SEGURIDAD EN REDES INALÁMBRICAS DE AREA LOCAL

Carlos Gaule Pantoja – Agustín González V.
Departamento de Electrónica, UTFSM
56-32-654759 / 56-086052351
cgaule@elo.utfsm.cl

Resumen

Este trabajo se describe los problemas de seguridad encontrados en las redes inalámbricas de área local basadas en el protocolo de seguridad *WEP*.

Se estudian las alternativas para dar seguridad y control de acceso a la red inalámbrica.

Se muestra el diseño y comentarios sobre la implementación realizada para el Departamento de Electrónica de la UTFSM, donde se tiene un desarrollo en base a perfiles de usuarios para la red inalámbrica.

Abstract

This work describes the security problems found in wireless local area network based on security protocol *WEP*. It also presents, alternatives to give security and control of access to the wireless network.

Then it shows the design and we comment on the implementation made for the Department of Electronics of the UTFSM, where a development on the basis of profiles of users for the wireless network .

1.- Introducción

El desarrollo y crecimiento de las redes de área local (*LAN*) han permitido el desarrollo de redes inalámbricas de área local (*WLAN*) ya que actualmente los requerimientos de los usuarios son estar permanentemente conectados a la red, los ejecutivos cuentan con equipos portátiles o agendas personales que les permiten trasladar su lugar de trabajo donde ellos sientan que es más cómodo, aunque este lugar sea un jardín o la cafetería.

Las redes inalámbricas se ven fuertemente apoyadas gracias al proceso de estandarización el modo de funcionamiento. Esto se realizó mediante protocolos, el primer acercamiento fue *IEEE 802.11* [1], pero el primero ampliamente aceptado fue *IEEE 802.11b* [1], ambos protocolos son parte del protocolo *IEEE 802.1* para redes de computadores de área local (*LAN*). *IEEE 802.11b* especifica la transmisión por el medio inalámbrico en la banda de los 2.4 GHz utilizando *CSMA* a una tasa de 11 mbps. *802.11b* incorpora *Wired Equivalent Privacy* (*WEP*) que cifra la comunicación inalámbrica entre los puntos de acceso y el cliente. Esto permite a la red inalámbrica un nivel de seguridad al menos equivalente al de la red cableada *Ethernet*.

El diseño de *IEEE 802.11* y *WEP* presentaron prontamente vulnerabilidades relativas a la seguridad, en *WEP* se descubrieron una serie de ataques posibles, llegando a considerarlo actualmente como un protocolo quebrantado. Este trabajo resume los tipos de ataque que se han encontrado.

Existen principalmente cuatro escenarios de uso de la tecnología inalámbrica:

i. Pequeñas oficinas y hogar: Que desean tener una pequeña red inalámbrica en su hogar; estas generalmente involucran un pequeño numero de computadores y un solo punto de acceso.

ii. *Hotspot*: Lugares de acceso público a la red, este puede ser gratuito o requerir algún tipo de pago.

iii. Redes corporativas: Redes privadas, pertenecientes a alguna empresa, se requiere de una red segura.

iv. Redes mixtas: Redes corporativas, que desean dar conectividad tipo *hotspot* a sus visitantes.

En las redes mixtas se requiere de la autenticación y autorización de los usuarios que son parte de la red corporativa hacia los recursos de esta, y tal vez sea deseable la contabilidad del tráfico y volumen generado por los visitantes del *hotspot*, que no deben ser parte de la red privada. Dentro de este tipo de redes se encuentra el Departamento de Electrónica de la UTFSM.

El objetivo de este trabajo, fue:

Estudiar los mecanismos de seguridad que se han utilizado en distintos escenarios para las redes inalámbricas de área local. Cómo se ha resuelto este problema en otras universidades, cómo empresas han implementado redes seguras y qué ofrecen actualmente los fabricantes componentes de redes inalámbricas.

Adicionalmente a esta búsqueda se realiza un estudio comparativo de sus características, qué problemas solucionan y cuáles no. Se analiza el impacto que tienen estas soluciones. Como también cuáles son los escenarios de uso de esta tecnología.

Se utiliza como caso de estudio al Departamento de Electrónica de la Universidad Técnica Federico Santa María. Se estudian sus requerimientos respecto a la red inalámbrica y se implementa, de las alternativas anteriores, la que mejor se amolda sus requerimientos.

2.- Problemas de seguridad de 802.11

802.11 y su protocolo *WEP* presentaron una serie de debilidades y carencias [2]. A continuación se resumen cuales son los ataques y problemas más comunes a los que se ve expuesta una red inalámbrica *802.11* protegida con *WEP*:

i. Manejo de llaves de encriptación*: IEEE 802.11* no específica un método para el manejo de las llaves de encriptación, este proceso se realiza manualmente entre las estaciones de los clientes y puntos de acceso. Dado que este proceso consume mucho tiempo las llaves no son cambiadas periódicamente, y peor aun, a menudo se deshabilitan las opciones de seguridad de los equipos para no tener que asumir el costo administrativo de poner las *llaves WEP* en las estaciones de los clientes.

ii. Largo de las llaves de encriptación*:* Originalmente el estándar propone que el largo de la *llave WEP* sean de 40 bit. Esta ofrece un nivel muy bajo de seguridad. Los fabricantes sacaron versiones con 104 bit (llamado *WEP2)* de largo para la *llave WEP* compartida. Sin embargo, el largo del *IV* se mantiene constante en 24 bit. Este factor provoca la vulnerabilidad de colisiones en el *IV*.

iii. Colisiones en el Vector de Inicialización (IV)*:* El *IV* en *WEP* está definido de un tamaño de 24 bit, éste describe un campo relativamente pequeño de direcciones, 16.777.216 frames. Esto para un escenario de bajo tráfico, como en un hogar, toma mucho tiempo recolectar esta cantidad de tráfico. Sin embargo, en redes con un alto nivel de tráfico, se puede producir colisiones en cosa de horas [2]

iv. Inserción de paquetes maliciosos (problemas con linealidad de CRC)*:* Si un atacante conoce la estructura de un paquete encriptado (reconoce el protocolo y las cabeceras, puede modificar el paquete intercambiando bits de modo de crear un paquete malicioso. Cambiando, por ejemplo direcciones de destino de modo de lograr que el paquete llegue a una máquina que el atacante controle. Este cambio debe ser realizado de modo de que *CRC* no detecte que se produjo un cambio en el contenido del paquete. El punto de acceso no logra detectar ningún cambio en el paquete y lo remite sin mayor problema, lo que permite al atacante obtener la información dentro del paquete.

v. Vectores de inicialización débiles*:* Existen algunas debilidades propias del algoritmo RC4[2], este ataque se basa en la existencia de vectores *IV* que permiten recuperar partes de la llave *WEP*. El proceso descansa sobre la recolección de suficientes vectores *IV* débiles, de modo de completar todas las partes de la llave *WEP*.

vi. Autentificación y control de acceso*: WEP* también es propuesto para dar autenticidad de los paquetes recibidos, esto descansa sobre el principio de que solo puedo desencriptar paquetes bajo mi llave *WEP* compartida. El control de acceso se basa en el conocimiento de la llave *WEP*. Para el control de acceso existe el uso de filtros de acceso a la red basado en la dirección física del adaptador de red (*dirección MAC*), esta es una funcionalidad que ofrecen algunos puntos de acceso pero que no es propia del estándar *802.11*. La mantención de estas listas de acceso puede resultar un proceso complicado en escenarios de cientos de clientes y decenas de puntos de acceso. Estas direcciones pueden ser clonadas por atacantes permitiéndoles el acceso a la red.

3.- Soluciones a los problemas de seguridad y control de acceso en WLAN

Para solucionar los problemas que presenta implementar *WLAN* en distintos escenarios se implementaron sobre estas algunas mejoras, que solucionaban algunos de los aspectos débiles.

Virtual Private Network (VPN): Una *VPN* (red privada virtual) es una técnica de encapsulación y encriptación de los paquetes de datos a distintos puntos de la red a través de infraestructuras públicas de transporte. El escenario mas común de esta tecnología es la de unir oficinas o la de permitir al personal que se encuentra de viaje acceder a la red interna de sus empresas, permitiéndole a éste obtener los servicios propios de la red interna.

En el caso de una red inalámbrica, la utilización de una *VPN* permite autenticar al usuario, cifrar los datos, pero a costa de un aumento del ancho de banda utilizado y de un cuello de botella en la red [3]. El esquema típico es montar la red inalámbrica fuera del cortafuego de la red interna, se toma entonces a esta red como una red insegura. De esta manera se puede ofrecer acceso público a visitantes y se utiliza *VPN* para cifrar el tráfico inalámbrico, autenticar a los usuarios y permitirles a estos acceder a los recursos propios de la red interna. La Ilustración 1 muestra como se conectan los usuarios de la red inalámbrica (*WLAN*) a la red interna (*LAN*) a través del *concentrador VPN*, y hacia Internet lo hacen de forma directa sin pasar por la red interna.

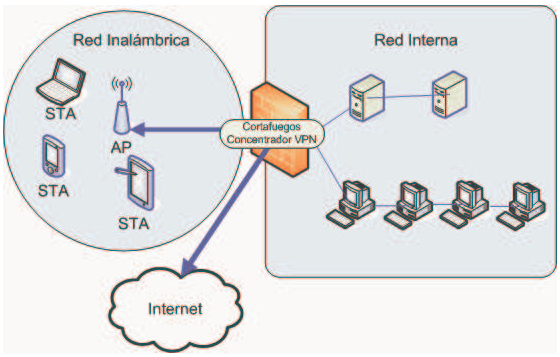

Ilustración 1 : Diagrama de red WLAN y LAN con VPN

Proxy-Web: Una de las alternativas más populares por su bajo costo, es la implementación de un *Proxy-Web*. La idea es realizar autenticación y autorización de los usuarios en escenarios como en Hoteles y aeropuertos, donde se requiere

entregar acceso público con algún tipo de restricción en el acceso. *Proxy-Web* no requiere de la instalación de ningún software adicional por parte del cliente. En la Ilustración 2 podemos apreciar el *cortafuegos dinámico* que es el encargado primero de redirigir el tráfico *Web* de los usuarios sin autenticar hacia el *Servidor de autenticación y página Web segura*, una vez que se supera la etapa de autenticación, el *cortafuegos dinámico* en base a la dirección *IP* y dirección física del adaptador de red (*MAC)* modifican las reglas para permitir el acceso a la red interna e Internet.

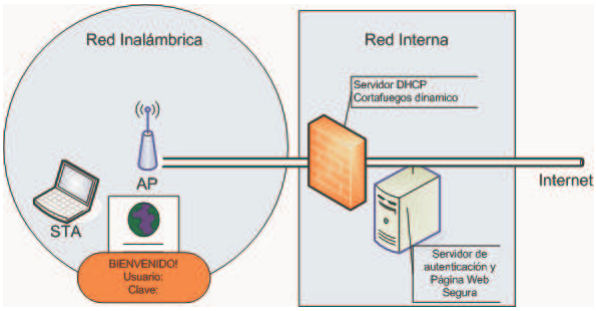

Ilustración 2 : Diagrama de Proxy-Web para autenticación en redes inalámbricas

IEEE 802.11i [4]: El Instituto de Ingenieros Eléctricos y Electrónicos *IEEE* propone el protocolo *IEEE 802.11i* o *Wireless Protected Access 2 (WPA2)* como la solución definitiva al problema de seguridad en redes inalámbricas de área local ante las debilidades encontradas en *802.11* y *WEP*. Este protocolo especifica los requerimientos para las redes inalámbricas de área local (*LAN*) a nivel de capa *MAC* y capa física (*PHY*), fue recientemente ratificado a principios de octubre del año 2004.

IEEE 802.11i incluye varias mejoras, las principales son tres nuevos algoritmos de encriptación: *TKIP* basado en *RC4* compatible con el hardware actual, *CCMP* y *WRAP* ambos basados sobre *Advanced Encription System (AES),* el cual es un algoritmo más robusto pero requiere de un mayor poder de calculo que *RC4*. También propone a *802.1x/EAP* para la autenticación para cualquiera de los tres modos de encriptación.

Una primera versión llamada *Wireless Protected Access* (*WPA*) basada en *IEEE 802.11i*, era la encargada de ofrecer una *WLAN* segura hasta la ratificación *IEEE 802.11i*. Esta ofrece mejoras bajo el hardware que actualmente poseen los usuarios (equipos *Wi-Fi*, que mediante un *update* de *drivers* o *firmware* se compatibilizan con lo que *WPA* propone). *WPA* utiliza como mecanismo de encriptación *TKIP* y autenticación basada en *802.1X/EAP*. Para escenarios donde no se quiere implementar *802.1X* se tiene un modo llamado *Pre-Shared Key (PSK)* que al igual que *WEP* utiliza una llave preconocida y compartida entre *AP* y *STA*, pero realiza una permanente rotación de llaves.

4.- Caso de estudio: Departamento de Electrónica UTFSM

El Departamento de Electrónica de la UTFSM está constantemente investigando los últimos avances en telecomunicaciones, ciencias de la computación y otras áreas de interés científico-tecnológico. Es por esta búsqueda en que el año 1999 se instaló el primer prototipo de red inalámbrica del Departamento. En una primera etapa la red cubrió un sector del área de oficinas de profesores, y en el año 2002 se toma la decisión de ampliar la cobertura, para abarcar la totalidad de las oficinas de profesores, la sala de reuniones y los laboratorios, quedando todo el Departamento cubierto con acceso a la red inalámbrica. El objetivo de esta red es entregar acceso a Internet a los docentes pertenecientes al Departamento. Para el control de acceso se activaron en ambos equipos el filtraje por *MAC* de las tarjetas de los clientes. Esto en una primera etapa resultaba satisfactorio, pues las redes inalámbricas aún no eran muy conocidas.

Actualmente los requerimientos han cambiado, ya existen alumnos con equipos portátiles y tarjetas de red inalámbricas, por otra parte es común que las visitas que asisten al Departamento vengan con sus equipos portátiles y quieran tener acceso a la red.

4.1.- Requerimientos

Para poder definir cual de las tecnologías existentes se ajusta de mejor manera a las necesidades del Departamento de Electrónica, se realiza un levantamiento de requerimientos de la solución. Estos requerimientos son resumidos en la siguiente sección y clasificados en requerimientos generales, que deberían ser satisfechos en toda implementación de red inalámbrica, y los requerimientos propios del Departamento de Electrónica de la UTFSM.

Generales:

I. Evitar el *eavesdropping* [1] de la información transmitida a través de la *WLAN*
II. Evitar modificación de las transmisiones en una red WLAN.
III. Impedir el acceso de usuarios no autorizados a la WLAN y la introducción de virus o código hostil dentro de la red interna
IV. DoS a nivel de capa de red (no es posible a nivel de radio)
V. Las medidas de seguridad no deben tener un impacto en la disponibilidad de la red así como tampoco deben provocar un incremento significativo en las labores administrativas de la red.

[1] *Eavesdropping* se refiere, en redes inalámbricas, al acto de escuchar las transmisiones y poder recuperar posteriormente información. Para evitarlo se deben usar métodos de encriptación en la comunicación

VI. El costo del desarrollo debe ser menor que el costo de oportunidad de tener un solo pequeño número de usuarios WLAN (se estima que menos del 10% de la fuerza de trabajo) que usaran la solución.
VII. Una amplia gama de clientes y dispositivos deben ser soportados dentro del diseño

Propios del departamento:

I. Encriptación de la información
II. Perfiles de usuario (alumnos, profesores e invitados)
III. Autenticación de los usuarios (alumnos y profesores)
IV. Distintos privilegios entre estas entidades (por ejemplo, se puede limitar el BW de las conexiones de los alumnos, no permitir tráfico de algún tipo, etc.)
V. Que utilice los sistemas actuales de autenticación de usuarios, tanto para alumnos como para profesores (como para futuras entidades)
VI. Que puedan definirse usuarios temporales, y que su ingreso a la red no tenga un alto costo administrativo (cuentas temporales)
VII. Que sea una solución lo más homogénea posible (distintos SO, pero que la solución no sea distinta para cada caso)
VIII. Que soporte plataformas Microsoft, Linux a lo menos.

4.2.- Diseño de la Solución

En base a al estudio de las tecnologías que se utilizan para dar seguridad y control de acceso en una *WLAN* se decide basar el diseño utilizando *IEEE 802.11i*, ya que es la solución más completa al problema de seguridad por que contempla una serie de mejoras, como autenticación de usuarios, rotación de las llaves de encriptación (siendo esto un proceso en que el usuario no interviene).

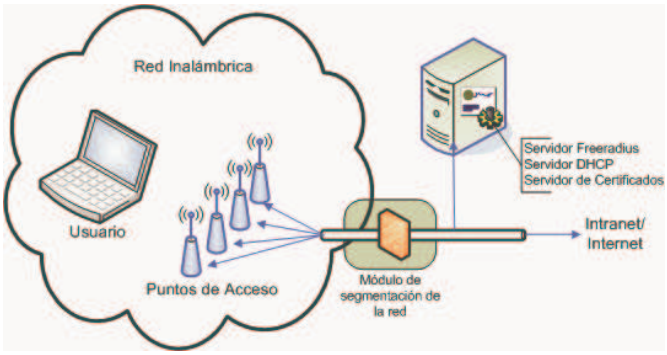

Ilustración 3 : Diagrama de la solución

La solución cuenta de cuatro partes: un *Supplicant* en este caso es el usuario del equipo portátil, un conjunto de *puntos de acceso* que hacen las veces de *Autenticador*, un *router* encargado de segmentar el tráfico de los usuarios y finalmente un *Servidor de autenticación* basado en un *servidor RADIUS*, adicionalmente se agregaran en este mismo equipo un *servidor DHCP (Dinamic Host Configuration Protocol)* y una implementación de *Public Key Infraestructure (PKI)*[2] necesaria para crear los certificados para tener *TLS* sobre *EAP*. La Ilustración 3 muestra como se relacionan cada una de las partes de la solución

Para lograr la segmentación de los usuarios se realizaron dos variantes de implementación: la primera basada en *VLAN* y la segunda basada en un *router* dinámico.

Queda pendiente la elección de los tipos de *EAP* que se utilizarán. Dentro de los que ofrecen autentificación mutua están *EAP/TLS, EAP/PEAP* y *EAP/TTLS*. *EAP/TLS* necesita certificados para la red y para cada cliente, lo cual puede ser muy complicado en un escenario de cientos de usuarios y no aprobecha la infraestructura anterior de servidores de dominio o de credenciales. Para solucionar el problema de tener que implementar certificados para cada cliente se crearon *EAP/PEAP* y *EAP/TTLS*, ambos son muy parecidos, implementan un túnel sobre *TLS*, los dos soportan varios métodos de autenticación, como nombre de usuario y clave, la diferencia radica en que *PEAP* fue desarrollado por *Microsoft* y *Cisco* y *TTLS* por *Funk Software.*

Se definieron tres perfiles de usuario: *profesor, alumno* e *invitado*, para el perfil profesor se utilizó *EAP/TLS* ya que no es problema crear una docena de certificados y de esta manera desligamos a los profesores de tener que utilizar una nueva clave para tener acceso a la red. Para el perfil alumno, se utilizó una conexión a base de datos, con nombre de usuario y clave. Para el perfil invitado, se presento el problema de que para una *SSID* solo puede haber un mecanismo de autenticación, es por esto que para el método de segmentación utilizando *router dinámico* se utilizo *EAP/PEAP* y en el método utilizando *VLANS* se utilizó autenticación abierta.

5.- Implementación

Uno de los desafíos de la implementación era lograr autenticación basada en *IEEE 802.1X/EAP* utilizando para esto software gratuito. El proyecto Open802.1X [5] concentra importante información, otro sitio abundante en referencias de implementaciones es la lista de usuarios de *freeradius* [6].

Para el servidor de autenticación se utilizo *freeradius*, un servidor *RADIUS* de código abierto y licencia GNU, corre en ambiente *UNIX,* en este caso se utilizo un servidor bajo *Linux, Debian 3.0.*

Para crear la infraestructura de certificados, *PKI,* se utilizó *Openssl*. En los clientes se utilizó el *supplicant* incluido en *Windows XP*, esto nos permitió tener disponibles *EAP/TLS* y *EAP/PEAP*.

[2] Un *PKI* es usado para el manejo de llaves criptográficas, llaves públicas y privadas, las transmisiones seguras y la autenticación de datos a través de redes públicas.

Para segmentación usando *VLAN* se utilizo un *AP Cisco Aironet 1100,* que tiene la capacidad de definir múltiples *SSID*, *VLANs*, autenticación basada en *802.1X/EAP*. Se definieron tres *SSID*, una para cada perfil de usuario, *profesores, alumnos* e *invitados*, a cada *SSID* se le asigno una *VLAN* de modo que el tráfico de usuarios con distintos perfiles no se mezcla. Para el *router* se configuró un servidor con sistema operativo *Linux*, se le habilito soporte para *VLAN* y el cortafuego se configuró de modo de dirigir el tráfico de cada *VLAN* por interfaces de red distintas, las cuales estaban conectadas a las redes de *profesores* y *alumnos*. Para el perfil *invitado* se limita el acceso a los recursos *Web* de la Intranet del departamento.

Para la segmentación usando un *router* dinámico se utilizo la experiencia de haber previamente implementado *NoCat* [7], el cual es un *Proxy-Web*. *NoCat* consiste básicamente en dos módulos, *NoCat-Auth* que implementa las páginas *Web* seguras para recibir las credenciales que entrega el usuario y *Gateway* que realizan el cortafuego dinámico sobre *iptables*. Aquí se aprovecho este último módulo para mantener los usuarios separados en tres perfiles. La razón principal de haber realizado estas dos implementaciones radica en que el costo del punto de acceso *Cisco Aironet 1100* es de tres veces el valor de un equipo simple como el *Dlink 2000AP+* utilizado para la segmentación utilizando *router*.

6.- Resultados obtenidos

Se implementaron dos soluciones, basadas en *802.1X* pero con métodos de segmentación diferentes. Adicionalmente se implemento un *Proxy-Web, NoCatAuth,* y también se estudia si cumple con las especificaciones.

En la *Tabla 1* se puede apreciar cómo las distintas alternativas comprometidas en los requerimientos de la solución se logran o no, (se utilizaron los números de cada requerimiento para identificarlos en la tabla). Se comentan además de los problemas que las distintas alternativas pueden presentar.

Al agregar el requerimiento de perfiles de usuario y acceso público a la red inalámbrica, el problema toma una completitud adicional, ya que para realizar esta separación de la forma más segura posible, se hace necesaria la compra de equipamiento que en general es más costoso económicamente. Sin embargo, existen varios escenarios donde no es prohibitiva la compra de este equipamiento.

El desafío en este desarrollo nace de la mano de realizar *802.1X* con software de libre distribución y de código abierto (salvo en los clientes), esto le da un valor agregado a la solución, ya que es posible instaurar *802.1X* en una red, tan solo contando con puntos de acceso inalámbrico que sean compatibles con *802.1X* un servidor bajo *Linux*, algunos paquetes de software, la correcta configuración de estos y algo de paciencia. Actualmente cualquier punto de acceso que sea compatible con *WPA* o *WPA2* es compatible con 802.1X.

		Implementación		
		802.1X VLAN	802.1X Router	NoCatAuth
Requerimientos técnicos	I	WPA		Sin encriptación, No cumple con esta restricción
	II	Autenticación dos extremos, evita el problema de *hombre en el medio*. *WPA* incorpora *MIC*, mejor que *RC4*		No cumple con esta restricción
	III	Se requiere autenticarse primero, se puede introducir virus a los del mismo perfil.		La segmentación y autenticación es al nivel del router, esto permite introducir virus en la red inalámbrica.
	IV	Posible, pero solo a un grupo o perfil	Posible y afectaría a todos los grupos	
	V	Uso de bases de datos, facilita el ingreso a nuevos usuarios, en el caso de utilizar *EAP/TLS* los *script* ayudan a crear las credenciales.		
	VI	Es necesario cambiar todos los puntos de acceso	Se utilizan los equipos actuales, solo es necesario implementar algunos servicios extra.	
	V	*Windows* XP/2000/2003, *Linux*, *Mac OSX*. Existen problemas con tarjetas 802.11b muy antiguas		Cualquier dispositivo WiFi
Requerimientos Propios del Departamento	I	Gracias a *WPA* el tráfico en la parte inalámbrica es encriptado.		No hay encriptación.
	II	Si, servidor *freeradius* + base de datos		
	III	Si		
	IV	Si, separadas en VLAN y segmentos de IP	Si, el *router* separa a los clientes acorde al grupo a que pertenezcan, pero estos grupos se pueden "ver" entre si en la red inalámbrica	
	V	Es necesario crear los certificados para los profesores (*EAP/TLS*) y crear cuentas para los alumnos bajo el servidor de Base de datos		Se requiere especificar las cuentas en el servidor *radius*, no se requieren certificados
	VI	Acceso público, sin intervención de un operador	Acceso publico requiere instar un certificado	Acceso publico, sin intervención de un operador
	VII	Cada SO presenta distintos programas para *802.1X*, Windows integra esta funcionalidad lo que lo hace homogéneo para los clientes *Windows XP/2000/2003*		Solo se requiere de un navegador *Web*
	VIII	Requiere de una tarjeta que sea compatible con WPA		Solo requiere de un navegador *Web*

Tabla 1 : Requerimientos comprometidos V/S Solución implementada

6.- Conclusiones y comentarios

Las redes inalámbricas se han presentado como una atractiva alternativa de conectividad a la red expandiendo el alcance de las redes de área local. Pero como se observó, se hace necesario estudiar la manera de implementar esta tecnología en nuestra red. Para esto es necesario tener en claro cuál es nuestro requerimiento hacia la red inalámbrica. Bajo este esquema, se tomó como caso de estudio al Departamento de Electrónica de la Universidad Técnica Federico Santa María, en donde se tiene un escenario mixto de acceso controlado a recursos de la red privada y se desea también ofrecer acceso público a parte de la red.

En general *IEEE 802.11i* es una alternativa muy robusta de seguridad para la red, su principal escenario es en redes privadas, como redes corporativas. Se requiere de infraestructura adicional en sus modos *TKIP, CCMP, WRAP*, como un servidor *radius* y un servidor *PKI* para la creación de las credenciales.

En escenarios en donde se requiera el uso de una red de acceso público, el *Proxy-Web* resulta una atractiva alternativa, ya que ofrece autenticación mediante un navegador *Web* que es algo con lo que siempre se cuenta en una estación móvil. Existen paquetes de software especialmente diseñado para esta tarea, de libre distribución y de código abierto, también existen productos de software diseñados para implementar una red pública, pero pagada, es decir, implementar todo el sistema de cobro hacia los usuarios, creación de cuentas, etc.

En los escenarios mixtos en donde se necesita el acceso privado y también se quiere dar un acceso publico se presentaron dos alternativas: *IEEE 802.1X + VLAN*, la cual presenta una serie de ventajas respecto a *IEEE 802.1X + cortafuegos dinámico*.

La primera alternativa resulta ser la técnicamente mejor, pero presenta el problema del costo de los equipos (*Cisco*) que presentan la característica de *VLAN*. Del trabajo realizado con este equipamiento se puede comentar al menos, tres casos de uso para esta tecnología:

Segmentación para evitar el abuso de la red*:* Este es el caso del Departamento de Electrónica de la UTFSM, el cual busca dar acceso a *Profesores* y *Alumnos*, al ser asignados a distintas *VLAN,* el *router* es el encargado de asignar el ancho de banda a cada segmento, evitando que el perfil de *Alumno* realice un abuso de la red.

Segmentación para evitar el abuso del espectro*:* En el caso de aeropuertos, si cada local comercial pone una red inalámbrica propia, se llegará a la situación de que se interferirán mutuamente logrando una degradación en la tasa de transmisión final. Para esto, el aeropuerto debería ofrecer la infraestructura de red, compuesta de equipos "tipo" *Cisco* (con las mismas características). Luego, se arrienda el uso de esta infraestructura a los interesados, para esto se define un *SSID* por cada proveedor de acceso a Internet. Aquí cada proveedor se hace responsable de qué protocolos utilizará para dar seguridad a su red inalámbrica.

Segmentación para dar acceso a equipos que no cumplen con los últimos estándares de acceso seguro a al red*:* Si se tiene una red bajo *802.1X*, se está dejando sin acceso a un grupo de usuarios, que tienen tarjetas de red *802.11b* que no son compatibles con *802.1X*, para que este grupo pueda tener acceso, deberán sacrificar su nivel de seguridad, a la utilización de *WEP*, o simplemente entrar por la *SSID* publica de la red.

Si el costo de un equipo inalámbrico que sea compatible con *VLAN* es prohibitivo para la empresa, *802.1X* también puede ser habilitado con equipos de menor costo, como los equipos *DLINK DWL-2000AP+*. Al implementar directamente esta solución no se dispone de múltiples *SSID* ni *VLAN* para segmentar a los usuarios. Sin embargo, si lo que interesa es dar red inalámbrica, y segmentar la red no es un requerimiento, entonces este tipo de puntos de acceso son una interesante alternativa. Si se deseara habilitar distintos niveles de acceso entre los usuarios, el uso del esquema con *cortafuegos dinámico* resulta una alternativa, pero, se tendrá que sacrificar parte de la seguridad del sistema, ya que la separación de los usuarios no sería hasta después del cortafuego dinámico. Aquí es importante el uso de cortafuegos en cada cliente, como también que los clientes utilicen protocolos seguros, como *https*, *pops*, *ssh*, etc.

Bibliografía

[1] http://grouper.ieee.org/groups/802/11/
[2] S. Fluhrer, I. Mantin, A. Shamir , "Weaknesses in the Key Scheduling Algorithm of RC4"
[3] Wireless VPN Performance Test, http://www.scd.ucar.edu/nets/projects/wireless/performance.tests.vpn.html
[4] IEEE Standard 802.11i/D7.0, "Draft Amendment to STANDARD FOR Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements", October 2003
[5] http://www.open1x.org/
[6] http://www.freeradius.org/
[7] http://nocat.net

Reseña biográfica

Carlos Gaule Pantoja es alumno de último semestre de Ingeniería Civil Electrónica en la Universidad Técnica Federico Santa María. Este trabajo esta basado en su trabajo de memoria "Seguridad en redes Inalámbricas".

Agustín J. González obtuvo el título de Ingeniero Civil Electrónico y un magíster en electrónica en la Universidad Técnica Federico Santa María. En 1997 y 2000 obtuvo un master y luego el doctorado en Computer Science en la Old Dominion University, EEUU. Actualmente se desempeña como profesor asistente del Departamento de Electrónica de la UTFSM.