UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

"ARQUITECTURA DE SEGURIDAD DE LA RED INALAMBRICA UNIVERSITARIA"

I N F O R M E

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A :

E D U A R D O E S P I N A G A R C I A

AVAL DE TITULACION: ING. ROBERTO RODRIGUEZ HERNANDEZ

MEXICO 2006

ÍNDICE

Índice de figuras

Índice de tablas

1. Objetivo

A partir de la iniciativa de la Universidad para dotar al campus de Ciudad Universitaria de una red inalámbrica se hizo evidente la necesidad de considerar la seguridad en cómputo desde la concepción misma del proyecto, por lo que el Departamento de Seguridad en Cómputo (DSC) de la UNAM adquirió la responsabilidad de aportar al proyecto los mecanismos que garantizaran una operación de la red que fuera segura y a la vez eficiente.

Como integrante del Departamento de Seguridad en Cómputo (DSC), en el cual laboro desde el año 2001, he participado en diversos proyectos universitarios relacionados a la seguridad de los sistemas y las redes que forman parte de la infraestructura de nuestra Máxima Casa de Estudios. Así, en Marzo de 2005 me integré al equipo de trabajo encargado de hacer de la red inalámbrica una realidad, a cargo del diseño de la arquitectura de seguridad de ésta.

Las actividades que llevé a cabo incluyeron la creación de las políticas de uso aceptable, las políticas de monitoreo, el análisis de riesgos, mapeo de redes inalámbricas, la selección del esquema de autenticación y control de acceso y el diseño y ejecución del protocolo de pruebas de seguridad a los diversos fabricantes de soluciones de conectividad inalámbrica.

El objetivo de las actividades que realicé en el periodo comprendido de Marzo de 2005 hasta Mayo de 2006 fue brindar una red segura y confiable a la Universidad por medio de un diseño acorde a las necesidades de la comunidad y también a las amenazas existentes que podrían poner en riesgo su operación.

1. Introducción

La Universidad Nacional Autónoma de México interesada en brindar a la comunidad universitaria tecnologías de vanguardia que apoyen las labores sustantivas propias de la Universidad como la investigación y la docencia, pone a disposición de su comunidad la Red Inalámbrica Universitaria (RIU), que permite el acceso a Internet desde distintas áreas de la Ciudad Universitaria a través de dispositivos móviles.

La RIU tiene cobertura en escuelas, facultades, institutos, centros de investigación, bibliotecas, recintos culturales y áreas de congregación de estudiantes e investigadores en Ciudad Universitaria.

Los servicios que se ofrecen en su primera etapa son:

- Acceso a la red para navegación por Internet.
- Acceso a la red para consulta de correo electrónico bajo interfases *web*.
- Asesoría para la conexión y configuración de dispositivos móviles.

3. Desarrollo

3.1. ¿Qué es la RIU?

La Red Inalámbrica Universitaria es una red de puntos de acceso (APs por sus siglas en inglés) instalados a lo largo de Ciudad Universitaria que basan su funcionamiento en los protocolos de comunicación 802.11a, 802.11g y 802.11b ó Wi-Fi. La RIU es un complemento de la red cableada RedUNAM que permite el acceso a la Internet proporcionando conexión móvil para la comunidad estudiantil y académica universitaria.

3.1.1. Su objetivo

La RIU tiene por objetivo proveer acceso a la Internet y sus aplicaciones a través del campus universitario como complemento a la RedUNAM, permitiendo así movilidad y mayor flexibilidad a sus usuarios.

3.1.2. Su alcance

Este proyecto de la red inalámbrica está planteado para dar cobertura inicialmente a las escuelas, facultades, institutos, centros de investigación, bibliotecas, recintos culturales y áreas de congregación de estudiantes e investigadores universitarios en la Ciudad Universitaria e irá creciendo conforme la demanda y servicios lo soliciten.

3.1.3. Su Infraestructura

La red está compuesta por diversos puntos de acceso, mismos que complementan a la red alambrada RedUNAM para extender la conectividad de la misma.

Cada una de las dependencias universitarias está provista con un número de APs que cubren áreas como auditorios, pasillos, bibliotecas, cafeterías, etc.

Los APs cuentan con una administración, control y monitoreo de forma centralizada y por sus características no pueden ser activados en otra red que no sea compatible con la marca de equipo de control central, el cual es específico para este fin.

En cuanto a comunicación los APs soportan los estándares 802.11 a, b y g.

Para seguridad la red soporta el protocolo de acceso inalámbrico protegido (WPA[1] por sus siglas en inglés). Los sistemas operativos de los dispositivos soportados son Windows XP en adelante, Macintosh y Linux

[1] Wireless Protected Access

3.2. Antecedentes de seguridad

Existen varias razones por las cuales la seguridad de la RIU fue un punto a considerar desde su planeación:

1. Las redes locales se han ido interconectando entre sí hasta formar redes de redes como Internet, enlazando usuarios con distintos perfiles y distintos intereses.
2. Los medios inalámbricos son, por naturaleza, susceptibles a interferencias, captura de la comunicación, etc.

En primer lugar, hemos visto una evolución a favor de la popularización de los medios electrónicos; recordemos que Internet fue inicialmente un proyecto con fines militares iniciado por DARPA[2] en 1969 y posteriormente se extendió hacia las universidades y centros de investigación en Estados Unidos.

En la actualidad la mayoría de usuarios de Internet, no está conformada por científicos ni militares estadounidenses, sino por un conglomerado de razas, edades, religiones, ideologías políticas, etc., que matizan tanto los intereses de los usuarios, como sus actividades dentro de la red. Dichas actividades pueden perseguir, en alguna medida, fines políticos, económicos o lúdicos que afecten a otros usuarios o a la misma infraestructura de la red.

En segundo lugar, las comunicaciones por medios no guiados, como las redes inalámbricas, presentan debilidades en su estructura derivadas de su propia naturaleza:

1. Susceptibles a interferencias electromagnéticas (otros equipos funcionando en la misma frecuencia, actividad solar, condiciones climáticas).
2. Pueden ser capturados por cualquier dispositivo habilitado para “escuchar” en la misma frecuencia.
3. Superan los límites físicos establecidos en una red cableada, llegando a grandes distancias.

La Universidad ha sufrido diversos ataques electrónicos en la historia de RedUNAM, uno de los más importantes se registró en 1993 contra la supercomputadora CRAY YMP, ubicada en la DGSCA en ese entonces.

El 10 de Julio de 1993 fue detectada una intrusión en la supercomputadora Cray que involucró otros equipos de la DGSCA y que, tras una exhaustiva investigación, se determinó que el ataque había sido originado dentro de la misma UNAM, en el Instituto de Ciencias Nucleares.

A raíz de este incidente se fundó el Equipo de Seguridad en Cómputo (ESC) de la UNAM, cuya función principal era atender las necesidades de seguridad de la UNAM, difundir la cultura de la seguridad en cómputo y ayudar a la comunidad universitaria ante cualquier eventualidad como la experimentada.

[2] DARPA es la Agencia de Investigación de Proyectos Avanzados de Defensa de los Estados Unidos de América

Este incidente y la seguridad que se implementó en consecuencia fueron detallados por Diego Zamboni en su tesis *"Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix"* [6].

A partir de la creación del ESC en 1994 se empezó a crear conciencia de las implicaciones de no atender a la seguridad en cómputo y empezaron a formarse foros y eventos de difusión que involucraron a todos los responsables de equipos y centros de cómputo de la UNAM; nacieron entonces la lista *GASU*[3] y sus seminarios, el Día Internacional de la Seguridad en Cómputo (*DISC*[4]).

Las diversas etapas de la evolución del ESC se listan a continuación:

- Equipo de Seguridad en Cómputo (ESC) 1994-1995
- Área de Seguridad en Cómputo (ASC) 1995-2000
- Departamento de Seguridad en Cómputo (DSC) 2000 a la fecha
- Equipo de respuesta a incidentes (UNAM-CERT) 2001 a la fecha

Actualmente, el Departamento de Seguridad en Cómputo tiene la siguiente misión:

Para con nuestra Universidad:

* Proporcionar servicios de asesoría y atención a incidentes en materia de seguridad informática a cada una de sus entidades que la conforman, satisfaciendo sus necesidades en base a la capacidad tecnológica que se disponga.

Para con la comunidad de usuarios de Internet:

* Proporcionar información clara, precisa y objetiva de los problemas de seguridad informática a los cuales se enfrentan cotidianamente, así como auxiliar en la solución de estos problemas.

Para con nuestros Académicos:

* Proporcionar las herramientas tecnológicas y el entorno adecuado para que desarrollen sus potenciales personales y profesionales.

De esta forma el Departamento de Seguridad en Cómputo / UNAM-CERT se ha vuelto un organismo reconocido a nivel internacional, formando parte de diversas agrupaciones mundiales en torno a la seguridad informática, entre las que sobresalen:

[3] Para más información se puede consultar http://www.seguridad.unam.mx/listas/gasu/
[4] La información puede ser consultada en http://www.disc.unam.mx/

1. FIRST[5] (Forum of Incident Response and Security Teams)
2. Red CLARA[6] (Cooperación Latino Americana de Redes Avanzadas)
3. APWG
4. Cymru
5. LACNIC

Así, con la importancia de la seguridad en cómputo en pleno auge y contando con un departamento especializado en la materia, la DGSCA incluyó al DSC/UNAM-CERT en todas las etapas de desarrollo de la RIU.

3.3. Requerimientos de seguridad de la RIU

Una de las tareas más importantes para establecer los requerimientos de seguridad de una organización es el llamado "análisis de riesgos".

La seguridad en cómputo tiene un costo en recursos (humanos, económicos, de tiempo), por lo cual, no siempre es asequible tener lo último ni lo más caro; en determinados casos el costo de la seguridad puede llegar a superar el costo de pérdida de lo que estamos protegiendo, por lo cual es importante definir los límites o rangos sobre los cuales se trabajará.

El análisis de riesgos comprendió diversos puntos a considerar:

1. Mapeo de redes inalámbricas existentes en CU y su periferia
2. Evaluación de los riesgos asociados a los diversos modelos de seguridad en redes inalámbricas

3.3.1. Mapeo de redes inalámbricas.

El objetivo de esta etapa fue detectar las redes inalámbricas existentes en Ciudad Universitaria, ya sea porque sus puntos de acceso están instalados dentro del campus o en la periferia de éste (puntos de acceso personales o de otras organizaciones).

El mapeo de redes o wardriving[7] lo realicé en vehículo utilizando una laptop con el sistema operativo Linux Debian[8] Sarge y los siguientes componentes (véase figura 1):

1. Tarjeta inalámbrica Orinoco Silver
2. Antena externa omnidireccional de 5dBi
3. GPS[9] Garmin eTrex
4. Software: Kismet[10], GPSd[11]

[5] Para mayor información consultar http://www.first.org
[6] Para más información se puede consultar http://www.redclara.net
[7] Wardriving es el nombre utilizado por hackers para referirse a este tipo de mapeo de redes
[8] http://www.debian.org
[9] Sistema de posicionamiento global
[10] http://www.kismetwireless.net
[11] http://gpsd.berlios.de/

Figura 1. Equipo utilizado para el mapeo de redes

La importancia de este estudio radica en que el ancho de banda disponible para las redes del tipo 802.11a/b/g está ubicado en una frecuencia no regulada, limitada, susceptible a interferencias y de uso creciente y desordenado entre la comunidad universitaria; por lo cual el conocer la ubicación y número de las redes existentes ayudó a conocer la disponibilidad de recursos y la problemática a la que se puede enfrentar la RIU.

Para entender mejor las implicaciones de la convivencia entre redes inalámbricas, es necesario conocer algunas de las características principales del protocolo 802.11a/b/g[12] (véase tabla 1):

	802.11a	802.11b	802.11g
Frecuencia de operación	5 GHz	2.4 GHz	2.4 GHz
Velocidad estándar	6 a 54 Mbps	1 a 11 Mbps	6 a 54 Mbps
Canales disponibles	12	11	11
Modulación	OFDM	CCK[13]	OFDM[14]
Alcance[15]	20 a 50 m.	35 a 180 m.	20 a 50 m.

Tabla 1. Comparativa de las variantes del protocolo 802.11

De la tabla anterior hay varias consideraciones importantes:

- Solamente hay 11 canales disponibles para ser usados de forma legal en México (en países como Japón hay 14 canales disponibles).

- De los 11 canales disponibles, solamente 3 no se traslapan (canales 1,6 y 11).

[12] El sitio oficial con el estándar puede ser consultado en http://www.ieee802.org/11/
[13] CCK es un esquema de modulación utilizado en redes inalámbricas, para mayor información consultar http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci996605,00.html
[14] http://en.wikipedia.org/wiki/OFDM
[15] Alcance según el fabricante de tarjetas inalámbricas Trend, para más información consultar http://www.trendnet.com/products/TEW-401PCplus.htm

- La velocidad teórica puede verse disminuida hasta en un 30% en ambientes reales.

- El alcance de la red (medido desde un punto de acceso hasta un cliente) varía por diversos factores como son: clima, objetos ubicados entre los dos puntos (árboles, paredes) y otros dispositivos que funcionan en la misma frecuencia como el protocolo bluetooth o hasta un horno de microondas estándar.

Estos puntos destacan en nuestro análisis de riesgos de seguridad en tanto que una de las características de un sistema seguro es la *disponibilidad*; entre más redes existan en un área geográfica delimitada más será la competencia por el medio y en consecuencia el ancho de banda y la calidad de servicio se verán disminuidos hasta un punto extremo de colapsar el servicio.

En la figura 2 se muestran las redes que fueron detectadas en un recorrido realizado por Ciudad Universitaria, se señala con círculos la localización aproximada de las redes protegidas con cifrado y sin protección.

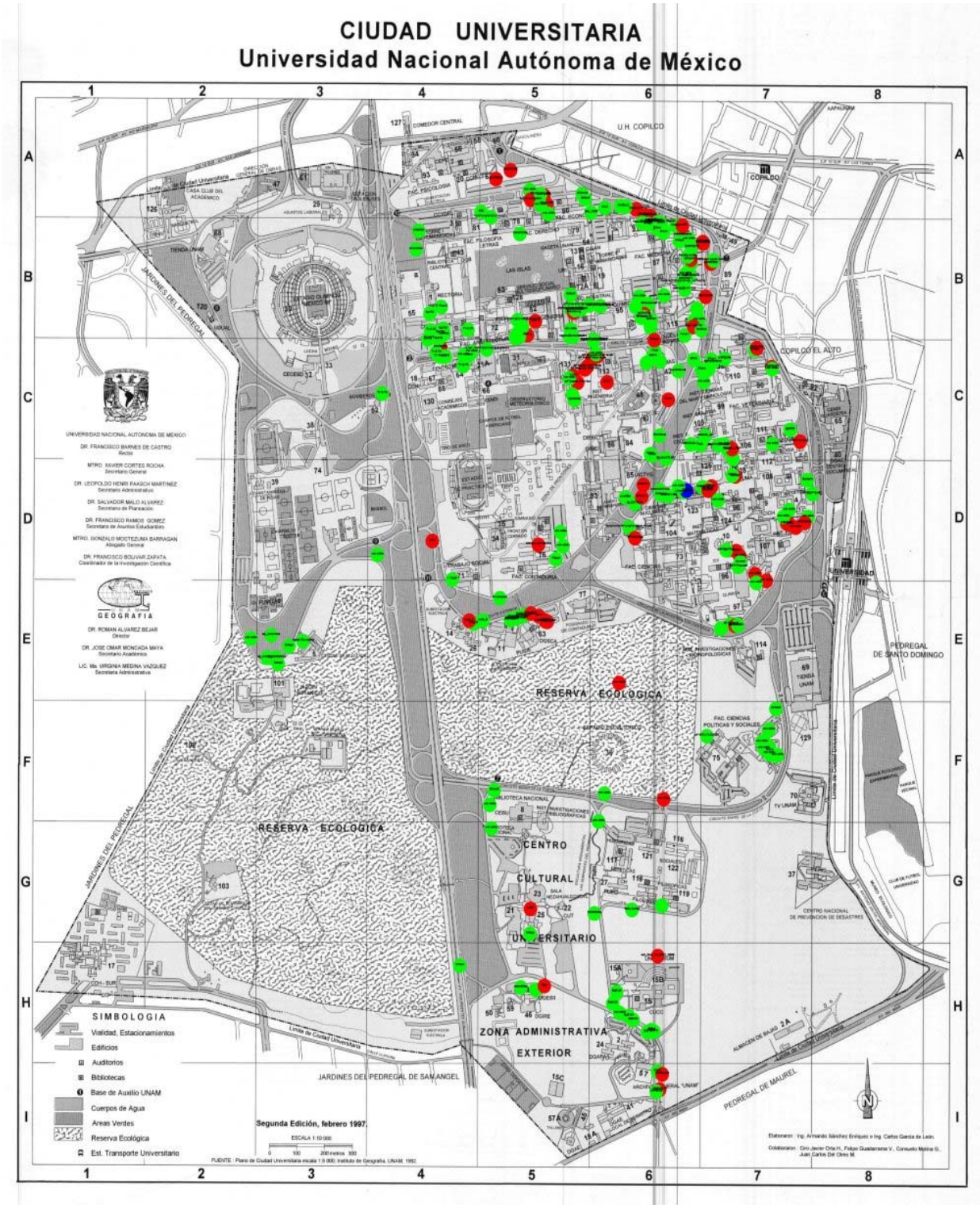


Figura 2. Resultado de mapeo a Campus CU - 27 de Marzo de 2005

En la figura 3 se muestra la cobertura aproximada de las diversas redes identificadas, la señal generada por estas redes puede interferir con la RIU.

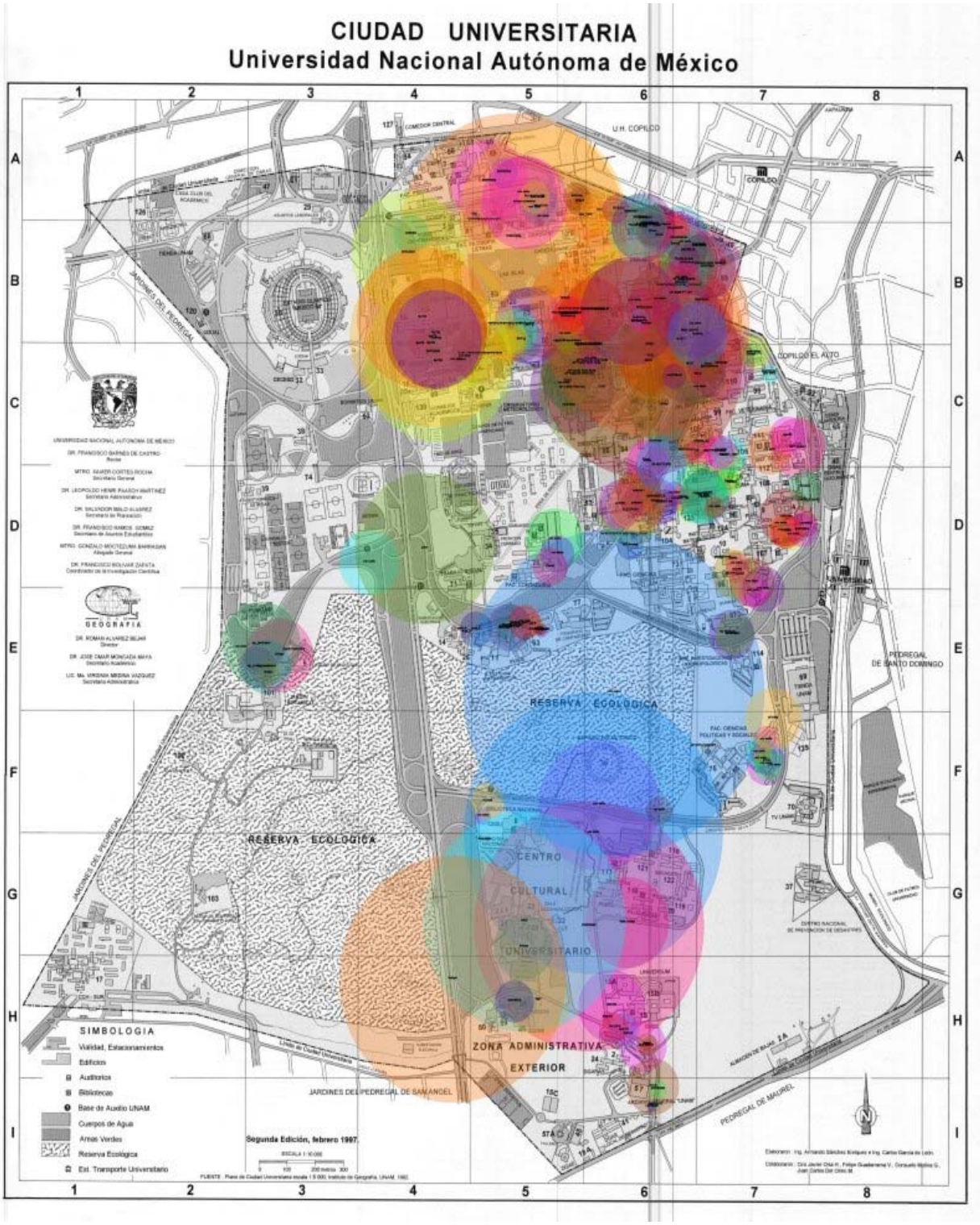


Figura 3. Cobertura de redes inalámbricas en Campus CU - 27 de Marzo de 2005

Se detectaron 278 redes en todo el campus. La mayoría de estas redes se distribuyen en los edificios de diversas dependencias de la UNAM, sin embargo también se detectaron redes de amplia cobertura en todo el campus y que tienen su origen fuera de éste.

El resumen de las redes detectadas en el mapeo se muestra en la tabla 2.

Fecha del mapeo	31 Marzo 2005 16:32:31
Total de redes	278
Total de redes con WEP	75
Total de redes sin WEP	203
% de redes con WEP	26.9%
Total de redes con configuración default	8
Total de clientes	920

Tabla 2. Resumen de redes detectadas en CU

Los resultados de este mapeo revelaron un importante número de redes inalámbricas existentes (278) en el Campus de Ciudad Universitaria que no se encuentran reguladas y que en muchos casos son incompatibles entre ellas.

Así mismo se detectó que solamente el 26.9% de las redes utilizaba algún mecanismo de seguridad y las restantes estaban abiertas a diversos ataques; por último se detectaron 8 redes que podían ser controladas por cualquier persona sin autorización.

3.3.2. Riesgos asociados a diversos modelos de seguridad en redes inalámbricas.

En las redes inalámbricas 802.11 existen diversos mecanismos de seguridad que permiten en mayor o menor medida establecer controles de acceso y autenticación, estos mecanismos han sido propuestos por diversos fabricantes y por organizaciones vinculadas a la seguridad en cómputo.

Para conocer las fortalezas y debilidades de cada uno de los mecanismos disponibles al momento del estudio se recurrió a establecer un laboratorio de pruebas en el DSC/UNAM-CERT. Existe documentación con respecto a las debilidades de ciertos mecanismos y los ataques que pueden vulnerarlos, a continuación se presenta una lista de los mecanismos revisados:

WEP

El mecanismo de seguridad WEP (Wired Equivalent Privacy), utilizado en los primeros dispositivos inalámbricos 802.11, enfrentó la realidad de su ineficaz diseño en el 2001 en un documento [2] que demostraba diversas vulnerabilidades presentes en su implementación.

Todas las características deseables en un sistema seguro son comprometidas bajo el funcionamiento de WEP:

- El cifrado utilizado es común para todos los usuarios, por lo cual no hay confidencialidad de la información, todos los usuarios pueden ver el tráfico de todos los demás usuarios utilizando un analizador de protocolos; en el mejor de los casos únicamente los usuarios de la RIU podrían espiar el tráfico de la red, en el peor cualquier persona con una laptop lo podría llevar a cabo.

- La información también puede ser modificada y reenviada al destinatario original, por lo cual no se puede asegurar que lo que recibe es lo que originalmente le enviaron.

- Bajo el esquema WEP de autenticación es necesario recurrir a un portal cautivo de autenticación. Para poder acceder a dicho portal se requiere asociar al usuario a la red para el intercambio de credenciales, lo cual implica que, aún sin haberse autenticado obtiene acceso a la red y puede iniciar actividades hostiles.

- Desde el punto de vista de operación del servicio se vuelve muy difícil cambiar la llave WEP de la red, dado que se requiere dar a conocer a cada usuario la nueva llave o no podrá acceder al servicio.

- La propagación de código malicioso y de ataques es fácil en el esquema WEP, los gusanos pueden replicarse fácilmente aprovechando el medio compartido, en términos reales equivale a que todos los usuarios se conectaran entre sí, nada impide el interferir con otra comunicación.

Las herramientas que permiten vulnerar el esquema WEP se encuentran disponibles en una gran variedad de páginas[16] web al alcance de cualquier usuario.

Las ventajas de WEP incluyen:

- Facilidad de uso. Los sistemas operativos desde finales de los 90s incluyen una configuración sencilla para el cifrado WEP.

- Compatibilidad. WEP es compatible con la mayoría de tarjetas existentes hoy en día y con las primeras tarjetas fabricadas.

En resumen, WEP agrega riesgos críticos a la operación de la RIU, aunque proporciona facilidad de uso al usuario final omite las mejores prácticas recomendadas para una red inalámbrica.

WPA

El estándar se divide en dos categorías WPA-PSK (uso casero y para pequeñas oficinas) y WPA Radius pensado para organizaciones con una gran cantidad de usuarios.

WPA (Wireless Protected Access) es un estándar de seguridad basado en la norma IEEE 802.11i, fue diseñado pensando en solucionar todos los problemas que fueron identificados en WEP y aprovechando el hardware existente, por lo que una cantidad importante de hardware viejo puede ser actualizado para cumplir con el estándar WPA.

[16] http://www.packetstormsecurity.org

WPA-PSK

WPA-PSK proporciona privacidad a los usuarios de la WLAN, puesto que se genera un canal cifrado independiente para cada uno de ellos. La llave de acceso (PSK) se proporciona a los usuarios antes de conectarse a la red (véase figura 4). Esto puede ser de forma escrita, telefónica, etc.

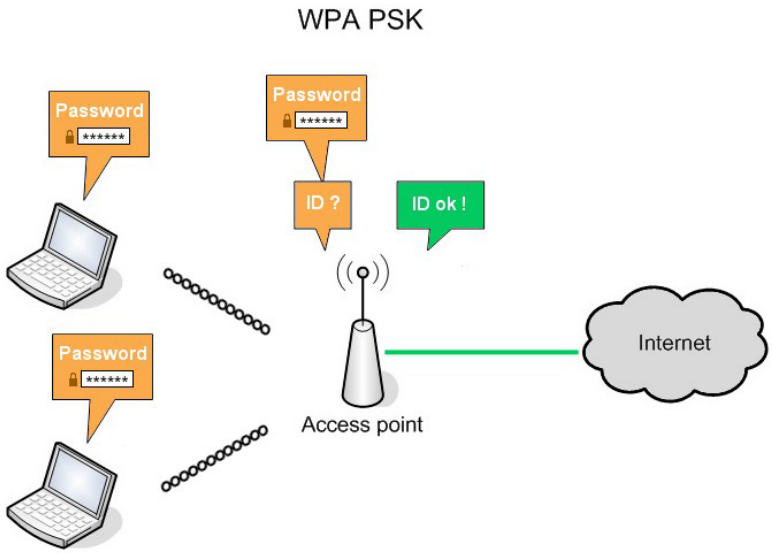


Figura 4. Configuración de red con el modelo WPA-PSK

Riesgos asociados a WPA-PSK:

- La llave utilizada para cifrar es común para todos los usuarios de la red, aunque representa un avance respecto a WEP, dado que el canal de comunicación está cifrado individualmente.

- WPA-PSK no proporciona control de acceso, cualquier usuario conociendo la llave (PSK) puede asociarse a la red.

- La forma de distribución de la llave PSK representa un problema logístico similar al de distribuir una llave WEP, puede volverse impráctico actualizar la llave de acceso a la red.

- El mecanismo se puede vulnerar por medio de un ataque de fuerza bruta fuera de línea [5]. Bajo este ataque un intruso sólo requiere grabar el inicio de sesión de un usuario en la red y posteriormente atacarlo en un equipo poderoso, limitando el tiempo de ruptura de la contraseña a unos cuantos minutos en un caso extremo.

- Captura de tráfico es posible por medio del ataque conocido como ARP cache poisoning[17] en diversos fabricantes.

[17] Para mayor información consultar http://www.webopedia.com/TERM/A/ARP_spoofing.html

Las ventajas de WPA son:

- Facilidad de instalación. En pequeñas oficinas o en el hogar es fácilmente configurable.

- Confidencialidad. Cada usuario cuenta con una llave de cifrado temporal única para cada usuario de la red.

WPA Radius

WPA soporta, en su versión fuerte, autenticación por medio del estándar 802.1x que se encuentra implementado en los servidores de autenticación Radius.

Se requiere un certificado x.509[18] del lado del servidor RADIUS. Los clientes sólo requieren un nombre de usuario y password para acceder a la red (véase figura 5).

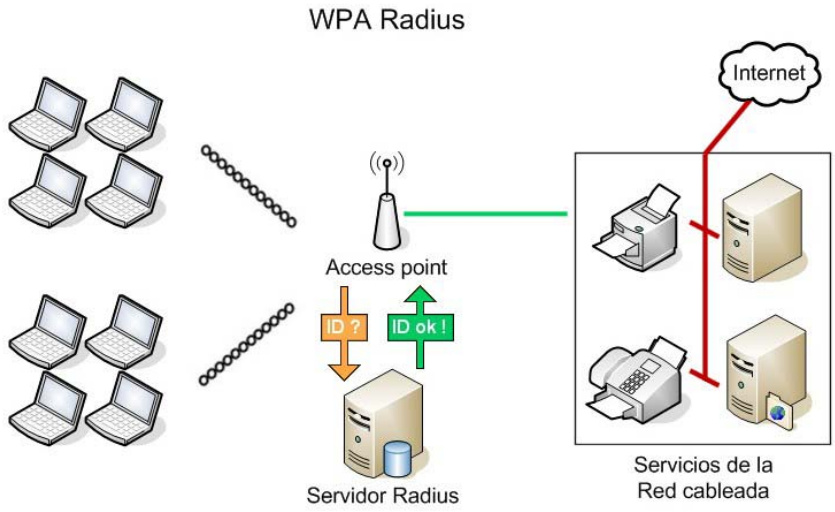


Figura 5. Configuración de red con el modelo WPA Radius

Los riesgos asociados a este esquema son los siguientes:

- El esquema es comprometido cuando un login/password es obtenido por un intruso. En términos prácticos esto sólo podría ser obtenido directamente del usuario o con un capturador de passwords instalado en el equipo víctima o engañando al usuario para que la revele.

- El usuario víctima puede ser engañado para conectarse a una red falsa pero muy similar a la auténtica para robar sus credenciales (ataque de evil twin). Este riesgo se mitiga utilizando un certificado x.509 firmado por una autoridad como Verisign o Thawte.

- La captura de tráfico es posible por medio del ataque conocido como ARP cache poisoning con diversos fabricantes.

[18] Los certificados de este tipo son utilizados comúnmente en banca electrónica en Internet http://en.wikipedia.org/wiki/X.509

- Existen otros riesgos asociados a cada subsistema de autenticación 802.1x que se analiza más adelante en *Mecanismos de control*.

WPA con Radius tiene las siguientes ventajas:

- Fácil administración de la red. Debido al uso de llaves dinámicas en todo momento, se pueden distribuir llaves de cifrado nuevas sin intervención de los usuarios.

- Nivel de seguridad. Los mecanismos de autenticación y auditoria son de los más fuertes hoy en día.

También se identificaron otros riesgos, independientes al mecanismo de autenticación y control de acceso.

- Transporte de la información del punto de acceso inalámbrico al ruteador. Este riesgo existe porque la información es transportada por red cableada que viaja por diversos switches, ruteadores y otros equipos de interconexión que no cumplen necesariamente con estándares de cifrado, por lo que la información podría ser capturada en tránsito por un intruso con capacidad de controlar al menos un equipo en la ruta trazada.

- Condiciones climáticas. La humedad, la lluvia y otros fenómenos naturales pueden degradar la calidad del enlace y poner en peligro su disponibilidad.

WEP	WPA
Confidencialidad. No es garantizada. El cifrado es fácil de romper. Llave común de cifrado para todos los usuarios, captura de tráfico trivial.	Confidencialidad. Cada usuario recibe una llave única dinámica. No es susceptible al ataque estadístico. Cada usuario sólo puede ver su propio tráfico.
Integridad. La información en tránsito puede ser modificada por un atacante.	Cuenta con mecanismos para evitar la duplicidad de datos y su modificación.
Control de acceso. Se utiliza un portal de autenticación que puede ser reemplazado por uno falso.	802.1x implementa diversos métodos de autenticación que usan certificados del lado del servidor o del cliente también.
Propagación de gusanos es fácil en un medio totalmente compartido.	La propagación de código malicioso está limitada al aislar a los usuarios entre sí.
Un atacante puede utilizar ancho de banda de la red sin estar autenticado.	Un atacante no puede hacer uso de la red hasta estar debidamente autenticado.
Facilidad de administración. Es difícil desplegar una llave nueva al usuario.	La llave nueva para cada sesión es suministrada automáticamente sin intervención del usuario.
Facilidad de instalación al primer uso, necesidad de ingresar login y password cada vez que se haga uso de la red.	Relativa inconveniencia al configurar por primera vez, el equipo queda listo para autenticarse automáticamente en siguientes ocasiones.
WEP fue declarado estándar sin haber sido revisado exhaustivamente.	WPA ha sido revisado por multitud de expertos para mitigar los problemas de WEP.
Estándar que es obsoleto.	Estándar que es de facto en la industria.

Tabla 3. Comparativa entre WEP y WPA

- Negación de servicio. Existen diversos ataques contra la infraestructura de una red inalámbrica bien documentados[19]. Algunos van desde saturar la frecuencia de radiofrecuencia utilizada por determinada red (RF jamming) o generar tramas de desconexión falsas que aparentan ser generadas desde los puntos de acceso a la red y que los clientes obedecen por falta de mecanismos para validar su autenticidad.

WPA2

WPA2 es un estándar basado en WPA pero que implementa un cifrado más fuerte conocido como AES. Es una alternativa que seguramente reemplazará a WPA en el mediano plazo, pero que requiere del uso de tarjetas de red totalmente nuevas por lo que no pueden actualizarse los dispositivos anteriores (véase tabla 4). La infraestructura de la RIU soporta la implementación de WPA2.

Presenta los mismos riesgos asociados que WPA con Radius.

Esquema de seguridad	Cifrado	Longitud de llave	Integridad de la comunicación
WEP	RC4	64/128 bits	No
WPA-PSK	TKIP	128 bits	Si
WPA Radius	TKIP	128 bits	Si
WPA2	AES	128 bits	Si

Tabla 4. Comparativa entre WEP, WPA y WPA2

Después de evaluar estos riesgos se determinó que el mecanismo más seguro, con más soporte y facilidad de mantenimiento era WPA Radius.

3.4. Arquitectura de seguridad

Las potenciales amenazas a las redes inalámbricas son numerosas, ataques de negación de servicio, robo de sesiones y captura de tráfico son sólo algunas de ellas. A pesar de que las redes inalámbricas son susceptibles de muchos ataques tradicionales existentes en redes cableadas, también existen ataques más destructivos enfocados a las redes inalámbricas.

Uno de los principales problemas es la naturaleza abierta de las redes Wi-Fi, debido a su propagación que supera los límites físicos de la organización es casi imposible tener un control de hasta donde llegará la señal. Esto lleva a una situación en la cual, al contrario de las redes cableadas, un intruso puede tener acceso a la información desde una ubicación geográfica no controlada.

[19] Los ataques pueden ser consultados en http://sysnet.ucsd.edu/~bellardo/pubs/usenix-sec03-80211dos-slides.pdf

Las redes Wi-Fi también pueden llegar a ser puertas traseras de las redes cableadas. Una organización puede invertir mucho dinero en dispositivos de monitoreo y control como lo son firewalls, detectores de intrusos, redes privadas virtuales, etc.; sin embargo, con un simple punto de acceso colocado de forma descuidada en la red se podría vulnerar su seguridad y abrir un punto de acceso a toda la infraestructura, volviendo inservibles los esquemas establecidos.

Una política de la red inalámbrica puede ayudar a combatir estas amenazas, y si dicha política se desarrolla en los inicios del proyecto es mucho más efectiva, como lo menciona Jamil Farshchi [1] en uno de sus artículos en Securityfocus[20].

El desarrollo de la política debe comenzar en las etapas iniciales de la iniciativa para desplegar una red inalámbrica. Los beneficios de identificar las necesidades de seguridad en el proceso de análisis son inmensos: menor costo, fácil implementación y seguridad desde el inicio de la implementación. Cuando, por el contrario, se desea agregar seguridad después de la implementación se pueden tener costos mayores al adquirir nuevo equipo que satisfaga carencias de lo implementado; en otros casos se requiere incluso rediseñar la red física o lógicamente o peor aún, tal vez la red ya haya sufrido algún incidente de seguridad.

Si la red ha sido operada sin seguridad, la política todavía proporcionará numerosos beneficios, aunque a un costo mayor del que se habría tenido si se consideraba desde un principio.

3.4.1. Beneficios de una política para la red inalámbrica

Una política no elimina las amenazas en las redes 802.11, pero ayuda a crear un ambiente proactivo donde las herramientas, métodos y procedimientos están listos para disuadir a los atacantes y combatir efectivamente dichas amenazas. Esta política servirá como guía para futuras implementaciones de redes inalámbricas, asegurando que los esfuerzos de expansión sean uniformes y compatibles con las implementaciones existentes.

3.4.2. Políticas de operación de la RIU

Los elementos que se consideraron para definir estas políticas[21] fueron los siguientes:

- Propósito de las políticas. Se deben involucrar los objetivos de la red inalámbrica para que las políticas hagan cumplir dichos objetivos.

- Mantenimiento de la infraestructura de la RIU. La finalidad de este punto es definir los lineamientos bajo los cuales se administrará la configuración de la

[20] El artículo puede ser consultado en http://www.securityfocus.com/infocus/1732
[21] Las políticas de operación de la RIU pueden consultarse en el apéndice E

red, es decir, las actualizaciones de software y hardware, alta y baja de equipos, etc.

- Sobre la interferencia entre elementos de la RIU. Todo el equipo que opere intencional o inadvertidamente en el espectro utilizado por la red inalámbrica debe ser instalado y configurado para evitar interferencias con otros elementos de la RIU. Las prioridades para solucionar conflictos de uso de frecuencia según su aplicación son las siguientes:

    1. Equipo de seguridad
    2. Investigación
    3. Enseñanza
    4. Administración
    5. Acceso público
    6. Personal

- Control de puntos de acceso (AP) no autorizados. Los APs no autorizados representan un obstáculo para el desempeño eficiente del servicio ofrecido por la red inalámbrica de la UNAM, debido a su posible interferencia en la frecuencia de radio utilizada; por lo que al menos se requiere que los APs no autorizados funcionen en las frecuencias más altas o limiten su área de cobertura.

- Sobre la autenticación de los usuarios. Definen el comportamiento de las sesiones de los usuarios cuando se han autenticado exitosamente (por ejemplo, después de 15 minutos de inactividad se dará por terminada la sesión). También especifican las medidas que se tomarán si no se logra autenticar exitosamente un usuario después de varios intentos fallidos (inhabilitación temporal de la cuenta).

- Distribución de contraseñas. Especifica cuales serán los lineamientos para la creación de cuentas de usuario y hace referencia al procedimiento específico para entregar las cuentas y como validar los requisitos.

- Sobre la confidencialidad. Con la finalidad de evitar problemas con la confidencialidad, la red inalámbrica no debe ser usada como sustituto de la red cableada de la Universidad, no se recomienda el uso de la RIU cuando se trate de comunicaciones de carácter financiero, misión crítica, registros académicos y en general de carácter confidencial.

- Seguridad de los AP. Los APs deben estar protegidos de accesos no autorizados. Físicamente deben estar fuera del alcance de un atacante, también deben ser protegidos de robo físico.

- Sobre la disponibilidad. La disponibilidad del hardware (uptime) debe monitorearse continuamente para garantizarla acorde a los estándares de la industria de telecomunicaciones (mayor al 99%). Por otro lado la disponibilidad de la cobertura de la señal puede garantizarse a un porcentaje menor debido a los diversos factores que la afectan y que son inherentes a las comunicaciones inalámbricas.

Es importante dejar claro que, la disponibilidad de hardware se refiere a que los equipos estén listos para prestar el servicio, y la disponibilidad de la cobertura se refiere al alcance y propagación de la señal en determinada zona geográfica.

- Integridad de la red. Se debe garantizar que los elementos de la RIU estén disponibles para cumplir su función dentro de la red.

- Monitoreo de la red. Se deben implementar mecanismos que permitan el monitoreo constante de los diversos componentes de la RIU, también deberán estar sujetos a auditorias aleatorias y externas a la operación. Se sugiere que se realice una auditoria cada semestre.

- Respuesta a incidentes. El Departamento de Seguridad en Cómputo/UNAM-CERT iniciará un reporte de incidente cuando sea solicitado por el Centro Operación de la Red (NOC[22]) y dará seguimiento hasta solucionar el problema; sólo si el problema ha sido erradicado entonces el DSC/UNAM-CERT dará por cerrado el reporte de incidente.

- Respaldos. Se debe garantizar la restauración de los sistemas de software y las bases de datos que forman parte de la infraestructura de la RIU en caso de un incidente que corrompa la integridad de ésta.

- Responsabilidades. Definen cuales son las obligaciones de cada una de las partes involucradas en la operación y prestación del servicio, en este caso el NOC y el DSC de la UNAM.

3.4.3. Políticas de uso aceptable

La definición de estas políticas[23] requirió revisar las políticas existentes de RedUNAM, puesto que gran parte de las aplicaciones que tendrá la red inalámbrica son similares en buena medida a las que se llevan a cabo en la red cableada de la Universidad.

Así mismo se consultaron los lineamientos sugeridos por algunas organizaciones de seguridad en cómputo reconocidas a nivel mundial y que han servido como referencia para una infinidad de universidades, empresas, etc.; dichas organizaciones son el SANS Institute[24] y el AUSCERT[25].

Los puntos que debieron definirse fueron los siguientes:

- Propósito de las políticas. Justifican su existencia con los usuarios de la red, como se mencionó previamente permiten establecer el marco de reglamentación

[22] http://www.noc.unam.mx
[23] Las políticas de uso aceptable de la RIU pueden consultarse en el apéndice D
[24] http://www.sans.org
[25] http://www.auscert.org.au/

para garantizar un servicio eficiente que permita alcanzar los objetivos de la prestación del servicio.

- Usuarios del servicio. Define a quienes aplican las políticas definidas en este documento, alumnos, profesores y académicos de la UNAM y visitantes de otras universidades.

- Horario y solicitud de servicio. Especifica en que horario se proporcionará el servicio y cuales son los mecanismos y requisitos para obtener una cuenta para uso de la RIU.

- Privacidad. Todos los elementos de la infraestructura de la RIU y la información que se transmite por ellos están sujetos a inspección y monitoreo en todo momento para garantizar el adecuado funcionamiento, para prevenir uso no autorizado y violaciones a los estatutos de seguridad, para prevenir actividad criminal y otros propósitos similares.

- Usos permitidos. Establece cuales son las aplicaciones y usos autorizados y de la misma forma determina cuales están específicamente prohibidos. Es un punto muy importante pues notifica a los usuarios de la RIU como deben comportarse en la red para promover un ambiente de trabajo óptimo que permita alcanzar los objetivos académicos establecidos.

- Sanciones. Después de establecer los usos permitidos y los prohibidos es indispensable definir las sanciones que habrá para las violaciones a las diversas reglas fijadas. Se definieron categorías de sanciones a las políticas:

    - Suspensión temporal de la cuenta. Son originadas por faltas no graves, que pueden ir desde propagación de código malicioso no intencional hasta compartir la cuenta de acceso a la RIU.

    - Suspensión definitiva de la cuenta. Se derivan de faltas graves como atentar contra la infraestructura de la RIU, actividades delictivas, conductas que atenten contra las normas aceptadas dentro de la comunidad en Internet, atacar a otros usuarios, etc.

      En este caso también aplican las sanciones contempladas por la legislación Universitaria y leyes nacionales e internacionales según sea el caso.

- Soporte del servicio. Determina cuales son las responsabilidades del NOC para prestar el servicio adecuado a la comunidad universitaria, como proporcionar la información necesaria para que los usuarios puedan hacer uso de la RIU; los usuarios también tienen responsabilidades sobre la configuración de su equipo y la instalación de herramientas de seguridad.

3.4.4. Protocolo de pruebas

El reto de la DGSCA es no sólo proveer una red más de las que actualmente ya existen en Ciudad Universitaria, sino el proveer una tecnología que además de dar el acceso inalámbrico, proteja la integridad tanto de las redes locales universitarias como de la información que es transportada en ellas. Asimismo, se establecerá una tecnología que permita de manera centralizada administrar los recursos tanto de las interfases aéreas como de las aplicaciones.

Se realizó un estudio de mercado de las empresas que ofrecían soluciones para redes inalámbricas y que son líderes a nivel mundial. Para llevar a cabo la selección de equipo, se realizó un protocolo de pruebas al que se sometieron las soluciones ofrecidas por las empresas consideradas. Se identificaron, con base en información de hojas técnicas, los principales productos que trabajan bajo un esquema de control central en administración, seguridad, gestión de recursos y autenticación de usuarios.

De acuerdo a los requerimientos que se establecieron para el diseño de la RIU y con las soluciones disponibles en el mercado se decidió que la tecnología utilizada debería cumplir con las características de la 3ª generación de redes inalámbricas[26]:

- Switch central inteligente. Recibe las tramas de 802.11 directamente de los puntos de acceso y procesa toda la información que recibe.

- Puntos de acceso ligeros (lightweight AP). Solamente son receptores de radio que reenvían las tramas de 802.11 al switch central, en consecuencia no requieren grandes capacidades de procesamiento, por lo cual se denominan ligeros.

- Seguridad de capa 2 (modelo OSI[27]), en la subcapa de control de acceso al medio [3] (MAC[28] por sus siglas en inglés) integrada en el switch central. Permite detectar ataques inalámbricos y mitigarlos.

- Movilidad en el área de cobertura. Los usuarios de la red pueden desplazarse entre los puntos de acceso sin perder la conexión.

- Manejo dinámico de frecuencias. Los puntos de acceso continuamente sensan la ocupación del ancho de banda en cada canal, cuando detectan una saturación cambian a un canal que tenga menos uso.

- Capacidad de autosanación. Se refiere al hecho de que si un punto de acceso falla en una zona geográfica, los puntos cercanos aumentan su potencia para cubrir la zona afectada.

[26] El calificador independiente Gartner ubica a Aruba en esta generación, para mayor información consultar http://www.gartner.com/DisplayDocument?doc_cd=129184
[27] OSI es el Sistema Abierto de Interconexión
[28] Medium Access Control

- Ubicación geográfica de usuarios. El switch central recolecta la información de usuarios conectados a través de los puntos de acceso, con lo cual puede generar un mapa geográfico y ubicar a cada usuario en el área de cobertura.

Con base en lo anterior, se llevó a cabo un protocolo con pruebas que detallan el comportamiento de los equipos en seguridad, administración y desempeño para la gestión centralizada de la RIU.

En la parte de seguridad, quedaron divididas las pruebas en 4 categorías:

1. Confidencialidad

- Ataque pasivo de captura de tráfico WEP. El objetivo es capturar tráfico de un cliente asociado a la red que utiliza WEP, una laptop realiza funciones de atacante y captura el tráfico que posteriormente se analiza para saber si pasó la prueba.

- Ataque pasivo de captura de tráfico WPA. La prueba es similar a la del punto anterior, pero se utiliza cifrado WPA con el algoritmo TKIP[29].

- Ataque para obtener la llave de cifrado WEP. Existe un ataque documentado contra las llaves débiles [2] de cifrado WEP. El escenario involucra una laptop que realiza una descarga de varios Megabytes (alrededor de 800) forzando el uso de las llaves débiles, mientras que un atacante captura este tráfico para realizar un criptoanálisis estadístico posterior.

- Ataque pasivo en el transporte cableado hacia el switch central. Un usuario navega web por la red inalámbrica, mientras un atacante realiza captura de tráfico en un hub conectado al punto de acceso cableado del punto de acceso.

2. Disponibilidad

- Prueba de control de ancho de banda. Su finalidad es probar la capacidad de control de ancho de banda por usuario de la red.

- Prueba de control de tráfico. Se mide la capacidad de filtrar todo el tráfico de entrada o salida hacia un cliente que no ha sido autenticado en la red.

- Ataque de negación de servicio al AP. En esta prueba se utilizan herramientas que generan tráfico masivo de solicitudes de conexión (tramas de asociación) de clientes inexistentes.

- Ataque de negación de servicio a los clientes. En este ataque se generan solicitudes de desconexión falsas (tramas deauth) pero con las direcciones legítimas de los clientes para que el AP los desconecte.

[29] Es el protocolo de integridad de llave temporal

3. Integridad

- Ataque de gemelo maligno (evil twin). Se utiliza un AP falso que utiliza los mismos identificadores de red (SSID) que la RIU para tratar de engañar a los usuarios y asociarse con ellos. Una vez que el usuario se autentica con el AP falso puede capturar su información.

- Propagación de un gusano en la red. Una laptop asociada a la red lanza un gusano para infectar a otros clientes asociados.

4. Autenticación

- Manejo de usuarios con WEP 128. Se prueba si la infraestructura redirecciona de forma automática a los clientes hacia un portal cautivo de autenticación.

- Manejo de usuarios con WPA TKIP. En esta prueba se verifica que los clientes con tarjetas de red soporten el estándar WPA TKIP, existente en la mayoría de tarjetas de modelos anteriores al estándar WPA2.

- Manejo de usuarios con WPA AES. El estándar WPA2 requiere del cifrado AES, por lo que se prueba si la infraestructura logra autenticar a los usuarios que soportan este mecanismo de seguridad.

- Autenticación de usuarios con WPA-TLS. Esta variante del estándar 802.1x implementa certificados x.509 utilizados en infraestructura de llave pública de cifrado.

- Autenticación de usuarios con WPA-PEAP. El protocolo de autenticación extensible protegido (PEAP[30] por sus siglas en inglés) utiliza un certificado x.509 del lado del servidor, se considera uno de los más seguros y cifra la comunicación de autenticación.

Después de evaluar diversos fabricantes y diversas soluciones tanto en el protocolo de seguridad como en el de administración determinamos que la mejor alternativa era Aruba Networks[31] (véase tabla 5).

[30] Protected Extensible Authentication Protocol, es uno de los protocolos de autenticación más seguros hoy en día
[31] http://www.arubanetworks.com

Pruebas realizadas	Aruba	Colubris	Foundry	Enterasys
Confidencialidad				
Ataque pasivo de captura de tráfico WEP	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
Ataque pasivo de captura de tráfico WPA	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
Ataque pasivo en el transporte cableado hacia el switch central	SI ■ NO □	SI □ NO ■	SI ■ NO □	SI ■ NO □
Disponibilidad				
Prueba de control de ancho de banda	SI ■ NO □	SI ■ NO □	SI □ NO ■	SI □ NO ■
Prueba de control de tráfico	SI ■ NO □	SI ■ NO □	SI □ NO □	SI ■ NO □
Ataque de negación de servicio	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
Integridad				
Ataque de gemelo maligno (evil twin)	SI ■ NO □	SI □ NO ■	SI ■ NO □	SI ■ NO □
Autenticación				
WEP 64 y 128	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
WPA (TKIP)	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
WPA (AES)	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
WPA TLS	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
WPA TTLS	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □
WPA PEAP	SI ■ NO □	SI ■ NO □	SI ■ NO □	SI ■ NO □

Tabla 5. Matriz de pruebas de seguridad

3.4.5. Despliegue de la RIU

El diseño de la RIU quedó definido por la topología que se muestra en la figura 6:

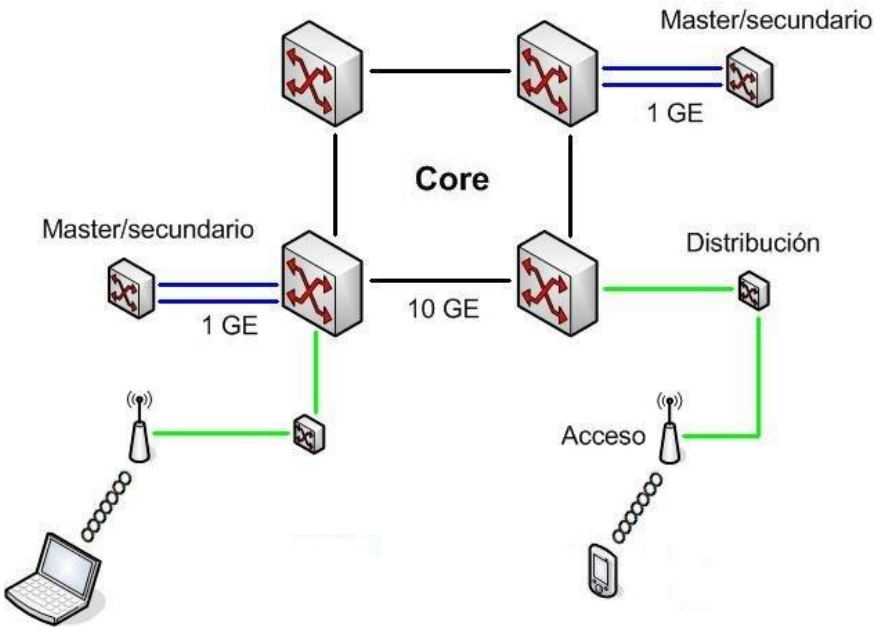


Figura 6. Configuración del Core de la RIU

La solución que cumplió los requerimientos de la RIU fue el Switch Aruba 6000, que presenta las siguientes características:

- Power over ethernet. Para alimentar a los APs sin necesidad de un contacto de corriente eléctrica.
- Operación en capa 2 y capa 3 del modelo OSI.
- Hasta 8192 usuarios simultáneos
- Hasta 512 APs
- Fuente de poder redundante
- Estándar 802.11 a, b y g
- Soporte a 802.1x
- Soporte a WPA2
- Cifrado WEP, WPA TKIP, WPA2, AES, 3DES, PEAP, TLS, TTLS.
- Certificado Wi-Fi
- Manejo inteligente de la radiofrecuencia
- Balanceo de carga
- Múltiples SSIDs por AP
- Triangulación geográfica de atacantes
- Movilidad por medio de roaming
- Calidad de servicio
- Soporte para VoIP[32]
- Soporte para Radius y LDAP
- Contramedidas de intrusión (IDS) en capa 2 del modelo OSI
- Consola de administración serial y web

Así, con los requerimientos cubiertos y con los elementos disponibles para cumplir con los objetivos de la Red Inalámbrica Universitaria, a continuación se

[32] Voz sobre IP

detallan los mecanismos utilizados para mitigar los riesgos identificados en las etapas iniciales de concepción de la RIU.

Control de acceso

Para el control de acceso a la RIU se implementó el estándar WPA con el protocolo de autenticación PEAP de 802.1x.

PEAP implementa seguridad de la capa de transporte (TLS[33] por sus siglas en inglés) en la negociación por medio de un certificado digital firmado por una autoridad por lo cual previene de un ataque de hombre en medio (MiTM[34]).

El usuario solamente requiere de un login y una contraseña como credenciales para acceder a la RIU; para evitar ser víctima de un ataque evil twin el usuario recibe un certificado firmado por Thawte Premium Server CA para cumplir con el estándar X.509[35]. Si el usuario sigue el procedimiento definido para conectarse se mitiga el riesgo de un engaño.

Es importante destacar que la empresa Thawte que firmó el certificado fue escogida de entre algunas otras como RSA y Verisign puesto que cuenta con oficinas de soporte en México y también representó la alternativa más competitiva en el aspecto económico.

PEAP está soportado en sistemas Windows, MacOS y Linux; la implementación la realizamos por medio de un servidor Radius y LDAP.

Integridad

El switch de Aruba permite monitorear el estado de los APs conectados a la RIU, con lo cual se puede saber si un punto de acceso incluso está bajo ataque.

Para garantizar la integridad de la RIU y mantenerla bajo control se definió la necesidad de contar con diversos sensores de tráfico y en particular de un dispositivo para prevenir intrusiones (IPS[36] por sus siglas en inglés) en la topología mostrada en la figura 7.

[33] Transport Layer Security
[34] En este ataque un intruso intercepta la comunicación, para mas información consultar http://en.wikipedia.org/wiki/Man_in_the_middle_attack
[35] Estándar de cifrado utilizado en transacciones bancarias en Internet http://en.wikipedia.org/wiki/X.509
[36] Intrusion Prevention System

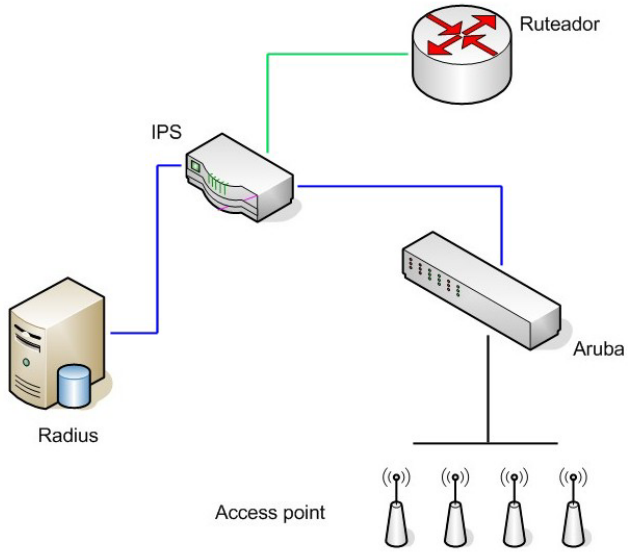


Figura 7. Sistema IPS para prevenir intrusiones

Para la selección de IPS se definió también un protocolo de pruebas y se invitó a varios fabricantes para realizar pruebas de laboratorio, las categorías principales de este protocolo fueron:

- Pruebas al motor de detección. Incluye pruebas para ataques de evasión e inserción, por ejemplo la fragmentación de paquetes IP es efectiva en muchos casos. Otra prueba muy importante en este rubro es la de los falsos positivos, eventos que son reportados como ataques y en realidad es tráfico inocuo.

  La anomalía de protocolos también forma parte de los ataques lanzados por los intrusos, por lo cual debe evaluarse.

  La habilidad de detectar un ataque nuevo es importante pues identifica un ataque por el fondo y no por la forma. Esta tecnología se basa en el uso de reconocimiento de patrones.

- Rendimiento. La capacidad de analizar información a gran velocidad es muy importante por dos razones: 1) no se debe aumentar latencia al tráfico mientras es analizado y 2) si se satura el procesador pueden pasar ataques desapercibidos.

- Administración y soporte. El IPS debe ser fácil de administrar, debe facilitar la labor del responsable del monitoreo y no dificultarla, también debe contar con las opciones necesarias para realizar un análisis a detalle de un ataque en progreso o un análisis forense.

  El soporte va enfocado a contar con las actualizaciones necesarias en forma y tiempo para disminuir el tiempo de exposición de nuevos ataques y de código malicioso.

Disponibilidad

Los riesgos evaluados fueron mitigados por los siguientes mecanismos:

- Redundancia de enlaces. Al contar con dos equipos en ubicaciones geográficas distintas se disminuye la probabilidad de que ambos fallen. Los dos equipos pueden funcionar como pasivo/activo y responder ante la falla del servidor establecido como primario.

- Autosanación. Cuando alguno de los puntos de acceso deja de funcionar, los APs cercanos aumentan su potencia de transmisión para cubrir el área sin servicio, esto se logra por medio de la administración centralizada del switch y de los algoritmos con los que cuenta para mitigar este riesgo.

- Triangulación de intrusos. Existen ataques que son difíciles de erradicar al 100%, como los de negación de servicio; en este caso los puntos de acceso distribuidos como células por todo el campus permiten triangular con exactitud de unos cuantos metros la ubicación de un equipo que esté lanzando un ataque.

  El switch de Aruba permite almacenar mapas arquitectónicos de los diferentes edificios o imágenes aéreas para gráficamente ubicar al atacante.

Confidencialidad

Para garantizar la confidencialidad de la información de los usuarios en la RIU se utilizaron varios mecanismos que funcionan en varias capas del modelo OSI.

- Aislamiento de usuarios. Para evitar la propagación de código malicioso los usuarios no pueden establecer conexiones directas con otros usuarios en el mismo punto de acceso.

- Se utiliza cifrado WPA TKIP que permite establecer un canal cifrado individual para cada usuario, por lo cual, incluso un usuario autenticado no puede capturar información de otro usuario.

  El cifrado TKIP hace uso del algoritmo RC4 de cifrado, similar a WEP pero con algunas mejores como lo son:

  - Llaves dinámicas
  - Verificación de integridad del mensaje (MIC - Message Integrity Check)

  En una etapa posterior se plantea utilizar WPA2 que reemplaza a TKIP por AES.

- Para el transporte de la información del AP al switch central se utilizan túneles con encapsulado genérico de ruteo (GRE[37] por sus siglas en inglés) que transportan el tráfico sin modificar los encabezados de los protocolos superiores; se utiliza el cifrado TKIP en dicho transporte, aún cuando un atacante tuviera la capacidad de recolectar todo el tráfico necesario para ejecutar un criptoanálisis no le serviría de nada encontrar la llave, puesto que es dinámica y no le serviría para romper el nuevo cifrado.

- Para evitar que los APs sean susceptibles de algún ataque externo se utilizan cortafuegos[38] o firewalls en las diversas dependencias donde se ubican los puntos de acceso.

[37] Generic Routing Encapsulation, encapsula tráfico para transportarlo, para mayor información consultar http://lartc.org/howto/lartc.tunnel.gre.html
[38] Cortafuegos o firewall es un dispositivo de cómputo que aísla una red privada de una pública

4. Conclusiones

El proyecto de la Red Inalámbrica Universitaria ha sido muy ambicioso desde su concepción, estableciendo sin duda una referencia en cuanto a su tamaño y su alcance.

Existe un gran panorama de tecnologías que se utilizarán en el mediano plazo y que utilizarán la RIU como plataforma, entre ellas está voz sobre IP (VoIP), la videoconferencia, clases a distancia y otras aplicaciones para las cuales está preparada la infraestructura.

El hecho de haber considerado la seguridad de la RIU desde su diseño tendrá beneficios que se reflejarán en el control de la infraestructura, la contención de daños en el caso de un incidente y un tiempo de respuesta menor.

Hemos visto a lo largo de la historia de las redes y de la seguridad en cómputo que los esquemas que un día se consideran seguros al día siguiente han sido vulnerados, razón por la cual la arquitectura de la RIU no está pensada como un sistema invulnerable, sino un sistema capaz de actualizarse de forma eficiente para responder a las amenazas del día de mañana y limitar el daño.

La proactividad en el diseño de sistemas ha sido algo por lo que el Departamento de Seguridad en Cómputo / UNAM-CERT ha pugnado desde sus inicios, es un hecho que la RIU ha iniciado bien y seguramente cumplirá con sus objetivos.

La RIU tampoco es un proyecto estático, irá transformándose según las necesidades de la comunidad Universitaria, por ello se han considerado metodologías que permiten escalar de una forma organizada las actualizaciones: entre ellas se encuentra ITIL[39].

ITIL (Information Technology Infrastructure Library) [4] agrega procesos a la operación de la RIU que permiten conocer la existencia de problemas, identificar los incidentes y programar cambios que solucionen a dichos problemas, todo en beneficio del usuario final.

Con la finalidad de mantener la información de los dispositivos de seguridad y la infraestructura actualizada es importante tener un repositorio de todos los archivos de configuración críticos y de los datos almacenados, ITIL introduce el concepto de CMDB (configuration management database), que funciona como repositorio central de la configuración de todos los elementos de configuración de la infraestructura.

Las Tecnologías de la Información cambian día con día, su dinámica representa un gran reto para las organizaciones que hacen uso de ellas, al apoyarse en ITIL se pueden afrontar los grandes retos que representa el cambio de tecnología, un caso muy representativo es el de la seguridad en redes inalámbricas.

[39] Information Technology Infrastructure Library http://www.ogc.gov.uk/index.asp?id=2261

ITIL modela los procesos sugeridos para mantener un adecuado control de la infraestructura y sobre todo para hacer más eficiente la operación y entrega de servicio de TI (en este caso, la Red Inalámbrica Universitaria, donde los clientes serían los estudiantes, investigadores, etc.), para robustecer la respuesta ante cambios futuros (que definitivamente son inevitables) y para reducir los costos asociados.

La RIU no es, sin embargo, el fin del proyecto, es en realidad el inicio de una herramienta que seguramente servirá para una infinidad de proyectos en las diversas áreas del conocimiento que se conciben y desarrollan en nuestra Universidad, donde se genera la mayor parte de la investigación científica de nuestro país. Por lo tanto, será de gran importancia facilitar el acceso a los usuarios que se apoyen en esta nueva tecnología.

Como experiencia personal puedo decir que el proyecto RIU me ha enriquecido en diversos aspectos.

Dediqué gran parte de mi trabajo a informarme sobre un gran número de aspectos de las redes, de la seguridad en cómputo y de las diversas tecnologías empleadas; la curva de aprendizaje durante el tiempo que duró el proyecto fue muy grande, consulté mucho material impreso, electrónico y en más de una ocasión recurrí a mis apuntes y mis libros de la Facultad de Ingeniería.

Gracias al renombre de nuestra Universidad los diversos fabricantes que participaron en el proyecto siempre me proporcionaron la información que solicité, incluso en aquellos casos en que la información requerida era un tanto cuanto rebuscada, en varias ocasiones tuvimos el soporte personal de ingenieros de otros países como Brasil, Colombia o Estados unidos que visitaron la UNAM.

Puedo decir con mucha satisfacción que en varias ocasiones recibí retroalimentación de parte de los fabricantes en el sentido de que nuestras pruebas eran bastante estrictas y nuestros requerimientos muy detallados, por los cuales incluso se llegaron a levantar solicitudes de funcionalidad adicional o de cambios (RFC[40] por sus siglas en inglés), particularmente para detectar ataques de negación de servicio.

Pero no todo el aprendizaje fue técnico, puesto que estuve colaborando en un grupo interdisciplinario enfocado a otros aspectos también importantes de la RIU, en particular tuve también una visión general de la administración de proyectos, que es muy importante para llevar de buena forma la realización de proyectos de ingeniería.

Como parte de la misma capacitación que la UNAM me proporcionó para el éxito del proyecto, recibí la certificación “Service Management Essentials” de ITIL, afianzando con esto la planeación de la seguridad de la RIU al aplicar las mejores prácticas recomendadas en los diversos documentos generados para el proyecto.

Definitivamente una de las mejores enseñanzas que me dejó el proyecto RIU fue el tomar con una gran responsabilidad el diseño de la arquitectura de seguridad con la que toda nuestra comunidad universitaria trabajaría día con día a partir de su apertura; lo cual implicó también considerar detalladamente las diversas soluciones que nos

[40] Request for change

presentaron los fabricantes: a un simple vistazo varias de las propuestas cumplían con el objetivo de proveer de conectividad inalámbrica al campus, sin embargo al compararlas con los lineamientos planteados al inicio del proyecto se hacía patente la importancia de haber realizado un buen análisis de requerimientos para el proyecto desde su concepción.

Finalmente, y no por ello menos importante el proyecto RIU, me permitió retribuir un poco a la UNAM de todo lo que me dio en mi estancia como estudiante, por lo cual estoy muy agradecido.

A. Apéndice A

Glosario

AES

Sistema de cifrado conocido originalmente como Rijndael. Es un cifrado de bloque simétrico que puede trabajar con claves de 128, 192 o incluso 256 bits.

AP

Punto de acceso de una red inalámbrica.

CCK

Tipo de modulación usada para codificar datos para velocidades de 5.5 y 11 Mbps en la banda de 2.4 GHz en redes inalámbricas 802.11b. Este código tiene propiedades matemáticas que permiten ser correctamente reconocidas por el receptor aún en presencia de ruido o interferencias.

Cray YMP

Supercomputadora de procesamiento vectorial que fue adquirida por la UNAM en 1991.

Firewall

Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

FIRST

Organización que agrupa diversos equipos de respuesta a incidentes de seguridad en cómputo a nivel internacional.

GPS

Sistema de posicionamiento global.

GRE

Enlace virtual entre dos equipos remotos de una red, es un túnel que transporta tráfico encapsulado.

IEEE

Organización creada en los Estados Unidos en 1963; entre sus competencias están la definición de las normas referentes a computadoras y comunicaciones.

IPS

Sistema que combina las capacidades de bloqueo de un firewall y las de análisis de un sistema detector de intrusos. Está diseñado para detener ataques antes de que tengan éxito.

ITIL

Conjunto de recomendaciones para aumentar la calidad en los servicios de Tecnologías de Información.

Kismet

Herramienta de software para sistemas Linux que sirve para detectar redes inalámbricas.

LDAP

Protocolo para el acceso a directorios jerárquicos de información.

Linux

Sistema operativo libre compatible con el estándar POSIX.

Macintosh

Sistema operativo utilizado por equipos del fabricante Apple.

MIC

Tecnología que permite evitar que un atacante capture información cifrada, la altere y la reenvíe en redes inalámbricas.

NOC

Centro de operaciones de la red.

OFDM

Tecnología de modulación desarrollada para aplicaciones inalámbricas. Mediante OFDM varias señales de diferentes frecuencias se combinan para formar una única señal para su transmisión.

PEAP

Protocolo de autenticación extensible protegido, utiliza TLS para autenticar al servidor.

POSIX

Norma del IEEE que define una interfaz entre los programas de aplicación y el sistema operativo Unix

RC4

Es un algoritmo de cifrado diseñado por la empresa RSA, basa su funcionamiento en permutaciones aleatorias.

Red CLARA

Red regional de telecomunicaciones de la más avanzada tecnología para interconectar a las Redes Académicas Nacionales de América

SANS

Instituto que ofrece entrenamiento en diversas áreas de la seguridad en cómputo, con sede en Estados Unidos ofrece varias certificaciones profesionales.

SecurityFocus

Portal de Internet especializado en seguridad, entre sus colaboradores se cuentan diversos expertos en todas las áreas de la seguridad en cómputo.

SSID

Nombre que identifica de forma única a una red inalámbrica. Los puntos de acceso inalámbricos difunden el SSID para que los usuarios finales puedan identificar la red local inalámbrica a la que se desean conectar.

Thawte

Es una empresa sudafricana que funge como autoridad certificadora en el esquema PKI.

TKIP

Parte del estándar del cifrado IEEE 802.11i para redes inalámbricas. Es la siguiente generación al protocolo WEP, empleado para asegurar las redes 802.11, corrigiendo los defectos del WEP.

TLS

Seguridad de la capa de transporte (Transport Layer Security). Es un mecanismo de seguridad utilizado en redes TCP/IP para la seguridad de transacciones confidenciales, implementa integridad y cifrado de datos.

Verisign

Una de las más conocidas autoridades de certificación de Internet. Emite certificados digitales RSA para su uso en las transmisiones seguras por TLS/SSL, principalmente para la protección de sitios en internet en su acceso por https.

WEP

Privacidad equivalente a la cableada (Wired Equivalent Privacy). Mecanismo de seguridad de 64 o 128 bits utilizado en redes inalámbricas, se ha demostrado que es muy inseguro.

WiFi

Wireless Fidelity. Es la certificación que avala el grupo Wi-Fi Alliance, que engloba diversos estándares de las redes 802.11.

Windows XP

Sistema operativo gráfico de la empresa Microsoft, que se encuentra instalado en la mayoría de computadoras personales a nivel mundial.

WPA

Norma Wi-Fi, aprobada en abril de 2003, desarrollada para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP. Incluye dos mejoras con respecto a WEP: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WPA PSK

WPA que usa una clave precompartida (WPA-PSK), no utiliza un servidor de autenticación.

WPA Radius

WPA que utiliza un servidor de autenticación centralizado, generalmente un servidor radius.

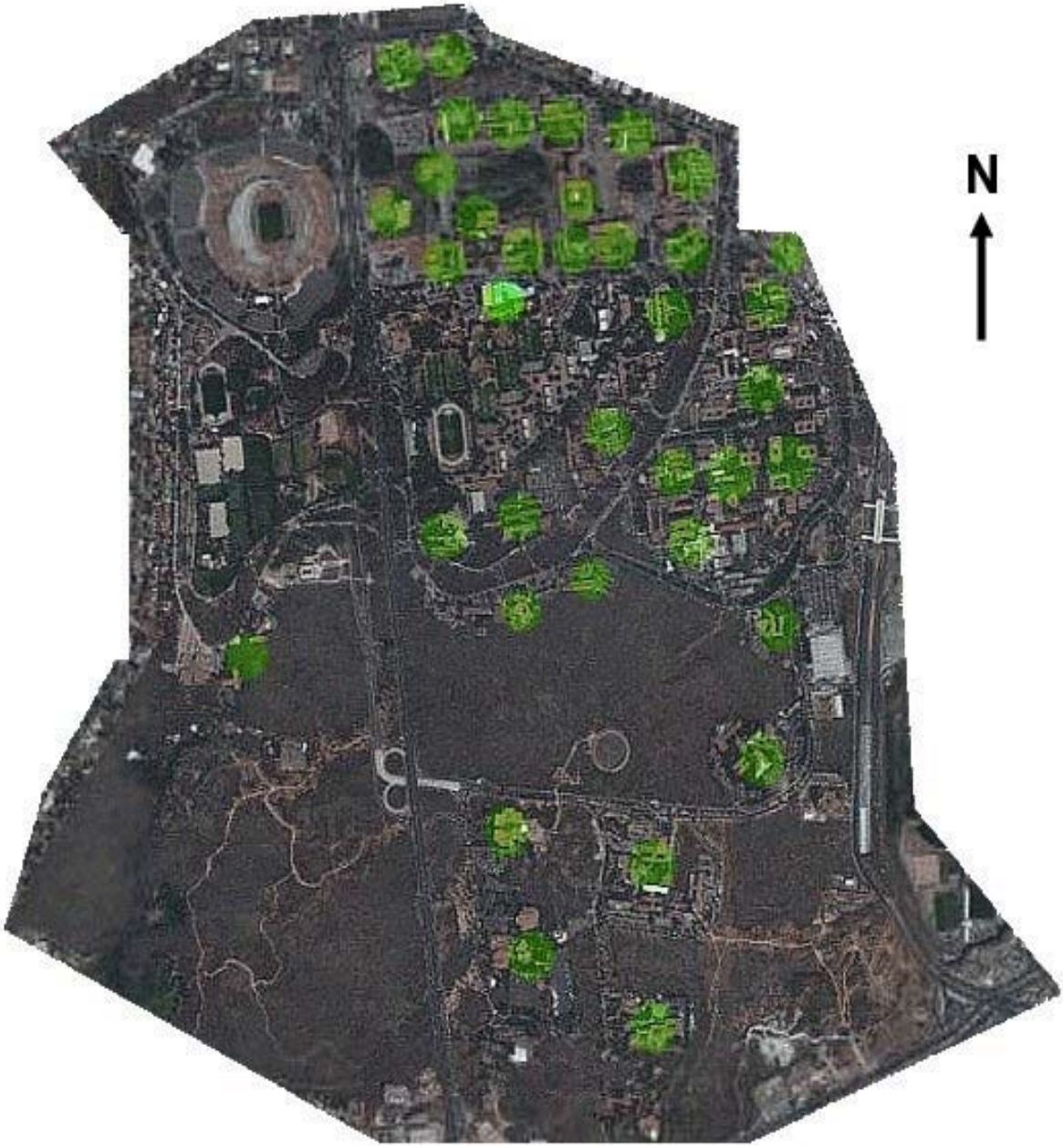
B. Apéndice B

Biblioteca Central
Biblioteca Nacional
Centro de Ciencias de la Atmósfera
Centro de Ecología
Centro de Enseñanza de Lenguas Extranjeras
Centro de Enseñanza para Extranjeros
Centro Coordinador y Difusor de Estudios Latinoamericanos
Centro de Investigación sobre América del Norte
Centro de Investigación Interdisciplinario en Ciencias y Humanidades
Centro Universitario de Investigaciones Bibliotecológicas
Coordinación de Humanidades
Coordinación de la Investigación Científica
Dirección General de Servicios de Cómputo Académico
Escuela Nacional de Trabajo Social
Facultad de Arquitectura
Facultad de Ciencias
Facultad de Ciencias Políticas
Facultad de Contaduría y Administración
Facultad de Derecho
Facultad de Economía
Facultad de Filosofía y Letras
Facultad de Ingeniería
Facultad de Medicina
Facultad de Medicina Veterinaria y Zootecnia
Facultad de Odontología
Facultad de Psicología
Facultad de Química
Instituto de Astronomía
Instituto de Biología
Instituto de Ciencias Nucleares
Instituto de Economía
Instituto de Fisiología Celular
Instituto de Geofísica
Instituto de Geografía
Instituto de Geología
Instituto de Investigación en Matemáticas Aplicadas y Sistemas
Instituto de Investigaciones Antropológicas
Instituto de Investigaciones Biomédicas
Instituto de Investigaciones Estéticas
Instituto de Investigaciones Históricas
Instituto de Investigaciones Jurídicas
Instituto de Investigaciones Sociales
Instituto de Matemáticas
Instituto de Investigaciones en Materiales
Instituto de Química
Jardín Botánico
Unidad de Seminarios
Universum

Relación de dependencias Universitarias con cobertura de la RIU

C. Apéndice C

Mapa de cobertura de la RIU



D. Apéndice D

Políticas de uso aceptable

GENERALIDADES

Aplicación.
Las presentes políticas establecen los lineamientos generales a seguir para el acceso y uso de la RIU y son aplicables a todos los usuarios del servicio proporcionado por la DGSCA.

Emisión y modificación de normas.
La DGSCA tiene la facultad de crear, modificar y emitir nuevas políticas de acceso a la RIU, en consecuencia se reserva el derecho de hacerlo en cualquier momento, sin previa notificación a los usuarios.

De la información transportada en la Red.
La DGSCA no controla ni es responsable del contenido y veracidad de la información que se transporta en la RIU, en consecuencia los usuarios aceptan utilizar el servicio de comunicación sólo para enviar y recibir mensajes e información que sean apropiados.

El acceso al contenido publicado en Internet, archivos descargados, programas ejecutados desde Internet, mensajes recibidos y demás información que pueda estar en Internet, es susceptible de contener virus informáticos. Por lo anterior es responsabilidad del usuario ingresar sólo a sitios que considere seguros.

Asignación del servicio.
Previo al cumplimiento de los requisitos que al efecto se establezcan, la DGSCA generará las cuentas de usuario para el acceso a la RIU a partir de un registro de los usuarios y distribuirá las contraseñas de manera presencial a través de la Coordinación del Centro de Atención a Usuarios, ubicada en el edificio principal de la DGSCA en el Circuito Exterior S/N, teléfonos 5665-1966.

El servicio de acceso a la Red Inalámbrica será proporcionado a la comunidad estudiantil y académica universitaria en forma gratuita.

Los estudiantes usuarios de la RIU actualizarán su registro semestral o anualmente de acuerdo a sus calendarios escolares y los académicos e investigadores lo harán anualmente.

Suspensión del servicio.
La DGSCA podrá suspender o desactivar temporalmente sus servicios o cancelarlos definitivamente, cuando detecte que el usuario realiza usos prohibidos del servicio. A juicio de esta instancia se reactivará el servicio cuando se considere que el usuario no volverá a incurrir en una conducta prohibida del servicio.

Las siguientes son causas de suspensión temporal de la cuenta:

- Distribuir virus, gusanos u otro código malicioso de propagación automática y de forma involuntaria.
- Compartir carpetas o archivos en red.

Las siguientes son causas de suspensión definitiva de la cuenta:

- Transmisión de contenido pornográfico.
- Distribuir virus, gusanos u otro código malicioso de propagación automática y de forma voluntaria.
- Realizar actividades delictivas.
- Envío de mensajes no solicitados (spam).
- Atacar a otros usuarios por cualquier medio (negación de servicio, phishing, etc.).
- Atentar contra la disponibilidad, integridad, confidencialidad de la red.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.
- Cuando el usuario completó su ciclo escolar o dejó de ser académico o investigador universitario.

Disponibilidad del servicio.
El servicio de conexión a la Red Inalámbrica Universitaria estará disponible las 24 horas del día, todos los días del año. Salvo en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados a la prestación del servicio de Internet.

Configuración
Los usuarios de la red son responsables de instruirse y configurar sus sistemas con los procedimientos básicos para su funcionamiento en la RIU y para contar con la seguridad mínima que brinde protección a sus dispositivos.

Cobertura
La Red Inalámbrica Universitaria tendrá un alcance de operación específico identificado en el plano de cobertura creado para ese fin. Este será aplicable únicamente a la Ciudad Universitaria como fase inicial de la RIU.

Responsabilidad.

1. La DGSCA es responsable de mantener la integridad y operación eficaz de los puntos de acceso a la RIU, pudiendo realizar acciones de actualización y mantenimiento del servicio sin previa notificación a los usuarios.
2. La DGSCA no se hace responsable por conductas difamatorias, obscenas u ofensivas que se realicen a través de los servicios que proporciona.

3. La DGSCA es responsable de confirmar que los usuarios que soliciten el servicio y adquieran contraseñas para su uso pertenecen a la comunidad universitaria ya sea como estudiantes, académicos, investigadores e invitados.
4. Es responsabilidad del usuario la seguridad física de su equipo, por lo que la UNAM no es en ninguna forma responsable por robo o daños al equipo del usuario.
5. El usuario acepta y reconoce que la DGSCA sólo provee de los recursos para acceder a los servicios que le son otorgados.
6. El usuario es responsable de la confidencialidad de sus contraseñas.

USOS PERMITIDOS

Usuarios Autorizados
Son usuarios autorizados los que, previa autorización y cumplimiento de los requisitos correspondientes, tienen acceso a la RIU y hacen uso de los servicios. Estos comprenden a los alumnos, académicos e investigadores de la UNAM así como estudiantes, académicos e investigadores invitados de otras instituciones.

Propósito de uso
En apego al quehacer de la UNAM, el uso de los recursos para estos servicios deberá estar relacionado con las actividades académicas, de investigación y difusión de la cultura.

USOS PROHIBIDOS

Queda prohibido:

- El uso personal de los recursos de estos servicios que generen un costo directo a la UNAM.
- El uso simultáneo de una cuenta desde dos dispositivos móviles diferentes.
- El uso para generar ganancias monetarias personales o propósitos comerciales que no estén directamente relacionados con asuntos que la propia Universidad autoriza, difunde y solicita a la comunidad universitaria incluyendo en situaciones de contingencia.
- Enviar copias de documentos o inclusión de trabajos de otros en el correo electrónico como propios violando las leyes de derechos de autor.
- Descargar servicios broadcast como audio y video.
- Compartirse archivos, carpetas y otros servicios (impresión, etc.).
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Extender el servicio de acceso a la RIU a más equipos por medio de una sola conexión a la red inalámbrica (Ej.: por medio de NAT, túneles, conexión compartida, etc.)
- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico (ej. antenas) más allá de los límites físicos de la

Universidad. El acceso a la red inalámbrica se restringe al campus universitario.

- El uso del servicio para molestar, acosar, intimidar, amenazar a otros o atente contra la integridad de los usuarios o para interferir con asuntos propios de las autoridades Universitarias.
- El uso del servicio para violar las políticas de uso aceptable del correo electrónico
- Transgredir cualquier recurso computacional, sistemas o sitios de telecomunicaciones a los que no le está permitido acceder.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.

MONITOREO DE COMUNICACIONES

A solicitud escrita de la autoridad competente o cuando exista alguna orden judicial para responder ante procesos legales, la DGSCA proporcionará la información transmitida en la RIU y que esté disponible para su acceso de conformidad con las leyes aplicables.

El usuario al momento de obtener su cuenta de acceso a la RIU, conoce y manifiesta su consentimiento para que la DGSCA realice monitoreos en su conexión de acceso a la RIU cuando lo juzgue necesario, únicamente con el propósito de mantener la integridad y operación efectiva de los puntos de acceso o cuando responda a un requerimiento de las autoridades administrativas o judiciales.

E. Apéndice E

Políticas de operación de la RIU

Propósito

El propósito de esta política es definir los lineamientos de operación de la red que permitan un funcionamiento óptimo que a su vez garantice la seguridad de la RIU.

Definiciones

RIU. Red Inalámbrica Universitaria
NOC. Centro de operaciones de la red de la UNAM.
DSC. Departamento de Seguridad en Cómputo.
Usuarios. Todos los usuarios de la red.

1.1 Sobre la infraestructura de la red

1.1.1. Todo equipo o sistema a ser implementado como parte de la infraestructura de la RIU deberá ser aprobado por el NOC/DSC para que cumpla con los estándares establecidos para la operación de la red. Las dependencias de la Universidad deberán consultar las políticas de la red inalámbrica sobre el uso del software y hardware, así como acudir con el NOC/DSC para obtener los lineamientos para el despliegue de redes inalámbricas dentro de cada dependencia.

1.1.2. Todos los puntos de acceso (APs) deberán ser registrados por el NOC, en el caso de que exista interferencia entre algunos de estos puntos de acceso se resolverá de acuerdo a la prioridad de uso de cada uno de ellos.

1.1.3. El despliegue y administración de los puntos de acceso que forman parte de la infraestructura son responsabilidad del NOC.

1.1.4. Para nuevas construcciones que sean realizadas dentro del campus deberán observarse los mismos lineamientos que hayan sido establecidos para el despliegue inicial de la infraestructura. Esta información estará disponible en el manual de procedimientos de seguridad de la red.

1.1.5. Todo cambio requerido de la configuración de la infraestructura deberá ser evaluado y aprobado por un comité de cambios y configuraciones conformado por miembros del NOC y del DSC de acuerdo a los lineamientos definidos en el manual de procedimientos de seguridad de la red.

1.2 Sobre la interferencia entre dispositivos

Todo el equipo que opere intencional o inadvertidamente en el espectro utilizado por la red inalámbrica debe ser instalado y configurado para evitar interferencias con otros elementos de la infraestructura. Para poder realizar esta tarea se debe considerar:

1.1.1. La instalación, administración y uso de los elementos de configuración de la infraestructura debe apegarse a los reglamentos en materia de telecomunicaciones y a los definidos por el NOC.

1.1.2. La prioridad para solucionar disputas por interferencia entre dispositivos será de acuerdo al siguiente listado:

1. Equipo de seguridad
2. Investigación
3. Enseñanza
4. Administración
5. Acceso público
6. Personal

1.1.3. El NOC atenderá reportes de dispositivos sospechosos de causar interferencia en la red del campus a través de los puntos de contacto definidos en el presente documento. Cuando la interferencia no pueda ser eliminada, el uso de dispositivos inalámbricos ajenos a la infraestructura de la RIU puede ser restringido por el NOC.

1.3 Sobre el uso de puntos de acceso (APs) no autorizados.

Los APs que no forman parte de la infraestructura de la red inalámbrica de la UNAM representan un riesgo a la seguridad de la información de los usuarios y de la red cableada de RedUNAM, por lo que se recomienda su reemplazo.

Así mismo, los APs no autorizados representan un obstáculo para el desempeño eficiente del servicio ofrecido por la red inalámbrica de la UNAM, debido a su posible interferencia en la frecuencia de radio utilizada; por lo que al menos se requiere que los APs no autorizados, que no sean posibles de reemplazar, funcionen en las frecuencias más altas.

En el caso del estándar 802.11b/g:

Canal 10 = 2.457 (freq. central)
Canal 11 = 2.462 (freq. central)

Así mismo, los APs que no puedan ser reemplazados, deberán ser registrados ante el NOC, incluyendo responsable del AP, ubicación física, dependencia, nombre de red, IP y dirección MAC.

1.4 Sobre la autenticación

1.4.1. Los usuarios de la red serán autenticados por medio de un login y una contraseña en un servicio RADIUS y LDAP.

1.4.2. El login será único e intransferible para cada usuario de la red.

1.4.3. Las contraseñas deben consistir de un mínimo de 8 caracteres (no deben ser palabras sencillas contenidas en un diccionario y deben contar con un número y un carácter especial al menos).

1.4.4. Las contraseñas deben ser renovadas al inicio de cada semestre escolar.

1.4.5. Las cuentas serán inhabilitadas temporalmente después de 10 intentos fallidos.

1.4.6. La sesión será cerrada después de 30 minutos de inactividad.

1.4.7. Las cuentas que muestren inactividad por un periodo de 2 meses serán inhabilitadas.

1.5 Sobre la distribución de contraseñas

1.5.1. El NOC realizará la distribución de contraseñas al inicio de cada semestre escolar en una ubicación centralizada designada para dicha tarea.

1.5.2. Los usuarios que no hayan obtenido su contraseña al inicio del semestre podrán realizar una solicitud durante el semestre directamente con el NOC en el centro de atención a usuarios de la RIU siguiendo el procedimiento para solicitud de servicio y cumpliendo con los requisitos estipulados en los lineamientos de uso aceptable de la RIU.

1.6 Sobre la confidencialidad

1.5.1. Con la finalidad de evitar problemas con la confidencialidad, la red inalámbrica no debe ser usada como sustituto de la red cableada de la Universidad, se recomienda el uso de la red cableada cuando se trate de comunicaciones de carácter financiero, misión crítica, registros académicos y en general de carácter confidencial.

1.5.2. El estándar de cifrado definido como mínimo requerido es WPA con TKIP. El estándar recomendado es WPA con AES.

1.7 Seguridad de los APs

1.6.1. Los APs deben estar protegidos de accesos no autorizados. Físicamente deben estar fuera del alcance de un atacante, también deben ser protegidos de robo físico.

1.6.2. La aplicación de parches de seguridad y/o actualización del firmware de los APs deberá realizarse en un ambiente de pruebas, previo a su despliegue en la totalidad de los APs que así lo requieran. Dicha aplicación de actualizaciones se llevará a cabo en horario y fecha aprobados por el comité.

1.8 Sobre la disponibilidad

1.7.1. Para proporcionar un servicio adecuado a los usuarios, deberá restringirse el ancho de banda disponible individualmente.

1.7.2. La disponibilidad del hardware (uptime) debe monitorearse continuamente para garantizar buenos niveles de operación.

1.7.3. La disponibilidad de la cobertura de la señal no puede garantizarse debido a los diversos factores que la afectan.

1.9 Integridad de la red

1.8.1. Implementar mecanismos de monitoreo que garanticen el funcionamiento adecuado de la infraestructura.

1.8.2. Se deben inventariar absolutamente todos los elementos de la infraestructura de la red y almacenar en una base de datos de configuración, que será administrada por el NOC para mantenerse actualizada ante cualquier cambio.

1.8.3. Se debe garantizar que dichos elementos estén disponibles para cumplir su función dentro de la red.

1.10 Monitoreo de la red

1.9.1. Todos los eventos de autenticación deben ser registrados en bitácoras y almacenados por 1 semestre escolar (exitosos o no exitosos).

1.9.2. Se debe contar con sensores de tráfico y detectores de intrusos instalados en diferentes puntos de la red inalámbrica.

1.9.3. Las bitácoras de acceso a la red deben ser revisadas diariamente (de forma manual o automática) en busca de actividad intrusiva (ataques de fuerza bruta, exploits, etc.).

1.9.4. Se debe promover entre los usuarios las señales que identifiquen un incidente de seguridad, a su vez contar con un punto de contacto por e-mail y teléfono en el NOC/DSC.

1.9.5. Cuando no esté en riesgo la operación de la red, se tratará de identificar al atacante antes de aplicar las medidas correctivas que puedan eliminar los rastros de éste.

1.9.6. Mensualmente deberá realizarse una junta del comité encargado de la operación de la red, conformado por miembros del NOC y DSC.

1.9.7. Todos los componentes de la infraestructura estarán sujetos a auditorias periódicas de seguridad.

1.9.8. El manual de procedimientos de seguridad de la red detallará los requerimientos de hardware y software para el monitoreo, control y autenticación de la RIU.

1.11 Respuesta a incidentes

1.10.1. Todos los reportes de posibles incidentes deben ser revisados por el NOC y en caso de detectar un incidente deberá ser reportado al DSC.

1.10.2. El NOC/DSC cooperarán con otras entidades externas cuando se registren fuentes de ataque en la red inalámbrica Universitaria para frenar dichos ataques.

1.10.3. El NOC/DSC sólo revelará información del incidente cuando sea requerido legalmente, en cuyo caso se acudirá con un asesor legal para determinar el curso de acción.

1.10.4. El DSC iniciará un reporte de incidente cuando sea solicitado por el NOC y dará seguimiento hasta solucionar el problema; sólo si el problema ha sido erradicado entonces el DSC dará por cerrado el reporte de incidente.

1.12 Responsabilidades

1.11.1. Es responsabilidad del NOC la operación de la red para garantizar la disponibilidad del servicio.

1.11.2. Es responsabilidad del DSC atender los incidentes reportados por el NOC para garantizar la seguridad de la RIU.

1.11.3. El DSC asesorará en todo momento que sea requerido por el NOC para la toma de decisiones contempladas y no contempladas en esta política.

1.11.4. El NOC y el DSC formarán un comité que permita mejorar el desempeño de la RIU y mantenerlo en niveles de operación adecuados a las necesidades de la comunidad universitaria.

1.13 Privacidad

1.12.1. Todos los elementos de la infraestructura de la RIU y la información que se transmite por ellos están sujetos a inspección y monitoreo en todo momento para garantizar el adecuado funcionamiento, para prevenir uso no autorizado y violaciones a los estatutos de seguridad, para prevenir actividad criminal y otros propósitos similares.

1.14 Respaldos

1.13.1. Se debe garantizar la restauración de los sistemas de software y las bases de datos que forman parte de la infraestructura de la RIU en caso de un incidente que corrompa la integridad de ésta.

1.13.2. El NOC es responsable de realizar respaldos periódicamente, así como almacenarlos hasta por un plazo de 1 año a partir de su fecha de realización.

1.13.3. Los respaldos deberán ser almacenados en una ubicación alternativa al de la locación original de los sistemas respaldados.

1.13.4. Los respaldos deberán ser probados para garantizar su integridad.

Bibliografía y Mesografía

[1] Farshchi, Jamil. *Wireless Policy Development*. http://www.securityfocus.com/infocus/1732

[2] Fluhrer, Scott. *Weaknesses in the Key Scheduling Algorithm of RC4.* http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[3] Institute of Electrical and Electronics Engineers. *Wireless LAN Medium Access Control and Physical Layer specifications*. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[4] itSMF. *IT Service Management*. http://www.itsmf.com/

[5] Takehiro, Takahashi. *WPA Passive Dictionary Attack Overview*. http://www.tinypeap.com/docs/TinyPEAP_White_Paper.pdf

[6] Zamboni, Diego. *Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix.* http://homes.cerias.purdue.edu/~zamboni/pubs/thesis-bs.pdf