Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Consideraciones para la implementacion de 802.1x en WLAN's

Hoy en dia, la implementacion de redes inalambricas es considerada como una solucion de movilidad, flexibilidad y productividad; por esto, el numero de implementaciones de este tipo de tecnologia aumenta y se confirma como una fuerte tendencia. Sin embargo, junto con su funcionalidad y demas atractivos, este tipo de implementaciones trae consigo importantes riesgos de seguridad que afrontar, muchos de ellos asociados a la inexistencia de perimetros fisicos claros, y otros mas importantes asociados a la carencia de meca...

Copyright SANS Institute

Author Retains Full Rights

AD

Consideraciones para la implementación de 802.1x en WLAN's

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Juan M. Chamorro
Location: SANS Local Mentor
Bogota – Colombia.

Abstract

Este documento presenta las principales consideraciones para implementar, de manera adecuada, un mecanismo para el control del acceso a la red y la protección de datos en una red inalámbrica, basado en el estándar 802.1x.

Febrero 24 de 2005

© SANS Institute 2000 - 2005 Author retains full rights.

Tabla de Contenido

1. Introducción 1
2. Conceptos 1
   2.1 Control de Acceso 1
   2.3 Encripción 3
   2.4 RADIUS (Remote Authentication Dial-In User Service) 4
   2.5 802.11 4
   2.6 802.1x 4
3 Por qué 802.1x 5
4 Análisis de Requerimientos 8
   4.1 Funcionalidad 8
   4.2 Seguridad requerida 9
   4.3 Requerimientos técnicos 9
5 Diseño 11
   5.1 Componentes del sistema de autenticación 11
   5.2 Selección mecanismo de autenticación 12
6 Implementación 13
   6.1 Cliente (Suplicante) 14
   6.2 Punto de Acceso (Autenticador) 14
   6.3 Servidor de Autenticación 14
   6.4 Otras consideraciones 14
7 Consideraciones finales 15
8 Conclusión 16
Referencias 17

© SANS Institute 2000 - 2005, Author retains full rights.

1. Introducción

Hoy en día, la implementación de redes inalámbricas es considerada como una solución de movilidad, flexibilidad y productividad; por esto, el número de implementaciones de este tipo de tecnología aumenta y se confirma como una fuerte tendencia.

Sin embargo, junto con su funcionalidad y demás atractivos, este tipo de implementaciones trae consigo importantes riesgos de seguridad que afrontar, muchos de ellos asociados a la inexistencia de perímetros físicos claros, y otros más importantes asociados a la carencia de mecanismos de seguridad suficientemente fuertes que protejan el acceso a los recursos tecnológicos y a la información.

Desde los inicios de esta tecnología, muchas recomendaciones se han generado para dotar a las redes inalámbricas de un nivel de seguridad adecuado. Inicialmente, algunas de estas recomendaciones solo pusieron en evidencia más riesgos, esto generó confusión y desconfianza, pero posteriormente y con base en iniciativas más serias al momento de valorar el riesgo asociado a esta tecnología, se han venido diseñando y estableciendo otros mecanismos que realmente permiten mejorar el nivel de seguridad en las redes inalámbricas

Este documento describe una de las soluciones de seguridad más eficientes para el control de acceso a los recursos y la protección de la información en redes inalámbricas, la cual se basa en el uso de autenticación para el acceso a la red y en el uso de encripción en las comunicaciones sobre este tipo de redes.
De manera especial se presentan las principales consideraciones que los encargados de la seguridad y de la administración de las infraestructuras informáticas deben tener en cuenta para llevar a cabo este tipo de implementación.

2. Conceptos

Para entender mejor el contenido de este documento, a continuación se presenta, de manera breve, los principales conceptos relacionados con la implementación de mecanismos de seguridad para el control de acceso en redes de datos cableadas e inalámbricas.

2.1 Control de Acceso

El control de acceso, en sistemas de información, es la capacidad de controlar la interacción de un elemento activo (usuario, dispositivo, servicio) con un

© SANS Institute 2000 - 2005 Author retains full rights.

recurso informático (red de datos, sistema, servicio). Adicionalmente, el control de acceso implica procedimientos de identificación, autenticación y autorización para permitir o denegar el uso de los recursos así como para llevar un registro de este.

2.2 Identificación, Autenticación, Autorización

Identificación
La identificación es el procedimiento mediante el cual un elemento presenta su identidad a otro componente.
Generalmente la identificación puede estar dada por un nombre de usuario, número de identificación o número de cuenta. Este parámetro no solo permite realizar la identificación, si no que habilita al sistema a relacionar la identidad con el uso de los recursos, donde dicho individuo es responsable de sus acciones (Accountability).

Autenticación
Es el proceso de validar la identidad de quien accede o provee un servicio, mediante la verificación de ciertas credenciales o parámetros que debe proveer la entidad que se autentica.
Entre los métodos más comunes de autenticación se encuentra el uso de una contraseña o clave personal (algo que usted sabe), sin embargo cada vez es más requerido el uso de otros factores de autenticación como tokens (algo que usted tiene) o Biometría (algo que usted es).
A nivel de enlace de datos, y de acuerdo al método y características de seguridad, existen diversos tipos de autenticación. A continuación se describen brevemente los principales protocolos de autenticación de este tipo:

PAP (Password Authentication Protocol)
Este protocolo realiza la validación cuando se establece la conexión entre el cliente y el servidor. Utiliza el nombre de usuario y contraseña como credenciales, las cuales son enviadas en texto plano sobre el enlace, por lo que se considera un método poco seguro.

CHAP (Challenge Handshake Protocol)
Provee un mejor nivel de seguridad, ya que realiza una validación de tres vías entre cliente y servidor, donde este último envía un parámetro de control (o desafío) a quien se autentica, este lo encripta con su contraseña y lo reenvía al servidor, donde se realiza el mismo procedimiento con la contraseña almacenada y se verifica si se obtiene el mismo resultado.

EAP (Extensible Authentication Protocol)
Es un protocolo que permite elevar aún más el nivel de seguridad de la autenticación, permitiendo diversos métodos autenticación y tipos de credenciales a utilizar (incluyendo la capacidad de manejar certificados

© SANS Institute 2000 - 2005, Author retains full rights.

digitales). De acuerdo a esto, diversos tipos de EAP se pueden implementar conforme a las características y condiciones propias de cada infraestructura donde se la requiera. Los principales tipos de EAP son:

- EAP-TLS
  Realiza la autenticación estableciendo un túnel cifrado entre los elementos para proteger las credenciales y datos que se intercambian. Utiliza certificados digitales para autenticar a cliente y servidor.
- PEAP
  Realiza la autenticación en dos fases. Primero establece una sesión TLS para autenticar al servidor y posteriormente se establece un segundo túnel para autenticar al cliente, permitiendo realizar autenticaciones de tipo CHAP (como el de Microsoft "MS-CHAP") de manera más segura. Es un protocolo comúnmente soportado por tecnologías de Microsoft.
- TTLS
  También se realiza la autenticación en dos fases, utilizando una sesión de TLS para proteger la autenticación del cliente (similar a PEAP). Puede utilizar tipos de autenticación diferentes a EAP, como CHAP, MS-CHAP y otros. Este tipo de autenticación no es comúnmente soportado, por lo cual suele requerir un software adicional en el cliente.
- LEAP
  Es un método de autenticación desarrollado por Cisco, que usa contraseña para autenticar al cliente. Generalmente se requiere de hardware/software Cisco para soportarlo. Adicionalmente, es susceptible a ataques de adivinación de contraseñas, y no permite autenticar equipos.

Autorización
La autorización establece lo que un usuario puede o no hacer una vez haya sido identificado y autenticado.

2.3 Encripción

La encripción en sistemas de información, es el proceso mediante el cual, utilizando una llave o un valor de control, un mensaje (generalmente datos en texto plano) es codificado para evitar que su contenido sea accedido y/o entendido por personal no autorizado.
Para poder acceder al mensaje cifrado es necesario desencriptar el mensaje, proceso mediante el cual, utilizando la llave indicada, se recupera la información del mensaje en su estado original.

Encripción simétrica
Es el proceso de cifrado de datos, en el cual se realiza la encripción y desencripción utilizando la misma llave.
La encripción simétrica es un procedimiento rápido, que provee mecanismos para asegurar la confidencialidad e integridad de la información que protege.

© SANS Institute 2000 - 2005, Author retains full rights.

Por otro lado el hecho de utilizar la misma clave en los procesos mencionados implica realizar una distribución segura de llaves por vías alternas a la que se quiere proteger. Por lo anterior también es recomendado utilizar la llave la menor cantidad de veces posible, idealmente una sola vez.
Algunos de los estándares de encripción simétrica más conocidos son: DES (Data Encription Standard) Triple DES y AES (Advanced Encription Standard)

Encripción asimétrica
Es el proceso de cifrado de datos, en el cual se utiliza llaves diferentes para la encripción y desencripción, una de estas de carácter privado o secreto y la otra es de acceso público (dentro de un sistema). También se le conoce como encripción de clave pública y se dice que se implementa bajo una infraestructura de clave pública (PKI).
Este tipo de encripción fue desarrollado a finales de los años 70's y adicionó nuevas funcionalidades a los mecanismos de encripción como la posibilidad de realizar autenticación fuerte, no repudio, y el hecho de mejorar y facilitar los esquemas de confidencialidad e integridad.
Algunos de los estándares de encripción asimétrica más conocidos son: RSA (Rivest, Shamir & Addleman), Diffie-Hellman y El Gamal.

2.4 RADIUS (Remote Authentication Dial-In User Service)

Es un protocolo de autenticación basado en cliente y servidor que le permite a un servidor de acceso remoto comunicarse con un servidor central para poder autenticar usuarios que acceden a la red y autorizar el uso de los servicios requeridos. Este sistema, generalmente se implementa mediante software, e inicialmente su función principal fue autorizar a los usuarios de acceso conmutado (dial-in) de un proveedor de servicios de Internet (ISP) para permitir su acceso a la red pública.

2.5 802.11

Es un estándar IEEE[1] que establece especificaciones para los dispositivos y las comunicaciones en redes inalámbricas de área local (WLAN), incluyendo espectros de frecuencias utilizados, velocidades de transmisión y demás parámetros que determinan esta tecnología.

Este estándar también especifica mecanismos de encripción para realizar la protección de los datos trasmitidos en ambientes WLAN. El mecanismo de seguridad que se incluyó como parte del estándar 802.11 fue WEP (Wired Equivalency Privacy), el cual fue rápidamente adoptado por los fabricantes de tecnología inalámbrica al ver que no existían mecanismos de seguridad adecuados para proteger este tipo de infraestructura.

[1] http://www.ieee.org

2.6 802.1x

802.1X es un estándar del IEEE para realizar el control de acceso a una red mediante un proceso de autenticación que habilita o impide el acceso de los dispositivos que se conectan a un puerto de red LAN. Este estándar puede implementarse en redes cableadas al igual que en redes inalámbricas 802.11. Adicionalmente este tipo de implementación puede utilizarse para administrar las claves utilizadas para proteger la información que trasmiten los dispositivos autenticados.

En la implementación 802.1x se requieren, mínimo, los siguientes componentes:

- Usuario que intenta acceder a la red, o "suplicante"
- Punto de acceso que habilita o impide el ingreso del suplicante, también llamado "Autenticador"
- Y el servidor de autenticación, quien negocia y valida la identidad del suplicante; y le informa el éxito o fracaso de este proceso al autenticador para que ejecute la acción indicada.

1X hace referencia al uso del protocolo de autenticación extensible EAP entre el suplicante (usuarios de acceso inalámbrico), el autenticador (switches o access points) y los servidores de autenticación (como el RADIUS por ejemplo).

3 Por qué 802.1x

Muchas prácticas se han establecido como recomendables para minimizar los riesgos asociados al acceso indebido en redes inalámbricas. Entre las principales recomendaciones de este tipo se encuentran:

- Evitar la difusión del identificador de red o SSID (Service Set Identifier).
- Establecer listas de control de acceso por direcciones físicas o de MAC (Media Access Control) de los dispositivos que acceden a la red.
- Utilizar cifrado en las conexiones inalámbricas.
- Segmentar los puntos de acceso inalámbricos en zonas de seguridad administradas por un firewall.
- Establecer redes privadas virtuales o VPNs en las conexiones inalámbricas.
- Combinar mecanismo de autenticación a la red y cifrado de datos
- No implementar infraestructura inalámbrica.

De estas prácticas, algunas se han implementado directamente en los dispositivos inalámbricos, como el uso de cifrado. Inicialmente surgió el protocolo WEP el cual utiliza una clave secreta estática (no hay renovación de la clave de manera automática y frecuente) que es compartida por el punto de acceso y todos los clientes que accedan a través de este a la red, y con la cual se realiza la autenticación a la red y la protección de los datos.

© SANS Institute 2000 - 2005 Author retains full rights.

Muchos fabricantes entonces, decidieron integrar esta funcionalidad y compatibilidad con WEP para ofrecer un mecanismo de seguridad para las redes inalámbricas, sin embargo, no pasó mucho tiempo para que se empezaran a detectar y difundir las debilidades o fallas de este mecanismo. Realmente WEP tiene debilidades de seguridad debido al manejo estático de su llave y al uso de un vector de inicialización (VI) que se puede identificar en los paquetes transmitidos, de manera periódica; lo que hace que este protocolo sea susceptible a ataques que permitan encontrar la llave de cifrado a partir de un tráfico capturado con un mismo VI; mas aún, hoy en día no se requiere una cantidad extremadamente grande de datos capturados ni de conocimiento para llevar a cabo este proceso, pues existen varias herramientas que automatizan y facilitan este proceso, entre las más conocidas se encuentran Kismet[2], Aircrak[3] y WepLab[4].

La IEEE consciente de estas fallas desarrolló del estándar de seguridad 802.11i para redes inalámbricas, que también se conoce como "red de seguridad sólida" (RSN). Por otro lado, el consorcio de proveedores de tecnología inalámbrica con mejor fidelidad "Wi-Fi[5]", generó el estándar WPA (Wi-Fi protected Access) para la protección delos datos y el control del acceso inalámbrico a las redes, el cual se basa en el estándar 802.11i y puede implementarse en las tecnologías inalámbricas de tipo Wi-Fi.
Este estándar incluye los mecanismos más adecuados para realizar el control de acceso y protección de datos en ambientes inalámbricos ya que integra mecanismos fuertes de autenticación, control de acceso, integridad y confidencialidad.
WPA utiliza 802.1x como mecanismo de control de acceso y autenticación a la red, y para generar y entregar las llaves de sesión WPA a los usuarios autenticados.
Para corregir las principales debilidades de WEP, WPA utiliza el protocolo TKIP (Temporal Key Integrity Protocol), el cual aumenta el tamaño de las claves, refresca dichas claves periódicamente, utiliza un contador de secuencia VI y realiza una función de mezcla de VI por paquete, previniendo así los ataques de clave de WEP.

Adicionalmente, WPA utiliza una función de encripción llamada MIC (Message Integrity Code) con la cual verifica la integridad de los mensajes transmitidos y previene que atacantes capturen paquetes, los modifiquen y los reenvíen.

El principal problema de WPA radica en que es un estándar que aún se encuentra en proceso de adopción, donde muchas tecnologías inalámbricas no están habilitadas para poder implementarlo. Adicionalmente el estándar 802.11i (también conocido como WPA2) aún se está ratificando y posteriormente se

[2] http://www.kismetwireless.net/
[3] http://www.cr0.net:8040/code/network/aircrack/
[4] http://weplab.sourceforge.net/
[5] http://www.wi-fi.org/

requerirá una actualización en el hardware y software de acceso inalámbrico para cumplir con este estándar.

Como alternativa realmente viable para quienes tiene dispositivos inalámbricos que no soportan WPA, surgió la integración del mecanismo de control de acceso y autenticación a la red 802.1x con el uso de cifrado WEP con manejo dinámico de claves (WEP dinámico).

La implementación de 802.1x para redes inalámbricas utiliza un servidor de autenticación como el RADIUS, el cual no solo es quien valida la identidad de quien accede a la red (a través de un método EAP) si no que es quien fuerza, con cierta frecuencia, la generación de una nueva clave de cifrado para la conexión establecida, haciendo que la probabilidad de que un ataque identifique de la clave de cifrado, sea mínima (con una adecuada configuración de la frecuencia de renovación de la clave de cifrado).

Adicionalmente, ciertos métodos de autenticación EAP como TLS y TTLS permiten elevar aún más la seguridad mediante el uso de certificados digitales de autenticación de usuarios o estaciones.

Otra ventaja de la implementación de 802.1x en redes inalámbricas es los costos asociados, ya que se puede utilizar servidores de autenticación (RADIUS, IAS[6]) que ya existen en las organizaciones y no se requiere actualizaciones firmware o compatibilidad con WPA en los dispositivos inalámbricos utilizados.

Finalmente, este tipo de implementación es fácilmente adaptable a los cambios o crecimientos de las infraestructuras tecnológicas y también se pueden utilizar modelos de autenticación distribuidos para organizaciones con varias sedes o varias redes LAN.

Entre las restantes recomendaciones de seguridad enumeradas no se puede dejar de considerar el uso de VPNs para proteger el acceso inalámbrico.

Esta alternativa se planteó desde el inicio de las tecnologías de acceso inalámbrico, principalmente impulsado por los desarrolladores de VPNs, y aunque es indudable el aporte de seguridad y protección de información que provee una VPN, su uso en el acceso inalámbrico en un ambiente corporativo presenta algunas desventajas en la funcionalidad, complejidad y en los costos asociados a estos sistemas.
Realmente una conexión VPN es muy dependiente del usuario ya que este debe establecerla y controlarla manualmente para mantener adecuadamente su funcionalidad (no es transparente para el usuario), y por otro lado, implica una infraestructura adicional que soporte estas conexiones, lo que representa

[6] Servicio de autenticación de Internet de Microsoft, http://www.microsoft.com/spain/seguridad/guidance/prodtech/IAS.mspx

gastos adicionales y contar con recursos humanos calificados para implementarlas y gestionarlas.
Adicionalmente, este mecanismo no permite autenticar a los dispositivos que acceden a la red, e incluso algunos tipos de VPNs no brindan mecanismos de autenticación suficientemente seguros.

Las restantes recomendaciones de seguridad para redes inalámbricas, como el control de acceso por dirección MAC (susceptible a ataques de captura de tráfico, y requiere una interacción continua para administrar adecuadamente este mecanismo y no limitar la operatividad y movilidad de sus usuarios), y la no difusión del SSID, se pueden considerar practicas complementarias ya que no suplen completamente todos los requerimientos de seguridad y funcionalidad de una infraestructura de acceso inalámbrico.

4 Análisis de Requerimientos

Una vez se haya decidido la implementación de un sistema de control de acceso a la red de datos basado en el estándar 802.1x, se debe determinar cuales son los requerimientos de funcionalidad que se deben suplir así como los requerimientos técnicos que implica la implementación de este tipo de solución, con lo cual se definirá el diseño y la selección del tipo de autenticación (EAP) a utilizar.
A continuación se describen los principales requerimientos funcionales y técnicos:

4.1 Funcionalidad

La implementación de una infraestructura de acceso inalámbrico a la red de datos de una organización puede ser conducida por diferentes requerimientos funcionales, algunos de los más comunes son:

- Ofrecer acceso a los servicios tecnológicos al creciente número de usuarios de la organización.
- Brindar acceso a algunos servicios para invitados, clientes o socios de negocio que visitan instalaciones habilitadas para el acceso inalámbrico.
- Ofrecer servicios de acceso a la red pública (Internet) y ofrecer servicios de valor agregado (ISP).
- Habilitar el acceso a los recursos informáticos para usuarios que requieren movilidad dentro de las instalaciones de la organización.

Cada uno de estos escenarios requiere la infraestructura inalámbrica adecuada con los mecanismos de seguridad adecuados, por lo cual, la selección de estos componentes puede variar ampliamente de un escenario a otro, por ejemplo, si los usuarios de la infraestructura inalámbrica ya hacen parte de el sistema o dominio de usuarios es recomendable un mecanismo de control de acceso que

© SANS Institute 2000 - 2005 Author retains full rights.

se integre a esta base o dominio de usuarios para poder establecer mecanismo más transparentes de autenticación (poder utilizar los mecanismos habituales) a la red. Por otro lado si se pretende ofrecer un servicio de acceso a Internet, puede ser recomendable aislar de manera segura el segmento de acceso inalámbrico y así poder implementar mecanismos de autenticación a la red no tan robustos.

Por lo anterior, es muy importante considerar la funcionalidad requerida para la selección y la implementación de los mecanismos de seguridad de la infraestructura de acceso inalámbrico, buscando siempre la mayor protección posible, sin comprometer la funcionalidad necesaria.

4.2 Seguridad requerida

El grado de seguridad requerido es una de las consideraciones en el momento de seleccionar el mecanismo de control de acceso y autenticación a la red.

Este grado de seguridad puede variar ampliamente entre una y otra organización; en otras palabras, si el nivel de riesgo que representa la infraestructura inalámbrica contra la integridad, confidencialidad y disponibilidad de la información no es considerable o se ha disminuido con otras medidas, tales como la autenticación en el acceso a servicios y aplicaciones, políticas de grupo, cifrado de información u otras; se puede seleccionar mecanismos de autenticación menos complejos pero acordes a dicho nivel de riesgo.

Un caso que ilustra lo anterior puede ser el de una organización que ofrece a sus invitados servicios de red para navegar (http) hacia Internet, implementado mediante un segmento de acceso inalámbrico controlado por un firewall donde las políticas de éste solo permiten tráfico http de los equipos conectados hacia direcciones IP públicas; en este caso, una autenticación basado en usuario y contraseña podría ser suficiente para controlar el uso de este servicio.

También el tamaño de las organizaciones y su limitación en recursos pueden conllevar a que se implementen mecanismos de seguridad menos robustos pero que disminuyen el riesgo a niveles aceptables; e incluso puede resultar más económico tecerizar el control del acceso a la red, con el mismo ISP, por ejemplo.

4.3 Requerimientos técnicos

Si funcionalmente ya se delimitaron los posibles tipos de autenticación a implementar, es importante validarlos y seleccionar el más indicado con base en los requerimientos técnicos que implica la implementación de estos posibles tipos de autenticación.

Integración y Compatibilidad

© SANS Institute 2000 - 2005 Author retains full rights.

En el momento de la implementación las organizaciones ya pueden contar con un servicio de autenticación de usuarios (como un servidor RADIUS o IAS, por ejemplo), el cual requieren mantener y poder integrar a la nueva infraestructura de acceso inalámbrico. Para esto, dichas organizaciones deben validar si estos servicios de autenticación son compatibles con 802.1x, y si es así, determinar los tipos de autenticación EAP que soportan.

Sin embargo, si el servicio de autenticación a la red con el que se cuenta no es compatible con los nuevos requerimientos para asegurar el acceso inalámbrico, se debe verificar si realizando una actualización del servicio este quede habilitado para implementar 802.1x, o si por el contrario se requiere implementar uno nuevo de las muchas alternativas comerciales y gratuitas disponibles que brindan amplias capacidades y compatibilidad con 802.1x

Otro punto importante es considerar la estructura de dominio de usuarios con la que se cuenta y si se pretende utilizar la misma base de datos de usuarios para validar la autenticación a la red en la implementación de 802.1x a realizar.

Generalmente, la mayoría de servidores de autenticación que soportan 802.1x permiten integrarse con las bases de datos de usuarios de la organización (directorios LDAP[7], dominios NT, bases de datos distribuidas u otras), para poder así utilizar las mismas credenciales almacenadas en estas, para la autenticación a nivel de acceso a la red. Sin embargo, es necesario verificar esta compatibilidad en el servidor de autenticación que se pretende utilizar, u optar por manejar una base de datos alterna, implementada sobre el mismo servidor, de acuerdo a las opciones que este brinde para realizar dicho proceso.

En los usuarios (Suplicantes)
Desde el punto de vista de los clientes de acceso inalámbricos, más exactamente sobre los requerimientos de la conexión, se debe validar si las plataformas utilizadas en los clientes soportan el tipo de autenticación elegido o si por el contrario requieren un componente de software que los habilite para realizarla.
A continuación se presenta una tabla con el tipo de soporte disponible en algunos sistemas operativos (los más comunes a nivel de cliente) para los diferentes métodos de autenticación EAP:

Sistema Operativo	EAP-TLS	EAP-TTLS	PEAP	LEAP
Win XP, 2000	Cliente Nativo	Cliente de Tercero	Cliente Nativo	Cliente de Tercero
Win 9x	Cliente de Tercero	Cliente de Tercero	Cliente de Tercero	Cliente de Tercero

[7] Protocolo de acceso ligero a directorio, basado en la estructura de directorio X.500 y el protocolo DAP, http://asg.web.cmu.edu/cyrus/email/standards-X500.html

Linux	Cliente de Tercero	Cliente de Tercero	No soportado	No soportado
MacOS	Cliente de Tercero	Cliente de Tercero	No soportado	No soportado

Tabla 4.1 Soporte de EAP en los principales sistemas operativos como cliente[8].

Es posible que organizaciones con diferentes plataformas a nivel de clientes (Windows[9], Linux[10], MacOS[11]) prefieran implementar un mismo cliente 802.1x para tener un sistema homogéneo y facilitar su administración.

En los Access Points (autenticadores)
Entre los principales requerimientos, sobre estos dispositivos, para poder implementar un mecanismo de seguridad para el control del acceso inalámbrico, se encuentran:

- Compatibilidad con 802.11 y soporte de cifrado (WEP al menos)
- Capacidad de implementar el servicio de control de acceso 802.1x

En el servidor de autenticación
Finalmente, los principales requerimientos en este componente, para poder implementar la solución de seguridad basada en 802.1x, son:

- Compatibilidad con 802.1x
- Soporte de diversos tipos de autenticación EAP (TLS, TTLS, PEAP)
- Capacidad de registro (Accounting)
- Soporte para el control de acceso en redes inalámbricas
- Flexibilidad para validar a los suplicantes mediante varios métodos (Base de datos de usuarios local, directorio de usuarios LDAP, certificados, entre otros)

Adicionalmente, en este componente se deben verificar las capacidades de integración con otros servicios de la red, como se describió anteriormente.

5 Diseño

5.1 Componentes del sistema de autenticación

Como se mencionó anteriormente, los componentes básicos de una implementación 802.1x son: el suplicante, el autenticador y el servidor de autenticación. Sin embargo, y de acuerdo a los requerimientos técnicos y funcionales, los elementos de este sistema pueden ser más. Para ilustrar lo anterior a continuación se presenta un escenario donde se integra la autenticación del esquema 802.1x con la base de datos de usuarios de la

[8] http://www.wi-fiplanet.com/tutorials/article.php/3075481

[9] http://www.microsoft.com/
[10] http://www.linux.org/
[11] http://www.apple.com/macosx/

organización, la cual se encuentra en un controlador tipo LDAP. Adicionalmente se presenta una segmentación en zonas de seguridad establecida por un firewall el cual únicamente habilita el tráfico permitido entre las diferentes zonas.

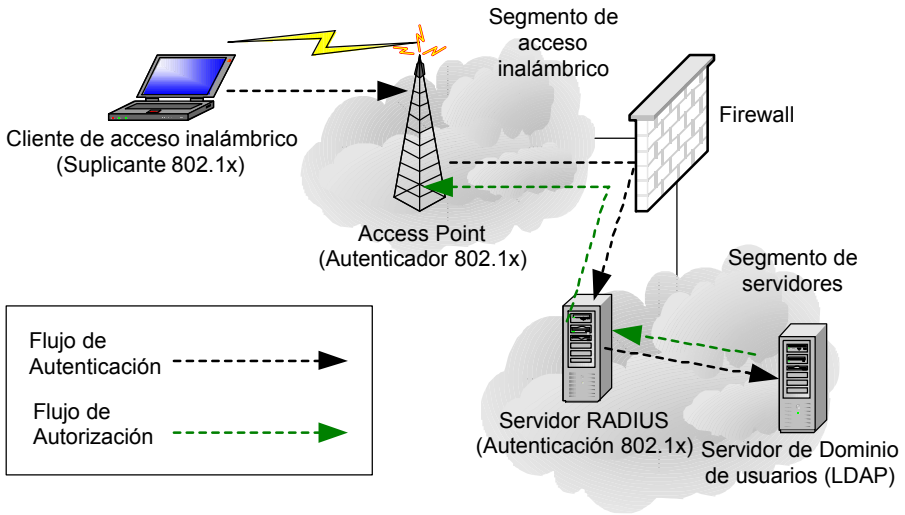

Fig. 5.1 Ejemplo de un escenario de implementación de 802.1x en una infraestructura de acceso inalámbrico.

Como podemos ver, es importante considerar en el diseño todos los elementos que se involucrarán con el esquema a implementar, para así considerar los requerimientos en cada uno de ellos y terminar de definir adecuadamente el plan de implementación.

5.2 Selección mecanismo de autenticación

De acuerdo a los requerimientos de seguridad y funcionalidad, se debe seleccionar el método de autenticación EAP adecuado, es posible que en pequeñas empresas, con un número de usuarios pequeño y recursos limitados se seleccione un método de autenticación como PEAP, el cual, por ejemplo, no requiere del uso de certificados digitales, significando esto menos complejidad y menores costos.
Por el contrario, para una empresa con gran cantidad de usuarios puede ser más funcional el integrar certificados para así poder tener un mejor control sobre los usuarios y equipos que se conectan a la red.
Hay que considerar los esquemas de seguridad ya implementados, como el uso de VPNs y si se ha expedido certificados a los usuarios para realizar la autenticación en este tipo de conexión. Si es así, sería conveniente seleccionar un tipo de EAP que utilice certificados (EAP-TLS, EAP-TTLS, por ejemplo) y así aprovechar los que ya se han expedido a los usuarios.

Los requerimientos técnicos pueden terminar de definir el esquema a

implementar, ya que se debe elegir un tipo de autenticación que se pueda soportar en los diferentes elementos que conforman la solución (ver 4.3).

Igualmente, y como se explicó anteriormente, es posible realizar la validación de la identidad (autenticación) que realiza el servidor de autenticación mediante varios métodos, de manera local en el servidor RADIUS o con respecto a una base de datos externa que puede ser de varios tipos, lo más común son las bases de datos de usuarios del domino tipo LDAP. Si este tipo de sistema de usuarios existe en la organización y los servicios de acceso inalámbrico son para los usuarios que hacen parte de este sistema, es recomendable integrar la autenticación del RADIUS con la base de datos que maneja estos usuarios (comúnmente tipo LDAP) para establecer un proceso más transparente para el usuario así como para aprovechar las características de estos sistemas que permiten realizar una mejor administración y autorización sobre el uso de los recursos informáticos.

Para ilustrar consideraciones e implicaciones interesantes, asumiremos una selección del método de autenticación EAP-TLS, el cual utiliza certificados digitales como credenciales de autenticación, asumiendo también que se integra a la base de datos de usuarios que ya posee la organización.

6 Implementación

A la hora de realizar la implementación surgen consideraciones igualmente importantes para el éxito de la solución. De manera general, la implementación de este tipo de sistemas requiere un conocimiento específico del estándar 802.1x y de tecnologías inalámbricas seleccionadas, por lo cual hay que verificar que se cuente con los recursos debidamente calificados para llevar a cabo esta implementación o si se requiere adquirir los servicios de un tercero.

Una vez se cuente con los recursos y se cumpla con los requerimientos técnicos es necesario realizar una planeación de la implementación considerando todos los componentes que podrían verse afectados durante este proceso, y de esta manera establecer que procedimientos, como y cuando se desarrollarían y así informarlo, autorizarlo y evitar impactos negativos considerables.

Se recomienda realizar, de manera previa, la implementación de la solución en un ambiente de desarrollo donde se realicen todas las pruebas necesarias para verificar la correcta funcionalidad en el uso de los servicios informáticos que se acceden. Posteriormente, se debe comenzar con la implementación de la solución en el ambiente de producción de manera gradual, es decir realizarla sobre un primer grupo de usuarios los cuales presenten un bajo impacto sobre los procesos de negocio críticos para la organización.

En el momento de implementación de la solución en cada uno de los

© SANS Institute 2000 - 2005, Author retains full rights.

elementos que la conforman, existen igualmente consideraciones particulares a tener en cuenta. A continuación se presentan las principales consideraciones para la implementación de 802.1x con EAP-TLS en cada uno de estos componentes:

6.1 Cliente (Suplicante)

Para poder realizar este tipo de autenticación (EAP-TLS) se debe contar con certificados digitales para autenticación, almacenados en el banco local del equipo, o asegurarse que los usuarios los tienen almacenados en un token o tarjeta inteligente y que este sistema este debidamente probado. Si aún no se tiene el certificado se debe obtenerlo a través de los mecanismos que la organización haya habilitado (solicitud a una RA o entidad de registro vía http, por medio del directorio LDAP como política de grupo, adquirido a un tercero, u otros).
Posteriormente, si el sistema operativo del suplicante requiere un software de un tercero para soportar EAP-TLS (Ver tabla 4.1) se debe instalarlo y luego se debe configurar los parámetros asociados a 802.1x y EAP-TLS en el asistente de conexión, incluyendo ubicación del certificado, autenticación del servidor, integración con usuario de dominio y demás parámetros.

6.2 Punto de Acceso (Autenticador)

Se debe activar el servicio 802.1x y configurarlo de acuerdo al diseño y demás componentes (incluyendo dirección del servidor RADIUS, autenticación del servidor, tipo de autenticación y demás parámetros)
Es muy importante que inicialmente se habilite 802.1x pero que no sea requerido, es decir implementar un esquema mixto y transitorio donde los usuarios que aún no estén completamente habilitados para 802.1x con EAP-TLS puedan acceder y utilizar los recursos mediante mecanismos de autenticación tradicionales como nombre de usuario y contraseña.

6.3 Servidor de Autenticación

Se debe configurar el tipo de autenticación seleccionado, en este caso EAP-TLS, así como los demás parámetros asociados a este mecanismo.
Si se decidió integrar la autenticación con una base de datos externa, se debe habilitar esta opción y establecer los parámetros adecuados (tipo de base de datos, servidores a integrar, entre otros). También se deben definir los autenticadores que van a trabajar con el servidor de autenticación, es decir definir los puntos de acceso que va a manejar este servidor.

Por seguridad este servidor se deberá autenticarse ante los demás componentes mediante el uso de un certificado digital valido para este propósito. Por lo anterior se debe obtener dicho certificado y almacenarlo en el banco local del servidor.

6.4 Otras consideraciones

Si este sistema se integra a un dominio administrado de usuarios, se debe establecer políticas adecuadas para los diferentes grupos de usuarios y de perfiles que acceden de manera inalámbrica. Esto permite realizar una mejor administración y autorización de los recursos, de acuerdo a las necesidades reales de los diferentes tipos de usuarios de acceso inalámbrico; mejorando así la productividad y la seguridad de la organización.

Se debe realizar una correcta administración de la PKI de la organización, y en especial de los certificados digitales utilizados, es decir expedirlos de acuerdo a las necesidades y realizar un control adecuado sobre el ciclo de vida de los mismos (revocación, renovación y demás).

Si se trabaja con zonas de seguridad administradas por un firewall se debe revisar las políticas y configuración de este elemento para que provea la funcionalidad necesaria, no solo en cuanto a al autenticación, si no a la habilitación del acceso a los recursos requeridos por los usuarios de acceso inalámbrico, sin que esto implique aceptar riesgos innecesarios.

Una vez configurado los componentes de la solución, se deben realizar pruebas para verificar las comunicaciones de extremo a extremo en el proceso de autenticación, y comprobar que este se ejecute correctamente y provea la funcionalidad esperada a los clientes de acceso inalámbrico.

Es recomendable realizar pruebas de análisis del tráfico generado por este sistema, ya que puede ser necesario depurar las configuraciones inicialmente establecidas en los diferentes elementos para corregir posibles problemas de la autenticación y/o lograr un mejor desempeño.

7 Consideraciones finales

Es importante tener en cuenta al momento de implementar un mecanismo de control de acceso basado en 802.1x que existen consideraciones no tan favorables para la red.

En primer lugar, al querer implementar un sistema de autenticación flexible y transparente para el usuario, se debe tener en cuenta que las tecnologías actuales no soportan un gran número de tipos de autenticación EAP.

Por otro lado, las implementaciones de WEP dinámico aún utilizan una clave estática para las comunicaciones globales (como las de difusión), las cuales no se renuevan frecuentemente. Esto abre la posibilidad de realizar ataques para obtener información de la red y combinarse con otro tipo de acciones indebidas que conlleven a impactar a las organizaciones de manera negativa.

Adicionalmente, con el continuo crecimiento de la capacidad computacional y las velocidades de transmisión, así como el desarrollo la criptografía, requerirán que las claves de cifrado (como las utilizadas en WEP dinámico) se deban renovar con mayor frecuencia. Esto a su vez podría elevar la carga de procesamiento del servidor de autenticación de manera que finalmente se comprometa la calidad del servicio.

Es muy probable que estas consideraciones finales no sopesen tanto frente a las ventajas y funcionalidad que ofrece en si la implementación de 802.1x en redes inalámbricas.

8 Conclusión

Después de describir los principales mecanismos para proteger las redes inalámbricas, se puede percibir que la implementación de 802.1x en entornos inalámbricos es un componente primordial de las mejores recomendaciones de seguridad actuales y futuras, por lo cual su adopción es una práctica que no solo eleva el nivel de seguridad de las infraestructuras de acceso inalámbrico actuales, si no que prepara a las organizaciones para llegar a cumplir con los futuros estándares de seguridad para este tipo de tecnología.

Adicionalmente, implementar 802.1x en ambientes inalámbricos es una posibilidad real que las organizaciones pueden llevar a cabo con su infraestructura tecnológica actual, y que se adecuará, sin mayores impactos económicos o funcionales, a su crecimiento y modernización.

© SANS Institute 2000 - 2005 Author retains full rights.

Referencias

Michael Ossmann "WEP: Dead Again, Part 1"
URL: http://www.securityfocus.com/infocus/1814 (Febrero 5, 2005)

Interlink Networks "WPA and 802.1x"
URL: http://www.interlinknetworks.com/resource/wa5-0-1.htm (Febrero 9, 2005)

Jim Geier "802.1X Offers Authentication and Key Management"
URL: http://www.wi-fiplanet.com/tutorials/article.php/1041171 (Enero 25, 2005)

Matthew Peretz "A Very Funky 802.1x Security Solution"
URL: http://www.wi-fiplanet.com/news/article.php/965961 (Febrero 17, 2005)

Lisa Phifer "Using RADIUS For WLAN Authentication, Part I"
URL: http://www.wi-fiplanet.com/tutorials/article.php/3075481 (Febrero 18, 2005)

Lisa Phifer "Using Deploying 802.1X for WLANs: EAP Types"
URL: http://www.wi-fiplanet.com/tutorials/article.php/3114511 (Febrero 19, 2005)

Lisa Phifer "Using RADIUS For WLAN Authentication, Part II"
URL: http://www.wi-fiplanet.com/reviews/ST/article.php/3287481 (Febrero 19, 2005)

Lisa Phifer "Using RADIUS For WLAN Authentication, Part III"
URL: http://www.wi-fiplanet.com/tutorials/article.php/3289231 (Febrero 19, 2005)

L. Blunk, J. Vollbrecht "PPP Extensible Authentication Protocol (EAP)"
URL: http://www.ietf.org/rfc/rfc2284.txt?number=2284

Microsoft Technet "Reforzamiento de la autenticación inalámbrica"
URL:http://www.microsoft.com/latam/technet/seguridad/articulos/ddmmyy_reforzamiento_autenticacion_inalambrica.asp (Febrero 13, 2005)

Microsoft Technet "Seguridad en LAN inalámbricas con PEAP y contraseñas"
URL: http://www.microsoft.com/spain/technet/recursos/articulos/peap_1.mspx (Febrero 13, 2005)

Wi-Fi Alliance "Wi-Fi Protected Access"
URL: http://www.wi-fialliance.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf (Febrero 10, 2005)

© SANS Institute 2000 - 2005 Author retains full rights.

Susan Hansche, John Berti, Chris Hare. "Official ISC2 guide to the CISSP exam" Boca Raton, Auerbach Publications, 2004.

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**