Diseño de arquitectura segura para redes inalámbricas

Alfredo Reino [areino@forbes-sinclair.com]

La tecnología de redes inalámbricas basada en el estándar IEEE 802.11 tiene unos beneficios incuestionables en el mundo empresarial. Algunos de estos beneficios son la flexibilidad, movilidad, reducción de costes de infraestructura de red, integración con dispositivos móviles y PDAs, y mejor escalabilidad de la red.

Riesgos

Sin embargo esta tecnología lleva aparejada una serie de riesgos que afectan directamente a la confidencialidad, integridad y disponibilidad de los activos e información empresarial.

Estos riesgos de Seguridad de la Información se resumen en los siguientes:

- Intercepción y escucha del tráfico en tránsito, que afecta a la confidencialidad de los datos. Permite al atacante espiar el tráfico de red, capturar contraseñas, leer correo electrónico y conversaciones realizadas a través de la red, y obtener información útil sobre la organización interna y la infraestructura de sistemas para preparar un ataque.
- Acceso no controlado a la red interna corporativa. Esto puede ser utilizado por el atacante para acceder a sistemas internos normalmente no accesibles desde el exterior. Si las contramedidas contra riesgos de seguridad habituales están desplegadas en el perímetro de la red, como suele ser habitual, una vez dentro, el atacante tiene vía libre a todos los sistemas de la red interna.
- Un intruso puede usar una red inalámbrica con poca o nula seguridad para acceder de forma gratuita a Internet a través de la red de la empresa. Mientras esto parece en apariencia inocuo, y los activos de información de la organización no se ven afectados, es una actividad que supone un uso no aceptado de recursos de la empresa por personal no autorizado. Además afecta a la calidad y disponibilidad del servicio de red de los usuarios legítimos, y puede suponer un problema legal para la organización si el intruso utiliza el acceso a Internet de la empresa para realizar acciones ilegales (*hacking*) o acceso a contenido de Internet inapropiado (por ejemplo, pornografía infantil).
- Denegación de servicio (*DoS*). Los servicios de red inalámbrica 802.11 son vulnerables a diferentes ataques de denegación de servicio (por ejemplo, generación de tráfico aleatorio excesivo, generación de puntos de acceso falsos, etc.)
- Un atacante podría instalar un punto de acceso inalámbrico de forma que se confunda con los puntos de acceso legítimos, provocando que un número de usuarios se conecte al del atacante. El atacante reenviaría el tráfico a los puntos de acceso legítimos. De esta forma se implementaría un ataque *man-in-the-middle* de modo que todo el

tráfico de red de los usuarios afectados sea monitorizado, almacenado y potencialmente alterado por el atacante.
- Un visitante a la empresa podría conectarse a la red con su portátil, de forma inadvertida o conscientemente, sirviendo como punto de entrada de virus, gusanos y troyanos.

Existen multitud de formas de mitigar algunos de estos riesgos, tales como usar cifrado WEP (*Wired Equivalent Privacy*), control de acceso por dirección física MAC, uso de VPN (*Virtual Private Networks*) y el uso de soluciones propietarias no soportadas por todos los fabricantes.

Cifrado y autenticación

Todos estos riesgos comentados (exceptuando algunos aspectos de Denegación de Servicio para los que hay difícil solución cuando el ataque se realiza contra la "capa física" de radiofrecuencia) se solucionan mediante tecnologías de cifrado y de autenticación.

Para implementar autenticación se configuran los puntos de acceso IEEE 802.11 de forma que utilicen el estándar IEEE 802.1x y servidores RADIUS para identificar, autenticar y autorizar a los usuarios y dispositivos mediante políticas de acceso centralizadas.

El estándar IEEE 802.1x es un estándar de autenticación para gestión de redes que permite autenticar al usuario o máquina contra un servicio RADIUS, LDAP o cualquier otro sistema de autenticación e identificación.

Para implementar cifrado de datos, hasta ahora el único sistema ampliamente implementado por los fabricantes de productos compatibles con 802.11 es el WEP (*Wired Equivalent Privacy*), disponible en versiones de 64 y 128 bits.

WEP no proporciona un mecanismo de gestión de claves adecuado, lo que hace que estas claves sean estáticas y compartidas por los usuarios. Además tiene problemas de diseño que hacen posible la obtención de las claves de cifrado con el tiempo. Esto es debido a que el Vector de Inicialización (*Initialization Vector, IV*) que se utiliza para generar la clave de cifrado de sesión junto con la Clave Compartida (*Pre-Shared Key, PSK*), tiene un caracter periódico. De este modo, una vez obtenida una cantidad suficiente de tráfico encriptado se hace trivial la desencriptación de los paquetes.

En la solución propuesta en este artículo, se utiliza la implementación RADIUS de Microsoft (IAS, *Internet Authorization Service*) que permite la utilización de claves dinámicas asignadas durante la identificación del cliente mediante certificados.

La solución a medio plazo es la utilización de WPA (*Wi-Fi Protected Access*), parte del futuro estándar IEEE 802.11i, pero que actualmente sólo es soportado por ciertos fabricantes y plataformas. El estándar IEEE 802.11i con WPA2 se espera que esté disponible a finales de 2005 o principios del

2005, y soluciona muchas de las vulnerabilidades y problemas de WEP y WPA.

De todos los protocolos de autenticación basados en el estándar EAP (*Extensible Authentication Protocol*) disponibles para plataformas Microsoft, los más importantes son EAP-TLS, PEAP, y EAP-MD5. EAP está definido por el RFC 2284 y constituye un protocolo general para autenticación, autorización y auditoria (AAA). Típicamente funciona en la capa de enlace (capa OSI 2) y fue desarrollado originalmente para ser utilizado en PPP (*Point to Point Protocol*) aunque ahora es parte opcional de IEEE 802.1

EAP-MD5 no soporta autenticación mutua entre cliente y punto de acceso, no soporta rotación de claves de cifrado y sólo soporta autenticación por contraseña, por lo que no es un candidato viable para la implementación de la arquitectura requerida.

PEAP y EAP-TLS ambos soportan autenticación mutua, claves de cifrado dinámicas e implementan una tecnología de autenticación segura. Las diferencias consisten en que PEAP sólo soporta contraseñas, y EAP-TLS sólo soporta certificados (generando el requisito de implantación de PKI)

La solución

La solución comentada en este artículo está basada en cifrado WPA siempre que sea soportado por el hardware. En cualquier caso, la arquitectura de la solución es tambien válida en caso de tener que usar WEP (128 bits) por compatibilidad con hardware actual. La solución usa claves dinámicas (*rekeying*) y autenticación 802.1X usando EAP-TLS apoyándose en una infraestructura de Active Directory y PKI. En principio la arquitectura propuesta es válida para cualquier organización de tamaño mediano a grande, cuya infraestructura de servicios de red esté basada en plataformas Microsoft Windows 2000 Server y Windows Server 2003, preferiblemente con Active Directory ya implantado.

Los requisitos de la solución son los siguientes:

- Reducir riesgos de seguridad asociados.
    - Interceptación del tráfico de red.
    - Acceso a la red de usuarios no autorizados.
    - Ataques DoS a nivel de red.
    - Uso no autorizado de la red.
- Facilidad de uso para los usuarios.
- Compatibilidad con amplio número de dispositivos *wireless.*
- Tolerancia a fallos de la arquitectura.
- Sencillez y bajo coste de escalabilidad.
- Uso de sistemas y protocolos estándares de la industria.
- Facilidad de monitorización y auditoría de acceso a la red.

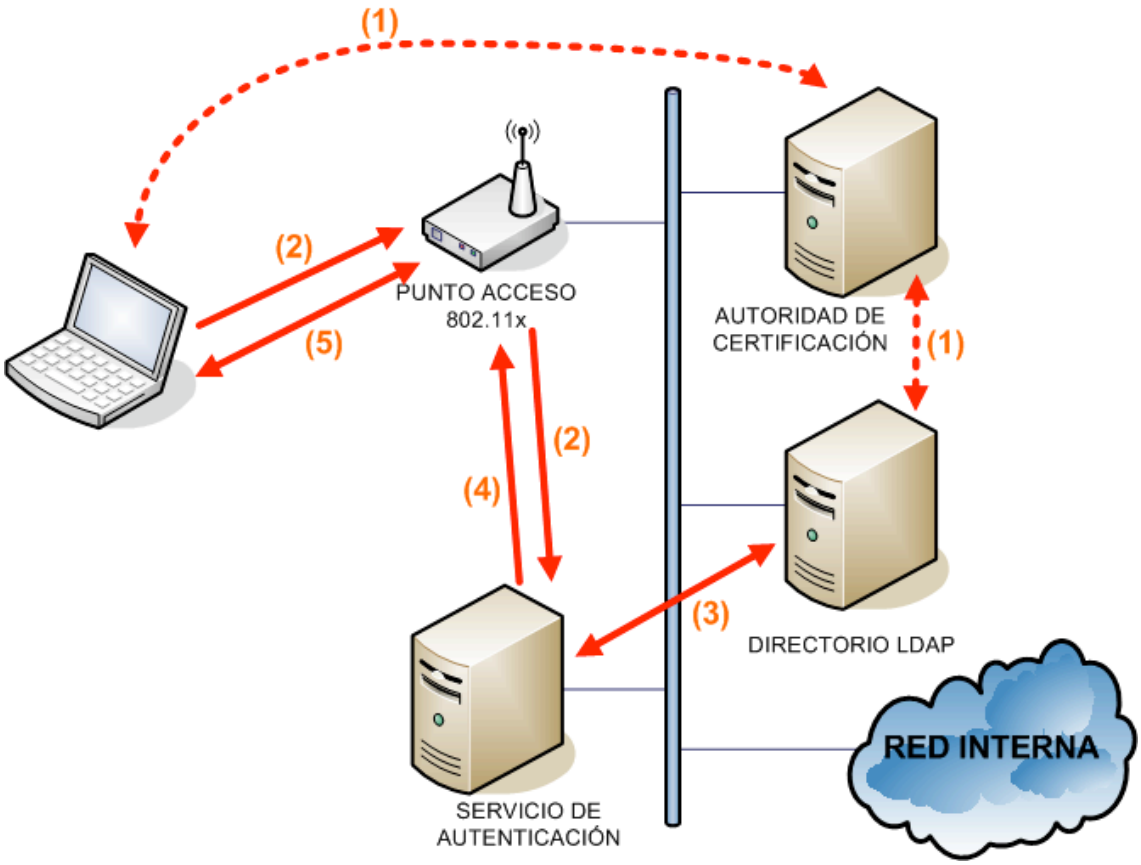
La solución propuesta consta de diferentes elementos importantes que se describen a continuación:

- Punto de Acceso 802.11x (AP)
    - Funciona como *bridge* entre la red inalámbrica basada en tecnología IEEE 802.11x y la red Ethernet.
    - Realiza funciones de control de acceso, ya sea por listas de direcciones MAC autorizadas, o mediante consultas a un servidor de autenticación RADIUS externo.
    - Realiza cifrado de datos entre el cliente *wireless* y el punto de acceso (AP) y permite el intercambio de claves con el cliente de forma segura para establecer el cifrado de la sesión.
    - Como requisito de hardware, el AP debería soportar las características citadas (validación contra RADIUS y cifrado de tráfico via WPA o WEP)
- Servicio de Autenticación
    - Implementa el protocolo RADIUS
    - Recibe las solicitudes de autenticación de los clientes, reenviadas por los puntos de acceso 802.11x
    - Consulta en el servicio de directorio LDAP las credenciales y certificados del usuario, así como las políticas de acceso.
- Directorio LDAP
    - Almacena de forma centralizada las cuentas de usuarios con sus características y credenciales (certificados digitales, etc.)
    - Almacena políticas de control de acceso de forma centralizada.
- Autoridad de Certificación
    - Parte fundamental del PKI (*Public Key Infrastructure*)
    - Emite los certificados digitales de los usuarios, cuya parte pública será almacenada en el directorio LDAP y la parte privada en el equipo del usuario.

En esta solución se ha optado por los servicios provistos por Windows Server 2003 debido a:

- Su disponibilidad como parte del sistema operativo sin necesidad de adquirir licencias para productos extra.
- La sencillez de la integración entre los servicios de autenticación (IAS, *Internet Authentication Service*), directorio LDAP (*Active Directory*) y autoridad certificadora del PKI (*Certificate Services*).
- Preexistencia de una infraestructura basada en plataforma Windows, en especial la existencia de Active Directory como directorio LDAP.
- Facilidad de implementar una infraestructura distribuida en diferentes localizaciones geográficas, de forma rápida, eficiente y robusta, mediante sincronización y replicación de Active Directory, que permita a los servidores RADIUS de cada localización acceder a información de usuarios y políticas de acceso actualizadas.

El esquema lógico de la solución es el siguiente:



En el proceso de autenticación y autorización de un usuario para acceder a la red, tienen lugar varios pasos:

1. Previo al acceso, el usuario tiene que tener generado un certificado digital por la Autoridad de Certificación (CA). Esta acción podrá ser realizada de forma más o menos automática dependiendo del grado de integración del PKI con el directorio LDAP, y también dependiendo del modelo de administración del control de acceso en la organización. El sistema puede ser tipo autoservicio basado en intranet (en el que el usuario solicita un certificado para determinado uso, y un administrador aprueba la solicitud) o de tipo manual (el administrador genera el certificado manualmente, almacena la parte pública del certificado en el directorio LDAP, e instala el certificado con la clave privada en el equipo del usuario).
2. El cliente *wireless* solicita al punto de acceso permiso para establecer una conexión y acceder a la red. Para ello le envía una solicitud firmada con su clave privada. El punto de acceso está configurado para reenviar la solicitud al servicio RADIUS.
3. El servicio RADIUS, consulta al directorio LDAP para comprobar las credenciales del usuario y su validez. Además también consulta al directorio LDAP las políticas de acceso (horarios de conexión, requisitos de cifrado y autenticación, pertenencia del usuario a ciertos grupos, etc.)

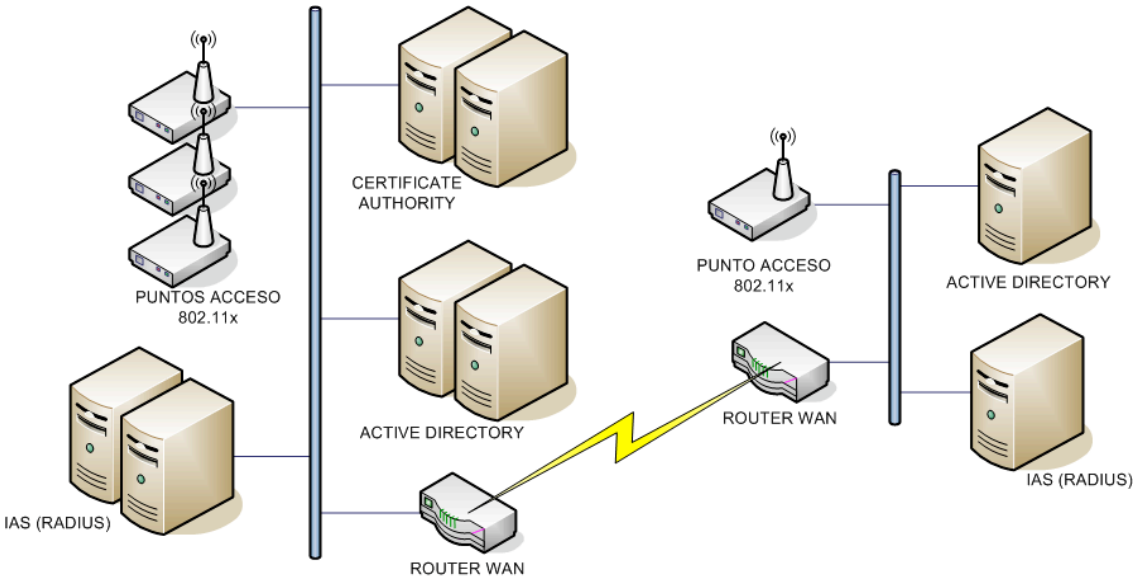
4. El servicio RADIUS determina si el usuario tiene acceso a la red y envía la autorización al punto de acceso.
5. El punto de acceso inicia un intercambio de claves para establecer un cifrado de sesión con el cliente, permitiéndole así acceder a la red de forma segura.

Consolidación de servidores y escalabilidad

Los tres servicios fundamentales (PKI, Active Directory y RADIUS) para la arquitectura de control de acceso que aparecen en el esquema pueden estar implementados físicamente de formas muy diferentes según el tamaño de la organización, su infraestructura de T.I., presupuesto para el proyecto, etc.

En un extremo podemos tener los tres servicios corriendo en el mismo servidor (quizá también DHCP y DNS) para una organización de tamaño pequeño con pocos requisitos de escalabilidad.

En otro extremo se puede tener una infraestructura totalmente redundante, tolerante a fallos, con distribución de carga y distribuida geográficamente en diferentes localizaciones de tamaños diversos.



En función del tamaño de la arquitectura, las decisiones de diseño serán diferentes para el PKI (modelo de provisionado de certificados, CAs integradas con Active Directory o *stand-alone*, CA "*root*" desconectada o no, etc.) y la infraestructura RADIUS (número de servidores, uso de múltiples *proxies* RADIUS y servidores RADIUS para tolerancia a fallos, escalabilidad y reparto de carga)

Otras consideraciones

Otros puntos que se tienen que tener en cuenta a la hora de implementar una arquitectura segura para redes inalámbricas son los siguientes:

- Sistema de gestión de contraseñas de administración de los puntos de acceso debe ser equivalente a la gestión de contraseñas de cualquier otro servidor. La administración de puntos de acceso debe hacerse por canales seguros (SSH, SSL, subred de administración segregada de la red principal, etc.)
- Considerar si es necesaria la retransmisión del SSID (*Service Set Identifier*)
- Gestión y monitorización de los puntos de acceso (mediante SNMP y/o syslog) integrada con infraestructura de monitorización y administración existente en la organización.
- Uso de segregación de redes, DMZs, *firewalls*, y asignación automática de VLANs para los clientes *wireless*, con objeto de realizar un mayor control sobre el acceso a la red y a los recursos.
- Estudio de la localización de los puntos de acceso para minimizar el tráfico inalámbrico y posibilidad de conexión a la red desde zonas no deseadas o fuera del ámbito de la organización.
- Uso regular y procedimentado de técnicas para detectar puntos de acceso no autorizados (Netstumbler, AirSnort, etc.)
- Monitorización y auditoría de los registros de acceso del servicio RADIUS.

Conclusión

Las redes inalámbricas basadas en el estándar IEEE 802.11 son una tecnología que aporta beneficios considerables en términos de flexibilidad, escalabilidad y movilidad, pero que tiene un gran impacto en la infraestructura, operaciones y Seguridad de la Información de las organizaciones.

La clave para un correcto y eficaz despliegue y explotación de este tipo de redes está en comprender los riesgos que entrañan, además de conocer las posibilidades de la tecnología con la que contamos en la actualidad para mitigarlos.