Vulnerabilidades en el Protocolo IEEE 802.16 WiMAX

Grupo de Investigación en Redes y Sistemas Distribuidos

Universidad EAFIT

UNIVERSIDAD EAFIT 1960 Abierta al mundo

ACIS

- El protocolo IEEE 802.16 ,*WiMAX*, es un estándar para la transmisión de datos de forma inalámbrica en la última milla, utilizado para el despliegue de redes comerciales de área metropolitana.
- Permite llevar conectividad de bajo costo a zonas remotas de manera Nómada y Móvil.
- Flexible y Rápido de instalar en zonas de catástrofe o guerra.

- Ataques heredados de Wi-Fi.
  - Ataque de reenvío.
    - Alto nivel de dificultad.
    - *Timestamp, Nonces*.
    - RES-CMD y DREG-CMD son potencialmente peligrosos.
    - HMAC como protección adicional calculada a partir del CID
    - Debe procesarlos a pesar de ser inválidos, lo que afecta el rendimiento
    - Con TDD el ataque es más complejo que con FDD.
    - Como el protocolo no tiene herramientas para controlar paquetes repetidos, el atacante podría reenviar un paquete real de manera que la BS desconecte la SS por la continua llegada de paquetes malformados.

- Ataque de suplantación de estación Base.

  - Engañar a los clientes que se conecten a éste, haciéndoles creer que están conectados al punto de acceso legítimo
  - Es posible porque la SS no autentica a la BS
  - Escuchar y guardar los parámetros de conexión que ofrece la BS a las SS
  - Cambio de dirección MAC del atacante por la de la BS.
  - Envío de paquetes de *Downlink* y *Uplink* para ofrecer conectividad.
  - Permitirle al cliente autenticarse con la estación base falsa.

- **ATAQUES PROPIOS DEL PROTOCOLO 802.16**

  La inyección de paquetes en la red varía dependiendo del esquema de transmisión *TDD* o *FDD.*

- Ataque de RNG-RSP
  - Los mensajes de RNG-RSP viajan sin cifrar, autenticación, son *stateless*.
  - Ajustes de tiempo, de potencia, cambio de frecuencia de *downlink*, cambio de canal, entre otros

- Service level prediction
  - SLP = 0: No hay un posible servicio para este cliente.
  - SLP = 1: Existe algún servicio disponible para este cliente.
  - SLP = 2: Para cada flujo de servicio, puede ser establecida una conexión MAC con un QoS especificado por el *AuthorizationQosParamSet*
  - SLP = 3: No hay nivel de servicio disponible.
- Crear una serie de paquetes RNG-RSP falsos, modificando el campo SLP y dándole el valor 0 e inyectarlos durante el *ranging*.

- **ATAQUES RELACIONADOS CON EL PROTOCOLO PKM**

Ataques en PKM v.1

- Ataque de autorización inválida
  - Este ataque se presenta en la máquina de estados del proceso de autenticación del cliente con la estación, los mensajes intercambiados son:
    - » Authorization Reject
    - » Authorization Invalid
    - » Key Reject
    - » Key Invalid

- *Authorization Invalid* puede ser enviado por parte de una BS a una SS sin ser solicitado o como respuesta a una SS.
- Un atacante podría utilizar el *Authorization Invalid* para provocar una denegación de servicio
- Se pueden enviar paquetes de forma continua hasta alcanzar el objetivo
- *Authorization Invalid* provoca que la SS afectada cambie a un estado de espera de reautorización y se quedará en él hasta la llegada del paquete de respuesta.

- Ataque de reenvío
  - Uso indebido del paquete *Auth-Req*. Aprovechando la falta de información transitoria.
  - Reenvío de los paquetes con las siguientes consecuencias:
    - » Denegación de servicio a la SS víctima por parte de la BS.
    - » Si la BS no usa el *timeout* y acepta todos los Request, tendrá que generar AK's para todos los clientes que hayan hecho una solicitud, lo que genera caída del rendimiento por consumo de los recursos disponibles.

- Ataque de hombre en el medio
  - Falta de autenticación de la BS en la SS.
  - El *ataque de reenvío en PKM* puede ser utilizado para generar un ataque de hombre en la mitad.
  - BS falsa intercepta mensajes de respuesta al mensaje de Request de PKM y luego, los utiliza para obtener la AK.
  - Los envía a la SS a su nombre, ganando control sobre la comunicación con esta SS.

Ataques en PKM V.2

Esta versión de PKM hace autenticación de dos vías

- Ataque de reenvío
- Carencia de firma en los mensajes en los mensajes emitidos por el cliente.
- Nada cambió desde la primera versión del protocolo.
- Es importante que el protocolo incluya el envío de la firma por parte de la SS

- Ataque de Interleaving

  - La SS original envía el mensaje de Request a la BS
  - Es interceptado por la SS falsa (FSS)
  - Luego es reenviado hacia la BS.
  - La BS al recibir este mensaje envía el mensaje de respuesta a la FSS, la FSS no está en posibilidad de enviar el último mensaje de confirmación para establecer la comunicación, debido a que no es capaz de descifrarlo, ya que viene cifrado bajo la clave pública de la SS original, este mensaje contiene la AK con la cual se cifra el resto de los mensajes.

- Para poder enviar el último mensaje de confirmación necesario para establecer la comunicación, la FSS realiza un procedimiento el cual tiene como fin utilizar la SS original como oráculo, es decir, hacer que esta genere el mensaje necesario y se lo envíe a él para poderlo reenviar a la BS.

- Para obtener esto, la FSS hace que la SS original genere un nuevo intento de conexión con la BS y responde a su mensaje de *Request* con un mensaje falso de respuesta.

- Finalmente este paquete de confirmación es interceptado por la FSS y reenviado a la BS concluyendo así de una manera exitosa el ataque de *Interleaving*.

- **ATAQUES ENCONTRADOS EN EL PROCESO DE INVESTIGACIÓN DE VULNERABILIDADES EN EL PROTOCOLO**

  - *Ataques DoS con ARQ*
    - Este ataque consiste en falsificar los paquetes de ARQ (NACKs) que son enviados al emisor cuando el paquete enviado no llegó correctamente.
    - Reenviará el mensaje o los mensajes que no llegaron al destino, la idea de este ataque es saturar la red.

- Para llevarlo a cabo se deben seguir los siguientes pasos:
  - Monitoreo de los paquetes: El atacante debe observar los paquetes ARQ que el emisor está enviando al receptor
  - BSN: Número de secuencia de los bloques ARQ. Este campo es importante porque el atacante deberá predecir el número del siguiente bloque ARQ ACK
  - CID: Indica a al receptor por cual CID enviar los bloques ARQ feedback.

- Type of Acknowledges: Observar el tipo de manejo que el transmisor y el receptor van a hacer de las verificaciones, este campo puede tener los siguientes valores:

  - 0x0 (Selective ACK entry)
  - 0x1 (Cumulative ACK entry)
  - 0x2 (Cumulative with selective ACK entry)
  - 0x3 (Cumulative ACK with Block Sequence ACK entry)

- Generación e inyección de bloques ARQ falsos

- Ataque de SBC-RSP

  - Después del proceso de *ranging* el cliente, hace un intercambio de información con la BS para negociar sus capacidades básicas.
  - La información es enviada mediante un paquete de SBC-REQ que la estación base analiza y compara con las capacidades del cliente que tiene contratado el servicio.
  - Verifica si las capacidades que está solicitando mediante el SBC-REQ están autorizadas.
  - La BS envía un mensaje de SBC-RSP poniendo en ***on*** el campo de las capacidades solicitadas.

- Si las capacidades solicitadas autorizadas, la estación base envía un mensaje de SBC-RSP ajustando en ***off*** el campo de las capacidades solicitadas que reinicia la MAC del cliente.
- El atacante podría servirse de estos paquetes para dejar sin conexión a un cliente.

CONCLUSIONES

- Todos los paquetes que no cuenten con una firma HMAC, información transitoria o no dependan de una máquina de estados son potencialmente peligrosos, ya que permiten la manipulación de ciertos comportamientos dentro del protocolo. Para que un paquete pueda representar amenaza al protocolo es vital que sea enviado antes del intercambio de claves, después de esto es poco probable que sea exitoso.
- Los dispositivos desarrollados tanto bajo la versión 802.16-2004 como los desarrollados con la versión 802.16e-2005 son vulnerables algunos ataques.
- Vulnerabilidades aún en nivel teórico, se espera verificar a nivel práctico en una implementación real de *WiMAX.*

BIBLIOGRAFÍA

- IEEE 802.16 Working Group, IEEE Standard 802.16e. Amendment and Corrigendum to IEEE Standard 802.16-2004, USA: IEEE Computer Society, Febrero 2006.
- Eugene Crozier, Allan Klein. "Wimax nlos features", WiMAX Forum, [En linea], Disponible en: http://www.wimaxforum.org.
- Maxim, Merritt and David Pollino, "Wireless Security", RSA Press, McGraw-Hill/Osborne, Berkeley, CA. 2002, [En línea], Disponible en http://www.securitytechnet.com/resource/rsc-center/vendor-wp/RSA/wireless02.pdf

- Jyh-Cheng Chen, Ming-Chia Jiang, Yi-wen Liu, "Wireless LAN security and IEEE 802.11i," *Wireless Communications, IEEE* , vol.12, no.1, pp. 27-36, Feb. 2005, [En línea], Disponible en http://ieeexplore.ieee.org/iel5/7742/30466/01404570.pdf?isnumber=30466&prod=JNL&arnumber=1404570&arnumber=1404570&arSt=+27&ared=+36&arAuthor=Jyh-Cheng+Chen%3B+Ming-Chia+Jiang%3B+Yi-wen+Liu

- Arkoudi-Vafea Aikaterini. Security of IEEE 802.16, Master's thesis: Royal Institute of Technology, 2006.

- Sen Xu Chin-Tser Huang. Attacks on pkm protocols of ieee 802.16 and its later versions, Technical report: University of South Carolina.

UNIVERSIDAD EAFIT 1960 Abierta al mundo

ACIS