Unidad 12

Seguridad en redes inalámbricas

Desarrollado por: Alberto Escudero Pascual, IT +46

Traducido por Laneta

Objetivos

- Ubicar, la seguridad en redes inalámbricas, en el contexto de la seguridad de información
- Entender la manera en que la seguridad se manifesta en las diferentes capas de protocolos OSI/Internet
- Identificar los elementos claves de seguridad que deben ser considerados al planear un diseño

Tabla de contenidos

Definiendo seguridad inalámbrica

- Seguridad es un concepto amplio
- ¿De qué ”seguridad” hablamos?
- Debemos comenzar por definir un contexto
- Presentaremos ”seguridad inalámbrica” en el contexto de la Seguridad de Información

Modelo de análisis/Metodología

- Para poder hablar de seguridad en redes inalámbricas vamos a usar un “marco de referencia”
- Un marco de referencia que distingue distintos atributos genéricos
- Aplicaremos este marco de referencia al caso concreto de las redes inalámbricas

¿Qué es seguridad de información? (COMSEC)

- Al final de los 70's, referida como ”Seguridad de Comunicación”
- COMSEC fue definido por la “U.S. National Security Telecommunications and Information Systems Security Instruction” (NSTISSI) como:

“medidas y controles usados para negar a personas no autorizadas, acceso a la informacion derivada de las telecomunicaciones y asegurar la autenticidad de esas comunicaciones.”

¿Qué es seguridad informática? (según COMSEC)

- Según COMSEC, la seguridad incluyó dos atributos de seguridad:
  - **Confidencialidad**
  - **Autenticación**

Confidencialidad

"Asegurar que la información no sea revelada a personas, procesos o dispositivos no autorizados."

Protección contra la divulgación no autorizada

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 información de una categoría específica"

Verificación de emisor

¿Qué es seguridad informática? (COMPUSEC)

- En los 80's, con el crecimiento de las computadoras personales se inició una nueva era
- 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"

¿Qué es seguridad informática? (COMPUSEC)

- COMPUSEC introdujo otros dos atributos relacionados con esta unidad:
  - **Integridad**
  - **Disponibilidad**

Integridad

”La calidad de un sistema de información refleja el correcto funcionamiento y confiabilidad del 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”

Los datos no pueden ser modificados de manera inadvertida

Disponibilidad

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

El acceso es "confiable"

¿Qué es seguridad informática? (INFOSEC)

- En los 90's COMSEC y COMPUSEC se fusionaron para constituir Seguridad de Sistemas de información (INFOSEC)

- INFOSEC incluyó los cuatro atributos: *Confidencialidad, Autenticación, Integridad y Disponibilidad* de COMSEC y COMPUSEC

¿Qué es seguridad informática? (INFOSEC)

- INFOSEC incluyó tambien un nuevo atributo:
  - **No-Repudiación**

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"

INFOSEC en 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 Metodología

Qué: La seguridad inalámbrica será presentada desde el punto de vista de INFOSEC

La Metodología

Por qué: Para dar un enfoque metodológico para diseñar la seguridad de una red inalámbrica

La Metodología

Cómo: Se presentan los cinco atributos de seguridad de INFOSEC y vemos de que manera se implementan

Dos detalles

- Antes de irnos a los cinco atributos de seguridad, dos recordatorios desde la unidad de la unidad de Redes Avanzadas (material en inglés en http://www.it46.se/courses)
  - Modelo OSI y normas inalámbricas
  - Cifrado a nivel de enlace

El modelo OSI y seguridad inalámbrica(Recordatorio)

- Las normas inalámbricas hacen referencia a las capas 1 y 2 del modelo OSI

- La seguridad inalámbrica tiende a ser identificada como una buena configuración de “cifrado en la capa de enlace”

El modelo OSI y seguridad inalámbrica(Recordatorio)

- Los mecanismos de seguridad en la capa 3 (red) no corresponden a “seguridad inalámbrica” y deben ser consideradas parte de una ”Unidad de seguridad a nivel de red o aplicación”

Cifrado en el nivel de enlace

Definición: es el proceso de asegurar los datos en el nivel de enlace, cuando los datos son transmitidos entre dos nodos instalados sobre el mismo enlace físico

Requerimientos: una clave secreta compartida entre las partes en contacto, y un algoritmo de cifrado previamente acordado

Cifrado en el nivel de enlace

- Cuando el transmisor y receptor no comparten un medio de transporte de datos en común, los datos deben ser descifrados y recifrados 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 cifrado de mayor nivel

Cifrado a nivel de enlace en la norma IEEE 802.11

- El algoritmo de cifrado mejor conocido para la norma IEEE 802.11 es el llamado en ingles Wired Equivalent Privacy (WEP)

- Está probado que WEP es inseguro

Cifrado a nivel de enlace en la norma IEEE 802.11

- Otras alternativas, como el protocolo Wi-Fi Protected Access (WPA), es considerado como standard (WPA2)

- La nueva norma IEEE 802.11i va a incluir una extensión de WPA, llamada WPA2

Cifrado a nivel de enlace en la norma IEEE 802.11

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

Cifrado a nivel de enlace en la norma IEEE 802.11

- Problemas del cifrado a nivel de enlace:
  - El cifrado a nivel de enlace requiere más recursos de hardware en los puntos de acceso
  - Administración y distribución de llaves

Cinco atributos de seguridad en WLAN

- Confidencialidad
- Autenticación
- Integridad
- Disponibilidad
- Non-repudio (Rendición de cuentas)

1

Confidencialidad inalámbrica

- 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

Confidencialidad inalámbrica

Debe asegurar que:

- la comunicación entre un grupo de puntos de acceso en un WDS esté protegida
- entre un punto de acceso (AP) y una estación o cliente, se conserve protegida contra intercepciones

WEP

- Fue parte de la norma IEEE 802.11 original, de 1999
- Brindaba, a las redes inalámbricas, un nivel de seguridad comparable al de las redes alambradas tradicionales
- Fue quebrado poco tiempo después de su aparición

WEP

- Fue demostrada su debilidad independientemente de la longitud de la llave
- WEP carece de un sistema de manejo de llaves como parte del protocolo

Primeras mejoras a WEP

- Nuevas alternativas, como WEP+ de Lucent, y WEP2 de Cisco
- Sus mejoras (WEP+, WEP2) ya son obsoletas
- Basado en el cifrado tipo RC4

WEP

- Existen varios programas que lo quiebran (Airsnort, wepcrack, kismac, aircrack etc).
- ¿Interesados en la historia de la seguridad de WEP?
- Ver ”recursos adicionales”

Nacen WPA y WPA2

WPA

- Fue propuesto en el 2003 mientras se debatió la norma IEEE 802.11i
- Fue dirigido a facilitar la actualización de los equipos antiguos. En 2004, se mejora para incluir AES y quedar certificado como parte de la norma IEEE 802.11i bajo el nombre de WPA2 (2004)

Nacen WPA y WPA2

WPA2

- Está diseñado para trabajar con o sin un servidor de manejo de llaves
- Si no se usa un servidor de llaves, todas las estaciones de la red comparten una “llave previamente compartida” (PSK)
- El modo PSK se conoce como WPA o WPA2-Personal

Nacen WPA y WPA2

WPA2

- Cuando se emplea un servidor de llaves, se le conoce como WPA2-Corporativo
- Una mejora notable en el WPA: la posibilidad de intercambiar llaves de manera dinámica

2

Autenticación en Redes inalámbricas

- Es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas

El derecho a enviar, al y mediante el punto de acceso

Mecanismos de asociación

- Autenticación abierta
  - NO hay seguridad y cualquiera puede hablarle al punto de acceso

Mecanismos de asociación

- Autenticación con llave compartida:
  - Se comparte una llave entre el cliente y el punto de acceso
  - Un mecanismo de reto/respuesta le permite al punto de acceso verificar que el cliente conoce la llave compartida, y entonces le permite el acceso

WEP
y la Autenticación en la capa 2

- La Autenticación con llave compartida de WEP es obsoleta

- Ataques tipo texto plano versus texto cifrado pueden ser logrados fácilmente

WEP
y la Autenticación en la capa 2

- Las llaves de Cifrado y Autenticación son el mismo secreto compartido

- Una vez que una resulta comprometida, la otra también

WEP
y la Autenticación en la capa 2

Recomendaciones:

- El uso del modo WPA2-corporativo
- La Autenticación en las redes inalámbricas, como las de los proveedores de servicios de internet inalámbricos, normalmente se implementa en capas de red mas altas (capa IP) mediante portales cautivos

WEP
y la Autenticación en la capa 2

Recomendaciones:

- Al transferir la Autenticación a un “portal cautivo” no tenemos un recurso para detener el flujo de tráfico que cruza nuestros puntos de acceso

Detener la difusión de la SSID

- Una variación de la ”Autenticaron abierta” es llamada ”Red cerrada”
- Las ”redes cerradas” no difunden el SSID mediante las ”tramas baliza” o ”beacon frames” (IEEE 802.11, capa de enlace)

Detener la difusión de la SSID

- Interrumpiendo la publicación de la SSID implica que los clientes de la red inalámbrica necesitan saber de manera previa el SSID de un punto de acceso
- ¿Es una media de seguridad?
- No impide que otro software de intercepción detecte la asociación que provenga de otro punto de la red

Detener la difusión de la SSID

- Encontrar la SSID de una red es tan sencillo como esperar que alguien se asocie a la red y entonces extraer la SSID de una trama de asociación
- Debe considerarse como una “precaución adicional”, más no una medida de seguridad efectiva

Filtrado de direcciones MAC como medida de seguridad

Muchos proveedores usan el filtrado de direcciones MAC :

- En el común de las redes inalámbricas pueden ser fácilmente modificadas
- Un esquema de autenticación basado SOLO en direcciones MAC es inseguro

Portales cautivos

- Llevando la autenticación fuera de la red inalámbrica: Portal Cautivo
- Existen varias implementaciones de Portales Cautivos
- La mayoría están basados en el mismo concepto: redirección HTTP y cortafuegos dinámicos

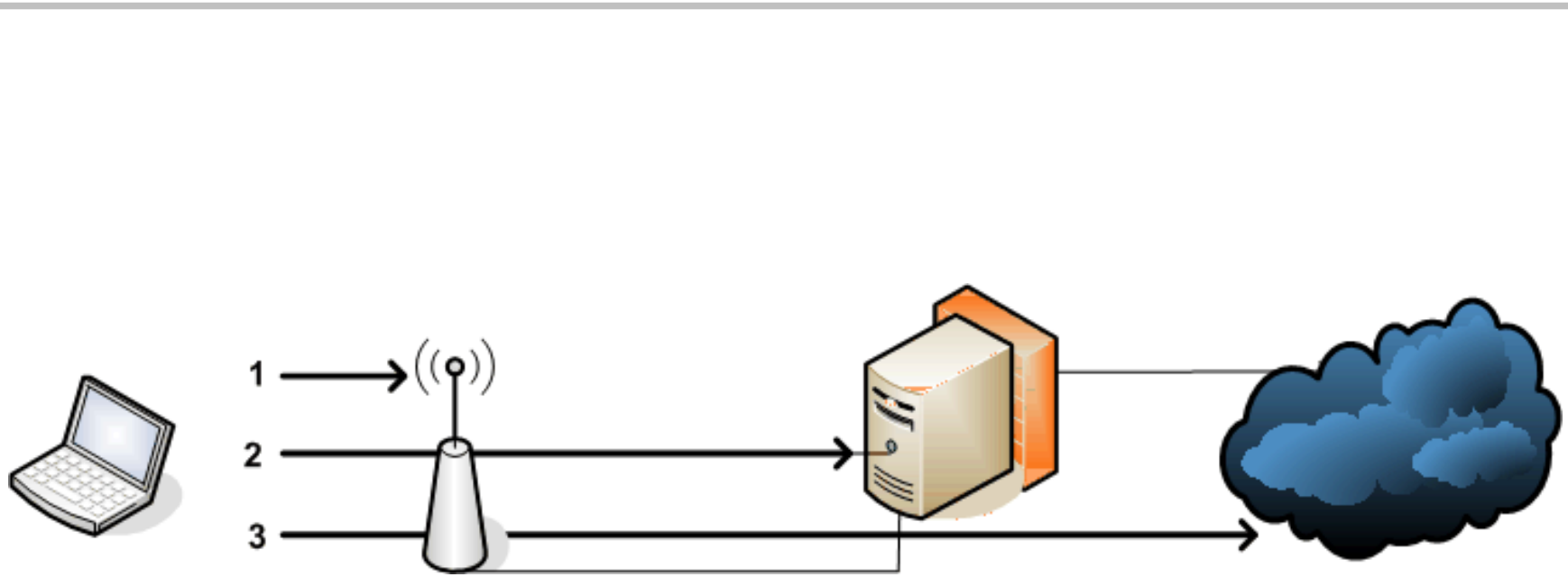
Portales cautivos

- Al cliente se le permite asociarse con un punto de acceso, y obtener una dirección IP por DHCP
- Una vez que obtiene la IP, todas las solicitudes HTTP son capturadas y el cliente debe autenticarse vía una página web

Portales cautivos

- El portal cautivo verifica la validez del nombre de usuario y contraseña, y entonces cambia el estado de un cortafuegos
- Las reglas del cortafuegos están basadas en los valores de la direcciones MAC e IP del cliente

Portal cautivo: autenticación en tres pasos



3

Integridad de datos en redes inalámbricas

- La capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas
- WEP buscó proveer integridad de tráfico de datos

Integridad de datos en redes inalámbricas

- El mecanismo de integridad, o CRC, es inseguro
- Permite la alteración del código CRC del tráfico, sin la necesidad de saber la llave WEP

Integridad de datos en redes inalámbricas

Resultado: El tráfico puede ser alterado sin que se note

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”

Integridad de datos en redes inalámbricas

WEP vs WPA2

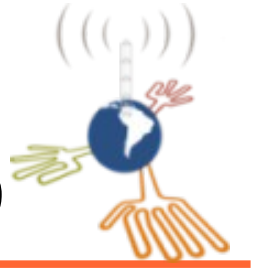
- La integridad de datos mediante WEP es obsoleta
- Se debe implementar WPA o WPA2 para lograr integridad de datos inalámbrica mediante cifrado en la capa de enlace

4

Disponibilidad en redes inalámbricas

"la capacidad de la tecnología que asegura un acceso confiable a servicios de datos e información para usuarios autorizados"

Interferencia en canales de radio



- Las redes inalámbricas operan en canales de radio predefinidos abiertos, sin restricciones de uso
- Prevenir la interferencia no autorizada es casi imposible
- Para evitar esta clase de ataques, intencionales o no, debe considerar el rastreo regular de frecuencias de radio

Negación de Servicio (DoS)

- Las redes inalámbricas son vulnerables a los ataques de Negación de Servicio mediante interferencia de radio, usando:
  - Un canal de radio idéntico o adyacente
  - Una SSID idéntica

Negación de Servicio (DoS)

- La DoS puede ser intencional o no
- Considerar el rastreo periódico de frecuencias de radio
- No sobrecargar la potencia de sus enlaces

Otras amenazas a la disponibilidad

- Presencia de nodos ocultos (exceso de retransmisiones)
- Virus (exceso de rastreo)
- Software para intercambio de archivos (exceso de tráfico)
- Spam (exceso de email)

5

Rendición de cuentas

- 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 superiores

10 amenazas de seguridad

1	Confidencialidad	Interferencia	- WPA2 - “cifrado” en protocolos superiores
2	Confidencialidad	Arrebato de tráfico, ataque de persona en el medio	- Usar (1) - Monitorear SNR, SSID y dirección MAC del punto de acceso
3	Autenticación	Acceso no autorizado a la red	- WPA2 - No basarse solo en filtrado por MAC - No difundir la SSID

10 amenazas de seguridad

4	Autenticación	Acceso no autorizado a la red y a Internet	- IEEE 802.1X - Portal captivo
5	Integridad	Modificación de tráfico	- “Cifrado” con protocolos superiores - WPA2
6	Disponibilidad	Interferencia inalámbrica, Negación de servicio inalámbrico	- Monitorear el espectro de radio - No sobrecargar la potencia de los enlaces
7	Disponibilidad	Ancho de banda no disponible por exceso de retransmisiones	- Buscar nodos ocultos y fuentes de interferencia - Verificar retransmisiones en el enlace

10 amenazas de seguridad

8	Disponibilidad	Ancho de banda no disponible debido a software maligno	- Monitorear trafico IP, (ICMP y UDP) - Implementar la detección de intrusos
9	Autenticación Rendición de cuentas	Acceso no autorizado a su intranet	- Red inalámbrica fuera del cortafuegos - Implementar VPN - Permitir conexiones solo vía la VPN
10	(Acceso a la red) Rendición de cuentas	Uso no autorizado de sus recursos de red	- IEEE 802.1X - Portal cautivo basado en firmas digitales

Conclusiones

1. Los atributos de seguridad, como son descritos en INFOSEC, pueden ser implementados en diferentes capas del modelo OSI

Conclusiones

2. Si se necesita seguridad a nivel de capa de enlace evite el uso de WEP, y use IEEE 802.11i (WPA2)

3. Tener una idea clara de los requisitos de seguridad, ya que la solución depende de cada escenario