autenticación, Integridad y Disponibilidad, pero también se agregó un nuevo atributo: No-repudio (non-repudiation)

4.5 No repudiación (rendición de cuentas)



Asegurar que el remitente de información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

5. Seguridad de información y las WLAN

La NSTISSI define el concepto de Seguridad de Sistemas de información como:



La protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el medio de almacenaje, procesamiento o tránsito, y contra la negación de servicio a los usuarios autorizados, o la provisión de servicio a usuarios no autorizados, incluyendo las medidas necesarias para detectar, documentar y contabilizar esas amenazas.

La seguridad inalámbrica se presenta desde el punto de vista de la “seguridad de los sistemas de información” o INFOSEC.

Es muy común describir, en la literatura relacionada con la seguridad WLAN, aspectos prominentes de seguridad sin dar un marco de seguridad apropiado. Al describir aspectos “prominentes” el lector tiende a recordar acrónimos pero olvida el beneficio de cada “prominencia”. Para evitar eso, no listaremos todos los atributos de seguridad que se presentan en WLAN, sino que presentaremos cada uno de los cinco atributos de seguridad de INFOSEC, y luego discutiremos la manera en que WLAN implementa cada uno de estos.

Este acercamiento ayudará al lector a tener un enfoque metodológico al diseñar redes inalámbricas seguras. Los cinco atributos de seguridad a discutir serán: Confidencialidad, Autenticación, Integridad, No-repudiación y Disponibilidad¹

1. Para un abordaje más formal sobre seguridad, lea: The Common Criteria for Information Technology Security Evaluation, typically abbreviated as just “Common Criteria” or “CC.” The CC provides both Functional and Assurance requirements for security products and systems.

6. Implementando los atributos de seguridad

El modelo de referencia OSI (Interconexión abierta de sistemas), creado por la ISO (organización internacional de estándares), es una descripción abstracta para diseño de protocolos de redes de cómputo. El modelo divide las diferentes funciones de comunicación en siete capas que pueden funcionar de manera independiente una de otra.

Así como se describe en la unidad “redes avanzadas”, el diseño de protocolos de la OSI sigue el principio de “pila”. Al tener un modelo de protocolos en capas o “apilado” implica que cada capa usa únicamente la funcionalidad de la capa inferior, y provee funcionalidad exclusivamente a la capa inmediata superior.

Este enfoque en capas tiene implicaciones directas en la manera en que podemos implementar atributos de seguridad.



Los estándares de redes inalámbricas se refieren, normalmente, a la capa 1 y capa 2 de la pila de protocolos OSI, conservando el paquete IP sin cambios. Los paquetes IP se transportan sobre protocolos del nivel físico y de enlace de datos que son específicamente de carácter inalámbricos.

Por ejemplo, si consideramos la “confidencialidad del tráfico de datos” entre dos puntos de acceso, podemos lograr resultados similares (protección de la información) actuando en tres capas diferentes:

- La capa de aplicación (mediante TLS/SSL)
- La capa IP (mediante IPSEC)
- La capa de enlace (mediante cifrado)

Recuerde que cuando hablamos de seguridad inalámbrica, sólo estamos examinando los mecanismos de seguridad en las capas 1 y 2, o sea, del cifrado (nivel de enlace). Otros mecanismos de seguridad presentes a nivel 3 y superiores son parte de la seguridad implementada en las capas de red o de aplicación.

6.1 Comentarios generales acerca del cifrado en el nivel de enlace

El cifrado en el nivel de enlace es el proceso de asegurar los datos cuando son transmitidos entre dos nodos instalados sobre el mismo enlace físico (puede ser también el caso de dos enlaces diferentes mediante un repetidor, ejemplo un satélite). Con cifrado a nivel de enlace, cualquier otro protocolo o aplicación de datos que se ejecuta sobre el enlace físico queda protegida de cualquier interceptación.

El cifrado requiere una clave secreta compartida entre las partes en contacto, y un algoritmo previamente acordado. Cuando el transmisor y receptor no comparten un medio de transporte de datos en común, los datos deben ser descifrados y nuevamente cifrados en cada uno de los nodos en el camino al receptor.

El cifrado en el nivel de enlace se usa en caso de que no se aplique un protocolo de mayor nivel.



Cifrado a nivel de enlace en el estándar IEEE 802.11

El algoritmo de cifrado mejor conocido para el estándar IEEE 802.11 es el llamado en inglés Wired Equivalent Privacy (WEP). Está probado que WEP es inseguro, y otras alternativas, como el protocolo Wi-Fi Protected Access (WPA), es considerado como el estándar recomendado. El nuevo estándar IEEE 802.11i va a incluir una extensión de WPA, llamada WPA2.

El cifrado a nivel de enlace no provee **seguridad de extremo a extremo**, fuera del enlace físico, y sólo debe ser considerada una medida adicional en el diseño de la red.

El cifrado a nivel de enlace requiere más recursos de hardware en los puntos de acceso y medidas especiales de seguridad en la administración y distribución de llaves.

7. Confidencialidad en redes inalámbricas

7.1 WEP o no WEP



Definimos la confidencialidad en redes inalámbricas como el acto de asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas. La confidencialidad debe asegurar que ya sea la comunicación entre un grupo de puntos de acceso en un sistema de distribución inalámbrico (WDS por sus siglas en inglés), o bien entre un punto de acceso (AP) y una estación o cliente, se conserva protegida contra interceptaciones.

La confidencialidad en redes inalámbricas ha sido asociada tradicionalmente con el término “privacidad equivalente a enlaces alambreados” o WEP, por su siglas en inglés. WEP fue parte del estándar IEEE 802.11 original, de 1999.

El propósito del WEP fue brindar, a las redes inalámbricas, un nivel de seguridad comparable al de las redes alambreadas tradicionales. La necesidad de un protocolo como WEP fue obvio, las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas.

La vida del WEP fue muy corta; un diseño malo y poco transparente condujo ataques muy efectivos a su implantación. Algunos meses después de que el WEP fuera publicado, el protocolo fue considerado obsoleto. Aunque la llave tenía una longitud limitada debido a restricciones de exportación, se pudo probar que el protocolo era débil independientemente de ese hecho.

No fueron solo las fallas de diseño las que hicieron que WEP fuera obsoleto, sino también la falta de un sistema de manejo de llaves como parte del protocolo. WEP no tuvo incluido sistema alguno de manejo de llaves. El sistema de distribución de llaves fue tan simple como teclear manualmente la misma llave en cada dispositivo de la red inalámbrica (un secreto compartido por muchos no es un secreto!).

WEP fue seguido por varias extensiones de carácter propietario que resultaron también inadecuadas, por ejemplo WEP+ de Lucent, y WEP2 de Cisco.



WEP y sus extensiones (WEP+, WEP2) son al día de hoy obsoletas. WEP está basado en el algoritmo de encriptación RC4, cuyas implementaciones en el estándar IEEE 802.11 se consideran inadecuadas.

Existen varios ataques y programas para quebrar el WEP (Airsnort, wepcrack, kismac, aircrack etc). Algunos de los ataques están basados en la limitación numérica de los vectores de inicialización del algoritmo de cifrado RC4, o la presencia de la llamada “debilidad IV” en un datagrama.

- Para los interesados en los aspectos históricos de la seguridad del WEP, pueden consultar los recursos adicionales de esta unidad.

7.2 WEP muere, nacen WPA y WPA2

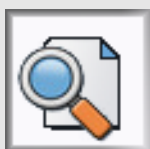
Luego del deceso del WEP, en 2003 se propone el Acceso Protegido a Wi-Fi (WPA, por sus iniciales en inglés) y luego queda certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 (en 2004).

WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves. Si no se usa un servidor de llaves, todas las estaciones de la red usan una “llave previamente compartida” (PSK - Pre-Shared-Key-, en inglés), El modo PSK se conoce como WPA o WPA2-Personal.

Cuando se emplea un servidor de llaves, al WPA2 se le conoce como WPA2-Corporativo (o WPA2-Enterprise, en inglés). En WPA-Corporativo, se usa un servidor IEEE 802.1X para distribuir las llaves. Una mejora notable en el WPA” sobre el viejo WEP es la posibilidad de intercambiar llaves de manera dinámica mediante un protocolo de integridad temporal de llaves (TKIP -Temporal Key Integrity Protocol).

WPA2 – Acceso protegido a Wi-Fi

WPA2 es la versión certificada de WPA y es parte del estándar IEEE 802.11i. Hay dos cambios principales en WPA2 vs. WPA:



1. El reemplazo del algoritmo Michael por una código de autenticación conocido como el protocolo “Counter-Mode/CBC-Mac “ (CCMP), que es considerado criptográficamente seguro.
2. El reemplazo del algoritmo RC4 por el “Advanced Encryption Standard (AES)” conocido también como Rijndael.

Recomendaciones para confidencialidad en datos:



Si se necesita confidencialidad mediante el cifrado a nivel de enlace: la mejor opción es WPA2 en modo “corporativo” (WPA2-Enterprise”).

En caso de usarse una solución más simple como la WPA2-Personal, deben tomarse precauciones especiales al escoger una contraseña (llave pre-compartida, PSK).

El protocolo WEP y sus variantes WEP+, y WEP2, deben ser descartados

8. Autenticación en Redes inalámbricas

En el contexto de las redes LAN, la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas. En otros términos, la autenticación inalámbrica significa “el derecho a enviar hacia y mediante el punto de acceso”.

Para entender “Autenticación” en redes inalámbricas es necesario entender qué sucede en el inicio de la sesión de comunicación entre un punto de acceso y una estación inalámbrica. El inicio de una comunicación comienza por un proceso llamado “asociación”.

Cuando el estándar IEEE 802.11b fue diseñado, se introdujeron dos mecanismos de “asociación”:

- Autenticación abierta y
- Autenticación con llave compartida

La autenticación **abierta implica NO seguridad y cualquiera puede hablarle al punto de acceso.**

En la autenticación **de llave compartida**, **se comparte una contraseña entre el punto de acceso y la estación cliente**. Un mecanismo de reto/respuesta le permite al punto de acceso verificar que el cliente conoce la llave compartida, y entonces conceder el acceso.

WEP y la Autenticación en la capa 2



La Autenticación con llave compartida implementada en WEP también es obsoleta. Varios ataques tipo texto plano versus texto cifrado pueden vulnerar la Autenticación basada en WEP. Debido al hecho de que la llave de cifrado y Autenticación son el mismo secreto compartido, una vez que una resulta comprometida, la otra también.

Recomendaciones de Autenticación inalámbrica:



La Autenticación inalámbrica mediante la capa 2 requiere el uso del modo WPA2-corporativo. La Autenticación en las redes inalámbricas, como las implantadas por los proveedores de servicios de internet inalámbricos, normalmente se utiliza en capas de red más altas (capa IP) mediante portales cautivos (que requieren identificarse ante un sitio web).

Es importante entender que al transferir la Autenticación a un “portal cautivo” no tenemos un recurso para detener el flujo de tráfico que cruza nuestros puntos de acceso.

8.1 Detener la difusión de la SSID como medida de seguridad

La firma Lucent Technologies desarrolló en el año 2000 una variación del esquema de Autenticación abierta llamado “red cerrada”. Las redes cerradas se diferencian del estándar IEEE 802.11b en que el punto de acceso no difunde periódicamente las llamadas “Tramas Baliza” o “Beacon Frames”.

Evitar la publicación de la SSID implica que los clientes de la red inalámbrica necesitan saber de manera previa que SSID deben asociar con un punto de acceso. Esta cualidad ha sido implantada por muchos fabricantes como una mejora de “seguridad”. La verdad es, mientras detener la difusión de la SSID previene a los clientes enterarse de la SSID por medio de una “trama baliza”, no impedirá que otro software de interceptación detecte la asociación que provenga de otro punto de la red cuando ésta eventualmente ocurra.

Deteniendo la difusión de la SSID



La detección de la difusión de la SSID no impedirá que una persona “interesada” encuentre la SSID de su red. Configurando la red como “cerrada” solo añadirá una barrera adicional a un intruso corriente. Detener la difusión de la SSID debe considerarse como una “precaución adicional”, más no una medida de seguridad efectiva.

8.2 Usando el filtrado de direcciones MAC como medida de seguridad

Se ha convertido en práctica común usar la dirección MAC de la interfaz inalámbrica como mecanismo para limitar el acceso a una red inalámbrica. La hipótesis detrás de esto es que las direcciones MAC están “alambradas” y no pueden ser modificadas por usuarios corrientes. La realidad es muy diferente y las direcciones MAC, en el común de las redes inalámbricas pueden ser fácilmente modificadas.



Usando direcciones MAC para Autenticación

Un mecanismo de Autenticación basado SOLO en direcciones MAC es inseguro.

8.3 Portales cautivos para redes inalámbricas

La discusión acerca de los “portales cautivos o captivos inalámbricos” merece una unidad completa, pero al menos haremos una pequeña introducción en esta unidad, dada su relevancia en seguridad inalámbrica.

Si bien hay varias implementaciones de portales cautivos, la mayoría de estos están basados en el mismo tipo de concepto. En una red donde la Autenticación se hace mediante portales cautivos, a los clientes se les permite asociar con un punto de acceso (sin Autenticación inalámbrica) y obtener una dirección IP con el protocolo DHCP (no se requiere Autenticación para obtener la dirección IP). Una vez que el cliente obtiene la dirección IP, todas las solicitudes HTTP se capturan y son enviadas al portal cautivo, y el cliente es forzado a identificarse en una página web.

Los portales captivos son responsables de verificar la validez de la contraseña y luego modificar el estatus del cortafuego. Las reglas del cortafuego esta comúnmente basadas en la dirección MAC del cliente y las direcciones IP.

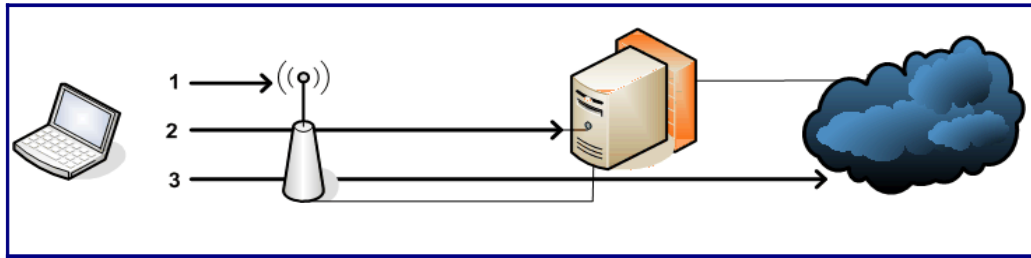


Figura 1: Un portal cautivo con Autenticación en tres pasos

En la figura, podemos ver la Autenticación del portal cautivo en tres pasos. El primer paso (1) requiere una asociación del cliente a la red inalámbrica. No se espera una Autenticación en términos de WEP-WPA, y normalmente se anuncia la SSID. En el segundo paso (2) el cliente obtiene una dirección IP mediante DHCP. El tráfico se enlaza a través del punto de acceso sin Autenticación alguna. En el último paso (3), el tráfico HTTP del cliente se redirecciona al servidor del portal cautivo. El cliente se identifica (usando, normalmente, HTTPS + nombre + contraseña). Finalmente el servidor del portal cautivo modifica o crea una regla en el cortafuego para permitir el tráfico hacia la internet.

Existen varios problemas de seguridad asociados con este tipo de implementación. Para más información vea los ejercicios propuestos.

9. Integridad de datos en redes inalámbricas



Definimos integridad de datos como la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas.

En 1999, el protocolo WEP también buscó proveer integridad de tráfico de datos, pero desafortunadamente el mecanismo de integridad, o CRC (código de redundancia cíclica), resultó inseguro. El diseño fallido de WEP permite la alteración del código CRC del tráfico, sin la necesidad de saber la llave WEP, es decir que el tráfico puede ser alterado sin que se note.

Los protocolos WPA y WPA2 resolvieron el problema de la integridad de datos en WEP mediante la inclusión de un mensaje de código de autenticación más seguro y la inclusión de un contador de segmentos (frames), que previene los “ataques por repetición” (replay attack). En un ataque de repetición el atacante registra la conversación entre un cliente y un punto de acceso, para obtener un acceso no autorizado. Al responder una conversación “antigua” el atacante no necesita saber la llave secreta WEP.



Integridad de datos: WEP vs WPA2

La integridad de datos mediante WEP es obsoleta.



Recomendaciones sobre integridad de datos:

Se debe implementar WPA o WPA2 para lograr integridad de datos inalámbrica mediante el cifrado en la capa de enlace.

9.1 Nota sobre seguridad acerca de WPA



WPA fue diseñado como un paso intermedio hacia WPA2 (estándar IEEE 802.11i). WPA sólo incluye un subconjunto de las características del estándar IEEE 802.11i y se enfoca en preservar la compatibilidad con adaptadores que funcionan con el estándar IEEE 802.11b.

WPA abordó las fallas encontradas en WEP. WPA incrementó la longitud de las llaves, el número de llaves en uso y agregó un nuevo mensaje de código de Autenticación. Se usó el algoritmo Michael debido a que es el más robusto y funciona con adaptadores de red antiguos. El algoritmo Michael es aun candidato a ser atacado y debido a ello las redes basadas en WPA implementan un mecanismo de suspensión de 30 segundos en caso de detección de ataque.

		WPA	WPA2
Modo corporativo	Autenticación	IEEE 802.1X / EAP ²	IEEE 802.1X / EAP
	Cifrado	TKIP ³ /MIC	AES-CCMP
Modo personal	Autenticación	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

Tabla 1: Autenticación y Cifrado en WPA y WPA2 (Modo corporativo y personal)

2. EAP stands for Extensible Authentication Protocol, it is a security protocol invoked by an IEEE 802.1X enabled Network Access Server (NAS) device such as an IEEE 802.11 a/b/g Wireless Access Point.
3. TKIP stand for the Temporal Key Integrity Protocol.

10. Disponibilidad en redes inalámbricas



Definimos disponibilidad de la red inalámbrica como la capacidad de la tecnología que asegura un acceso confiable a servicios de datos e información para usuarios autorizados.

Lo primero a considerar es que no es simple detener a alguien que busca interferir con su señal de radio. Las redes inalámbricas operan en canales predefinidos que cualquiera puede usar para enviar señales de radio. La prevención de la interferencia por parte de usuarios no autorizados es prácticamente imposible. Lo único que puede hacer es monitorear cuidadosamente su enlaces para identificar fuentes potenciales de interferencia (ver la unidad de monitoreo y administración).

Negación de servicio



Las redes inalámbricas son vulnerables a los ataques de Negación de Servicio mediante interferencia de radio. Considere un escenario donde otro operador de red decide configurar sus dispositivos de radio en el mismo canal en el que opera su red. Puede imaginar además qué sucede si se publica un SSID idéntico.

Para evitar esta clase de ataques, intencionales o no, debe considerar el rastreo periódico de frecuencias de radio.

Para evitar la interferencia con otras redes, no sobrecargue la potencia de sus enlaces

Existen varias razones para que un enlace de desempeño de manera deficiente o no esté disponible. La presencia de nodos escondidos puede afectar el desempeño de la familia de protocolos IEEE 802.11. Virus, software de intercambio de archivos, “spam”, etc., pueden inundar su red con tráfico y limitar el ancho de banda disponible para las conexiones autorizadas a servicios legítimos

Como se discutió en la sección de Autenticación de esta unidad, es difícil prevenir que usuarios ilegítimos se comuniquen con su punto de acceso o portal cautivo. La disponibilidad en redes inalámbricas requiere de buenas prácticas de monitoreo.

11. No repudiación en redes inalámbricas (rendición de cuentas)

La familia de estándares IEEE 802.11 no se hace cargo de la “rendición de cuentas” en el tráfico de datos. Los protocolos inalámbricos no tienen un mecanismo para asegurar que el emisor de datos tenga una prueba de envío de la información y que el receptor obtenga una prueba de la identidad del emisor. La rendición de cuentas debe ser implementada en protocolos de capas superiores.

12. Amenazas de seguridad en redes inalámbricas

La tabla siguiente presenta la diez amenazas de seguridad más relevantes en redes inalámbricas y provee un conjunto de recomendaciones para cada una de éstas.

1	Confidencialidad	Riesgo de interferencia, usuarios no autorizados pueden obtener acceso al tráfico de datos en su red.	Usar cifrado en la capa de enlace en sus enlaces inalámbricos (WPA2). Recomendar a sus usuarios el uso de “cifrado” en protocolos de alto nivel (SMTP seguro, HTTPS)
2	Confidencialidad	Riesgo de arrebato de tráfico y riesgo de un ataque tipo de intermediario	Recomendación 1 + Monitorear la SNR, la SSID y la dirección MAC de su conexión
3	Autenticación	Riesgo de acceso no autorizado a su red inalámbrica	Implemente IEEE 802.1X (WPA2) No dependa solo de un esquema de autenticación basado en direcciones MAC. No publique su SSID
4	Autenticación	Riesgo de acceso no autorizado a su red inalámbrica y al Internet	Implemente IEEE 802.1X Implemente un portal cautivo
5	Integridad	Riesgo de alteración de tráfico en la red inalámbrica	Recomiende a sus usuarios el uso de cifrado en capas superiores (HTTPS, SMTP seguro) Use cifrado en su enlace inalámbrico (WPA2)
6	Disponibilidad	Riesgo de interferencia Negación de servicio (Congestionamiento)	Monitoree periódicamente el espectro de radio No sobrecargue la potencia de sus enlaces
7	Disponibilidad	Riesgo de no disponibilidad de ancho de banda debido a retransmisiones de radio	Busque nodos ocultos y fuentes de interferencia Monitoree retransmisiones de capa de

			enlace en Puntos de Acceso
8	Disponibilidad	Riesgo de no disponibilidad de ancho de banda debido a software malicioso	Monitorear tráfico IP, especialmente de tipo ICMP y UDP Incluya detectores de intrusión
9	Autenticación Rendición de cuentas	Riesgo de acceso no autorizado a su Intranet	Implemente la red inalámbrica fuera de su cortafuegos Implemente una Red Privada Virtual y permita conexiones solo vía el concentrador VPN
10	(Acceso a la red) Rendición de cuentas	Riesgo de uso no autorizado de recursos de la red.	Implementado en IEEE 802.1X Implemente un portal cautivo basado en firmas digitales

Tabla 2: Las diez amenazas de seguridad más relevantes a redes inalámbricas, con las medidas preventivas recomendadas.

13. Conclusiones

Esta unidad presenta la seguridad inalámbrica desde el punto de vista de la “seguridad de los sistemas de información” o INFOSEC.

Existen 5 atributos de seguridad: Confidencialidad, Autenticación, Integridad, No-Repudiación y Disponibilidad, presentados en el contexto de las redes inalámbricas.

Dado que la formulación de los estándares de enlaces inalámbricos como el IEEE 802.11 solo hacen referencia a las capas 1 y 2 del modelo OSI, algunos atributos de seguridad pueden ser implementados por protocolos que corresponden a capas superiores.

Un buen diseño de red inalámbrica debe incluir el lugar para implementar cada atributo de seguridad. Por ejemplo, el cifrado para efectos de confidencialidad puede ser implementado en la capa de enlace, en la capa IP o en la de aplicación; la SSID puede ser difundida o no, la autenticación puede ser implementada usando IEEE 802.1X, un portal cautivo o filtrado a nivel de direcciones MAC.

Cualquier implementación va a depender siempre de escenarios y aplicaciones específicas.

Los 5 temas principales de esta unidad que deben ser recordados pueden resumirse como:

1. La seguridad meramente inalámbrica solo incluye mecanismos de seguridad presentes en las capas 1 y 2.
2. La encriptación a nivel de la capa de enlace (WEP, WPA, WPA2) es una medida de seguridad comúnmente utilizada pero no garantiza confidencialidad punto-a-punto. Si se necesita seguridad a nivel de capa de enlace evite el uso de WEP, y use IEEE 802.11i (WPA2).

La supresión del anuncio de la SSID y el filtrado mediante direcciones MAC no son métodos de autenticación seguros. Es necesario un método de autenticación de más alto nivel, como por ejemplo un portal cautivo.

3. Una red puede tornarse inoperativa como resultado de ataques de Negación de servicio o software malicioso, pero también debido a nodos ocultos de los que no tenemos idea de su existencia, y problemas de interferencia. Solo mediante el monitoreo de tráfico en la red, se pueden encontrar las causas reales de un problema.
4. No hay una solución estandar de seguridad para todas las redes inalámbricas. Es necesario tener una idea clara de los requisitos de seguridad, y la solución depende de cada escenario.

14. Declaración de Derechos de Propiedad Intelectual

Los materiales desarrollados en el marco del proyecto TRICALCAR utilizan una versión resumida del formato MMTK – Multimedia Training Kit. Han sido desarrollados para ser utilizados y compartidos libremente por instructores/as vinculados a proyectos de nuevas tecnologías para el desarrollo.

Todos los materiales están disponibles bajo una de las licencias Creative Commons <<http://creativecommons.org/>>. Estas licencias han sido desarrolladas con el propósito de promover y facilitar que se compartan materiales, pero reteniendo algunos de los derechos del autor sobre la propiedad intelectual.

Debido a que las organizaciones del Proyecto TRICALCAR que usan el formato MMTK para el desarrollo de sus materiales tienen diversas necesidades y trabajan en contextos diferentes, no se ha desarrollado una licencia única que cubra a todos los materiales. Para mayor claridad sobre los términos y condiciones en las que usted puede utilizar y redistribuir cada unidad temática, por favor verifique la declaración de derechos de propiedad intelectual incluida en cada una de ellas.

Provisiones de derechos de propiedad intelectual para esta unidad: Esta unidad temática se ha hecho disponible bajo los términos de la licencia **Atribución-No Comercial-Licenciamiento Recíproco**, bajo los siguientes términos:

- **Atribución.** Reconocer la autoría del material en los términos especificados por el propio autor o licenciante.
- **No comercial.** No puede utilizarse este material para fines comerciales.
- **Licenciamiento Recíproco.** Si altera, transforma o crea un material a partir de este, solo podrá distribuir el material resultante bajo una licencia igual a ésta.

Documento preparado para el taller de comunicaciones inalámbricas de Tshwane en Sudáfrica (c) 7th September 2005, Creative Commons Deed. Attribution-NonCommercial-ShareAlike 2.0 (c) 21 Abril 2007. Traducción de LaNeta.