Despliegue de redes inalámbricas seguras sin necesidad de usar VPN

Secure Wireless Networks Deployment without Using VPN

E. Alcantud, F. Sampalo, J. M. Malgosa et al.

Resumen

La migración a la tecnología inalámbrica facilita la movilidad de usuarios y la creación de nuevas aplicaciones para la mejora de la situación tecnológica de las universidades. Sin embargo, ¿son realmente seguras estas redes? Presentamos un sistema de acceso inalámbrico realmente seguro con servicio de autenticación de usuarios. Se ha instalado un servidor de acceso y diseñado una arquitectura de red adaptable a los distintos perfiles de usuario que en la universidad encontramos.

Este sistema garantiza la privacidad del tráfico y el registro de clientes, evitando las complicaciones inherentes a las VPNs: instalación de una PKI y complejidad de uso para la gran mayoría de los usuarios a los que va dirigido el servicio.

Palabras clave: EAP-TTLS, Servidor RADIUS, 802.1x, WEP, licencia libre, certificados, VLAN, LDAP.

Summary

Wireless technology migration makes easier clients' mobility and the creation of new applications in order to improve the technological situation of universities. However, are really secure these networks?. We present a really safe wireless system with user's authentication service. An access server has been installed and we have designed an user profile adaptable network architecture according to the existing profiles in the university. This system guarantees traffic data privacy and registers users, avoiding VPN development, a much more complicated system for most of clients that are thought to use this service.

Keywords: EAP-TTLS, RADIUS Server, 802.1x, WEP, free-license, certificates, VLAN, LDAP.

1.- Introducción

Hoy en día las redes inalámbricas están en auge debido a su principal característica: la ausencia de cable. Esta ausencia de cable además de facilitar la creación de nuevos servicios, permite el acceso a estos en cualquier lugar y momento, situación antes insospechada. En el medio abierto en el que se transmite la señal pueden realizarse fácilmente escuchas y entradas no autorizadas a recursos. La habilitación de puntos de acceso para una red segura en zonas comunes del campus se presenta como una mejora del servicio a todos los miembros de éste. Queda demostrado que el sistema de seguridad básico del protocolo empleado es bastante vulnerable. Desarrollar un sistema organizativo que garantice un control de acceso robusto y la privacidad del tráfico supone la inversión de cierto tiempo de estudio y medios técnicos que, normalmente, en sistemas pequeños ni se consideran.

Desarrollar un sistema organizativo que garantice un control de acceso robusto y la privacidad del tráfico supone una inversión que, normalmente, en sistemas pequeños ni se considera

Ante las muchas alternativas, en este proyecto se evita el empleo de VPN, sistema cuyas robustez y seguridad están más que demostradas y que ya está estudiado y en marcha en algunas organizaciones, en aras de una búsqueda de sencillez y empleo de claves de sesión, tras un proceso transparente y sencillo para todos los usuarios.

Este artículo describe a grandes rasgos la problemática del sistema básico de seguridad de estas redes, presentando el diseño de la arquitectura de red inalámbrica más adecuado.

2.- Sistema de cifrado WEP

WEP (Wired Equivalent Privacy) es un estándar de encriptación de flujo (no de bloque) opcional implementado en la capa MAC soportada por la mayoría de tarjetas de red y puntos de acceso. Si un

usuario activa el WEP, la tarjeta encripta el cuerpo de trama y el CRC de cada trama 802.11 antes de su transmisión empleando un flujo de cifrado RC4. La estación receptora, un punto de acceso u otra NIC, desencripta cada una de las tramas. Como resultado, el mecanismo WEP sólo encripta los datos entre estaciones 802.11. Una vez que la trama se introduce en una red cableada, este cifrado no se aplica.

WEP ha sido parte del estándar 802.11 desde su declaración oficial en septiembre de 1999 y ha sido muy criticado en estos últimos años. La principal característica de WEP, y también la causa de sus debilidades, es que no proporciona ningún mecanismo de intercambio de claves entre estaciones. Como resultado, los administradores del sistema y los usuarios emplean normalmente la misma clave durante semanas, facilitando la posibilidad de que un intruso obtenga una monitorización lo suficientemente larga de tráfico cifrado con una misma clave. Así, las capturas dentro de la red y la monitorización desde el exterior del tráfico son los principales problemas de este sistema de cifrado.

EAP es un estándar muy flexible, ya que debe responder a las muy diversas necesidades de seguridad de las WLANs

3.- Alternativas al WEP

WEP resulta insuficiente para muchas situaciones no garantizando la protección de nuestros recursos. Han surgido numerosas propuestas de soluciones sobre el WEP actual, entre las que destacamos:

- Cifrar la información en los niveles superiores (IPsec, SSH, SCP, etc.).
- Cambiar las claves WEP de cada usuario muy frecuentemente.

Lógicamente, la primera alternativa no depende de la infraestructura de la red y por lo tanto, puede utilizarse siempre que el usuario lo estime oportuno. Sin embargo, la segunda debe configurarse a nivel de enlace por el administrador de la red. Esta opción proporciona una comunicación lo suficientemente segura, incluso en aquellos casos en que no se emplea ningún mecanismo de seguridad en los niveles de red, transporte o aplicación.

4.- Métodos EAP y EAP-TTLS y sus correspondientes características

4.1.- EAP

IEEE 802.1x-EAP reduce al mínimo los riesgos de seguridad en las redes inalámbricas, en el acceso no autorizado a los recursos de la red y el espionaje al ofrecer identificación de usuarios y equipos, autenticación centralizada y administración dinámica de claves. IEEE 802.1x es compatible con el Servicio de Autenticación de Internet (IAS), que implementa el protocolo Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). En esta implementación, un punto de acceso inalámbrico sirve de elemento intermedio entre un cliente de RADIUS, que envía una solicitud de conexión y mensajes de cuentas, y un servidor central de RADIUS. El servidor central de RADIUS procesa la solicitud y concede o rechaza la solicitud de conexión. Si se concede la solicitud, se autentica al cliente y se generan claves únicas (de las que se obtiene la clave WEP) para dicha sesión, dependiendo del método de autenticación elegido.

EAP es un estándar muy flexible, ya que debe responder a las muy diversas necesidades de seguridad de las WLANs. Abarca diversos métodos de autenticación, incluyendo: MD5, TLS, LEAP, PEAP, SIM, AKA y TTLS. Este último es el seleccionado para la implantación de la red inalámbrica de la UPCT.

4.2.- EAP-TTLS

TTLS (Tunneled Transport Layer Security) es una extensión de TLS y fue desarrollada para sobreponerse a la desventaja creada por TLS en cuanto a la necesidad de poseer un certificado por

cada cliente. Con TTLS sólo se transfiere el certificado del servidor. En el primer paso, un algoritmo asimétrico basado en la clave pública del servidor es empleado para verificar la identidad del servidor y establecer un túnel simétrico encriptado. En el segundo, tiene lugar la autenticación del cliente empleando un segundo método de autenticación dentro del túnel seguro previamente creado. Este segundo método puede ser de un tipo EAP (normalmente MD5) o cualquier otro, tal como PAP, CHAP, MS-CHAP ó MS-CHAP-V2.

El túnel se emplea sólo para proteger al método de autenticación del cliente. Una vez verificado, desaparece y depende de los elementos inalámbricos el crear un túnel de encriptación WEP para la privacidad de los datos, que a su vez puede ser dinámico. Esto ofrece una seguridad robusta durante el proceso de autenticación y una gran comodidad ante la posibilidad de emplear métodos de autenticación muy sencillos para el cliente (tales como pares id/password).

Los principales rasgos de TTLS que se tienen en cuenta son:

- Que soporta protocolos de autenticación basados en login y passwords.
- Que la información basada en el password y la identidad del usuario no son observables en el canal de comunicación entre el nodo cliente y el proveedor de servicio lo que le protege contra ataques de diccionario y suplantaciones.
- Que el proceso de autenticación finaliza en la distribución de la información de clave compartida entre el cliente y el punto de acceso.
- Que el mecanismo de autenticación soporta traspasos entre pequeños dominios en los que el usuario no tiene relación previa (Roaming) gracias a su definición en 802.11. Sin embargo 802.1X estipula que mientras se esté reautenticando al cliente éste no tendrá acceso a la red.

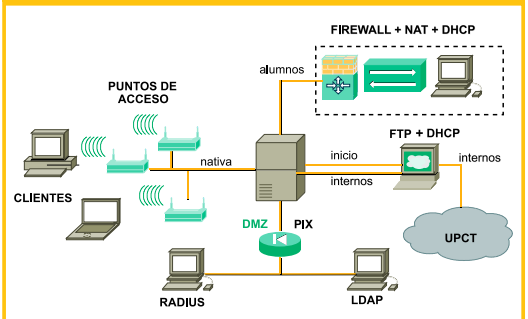
Para la integración de la red inalámbrica en la arquitectura se deben incluir distintos servidores que gestionen el acceso tras la autenticación

5.- Estructura

5.1.-Arquitectura de acceso

Para la integración de la red inalámbrica en la arquitectura se deben incluir distintos servidores que gestionen el acceso tras la autenticación. La siguiente figura muestra la situación de los servidores dentro del sistema, además de los elementos de interconexión y distintas zonas de la red.

FIGURA 1: ESQUEMA DE LA RED



Se han definido tres VLANs, aparte de la nativa, para el servicio inalámbrico mapeadas con los diferentes SSID (nombre de la red inalámbrica):

- SSID "inicio": VLAN privada a la que se conecta por defecto cualquier cliente la primera vez y que sólo permite el acceso al servidor FTP para descarga del cliente TTLS e instrucciones.
- SSID "alumnos": VLAN con direccionamiento privado mediante DHCP accediendo a la red externa a través de un Firewall haciendo NAT.
- SSID "internos": VLAN con direccionamiento público para la red interna de la UPCT (reservada a personal de la Universidad).

Mediante atributos del servidor RADIUS se garantiza que cada perfil de usuario pueda acceder únicamente a la VLAN que le corresponda. Se necesita que los puntos de acceso soporten 802.1Q 'trunking'.

5.2.-Elementos de autenticación

En el proceso de autenticación participan el servidor RADIUS, el directorio LDAP y el cliente. El punto de acceso actúa de forma transparente en este proceso.

- Servidor RADIUS FreeRADIUS. Software de licencia libre. Gestiona el acceso a la red y asigna VLANs según el tipo de usuario.
- Directorio LDAP de Novell. No necesita extensiones para este tipo de consultas. Realiza autenticación PAP.
- Cliente SecureW2. Cliente EAP-TTLS de licencia libre para Windows XP/2000. Gestiona los certificados y credenciales. (Existen clientes Linux)

No se ha utilizado un hardware específico para el servidor, puede instalarse en cualquier máquina con sistema operativo Linux no necesitando ningún requerimiento especial

6.- Hardware y Software

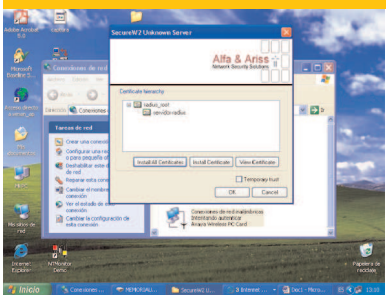
No se ha utilizado un hardware específico para el servidor, puede instalarse en cualquier máquina con sistema operativo Linux no necesitando ningún requerimiento especial. En nuestro caso se ha empleado un Intel Pentium Xeon 3GHz-2Gb RAM-Disco SCSI (RAID1). Para el servidor se emplea la versión 1.0.1 de FreeRadius (licencia libre), necesitando previamente distintos módulos y librerías (ldap, krb5, gdbm, sasl, pam, etc.). Para la creación de certificados y archivos de encriptación se debe instalar Openssl 0.9.7. (o versión posterior). Además, se necesita un archivo "random" para creación de claves y un archivo de extensiones OID. Para los usuarios que deseen conectarse se ha de descargar el cliente EAP-TTLS (Windows XP/2000) SecureW2.

7.- Pasos en la autenticación

Para la autenticación con el servidor RADIUS necesitamos un cliente, que se descarga en un servidor FTP a través de una red inalámbrica inicial. Cuando el usuario posea el cliente instalado debe seleccionar este software, en lugar de "Tarjeta inteligente o certificado" en la opción de configuración Windows para autenticación de redes inalámbricas.

Cuando la tarjeta detecta la red el servidor envía sus certificados y tras su instalación mediante la ventana que aparece en la figura, el cliente abre otra de credenciales (usuario y contraseña) y éstas se envían al servidor de autentificación (RADIUS). Tras la instalación del certificado continúa el diálogo TLS. En caso de autenticación satisfactoria se generan las claves de sesión que permitirán al cliente entrar en red a través del punto de acceso.

FIGURA 2: VENTANA DEL CLIENTE PARA INSTALACIÓN DE CERTIFICADOS



8.- Conclusiones

La elección de un sistema de autenticación tunelizado basado en certificados y consultas al LDAP universitario, resulta el más adecuado. El disponer de un

directorio central de usuarios y el aprovechamiento de recursos propios son dos grandes prioridades. La inversión de presupuesto en el sistema es mínima.

Todo el sistema está basado en software en desarrollo y con licencia libre, con lo que en el futuro pueden realizarse extensiones del mismo. Por parte del cliente, las únicas interactuaciones consisten en la introducción de credenciales e instalación de certificados, así cualquier usuario no cualificado puede acceder al sistema.

Con esto comprobamos que tras un proceso aparentemente sencillo y casi transparente para el usuario, se encuentra un complejo sistema de interoperabilidad entre máquinas e integración de protocolos. El despliegue de esta red garantiza una importante mejora en la calidad de servicio. Los usuarios pertenecientes a la comunidad pueden, de esta manera, acceder a los servicios académicos, de gestión e Internet entrando en la red inalámbrica a través de sus ordenadores de sobremesa o equipos portátiles.

Todo el sistema está basado en software en desarrollo y con licencia libre, con lo que en el futuro pueden realizarse extensiones del mismo

Elena Alcantud Pérez,
(elena.alcantud@si.upct.es)
José Mª Malgosa Sanahuja,
(josem.malgosa@upct.es)
Mercedes Cava Roda,
(mercedes.cava@si.upct.es)
Ana Belén Díez Barreiro,
(anab.diez@si.upct.es)
Francisco Sampalo Lainz,
(paco.sampalo@si.upct.es)
Servicio de Informática
UPCT