



albentia
systems

SEGURIDAD EN REDES

derDOCSIS

La seguridad en redes de datos es un concepto que cobra cada día más importancia, en especial en redes inalámbricas. Este documento pretende describir los mecanismos que establece el estándar IEEE 802.16-2017 para garantizar completamente la seguridad en las comunicaciones, explicando conceptos como certificado X.509, firma digital o clave dinámica.

Asimismo, se realizará una comparativa con la forma de implementar la seguridad que establece el estándar Wi-Fi (802.11a/b/g/n/ac), ya que, a pesar de ser una tecnología muy distinta a 802.16-2017, es muy popular y ha generado una cierta desconfianza hacia la seguridad en redes inalámbricas. En este documento se describirán también los mecanismos de Seguridad que implementa Wi-Fi y por qué es una tecnología más vulnerable que 802.16-2017.

SEGURIDAD EN REDES

PRINCIPIOS BÁSICOS

Cuando se habla de seguridad de la información en cualquier tipo de red de datos, el objetivo es poder garantizar estos tres conceptos:

Confidencialidad

Es la garantía de que un mensaje no ha sido leído por nadie que no sea el receptor para el que estaba destinado. Por ejemplo, un número de tarjeta de crédito se debe mantener de manera confidencial al enviarse a través de Internet. Un ejemplo de mecanismo destinado a preservar la confidencialidad es el cifrado de datos, mediante el cual la información solo puede ser legible aplicándole una cierta clave que solo emisor y receptor conocen.

Autenticación

Es la comprobación de una identidad reivindicada. Por ejemplo, al utilizar una cuenta bancaria, es imperativo que solo el propietario real de la cuenta pueda hacer operaciones. Varios recursos pueden proporcionar la autenticación. Un ejemplo común de autenticación es un sistema simple de usuario y contraseña.

Integridad

La información debe mantenerse completa y libre de manipulaciones fortuitas o deliberadas. La integridad es la garantía de que los datos son completos y precisos, y que no se ven alterados en su recorrido de emisor a receptor. La integridad de los datos es la que se encarga, por ejemplo, de garantizar que una transferencia realizada mediante banca electrónica sea del importe deseado. Un ejemplo de mecanismo para garantizar la integridad de los datos es la firma digital en un correo electrónico, un método criptográfico que garantiza la autoría del mensaje y la no manipulación del contenido.

¿POR QUÉ ES TAN IMPORTANTE LA SEGURIDAD EN AERDOCSIS?

La seguridad es un concepto siempre importante en redes de datos, pero que cobra especial importancia en redes inalámbricas y concretamente en los escenarios hacia los que se orienta la tecnología aerDOCSIS, por diversos motivos:

En redes cableadas es complicado infiltrarse de forma ilegítima ya que es necesario conectarse físicamente mediante un cable. aerDOCSIS es una tecnología inalámbrica y por tanto los datos fluyen por el aire a través de ondas de radio.

aerDOCSIS es una tecnología diseñada para entornos exteriores con áreas de cobertura de varios km cuadrados, con lo que existe una zona relativamente grande que está potencialmente expuesta a un acceso no autorizado.

aerDOCSIS no se diseñó como tecnología de redes local (LAN) sino que se orientó más hacia las redes MAN/WAN. Es una tecnología de operador pensada en dar servicio a múltiples usuarios simultáneamente, y tiene por tanto que garantizar que unos usuarios no sean capaces de acceder a la información destinada a otros.

Al igual que en el resto de redes, si alguien consigue entrar a nuestra celda nos arriesgamos a que use la conexión a Internet, que acceda a los equipos y a sus ficheros, o que analice (mediante sniffers de tráfico) la información que circula por la red, entre la que pueden encontrarse correos electrónicos o contraseñas, por ejemplo. Resulta por tanto fundamental tener el control absoluto del acceso a la red.

Si la infiltración no autorizada en redes inalámbricas ya resulta grave en entornos domésticos, resulta más peligroso si cabe en un despliegue corporativo, gubernamental o incluso militar, escenarios habituales para la tecnología aerDOCSIS. Aplicaciones y entornos más críticos necesitan las máximas garantías de seguridad.

SEGURIDAD EN REDES WIMAX (IEEE 802.16-2017)

Conscientes de los retos y las necesidades de seguridad a las que se iban a tener que enfrentar, los autores del estándar IEEE 802.16-2017 hicieron grandes esfuerzos en conseguir una tecnología inalámbrica realmente segura. aerDOCSIS define en su pila de protocolos una subcapa de seguridad dedicada específicamente a proporcionar privacidad, confidencialidad y autenticación a los usuarios que quieran utilizar la red. aerDOCSIS basa su sistema de seguridad en los principios de Autenticación y Cifrado, los cuales hacen de ella una tecnología hoy en día prácticamente invulnerable.

Además, la propia tecnología posibilita que el Acceso al Medio sea más controlado y por lo tanto seguro. A continuación, se explican en detalle estas cuestiones.

AUTENTICACIÓN

OSA (Open System Authentication)

El cliente realiza una solicitud de autenticación asociada a su dirección MAC, a lo que sigue una respuesta de la Estación Base (en adelante, BS) con la aceptación o denegación. La BS realiza únicamente y de forma opcional un filtrado por dirección MAC.

SKA (Shared Key Authentication)

Se utilizan en el proceso claves compartidas que ambos extremos deberán conocer para garantizar una autenticación más segura. De aquí en adelante comentaremos estos mecanismos de autenticación.

Para la autenticación mediante claves compartidas, aerDOCSIS define el protocolo PKM (Privacy Key Management) para que una Estación de Usuario (en adelante, SS) pueda intercambiar claves y obtener autorización de la BS. PKM también se encarga de otras cuestiones relacionadas como el refresco de las claves, la re-autorización periódica, etc. El proceso de Autenticación entre BS y SS se puede describir de forma simple de la siguiente forma:

1. Una SS envía un mensaje PKM (Privacy Key Management) solicitando autenticación a la BS e incluyendo su certificado digital X.509. Este certificado es único por equipo e infalsificable, con lo que le define de forma unívoca y evita los ataques por suplantación de MAC.
2. La BS procede a autenticar y a verificar el certificado comprobando la firma digital del fabricante incluida en el certificado.
3. Si el certificado X.509 es aceptado, la BS genera la clave de autenticación (AK) y la cifra mediante la clave pública de 1024 bits contenida en el propio certificado X.509.

CIFRADO

Después de que la BS autorice a la SS, son necesarios también mecanismos de cifrado para velar por la confidencialidad y la integridad de los datos. Para ello, la SS envía a la BS una solicitud de claves de cifrado llamadas TEKs (Traffic Encryption Keys), que son enviadas por la BS en un mensaje de respuesta. Estos mensajes a su vez están cifrados con una clave conocida por ambas partes. El algoritmo empleado para el cifrado de las TEKs puede ser de tipo 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard), o RSA.

Una vez conocidas las TEKs, diversas técnicas pueden ser utilizadas para cifrar los datos: CBC(DES), CBC (AES), CTR(AES), CCM(AES).

Algunas de las ventajas de los mecanismos de cifrado que implementa aerDOCSIS respecto a los de otras tecnologías son:

- Los algoritmos empleados son muy robustos.
- Soportan generación de claves dinámicas con tiempos de vida variables.
- Permiten realizar un cifrado independiente para cada flujo de datos.

Todo esto se realiza con el objetivo de garantizar la confidencialidad en las redes WiMAX.

CERTIFICADO DIGITAL X.509

Un certificado digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Existen varios formatos para certificados digitales, pero uno de los estándares más populares es el UIT-T X.509 (usado también en el DNI electrónico, por ejemplo). El certificado contiene habitualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado, de forma que el receptor pueda verificar que ésta última ha establecido realmente la asociación.

Claves estáticas

No se actualizan, son muy vulnerables y fáciles de adivinar.

Claves dinámicas (aerDOCSIS)

Tienen un tiempo de vida limitado, cambian y se renuevan automáticamente. Máxima seguridad.

SEGURIDAD AÑADIDA APORTADA POR LA PROPIA ARQUITECTURA DE AERDOCSIS

Independientemente de los mecanismos de cifrado o autenticación, el propio diseño de la tecnología aerDOCSIS implica un valor añadido en cuestiones de seguridad:

Las redes locales LAN fueron diseñadas para interconectar equipos “amigos” en entornos reducidos, con lo que los mecanismos de seguridad que incorporan son menores (resulta más complicado pensar en que el enemigo va a estar “en casa”). aerDOCSIS en cambio no se diseñó como una red local de acceso al usuario final, sino más bien como una tecnología MAN/WAN de operador que tiene que poder interconectar muchos usuarios que necesariamente no tienen que ser “amigos”. Al ser una red a mayor escala, la propia tecnología se diseñó para poder velar por la seguridad con total garantía.

El Acceso al Medio no es aleatorio, sino completamente determinista, y regido por una BS que actúa en todo momento como árbitro controlando las transmisiones. Ningún terminal no autorizado puede transmitir datos indiscriminadamente hacia la BS o hacia otros SSs de una celda inundando el espectro radio, con lo que los ataques tipo DOS (Denial of Service) son más difíciles que en tecnologías de acceso aleatorio.



PREGUNTAS RESUELTAS SOBRE LA SEGURIDAD EN AERDOCSIS

¿Puede alguien ajeno a mi red leer la información que circula en una red aerDOCSIS?

No. Toda la información que circula por el aire va a ir cifrada por los más potentes mecanismos de cifrado (AES, 3DES...) basado en claves dinámicas. Esto garantiza la Confidencialidad de la información.

¿Puede alguien ajeno a la red acceder a ella?

No. La Autenticación se realiza mediante certificados digitales X.509 y su firma digital asociada que representan de forma unívoca e infalsificable a cada equipo de la red.

¿Puede alguien ajeno a la red realizar IP Flooding (inundar de forma masiva la red con datagramas IP)?

No. aerDOCSIS es una tecnología de operador con acceso determinista y en el que la BS controla todas las transmisiones, con lo que un equipo malicioso no puede enviar “tráfico basura” a ningún equipo de la red en ningún momento.

COMPARATIVA CON WIFI (IEEE 802.11 a/b/g/n/ac)

AUTENTICACIÓN Y CIFRADO

Cuando un equipo quiere acceder a una red Wi-Fi lo primero que necesita es asociarse a un AP (Access Point), con lo que es el AP el que se encarga de la Autenticación. El estándar IEEE 802.11 contempla las dos filosofías de autenticación, OSA y SKA. A los mecanismos de autenticación se añaden también mecanismos de cifrado para velar por la confidencialidad y la integridad de los datos. Los sistemas más populares de Autenticación y Cifrado que define la tecnología Wi-Fi son:

WEP (Wired Equivalent Privacy)

Es un sistema de autenticación y cifrado que codifica los datos antes de enviarlos al aire mediante una clave compartida estática (64, 128 o 256 bits) que es la misma para todas las estaciones inalámbricas y el AP. Esta técnica presenta muchas vulnerabilidades (clave estática, vector de inicialización que se repite y no se cifra, ...) que hacen que hoy en día una protección WEP pueda ser violada muy fácilmente.

WPA (WiFi Protected Access)

Presenta mejoras respecto a WEP como la generación dinámica de la clave de acceso. Las redes básicas suelen usar una versión más simple de WPA, llamada WPA-PSK (Pre-Shared Key), que implementa la misma clave compartida en todos los dispositivos. WPA emplea RC4 como algoritmo de Cifrado y TKIP (Temporary Key Integrity Protocol) como algoritmo de gestión de claves. Entre sus defectos, citaremos que TKIP presenta ciertas vulnerabilidades, ya que permite el acceso a algunos de los paquetes que van desde el AP hasta los terminales de red.

WPA2

Es una mejora relativa a WPA y es la versión certificada del estándar IEEE 802.11i. Utiliza como algoritmo de cifrado CCMP (AES) (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol + Advanced Encryption Standard). Hoy en día es el protocolo de seguridad más fiable para Wi-Fi y lo implementa gran parte del nuevo equipamiento. Tiene la “desventaja” de que puede no estar soportado por equipos más antiguos.

PROBLEMAS DERIVADOS DEL ACCESO AL MEDIO

El acceso al medio en IEEE 802.11 b/g/n/ac se basa en el protocolo en CSMA/CA (Carrier Sense, Multiple Access, Collision Avoidance), en el que cuando los terminales creen que el medio está libre transmiten libremente. Es por tanto, un acceso al medio aleatorio e incontrolado. Teniendo en cuenta que el espectro radioeléctrico es limitado, un usuario no autenticado podría inundar el aire con “tráfico basura”, un ataque típico de las redes Wi-Fi que puede tener distintas finalidades, como ataques DOS (Denial of Service) o la obtención de información de la red.

Este tipo de ataques no se pueden solucionar con mecanismos de cifrado más sofisticados, sino que son problemas inherentes a la propia tecnología de acceso al medio aleatorio, y por tanto no pueden ser evitados.

CONCLUSIONES

A continuación, se resumen los puntos más interesantes que se han desarrollado a lo largo del documento:

Autenticación

La autenticación en aerDOCSIS es muy confiable gracias a los certificados X.509 y sus firmas digitales, que definen unívocamente a cada equipo que solicita entrar en la celda, así como a las claves dinámicas que cambian periódicamente y a las solicitudes automáticas de re-autenticación que realiza la BS. Estos certificados no pueden ser falsificados e impiden que cualquier equipo no autorizado entre a la red.

La tecnología WEP de autenticación y cifrado mediante el uso de claves estáticas ha sido el gran fracaso de Wi-Fi a nivel de seguridad, ya que ha resultado ser increíblemente vulnerable. Cualquier red que utilice este sistema hoy en día está expuesta a todo. A pesar de que WPA y WPA2 han corregido gran parte de los inconvenientes de los mecanismos que implementaba WEP, es necesario que el equipamiento sea relativamente moderno, ya que equipos de red algo más antiguos puede que únicamente soporten WEP. Además, la realidad dice que por desconocimiento mucha gente sigue utilizando WEP sin saber los riesgos que entraña.

Cifrado

WiMAX utiliza los cifradores de bloque básicos AES y DES. La complejidad de los algoritmos está en cómo seleccionar, transponer e interrelacionar los bloques dentro de un mensaje. De hecho, y para ser estrictos, deberíamos hablar de que aerDOCSIS usa CBC(DES), CBC(AES), CTR(AES), CCM(AES). Estos no es que sean superiores tecnológicamente a otros (como los de Wi-Fi), sino que se usan correctamente, es decir, con claves dinámicas que expiran al cabo de un tiempo y se renuevan automáticamente, sin repetir vectores de inicialización, cifrando independientemente por flujo de datos de cada SS.

WEP y WPA en Wi-Fi han presentado vulnerabilidades graves en materia de cifrado, y sólo puede realizar un cifrado comparable a aerDOCSIS usando el sistema WPA2.

Acceso al Medio

La propia tecnología tiene gran impacto en la seguridad. aerDOCSIS define un Acceso al Medio plenamente determinista y controlado en todo momento por la BS. Ninguna estación puede transmitir un solo bit si no lo ha permitido la BS, con lo que automáticamente tenemos todo el control del espectro radioeléctrico y evitamos muchos tipos de ataques.

Otras tecnologías, como ocurre en Wi-Fi y su capa MAC basada en CSMA/CA, utilizan Acceso al Medio aleatorio y no controlado, haciendo que cualquier equipo pueda inundar de tráfico el aire, incluso sin necesidad de que se haya registrado en el AP correspondiente. Esto provoca que estas redes sean más vulnerables a muchos ataques de tipo DOS (Denial Of Service).

Tecnología de operador: MAN/WAN vs LAN

WiMAX no se pensó como una tecnología de red local LAN, sino más bien como tecnología de operador orientada a redes MAN o WAN (Metropolitan, Wide-Area). Esto implica funcionamiento en exteriores, áreas de cobertura extensas, servicio a múltiples usuarios independientes. Por tanto, se diseñó siendo conscientes de que la seguridad debía jugar un papel muy importante. aerDOCSIS se ha creado a conciencia para que no haya ningún tipo de vulnerabilidad y para que ofrezca Integridad, Confidencialidad y Autenticación por sí mismo. aerDOCSIS se usa actualmente en entornos militares en donde se precisan los máximos niveles de Seguridad.

Wi-Fi es una tecnología muy diferente y con otros fines: es una tecnología orientada directamente al gran público, pionera en redes inalámbricas y pensada fundamentalmente para redes locales pequeñas, con lo que nació con carencias en temas de seguridad. Además, su éxito ha hecho que existan millones de terminales Wi-Fi en el mundo y que sea una tecnología de bajo coste y accesible para todos. Esto tiene muchas ventajas, pero implica sus riesgos: a mayor número de terminales resulta evidente pensar que es más probable que existan potenciales atacantes. La comunidad de hackers especializados en violar redes Wi-Fi es bastante numerosa y existen multitud de aplicaciones específicas, mientras que el mundo aerDOCSIS, por el momento, no sufre estos problemas.

No necesidad de seguridad por otros medios

Las carencias en cuanto a seguridad de cualquier tecnología se pueden mitigar mediante el uso de protocolos de seguridad específicos de nivel superior o de servidores y equipamiento adicional: Radius, Kerberos, PAP(LDAP), EAP... Estas medidas “externas” proporcionan seguridad, pero implican equipamiento y costes adicionales. Si el propio estándar aporta los mecanismos de seguridad necesarios, como ocurre en el caso de aerDOCSIS, tendremos una red más sencilla y económica sin necesidad de incorporar otros medios.