DESARROLLO DE UNA PLATAFORMA DE SIMULACIÓN DE REDES INALÁMBRICAS PARA EL ANÁLISIS Y EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD DEL ESTÁNDAR 802.11i

Josué Conrado Mena
e-mail: conricks2003@hotmail.com

Carlos Romero Gallardo
e-mail: cgromero@espe.edu.ec

Fabián Sáenz Enderica
e-mail: fgsaenz@espe.edu.ec

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA
ESCUELA POLITÉCNICA DEL EJÉRCITO
SANGOLQUI – ECUADOR

RESUMEN

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo los usuarios de un sistema identificados con nombre/contraseña o la posesión de un certificado digital.

802.11i limita mediante mecanismos de seguridad el acceso a la red para usuarios no autorizados, para ello emplea claves, encriptación, cifrado y servidores externos AAA que elevan la seguridad de las redes. Para el análisis redes inalámbricas se da como solución, la simulación para evaluar diferentes topologías.

Para realizar estudios específicos se emplean simuladores sobre los cuales se experimenta en base a topologías específicas, condiciones controladas para determinar la confiabilidad de los mecanismos de seguridad.

Con la elección del software Packet Tracer 5.3 se analizará la robustez o falencia de cada topología configurando WEP, WAP, WAP2.

INTRODUCCIÓN

El desarrollo de la plataforma de simulación está enfocado a analizar y evaluar el acceso no autorizado a redes inalámbricas sin seguridad, y con seguridad basadas en el estándar 802.11i.

Se justifica el desarrollo de la plataforma de simulación para redes inalámbricas para determinar y evaluar qué mecanismos de seguridad son óptimos frente a determinada topología y así evitar accesos no autorizados a la red, más aún si se trata de una red privada, donde toda la información debe ser

protegida de agentes externos, solo los usuarios validados bajo los mecanismos de protección que conlleva el estándar 802.11i tendrán acceso a la red.

Por medio del desarrollo de esta plataforma se podrán realizar investigaciones en el área de seguridad de la información, así también será un apoyo a procesos de docencia e investigación para la creación de nuevos proyectos que desarrollen aún más la plataforma propuesta en este proyecto.

Qué es 802.11i?

Debido a la complejidad que se introduce la seguridad en las WLAN con el estándar 802.11i, gran parte de usuarios posponen su adopción por cuestiones de coste, complejidad e interoperabilidad; en lo posterior todos los usuarios y de acuerdo a las políticas de las organizaciones implementarán este tipo de seguridad haciéndose obligatorio para el uso interno de los recursos de las instituciones.

Desde un tiempo atrás en el mercado los productos Wireless LAN (WLAN) que implementan el nuevo estándar de seguridad inalámbrica 802.11i resuelven sin duda algunos de los inconvenientes que las organizaciones presentan a la introducción de manera indiscriminada de redes inalámbricas en sus empresas.

Dicho estándar elimina muchas de las debilidades de seguridad de los estándares predecesores, tanto en lo que autenticación de usuarios como a robustez de los métodos de encriptación se refiere. Esto se logra gracias a la capacidad para trabajar en colaboración con 802.1X e incorporación de encriptación Advanced Encryption Standard (AES), también reduce considerablemente la complejidad y el tiempo de roaming de los usuarios entre varios puntos de acceso.

El estándar 802.11i es una mejora y una evolución de las tecnologías anteriores, WEP (Wired Equivalent Privacy) es el primer protocolo de seguridad inalámbrica que la IEEE reconoció. Este permite utilizar claves encriptadas de 40 bits según el algoritmo de encriptación RC4 asignando a cada usuario una clave por sesión. Pero desde que en el verano de 2001 fuera hackeado empezó a considerarse como el Talón de Aquiles de la cadena de seguridad inalámbrica. Se trató de reparar en algo lo ocurrido combinando WEP con el protocolo de autenticación 802.1X, ya que con esta implementación el usuario WEP está obligado a solicitar acceso a la red utilizando EAP (Extensible Authentication Protocol), esto es mencionado en 802.1X.

La mejora de seguridad propuesta no tuvo los resultados esperados, debido a que solamente cubría la deficiencia de WEP en el área de la autenticación, dejando sin procesar y aun lado la falencia sobre una parte de la ecuación, la encriptación. Debido a este proceso sin término se desarrolla WPA, que incrementa la potencia de la encriptación mediante la aplicación de la técnica TKIP (Temporal Key Integration Protocol). Mediante este protocolo, la clave utilizada por cada usuario cambia por varias ocasiones durante cada sesión. Aparte de TKIP, otro cambio fue dado en la sustitución de RC4 por el algoritmo

más robusto AES, desarrollado para el ejército estadounidense por el National Institute of Standards, aportaba una ventaja más a las prestaciones de seguridad ideadas para WPA.

A la final WPA no concluyó con AES debido a la impaciencia de los fabricantes ante la urgente demanda de productos WLAN con mayores niveles de seguridad que los proporcionados por WEP. Como tal, se empezó la comercialización de productos WPA sólo con TKIP.

La técnica de TKIP fue ideada como solución temporal para WEP, incluyendo en su solución gran parte de las características, como son el mecanismo de encriptación y el algoritmo RC4. La principal característica y ventaja es el carácter temporal en las claves utilizadas, pudiendo cambiar incluso para cada paquete dentro de una misma sesión. De la misma manera, las claves son de mayor longitud, siempre de 128 bits; por lo que resulta más difícil el acceso no autorizado o violación que las claves utilizadas en el modelo WEP con RC4. A pesar de que TKIP (con WPA) constituyó probablemente en su momento la mejor solución disponible, nunca se superó los problemas que acarreaba ya que el protocolo debía operar sobre el hardware existente y, por tanto, no puede introducir encriptación avanzada si antes dicho hardware no se actualiza con más potencia informática.

Otras tecnologías de seguridad que sugiere el organismo Wi-Fi son servidores RADIUS, para trabajar con claves de acceso en usuarios inalámbricos y remotos, VPN (Virtual Private Network), que supone un canal más seguro entre el usuario y la red, Firewalls, para controlar los datos salientes y entrantes de las máquinas de tal manera de impedir que usuarios sin autorización tengan acceso a la información, y Kerberos, servicio de autentificación desarrollado en el MIT (Massachussets Institute of Technology).

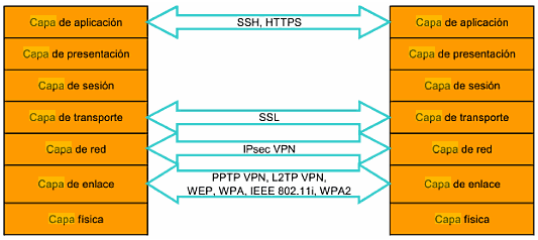

Figura. 1. Mecanismos de seguridad existentes en las distintas capas del modelo OSI

Servicio AAA

El estándar AAA bajo las notas del RFC 2903 establece la arquitectura para configurar un sistema de seguridad en la red, se indican tres funciones principales que son:

- Autenticación.
- Autorización.
- Auditoria.

El servicio AAA está en la capacidad de establecer políticas de autenticación para los solicitantes, responder de manera directa y sin errores a las peticiones de autorización de los usuarios, y por último recolectar datos que faciliten realizar una auditoría sobre los recursos a los que se ha tenido acceso en la infraestructura de red.

A continuación se definen los tres procesos del modelamiento AAA:

Autenticación

Proceso de identificar a los usuarios, con el nombre de usuario y contraseña, desafío y respuesta, soporte de mensajería, y, según el protocolo de seguridad que seleccione, puede ofrecer cifrado.

Es el método que permite identificar a un suplicante antes de conceder acceso a la red y los servicios que esta contiene. Configurar la autenticación AAA mediante la definición de una lista llamada métodos de autenticación, y luego aplicando esa lista a varias interfaces. En la lista de métodos se definen los tipos de autenticación a realizar y la secuencia en la que se llevará a cabo, esto debe ser aplicado a una interfaz específica antes de que cualquiera de los métodos de autenticación definidos se utilicen. La única excepción es la lista método por defecto (que se denomina "default").

La lista método por defecto se aplica automáticamente a todas las interfaces si ninguna lista de otro método está definida. Una lista de método definida reemplaza automáticamente la lista de método por defecto.

Todos los métodos de autenticación, excepto local, line de contraseña y habilitación de la autenticación, deben ser definidas a través de AAA.

La autenticación se puede realizar por diversos esquemas:

- **Secuencia de agente:** el servidor AAA permanece como delegado entre el equipamiento que presta el NAS y el usuario final. El usuario contacta inicialmente con el servidor AAA, quien autoriza su petición y notifica al equipamiento de su decisión para que se le preste el servicio al usuario. El equipamiento del servicio notifica al servidor AAA cuando ha cumplido su petición, y el mismo servidor AAA notifica en última instancia al usuario.

- **Secuencia de tiro o *pull*:** servicio dial tradicional de marcación telefónica. El usuario realiza la petición directamente al NAS y éste comprueba con el servidor AAA si debe proporcionar acceso.

- **Secuencia de empuje o *push*:** el usuario pide una certificación al servidor AAA, la cual deberá presentar más tarde al equipamiento que presta el servicio para garantizar su identidad y acceso al mismo.

Autorización

No es más que la asignación de recursos para tener un control de acceso definido a cada usuario después de la autenticación.

En esta fase del modelamiento, mediante un grupo de reglas se establece lo que el usuario está habilitado a usar o acceder en la red interna o externa. Estas reglas son comparadas con la información que contiene la base de datos que se encuentra en el servidor AAA para denegar o permitir la capacidad del

usuario. En algunos casos la base de datos se almacena en un servidor remoto de seguridad, RADIUS o TACACS+. Estos servidores o los responsables de autorizar a los usuarios los derechos específicos que cada uno posee con la asociación de las reglas antes definidas.

Todos los métodos de autorización deben ser definidos a través de AAA. Así como en la autenticación, configurar AAA Autorización es definida por una lista llamada métodos de autorización, y luego aplicando esa lista a varias interfaces.

Registro o Contabilización

Es la última fase del modelamiento AAA ya que recolecta y envía la información al servidor de seguridad, el cual valida:

- Nombres de usuarios.
- Tiempo de inicio y final.
- Comandos ejecutados (como PPP).
- Cantidad de paquetes enviados.
- Número de *bytes*.

Gracias a esta fase se realiza el seguimiento de todos quienes tengan acceso a los servicios, así como el consumo de recursos que cada usuario genera. Una vez se detecta actividad, el acceso a la red del servidor informa la actividad del usuario al servidor de seguridad en forma de los registros contables, estos se guardan en un servidor de control de acceso.

Estos métodos de registro son definidos a través de AAA, al igual que con la autenticación y autorización, se configura el registro mediante la definición de una lista llamada métodos de registro, y luego la aplicación de esa lista a varios interfaces.

AAA provee los siguientes beneficios:

- Incrementación de flexibilidad y control de configuración de acceso.
- Escalabilidad.
- Métodos de autorización estandarizados, como RADIUS, TACACS+ o Kerberos.
- Múltiples sistemas de *backup*.

AAA permite que el administrador de la red pueda configurar dinámicamente el tipo de autenticación y autorización, por usuario o por servicio base (IP, IPX, o VPDN).

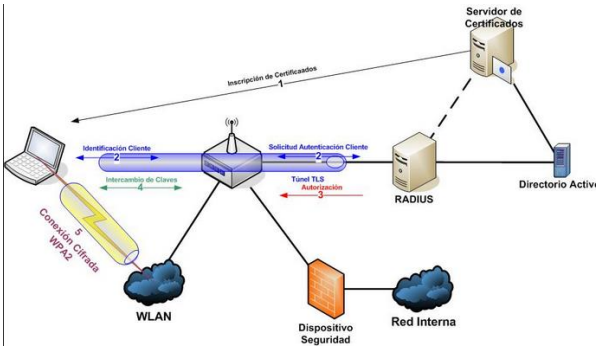

Figura. 2. Establecimiento de la conexión

Los protocolos AAA más utilizados para configurar el acceso son:

- Radius (Remote Authentication Dial-in User Service).
- TACACS+ (Terminal Access Controller Access Control System Plus).

RADIUS *Remote Authentication Dial-in User Service*

RADIUS es una implementación concreta del modelamiento AAA, se encuentra definido en los RFC 2865 para la autentificación y autorización, y RFC 2866 para el registro (*accounting*).

Los mensajes de intercambio de RADIUS se envían como mensajes de datagramas UDP. El puerto UDP 1812 se utiliza para los mensajes de autenticación y el 1813 para los mensajes de administración. La carga UDP de un paquete RADIUS sólo incluye un mensaje RADIUS.

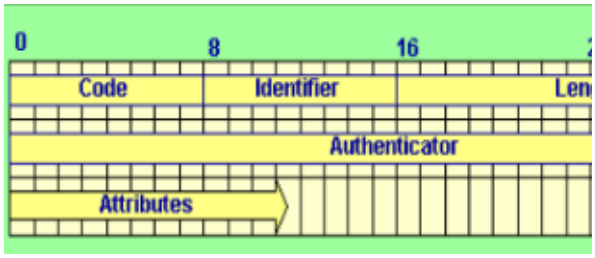

Figura. 3. Formato de mensaje RADIUS

Los campos en un paquete RADIUS son:

- *Code* (Código), octeto que contiene el tipo de paquete.
- *Identifier* (Identificador), octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada.
- Length, longitud del paquete de 2 octetos.
- *Authenticator* (Verificador), es un valor que sirve para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de contraseña.
- *Attributes* (Atributos), se almacenan atributos variables. Los únicos atributos obligatorios son el usuario y contraseña.

Provee varios servicios comunes personalizables que utilizan un esquema de autorización de secuencia *pull.*

Debilidades

- RAIUS utiliza MD5 como algoritmo de dispersión para almacenar contraseñas, lo cual no es seguro

- La escalabilidad presenta problemas.

- Al basarse en UDP y no estar orientado a la conexión, no tiene control sobre el uso de los servicios cuando ya ha sido autenticado.

- Es un protocolo salto a salto, las cadenas de autenticación son largas e implican diversos servidores de distintas agrupaciones. Por lo que el modelo salto a salto es inseguro.

Este protocolo utiliza identificadores llamados *realms* o dominios para realizar una discriminación

de cada usuario y saber en todo momento quién debe autenticarlos. Los dominios se presentan como sufijos o prefijos ubicándose junto al nombre de usuario, separados por caracteres como barras o arrobas. Por tal motivo un servidor RADIUS pronostica patrones en los nombres de los usuarios para autenticar a un usuario cuando lo amerite.

Integración y funcionabilidad de un servidor AAA

1. El suplicante inicia solicitando conexión de red. Se inicia el proceso de autenticación enviando un mensaje EAPoL de inicio hacia el equipo de acceso AP.
2. El autenticador envía un mensaje de solicitud de identidad al usuario.
3. El usuario envía un EAP de identidad al autenticador.
4. La trama *EAP response identity* se encapsula en un mensaje RADIUS y el autenticador envía un mensaje de petición de acceso al servidor RADIUS.
5. El servidor RADIUS inicia la negociación del método EAP que se utilizará para el establecimiento del canal seguro enviando una trama RADIUS *Access-challenge*.
6. El autenticador envía al usuario un EAP con petición de establecimiento de canal con EAP de tipo PEAP.
7. El usuario negocia el método de la conexión y envía al autenticador un EAP de respuesta con el saludo para establecimiento del canal TLS (*client hello*).
8. El autenticador encapsula el mensaje EAP-*Response* en un mensaje RADIUS-*Request* y lo envía al servidor.
9. El servidor verifica el mensaje enviado por el usuario y le responde con su certificado en un mensaje RADIUS-*Challenge*. El mensaje contiene un *server hello+ server certificate + server hello done*.

    a. *Server hello*.- Saludo del servidor en respuesta de un *client hello*.
    b. *Server Certificate*.- Certificado del servidor).
10. El autenticador recibe el mensaje RADIUS y envía el certificado del servidor al usuario en un EAP-*Request* TLS de credencial del usuario.
11. El usuario responde un mensaje EAP intercambiando la contraseña en el canal cifrado. El mensaje EAP-*Response* TLS contiene el *client key Exchange, change cipher spec* y *encrypted handshake message*.
12. La trama EAP-*Response* TLS se encapsula en un mensaje RADIUS-*Request* y se envía al servidor RADIUS, el mensaje llega encriptado con la contraseña del usuario y es verificada en la base de datos LDAP.
13. El servidor responde:

    a. Si la contraseña del usuario es correcta el servidor responde con un mensaje RADIUS-*Challange* para finalizar el

establecimiento del canal TLS.

b. Si las credenciales no son correctas rechaza la conexión (RADIUS-*Reject*) y el puerto del *switch* al que se conecta el usuario se pone en estado *down*.

14. El autenticador recibe un RADIUS-*Challenge* para finalizar de establecer el canal TLS y le envía al usuario un EAP-*Request* de canal cifrado completo.
15. El usuario envía un mensaje EAP-PEAP de respuesta y solicita acceso a la red.
16. La solicitud de acceso a la red es enviara al servidor mediante un mensaje RADIUS-*Request*.
17. El servidor responde con un mensaje de RADIUS-*ACCEPT* hacia el autenticador.
18. El autenticador envía un mensaje EAP-*Succsess* y el usuario ya se encuentra habilitado para usar los recursos de la red.

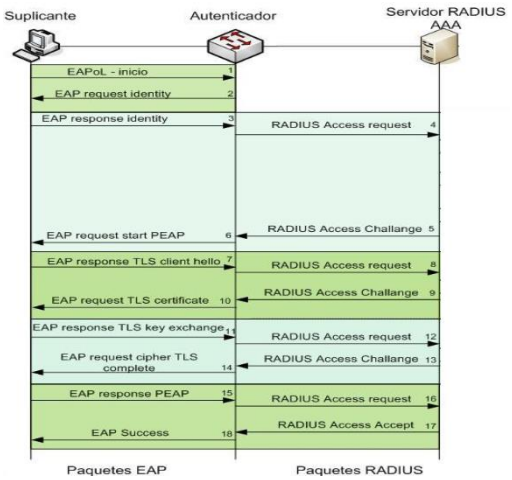

Figura. 4. Funcionamiento de Autenticador - AAA RADIUS

CONCLUSIONES

La vulnerabilidad de las redes inalámbricas con los mecanismos de seguridad desarrollados por la IEE 802.11i para redes en modo infraestructura son casi nulos ya que mediante su encriptación y cifrado apoyados en servidores AAA, solamente permiten el ingreso a una red privada a los usuarios sobre los cuales se tengan configurados sus credenciales con sus respectivos permisos.

Para las redes Ad-Hoc la seguridad tiene un gran vacío ya que no existe un dispositivo de control o autenticador que valide la conexión de usuarios seguros.

El análisis de los mecanismos de seguridad permite visualizar la complejidad de las tramas que se transmiten para su validación, es decir, las llaves que se generan en los diferentes protocolos WPA, WPA2; cada mecanismo cuenta con una configuración específica que permite que la generación de llaves sea dinámico, se lo administre desde un servidor de autenticación externo.

Existen muchas soluciones en software para el desarrollo de topologías y ambientes controlados que facilitan el análisis de seguridad que sucede en la red, al mismo tiempo no existen simuladores que reflejen características completas de análisis, es decir, solamente se ven limitados a la configuración y análisis de tramas básicas que no dejan obtener datos completos para observar el

intercambio de paquetes en una comunicación de seguridad.

A pesar de la configuración que permite el simulador Packet Tracer 5.3, no se obtuvieron resultados satisfactorios en cuanto a captura de tramas se refiere, el nivel de paquetes obtenidos es básico y no contiene toda la información de un análisis en ambiente real. Se analizaron diversas soluciones en software como la potente herramienta que es GNS3 pero no cada solución no contiene los elementos activos necesarios para desarrollar las topologías como en este caso no cuenta con herramientas inalámbricas de simulación.

No se tiene una conclusión determinante de la evaluación de los mecanismos de seguridad por la limitante en software, la cual no permitió un análisis completo de cada mecanismo de seguridad.

.

REFERENCIAS

[5] (s.f.). (Corelan Team) Recuperado el 11 de 2012, de http://www.corelan.be:8800/index.php/2009/02/24/cheatsheet-cracking-wpa2-psk-with-backtrack-4-aircrack-ng-and-john-the-ripper/

[6] Balao, M. (17 de 03 de 2012). Recuperado el 09 de 2012, de http://martin.com.uy/sec/autenticacion-de-mensajes-cbc-mac/

[7] Cabrera E., C. (01 de 2009). Recuperado el 08 de 2012, de http://cesarcabrera.info/blog/explorando-el-sdm-con-gns3/

BIOGRAFÍA

Josué Israel Conrado Mena

Nació en Quito, Ecuador el 05 de julio de 1986.

Sus estudios primarios los realizo en la “Unidad Educativa Abdón Calderón” y sus estudios secundarios en el Colegio “Dominicano San Fernando”, obteniendo el título de Bachiller Físico Matemático. Obtuvo su título en Ingeniería Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército. Entre sus áreas de interés se encuentran Networking, Desarrollo de Proyectos.

Fabián Gustavo Sáenz Enderica

Ingeniero en Electrónica, graduado en la Escuela Politécnica del Ejército, con Maestría en Ciencias en Ingeniería Electrónica y especialidades en Redes de telecomunicaciones, así como Administración y Economía de las Telecomunicaciones.

Ha trabajado en varias empresas de comunicaciones, así como es docente Universitario, de pregrado y postgrado en el Ecuador.

Ha sido representante de la CEPAL en el tema de TIC´s y discapacidades, así como coordinador del grupo de investigación

en ayudas tecnológicas para discapacitados en la ESPE.

Actualmente se encuentra realizando su tesis doctoral, relacionada a dar soluciones tecnológicas de soporte para personas con discapacidad auditiva.

Carlos Gabriel Romero Gallardo

Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército (2002) y Especialista en Proyectos de Investigación Científica y Tecnológica en la Universidad Complutense de Madrid (2006). Candidato a PhD Universidad Nacional de la Plata. Es profesor de la Escuela Politécnica del Ejército. Sus áreas de interés e investigación son Networking con TCP/IP e Implementación de servicios y aplicaciones con software libre.