DISEÑO DE REDES LAN INALÁMBRICAS (SEGURIDAD: PASADO, PRESENTE Y FUTURO; INCLUYE IMPLEMENTACIÓN DE CASOS)

ERIKA JOHANA MULETT FLOREZ
DAVID LÓPEZ DE LA ESPRIELLA

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
CARTAGENA DE INDIAS
2009

DISEÑO DE REDES LAN INALÁMBRICAS (SEGURIDAD: PASADO, PRESENTE Y FUTURO; INCLUYE IMPLEMENTACIÓN DE CASOS)

Trabajo presentado como requisito para optar al titulo de;
INGENIERO DE SISTEMAS

Director
ISAAC ZÚÑIGA SILGADO
Ingeniero de Sistemas

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
CARTAGENA DE INDIAS
2009

Cartagena de Indias, 5 de Junio del 2009

Señores:
UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Ciudad.

Estimados señores:

De la manera más cordial, los estudiantes Erika Johana Mulett Florez con c.c. 23.182.621 de la ciudad de Sincelejo y David López de la Espriella con c.c. 73.202.692 de Cartagena, autorizamos a la Universidad Tecnológica de Bolívar, para publicar y hacer uso de nuestra monografía titulada "DISEÑO DE REDES LAN INALÁMBRICAS (SEGURIDAD: PASADO, PRESENTE Y FUTURO; INCLUYE IMPLEMENTACIÓN DE CASOS)"

Cordialmente,

_____

ERIKA JOHANA MULETT FLOREZ
C.C Nº 23.182.621 DE SINCELEJO - SUCRE

_____

DAVID LOPEZ DE LA ESPRIELLA
C.C Nº 73.202.692 DE CARTAGENA

Cartagena de Indias, 5 de Junio del 2009

Señores:
UNIVERSIDAD TECNOLOGICA DE BOLIVAR
COMITÉ DE EVALUACIÓN DE PROYECTOS
Ciudad.

Estimados señores:

Mediante la presente me dirijo a ustedes, para poner a consideración el trabajo final que lleva como nombre "DISEÑO DE REDES LAN INALÁMBRICAS (SEGURIDAD: PASADO, PRESENTE Y FUTURO; INCLUYE IMPLEMENTACIÓN DE CASOS)", realizado por ERIKA JOHANA MULETT FLOREZ y DAVID LOPEZ DE LA ESPRIELLA, bajo mi orientación como director.

Cordialmente,

_____
ISAAC ZUÑIGA SILGADO

Cartagena de Indias, 5 de Junio del 2009

Señores:
UNIVERSIDAD TECNOLOGICA DE BOLIVAR
COMITÉ DE EVALUACIÓN DE PROYECTOS
Ciudad.

Estimados señores:

Nos permitimos presentar a ustedes para su estudio, consideración y aprobación el trabajo final titulado "DISEÑO DE REDES LAN INALÁMBRICAS (SEGURIDAD: PASADO, PRESENTE Y FUTURO; INCLUYE IMPLEMENTACIÓN DE CASOS)", presentado para optar por el título de ingeniero de Sistemas.

Cordialmente,

_____

ERIKA JOHANA MULETT FLOREZ
C.C Nº 23.182.621 DE SINCELEJO – SUCRE

_____

DAVID LOPEZ DE LA ESPRIELLA
C.C Nº 73.202.692 DE CARTAGEN

NOTA DE ACEPTACION

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Cartagena, 5 de Junio del 2009

DEDICATORIA

A Dios por colocar en mi corazón el deseo de estudiar una carrera de proyección social, por la sabiduría para enfrentar el desafío de cada semestre, por la vida y la oportunidad de ver alcanzado este triunfo y disfrutarlo con quienes amo.

A mis padres por todos los sacrificios que han hecho para sacarme adelante, por su comprensión y apoyo en los momentos que sentí desfallecer, por siempre creer en mí y en mis capacidades, pero sobre todo por su infinito amor, ese amor que solo unos padres pueden dar.

A toda mi familia y amigos que creyeron en mí.

A Dairo Ballestas por su comprensión y apoyo moral en los momentos que mas lo necesité.

ERIKA JOHANA MULETT FLOREZ

A Dios que me indicó el camino a tomar, en la elección de la carrera y me brindó la fortaleza suficiente para no desfallecer ante las dificultades presentadas.

A mis padres y hermanos por su apoyo y comprensión en los momentos difíciles, que se sacrificaron dando todo lo que estaba a su alcance y depositaron su confianza en mí.

DAVID LOPEZ DE LA ESPRIELLA

AGRADECIMIENTOS

Los autores expresan sus más sinceros agradecimientos a:

La Universidad Tecnológica de Bolívar por facilitarnos las herramientas necesarias para convertirnos en profesionales y personas de beneficio a la sociedad. Además de las condiciones para la realización de la presente investigación.

A los docentes; Isaac Zúñiga, Giovanny Vásquez y demás docentes por sus aportes teórico-científicos, que contribuyeron a la culminación con éxito del proyecto.

A todos los que de alguna manera colaboraron en la realización y culminación de la investigación.

BREVE DESCRIPCION DEL PROBLEMA

Como en todo desarrollo tecnológico nuevo, en la operacionalidad de las Redes de Área Local Inalámbricas (LAN), el objetivo es lograr la funcionalidad aunque eso implique no tomar en cuenta otros requerimientos que ayuden a tener un óptimo rendimiento, como es la seguridad, que podría formar parte del desarrollo de una aplicación, pero por naturaleza los conceptos de seguridad son complejos por si mismos. Esto resulta en una tarea difícil de entender, además los servicios de seguridad pueden degradar el rendimiento, bajando con ello los niveles de calidad de servicio (QoS) de la aplicación multimedia. Es por eso que casi todos los desarrolladores de aplicaciones multimedia ignoran los mínimos requerimientos de seguridad para garantizar confiabilidad e integridad de los datos.

Actualmente existen mecanismos de seguridad utilizados para proporcionar la autenticación del usuario. Sin embargo, estas soluciones no son suficientes porque el protocolo WEP solo se puede utilizar para las redes inalámbricas, además que tiene defectos en su diseño que ponen en riesgo su seguridad. Además, aunque el SSL se considera seguro, es complicado y difícil de implementar y puede por ello no ser factible en los dispositivos móviles con capacidades de procesamiento y memoria limitados. La seguridad proporcionada a través de hardware es claramente inflexible pues requiere tener preestablecido los mecanismos de seguridad. Otra cosa importante es que estas soluciones no proporcionan niveles ajustables de seguridad para diversas preferencias del usuario y de la aplicación. Por otro lado las soluciones actuales no consideran la cantidad de recursos disponibles en los diversos dispositivos en el ambiente.

En síntesis, las tecnologías integradas no garantizan la seguridad de las redes LAN inalámbricas que han mostrado ser más que vulnerables y con muchos “agujeros”. El problema es serio y podría representar un freno para la posterior difusión de las redes WLAN, la extrema vulnerabilidad de las redes Wi-Fi y la facilidad con la que los hackers, pueden violarlas enmarca una gran problemática en el tema de buenas prácticas de implementación y administración de redes telemáticas seguras.

JUSTIFICACIÓN

Muy pocos conceptos en el mundo de la interconexión actual son tan confusos como Redes Virtuales. Las Redes Virtuales son muy nuevas, y su uso a nivel mundial esta sólo comenzando. La cantidad de datos que es transportada mediante las redes de área local (LAN) ha crecido firme y rápidamente. Esto se debe básicamente al crecimiento de las aplicaciones existentes, hoy en día casi todas las personas tienen un Computador en su escritorio o su casa, y casi todos están conectados en red. Esto difiere mucho de la situación presentada hace unos pocos años, inclusive en redes extensas.

Hoy, las instituciones educativas han incorporado en los procesos de formación que desarrollan, el uso cada vez más intensivo de las nuevas tecnologías de la comunicación existentes, como respuesta a los retos que demanda la sociedad y el entorno empresarial nacional e internacional. Se ha venido estimulando el uso de nuevas tecnologías para fomentar en los aprendices competencias enmarcadas en el liderazgo, la competitividad y la conciencia crítica.

Esta monografía se hace necesaria para identificar y documentar la información existente respecto a la seguridad en redes LAN inalámbricas con miras a la innovación, emprendimiento y liderazgo para el desarrollo social y económico del país que requieren la incorporación de las Tecnologías de Información y Comunicaciones, en todos los procesos de aprendizaje que facilitan el acceso a las fuentes de conocimiento y el desarrollo de competencias de estudiantes, el sector productivo relacionado y la comunidad en general.

Con esta propuesta se espera dar solución al vacío de conocimiento existente sobre seguridad en redes LAN, al tiempo que busca integrar a la sociedad del conocimiento tecnológico los estudiantes de Ingeniería de Sistemas de la Universidad Tecnológica de Bolívar, respondiendo así a la política del Gobierno Nacional de cerrar la brecha digital y fortalecer las capacidades del capital humano en formación, para poder avanzar al ritmo que lo demanda la ciencia, la tecnología y los mercados tanto nacional como internacional. Para lograr resultados en equidad, lucha frontal contra la pobreza e incrementos en la competitividad y productividad de trabajadores y de empresas del país.

RESUMEN

Con la finalidad de contribuir en la identificación y planteamiento de posibles soluciones a los principales problemas de seguridad hoy presentes en las WLAN, para responder a buenas prácticas de implementación y administración de redes telemáticas seguras. Fue realizada una extensa y rigurosa revisión biográfica; que arrojó dentro de los resultados más relevantes las diferentes opciones de seguridad existentes, sus fortalezas y debilidades, al igual que las limitaciones en la transferencia de datos sobre una Red de Área Local Inalámbrica. Proporcionando a los usuarios del sistema conocimiento que les permitirá ajustar de manera flexible los niveles de seguridad, sin que se vea comprometida la calidad del servicio, de tal manera que se establezca un equilibrio entre los dos componentes (calidad de servicio y seguridad).

Se pudo concluir que la monografía logra exponer claramente temas a nivel académico. Adicionalmente permite determinar la habilidad para hacer investigaciones académicas de los futuros profesionales además de disciplinarnos en el manejo de gran cantidad de información. En cuanto al tema de seguridad en redes LAN permiten concluir que la seguridad de los sistemas informáticos es una tarea difícil de efectuar, ya que implica de gran experiencia de los diseñadores del sistema y de mayores recursos computacionales.

Recientemente, ha habido numerosas investigaciones dedicadas a brindar mayor seguridad a sistemas de cómputo, sin embargo, siempre existen vulnerabilidades en el sistema que impiden garantizar totalmente seguridad de un sistema.

Palabras Clave: Redes LAN, seguridad, protocolo, internet, Inalámbrico.

ABSTRAC

With the purpose to contribute in the identification and exposition of possible solutions to the main today present problems of security in the WLAN, to respond to good practices of implementation and safe telematics network management. An extensive and rigorous biographical revision was realised; that I throw within the most excellent results the different existing options of security, its strengths and weaknesses, like the limitations in the data transfer on a Wireless Local area network. Providing to the users of the system knowledge that will allow to fit of flexible way the security levels them, without it is seen it jeopardize the quality of the service, in such a way that a balance settles down enters both component (quality on watch and security). It was possible to be concluded that the monograph obtains set out clearly subjects at academic level. Additionally it allows to determine the ability to make academic investigations of the professional futures besides disciplining us in the handling of great amount of information. As far as the subject of security in networks LAN they allow to conclude that the security of the computer science systems is a task difficult of carrying out, since it implies of great experience of the designers of the system and of majors computer resources. Recently, there have been numerous dedicated investigations to offer to major security to calculation systems, nevertheless, always exist vulnerabilities in the system that they prevent to guarantee security of a system totally.

Key words: Networks LAN, security, protocol, Internet, Wireless

CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

En los últimos años las Redes de Área Local Inalámbricas (WLAN) han ganando mucha popularidad, que se ha visto acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones. Las WLANs permiten a sus usuarios acceder a información y recursos sin necesidad de estar conectados físicamente a un determinado lugar. Una WLAN por sí misma es móvil, elimina la necesidad de cables y establece nuevas aplicaciones añadiendo flexibilidad a la red. Un usuario dentro de una Red de Área Local Inalámbrica puede transmitir y recibir datos (de voz, vídeo, imágenes, entre otros) dentro de edificios, entre edificios e inclusive en áreas metropolitanas, a velocidades que exceden los 10 Mbps.

Esto hace que la tendencia actual en desarrollo tecnológico se encamine a la creación de dispositivos que incluyen dentro de sus principales beneficios hardware de comunicación inalámbrica, permitiendo con ello que gran variedad de aplicaciones de comercio electrónico y multimedia sean ejecutadas eficientemente. Sin embargo, como en todo desarrollo tecnológico nuevo, el objetivo es lograr la funcionalidad aunque eso implique no tomar en cuenta otros requerimientos que ayuden a tener un óptimo rendimiento, ocasionando que en la mayoría de los casos no exista compatibilidad y que además resulte en vulnerabilidades a la seguridad del sistema.

Es así, como la seguridad de las WLAN necesariamente debe formar parte del desarrollo de una aplicación, sin embargo, por naturaleza los conceptos de seguridad son complejos por si mismos, lo que resulta una

tarea difícil de entender. Adicionalmente debe considerarse que los servicios de seguridad podrían llegar a degradar el rendimiento, bajando con ello los niveles de calidad de servicio (QoS) de la aplicación multimedia. Por lo que casi todos los desarrolladores de aplicaciones multimedia ignoran los mínimos requerimientos de seguridad para garantizar confiabilidad e integridad de los datos.

Actualmente existen posibles soluciones para adecuar seguridad, en la práctica encontramos que se necesita la mayoría de las veces del hardware dedicado. Por ejemplo, en la capa enlace de datos, la seguridad se puede proporcionar por el protocolo WEP (Intimidad Equivalente De alambre) del estándar IEEE 802.11. En la capa de aplicación, se encuentra la capa de seguridad de sockets (SSL, Capa de Enchufes Segura) que se utiliza comúnmente. Alternativamente, existen mecanismos de seguridad que se utilizan para proporcionar la autenticación del usuario.

Sin embargo, estas soluciones no son suficientes porque el protocolo WEP solo se puede utilizar para las redes inalámbricas además de presentar defectos en su diseño que ponen en riesgo su seguridad. Además, aunque el SSL se considera seguro, es complicado y difícil de implementar y puede por ello no ser factible en los dispositivos móviles con capacidades de procesamiento y memoria limitados. Adicionalmente estas soluciones no proporcionan niveles ajustables de seguridad ni para las diversas preferencias del usuario ni para la Aplicación.

A lo largo de este documento se tratará de describir brevemente los estándares de seguridad actualmente existentes para las WLAN, al igual que sus principales deficiencias y posibles soluciones, con miras a la implementación de redes seguras. Se profundizará en aspectos de

autenticación, control de accesos y confidencialidad. El capitulo de estado actual de redes LAN describe la evolución seguida en este campo: desde WEP hasta WPA2. Se explicará en detalle la solución inicial adoptada: WEP y porqué actualmente esta no es una buena alternativa. Se describirán sus vulnerabilidades y cómo aprovecharlas con el uso de las herramientas adecuadas.

La finalidad del presente trabajo investigativo es contribuir en la identificación y solución de principales problemas de seguridad hoy presentes en las WLAN, para responder a buenas prácticas de implementación y administración de redes telemáticas seguras.

1. ESTADO ACTUAL DE REDES LAN INALAMBRICAS (WLAN)

1.1. ANTECEDENTES Y EVOLUCION

Los primeros PC's y Macintosh revolucionaron tanto la computación como la interconexión en redes. Las redes anteriormente transportaban imágenes desde los computadores grandes hacia los terminales, y señales de mandatos o instrucciones desde los terminales hacia el computador central. Esto cambio radicalmente con la estaciones de trabajos inteligentes. Hoy, existe necesidad de mover archivos, y los antiguos enlaces de 9.6 Kbps no son lo suficientemente rápidos. Ethernet y Toque (Anillo) fueron presionadas a prestar servicio para mover archivos de programas, impresión y comparación de recursos.

Las antiguas estaciones de trabajo estaban limitadas en el procesamiento y manejo de información debido a su poca capacidad y rendimiento (capacidad de disco, memoria, MIPS, flujo de la red, etc.). Como resultado, cada máquina es capaz de colocar una carga mayor en la red a la cual está conectada. Inclusive hasta después de la "Revolución de los PC's" que reemplazó los terminales por computadores de escritorio, la naturaleza esencial de los datos permanecía sin cambio excepto por algunas aplicaciones científicas y de diseño, la gran mayoría de la información que se transportaba a través de la red era textual lo que limitaba severamente la cantidad de información que necesitaba ser movida.

Contrario a esto las aplicaciones de hoy transfieren grandes cantidades de información gráfica. Las operaciones de manufactura utilizan gráficos para guiar a los trabajadores interactivamente en nuevos procesos. Las firmas

de abogados y compañías de seguro digitalizan grandes volúmenes de documentos, utilizando en muchos casos bitmaps para preservar documentos hechos a mano. Una amplia variedad de procesos médicos también usan imágenes para guiar a radiólogos, cirujanos y otros especialistas en sus diagnósticos y procedimientos. Eventualmente, se incluye video a través de la LAN, aplicación que requiere aún anchos de banda mayores.

Para cubrir este requerimiento se crean los Switches LAN que hacen posible transmitir cantidades mayores de datos de lo que es posible transmitir con concentradores y Routers.

Segmentos Ethernet y Toque(Anillo) pueden ser dedicados a dispositivos individuales, o a pequeños grupos de dispositivos, pero los Switches LAN alcanzan sus niveles de alto rendimiento utilizando procesos simplificados, que son básicamente Puentes, no ruteadores, ellos conmutan o "switchean" a través de la segunda capa las direcciones de destino/origen ("MAC"), que es mucho más simple que rutear.

Los Routers deben manejar una variedad de protocolos (selección de rutas, resolución de direcciones, transferencia de paquetes internet, control de mensajes internet, etc.) sólo para mover información en una sola " montón " de protocolo, como TCP/IP por ejemplo. Muchas redes combinan una variedad de montón, y cada una de ellas necesita un completo set de protocolos.

No hay nada nuevo en el uso de Puentes, para construir redes locales, las primeras LANs fueron creadas con Puentes, sencillos, la diferencia radica

en que hoy por hoy el hardware a avanzado significativamente, y enormes volúmenes de tramas pueden ser manejadas en un simple Switch.

Todas las redes interconectadas a través de Puentes,, tienen una limitación básica: los Puentes,, dado que ellos no participan en los protocolos de la capa tres (modelo OSI), la cual usa MAC difusión (o envío de paquetes a direcciones específicas), sino que envía paquetes a todos los puertos o direcciones, aunque el tráfico es aislado para los puertos específicos que envían y reciben esos paquetes, deben ser enviados a todas partes. En la mayoría de las redes de mediano tamaño, este "flujo" no tiene mayor impacto en los otros tráficos, no hay más que unos cuantos " difusión " y las direcciones MAC se aprenden rápidamente, pero en una red bastante grande o en una que exista niveles inusuales de difusión, es posible que este flujo impacte en el tráfico punto a punto de las estaciones. Cuando esto pasa es importante mantener estos difusión aislados en lo que se llama "Dominios de difusión ".

El proceso de desarrollo de las redes LAN se puede sintetizar de la siguiente forma;

• 1969: Nace ARPANET, red del Departamento de Defensa (DoD) americano con ordenadores conectados punto a punto.

• 1970: Abramson crea red Alohanet en Univ. De Hawai utilizando emisoras de radio taxis viejos para interconectar el ordenador de la isla de Hawai, Maui y Kauai con Honolulú.

• Arquitectura maestro-esclavo (como los radio taxis)
• Dos canales:

– Descendente (Maestro→Esclavo): un solo emisor

– Ascendente (Esclavo→Maestro): compartido por 3 'esclavos' ubicado en cada isla.

Tomado de: Redes Locales y protocolos MAC (Tecnologías LAN) Fundamentos de Telemática (Ingeniería Telemática)

•1970: Robert Metcalfe, estudiante del MIT, empieza una tesis doctoral en Harvard sobre optimización del protocolo Aloha de Abramson.

• 1972: Metcalfe con 27 años, se traslada al Xerox PARC (Palo Alto Research Center, Silicon Valley) donde se le encarga diseñar la red del laboratorio. Le ayuda un estudiante de Stanford, David Bogas.

• 22 de mayo de 1973: Metcalfe y David Boggs anuncian la comunicación de dos ordenadores con una red llamada Ethernet (2,94 Mb/s con 1600 metros de coaxial de 50 ohms) con protocolo CSMA/CD.

• 1975: Boggs crea el primer router y una aplicación para servicio de nombres.

•1976: Xerox crea una nueva división para el lanzamiento comercial de los PCs y de Ethernet, pero el intento fracasa.

• 1979: Metcalfe abandona Xerox y promueve la creación del consorcio DIX (Digital-Intel-Xerox) para potenciar el uso de Ethernet (ya entonces a 10 Mb/s). Además, como Xerox no puede producir tarjetas de red, crea la empresa “Ordenadores, Comunicaciones y Compatibilidad” 3COM.

• 1980: DIX publica Ethernet v 1.0, pero IEEE busca una estandarización.

• Febrero de 1980: El IEEE crea el proyecto 802 para aprobar el estándar de LAN.

• IEEE 802 recibe tres propuestas:

– CSMA/CD (DIX): DIX intenta ‘imponer’ EN a 802
– Token Bus (General Motors)
– Token Ring (IBM)
• 1984: Boggs deja Xerox y pasa a Compaq.

WiFi (Fidelidad Inalámbrica) es un nombre comercial desarrollado por un grupo de comercio industrial llamado WiFi Alianza (Inicialmente: 3Com – Aironet [hoy parte de CISCO] – Harris – Lucent – Nokia y Symbol technologies, hoy más de 150 miembros), el nombre “oficial” de esta alianza es **WECA** (Radio Alianza de Compatibilidad de Ethernet) y son los primeros responsables de 802.11b.

• El estándar **802.11** de IEEE se publica en junio 1997, luego de seis años de proceso de creación. Propone velocidades de 1 y 2 Mbps y un rudimentario sistema de cifrado (**WEP**: Intimidad Equivalente De alambre), opera en 2,4 GHz con RF e IR. Aunque WEP aún se sigue empleando, ha sido totalmente desacreditado como protocolos seguro.

En septiembre de 1999 salen a la luz el estándar **802.11b** que ofrece 11Mbps y el **802.11a** que ofrece 54 Mbps, si bien los productos de la primera aparecieron en el mercado mucho antes algunos fabricantes ofrece velocidades de 72 e incluso 108 Mbps. Estos procesos, lo logran mediante la "Vinculación de canales", es decir, dos canales son multiplexados juntos empleando el total de velocidad de la suma de ambos, esto si bien es favorable aparentemente, tiene las desventajas de no respetar el estándar y de sacrificar la mitad de los canales de 802.11a.
La familia 802.11, hoy se encuentra compuesta por los siguientes estándares:

• **802.11a:** (5,1-5,2 Ghz, 5,2-5,3 Ghz, 5,7-5,8 GHz), 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal.

• **802.11b:** (2,4-2,485 GHz), 11 Mbps.

• **802.11c:** Define características de AP como Puentes.

• **802.11d:** Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).

• **802.11e:** Calidad de servicio (QoS).

• **802.11f:** Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP Enterrar el Protocolo de Punto de Acceso.

• **802.11g**: (2,4-2,485 GHz), 36 o 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.

• **802.11h:** DFS: Dynamic Selección de Frecuencia, habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.

• **802.11i:** Seguridad (aprobada en Julio de 2004).

• **802.11j:** Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).

• **802.11m:** Mantenimiento redes wireless.

Quizás el tema más importante a destacar es la posibilidad de expansión de 802.11. El incremento constante de mayores velocidades, hace que los 11 Mbps de 802.11b, estén quedando pequeños. La migración natural es hacia 802.11g, pues sigue manteniendo la frecuencia de 2,4GHz, por lo tanto durante cualquier transición en la que deban convivir, ambos estándares lo permiten, en tanto que si se comienzan a instalar dispositivos 802.11a, los mismos no permiten ningún tipo de compatibilidad con 802.11b, pues operan en la banda de 5 GHz.

1.2. MODOS DE TRANSMISIÓN.

Transmisión Inalámbrica. Las redes WLAN utilizan ondas electromagnéticas dentro del espectro de radio frecuencia (RF) e infrarrojo (IR) para transferir datos desde un punto a otro. Los organismos encargados de regular la concesión de licencias sobre el espectro de radio frecuencia han dispuesto una serie de frecuencias para el uso comercial sin licencia.

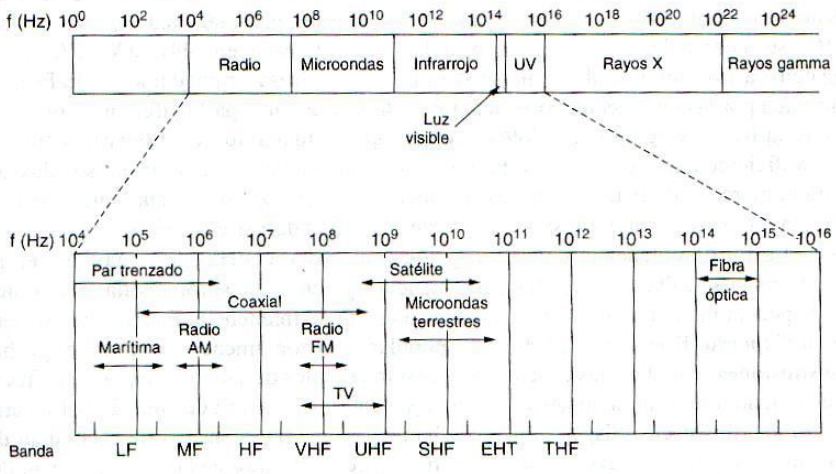
Estas bandas ISM (bandas de uso industrial, científico y medico) incluyen las bandas de 900 MHz, 2.4 GHz y 5 GHz utilizados por que en ella se generan. Hay varios medios de transmisión capaces de transferir datos mediante ondas electromagnéticas. Al igual que sucede con casi todas las tecnologías, cada uno de esos medios tiene sus propias ventajas y limitaciones.

Espectro Electromagnético. Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar en el espacio libre, aun en el vacío. La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia***, f,*** y se mide en Hz. La distancia entre dos máximos o mínimos consecutivos se llama longitud de onda y se designa con la letra griega ***l***.

Al conectarse una antena apropiada a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio. En el vacío todas las ondas electromagnéticas viajan a la misma velocidad, sin importar su frecuencia, esta velocidad, usualmente

llamada velocidad de la luz***, c***, es aproximadamente 3x108 m/seg. La figura 1. Muestra el espectro electromagnético. Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas.

Figura 1. Espectro electromagnético



Radio Transmisión. Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto de interiores como de exteriores. Las ondas de radio también son omnidireccionales, es decir, viajan en todas las direcciones desde la fuente, por lo cual el transmisor y el receptor no tienen que alinearse. Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos.

Estas también son absorbidas por la lluvia. Todas las ondas de radio están sujetas a interferencia por los motores y equipos eléctricos, debido a la

capacidad de viajar distancias largas y la interferencia entre usuarios, los gobiernos legislan el uso de radiotransmisores.

Sistemas de radio de banda estrecha. Los sistemas de radio de banda estrecha transmiten y reciben datos en una frecuencia de radio específica. Los diferentes usuarios se comunican en frecuencias alternativas o canales, para garantizar un cierto nivel de intimidad y evitar las interferencias. Los receptores de radio se construyen para ponerse en escucha solo en su frecuencia designada, filtrando todas las restantes. La limitación natural de este sistema es clara: si otro transceptor está operando a la misma frecuencia y dentro del rango de cobertura, se producirá interferencia y los datos se perderán o corromperán.

Sistemas de radio de banda ancha (Expansión de espectro). Los sistemas de radio de banda ancha en lugar de utilizar una única frecuencia, la tecnología de expansión de espectro, como su nombre lo indica, recorre las bandas de frecuencias disponibles para transmitir los datos de manera fiable. Originalmente fue empleada por militares, la tecnología de expansión de espectro distribuye la señal sobre un amplio rango de frecuencias de manera uniforme, consumiendo así mayor ancho de banda a cambio de conseguir mayor fiabilidad, integridad y seguridad de las comunicaciones.

Esta forma de transmisión permite a los dispositivos evitar interferencias y ruidos provocados por otras señales. Existen dos tecnologías de banda ancha: la tecnología de expansión de espectro por secuencia directa (DSSS, Dirijas Espectro de Extensión de Seequence) y la tecnología de expansión de espectro por salto de frecuencia (FHSS, Frecuencia que Salta

Espectro de Extensión). En la secuencia directa (DSSS) el flujo de bits de entrada se multiplica por una señal de frecuencia mayor (señal portadora), basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor relacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital (DSP) para relacionar la señal de entrada.

El salto de frecuencia (FHSS), es una técnica en la que los dispositivos receptores y emisores se mueven de forma sincrónica en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método DSSS, los datos deben ser reconstruidos con base en el patrón de salto de frecuencia. Este método es viable para redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 MHz que son utilizadas por hornos de Microondas.

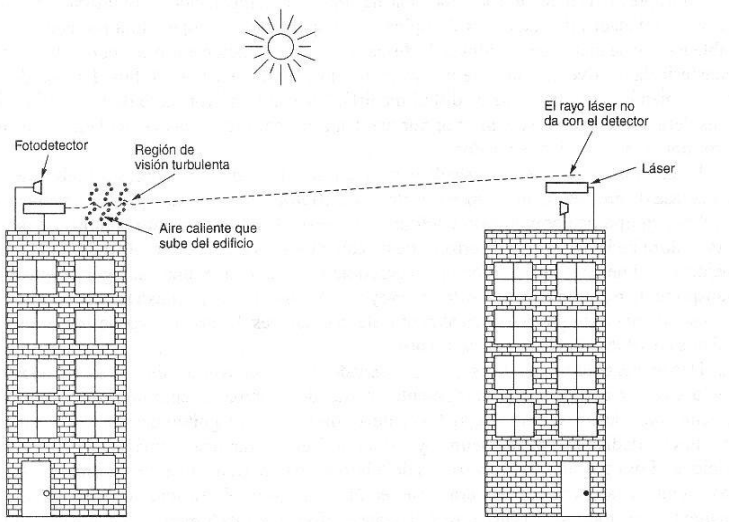
Transmisión Por Microondas. Por encima de los 100MHZ las ondas viajan en línea recta, por tanto se pueden enfocar en un haz estrecho. Concentrar toda la energía en haz pequeño con una antena parabólica produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora se deben alinear entre si.

Ondas Infrarrojas. Se usan mucho para la comunicación de corto alcance. Por ejemplo los controles remotos de los equipos utilizan comunicación infrarroja. Estos son direccionales, tienen el inconveniente de no atravesar los objetos sólidos. Lo que es una ventaja, por lo que un sistema infrarrojo no interferirá un sistema similar en un lado adyacente. Además la

seguridad de estos sistemas contra espionaje es mejor que la de los sistemas de radio. Este sistema no necesita de licencia del gobierno para operar en contraste con los sistemas de radio. Esta propiedad ha hecho del infrarrojo un candidato interesante para las WLAN en interiores.

Transmisión Por Ondas De Luz. Este tipo de transmisión se ha usado durante siglos. Una aplicación es conectar las LAN de dos edificios por medio de láser montados en la parte más alta de estos, esta señalización óptica es unidireccional por lo que cada edificio necesita su propio láser y su propio foto detector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. Fácil de instalar y no requiere de licencia. Por ser un haz muy estrecho tiene ventajas pero también debilidades. La desventaja es que los rayos láser no pueden penetrar la lluvia ni la niebla densa, funcionan bien en días soleados.

Figura 2. Transmisión Por Ondas De Luz



1.3. RED DE ÁREA LOCAL LAN (Local Area NetworK)

A medida que la necesidad de comunicación e intercambio de información se convirtió en necesidad cada vez grande, tanto en pequeñas como en grandes empresas, la industria de telecomunicaciones empezó a crear soluciones que permitieran de forma ordenada, poner al alcance de los usuarios finales dichos servicios.

Desde ese momento, emergió el concepto de “Redes de computadores”, o lo que se conoce como Redes de Área Local (LAN). Esta solución, que no es más que la combinación de hardware de computo y medios de transmisión relativamente pequeños, por lo regular no sobrepasa las decenas de kilómetros y comúnmente utilizan un solo medio de transmisión. En términos generales, una LAN queda comprendida dentro de un edificio.

Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI. La capa física indica como son enviados los bits de una estación a otra[1]. Una WLAN puede ser configurada como una red punto a punto (llamada red ad-hoc) donde dos o más estaciones de trabajo directamente intercambian información de una a otra, o bien puede ser en modo infraestructura donde un punto de acceso (AP, Punto de Acceso) central encierra todas las comunicaciones entre las estaciones de trabajo que se encuentran alrededor de él.

[1] González N, L. Seguridad en redes inalámbricas para sistemas multimedia de tiempo real

Modo ad-hoc. Cuando dos o más nodos están lo suficientemente cerca como para comunicarse uno con otro, se forma un conjunto de servicio básico (BSS, Servicio Básico Set). El mínimo BSS consiste en dos estaciones. Un BSS que se encuentra solo y que no esta conectado a un AP es llamado "conjunto de servicio básico independiente" (IBSS, Servicio Independiente Básico set) o "red ad-hoc".

Un conjunto de servicio extendido (ESS, Servicio Ampliado Set) es formado cuando dos o más BSSs operan dentro de la misma red (Figura3). Una red ad-hoc es una red cuando las estaciones se comunican solo a través de la configuración peer-to-peer (entre iguales). No hay APs, y no se necesita permiso para la comunicación. La mayoría de estas redes son espontáneas y se pueden configurar de manera rapida[2]

Figura 3. Conexión *peer to peer*

Tomado de: Redes Inalámbricas: IEEE 802.11. Disponible en www.canal-ayuda.org/.../new_pa14.jpg

[2] Vega B A y Martínez D. Seguridad Wifi. Asignatura: Redes y Sistemas de Radio Curso: 2004/2005.

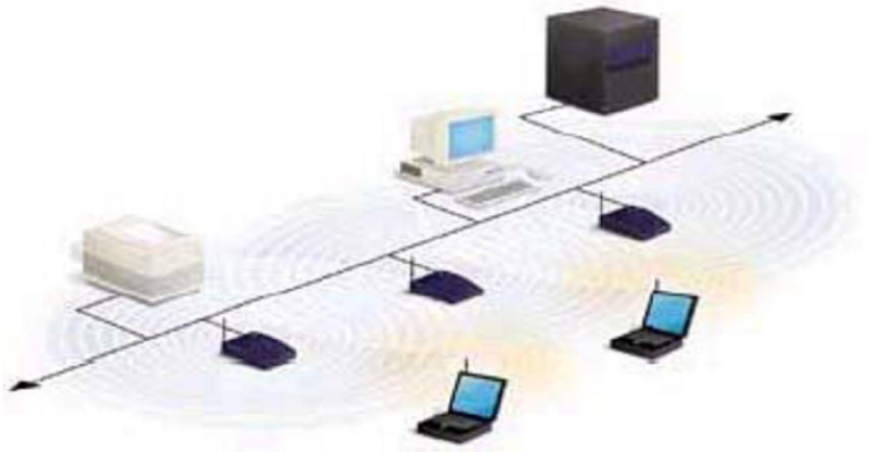
Modo infraestructura. Se dice que una WLAN esta siendo operada en un modo infraestructura cuando dos o más BSSs son interconectados usando un punto de acceso (AP). Un punto de acceso actúa como concentrador para los nodos de la red inalámbrica. Un AP encamina el tráfico entre los BSSs (Figuras 4, 5).

Algunas veces los puntos de acceso están conectados a las redes comunes (es decir las redes cableadas) para proporcionar o compartir los recursos de dicha red, a los nodos de la red inalámbrica. Las redes inalámbricas en modo infraestructura son la configuración más común en redes grandes.

Figura 4. Utilización de un *Punto de acceso*

Tomado de: Redes Inalámbricas: IEEE 802.11. Disponible en www.canal-ayuda.org/.../new_pa14.jpg

Figura 5. Utilización de un varios *Puntos de acceso*



Tomado de: Redes Inalámbricas: IEEE 802.11. Disponible en www.canal-ayuda.org/.../new_pa14.jpg

1.3.1. Estándares de redes inalámbricas. Bluetooth. Representa una alianza entre las comunicaciones móviles y compañías de cómputo móvil. La alianza se formó en 1998 promovida por manufactureras como Ericsson, Nokia, IBM, Intel y Toshiba. Una de las razones para el desarrollo de Bluetooth fue que entre la gran variedad de opciones de conectividad no se tenía compatibilidad entre una y otra[3].

La pila de protocolos de Bluetooth no esta representada por las siete capas clásicas del modelo de referencia OSI. Esto porque Bluetooth es un intento por ínteroperar con módems, teléfonos y otros dispositivos, catalogada como una red de área personal (PAN, Personal Área Network,), es decir, es

[3] Ganz A, Ganz Z, y Wongthavarawat K. Multimedia Wireless Networks: Technologies, Standards and QoS. Prentice Hall, USA 2003.

una red de modo ad-hoc y su principal ventaja es su mínimo consumo de energía.

HiperLAN. Es un estándar de telecomunicaciones desarrollado en Europa por el ETSI (Instituto de Normas de Telecomunicaciones Europeo). Considerado como el estándar más parecido al 802.11b de IEEE. HiperLAN tiene dos estándares:

HiperLAN/1: En 1991 el ETSI formó el comité subtécnico RES10 para desarrollar HiperLAN. El resultado fue el estándar de Hiper- LAN/1 (aprobado en 1996) que define la capa física (PYH) y la capa de acceso al medio (MAC) especificaciones para las redes inalámbricas de alta velocidad de comunicaciones. HiperLAN/1 usa GMSK (pulsación de cambio(movimiento) gaussiana mínima) y especifica la tasa de transferencia por arriba de 20 Mbps entre dispositivos portátiles.

Una ventaja de HiperLAN/1 es que trabaja en un ancho de banda dedicado (5.1 a 5.3 GHz, solo disponible en Europa), adicionalmente no usa la tecnología de Extensión Espectro en orden para coexistir con otra frecuencia de radio como es el caso del rango ISM 2.4GHz. También, el protocolo usa una variante de CSMA/CA y opcionalmente incluye cifrado de la información.

Otra característica de HiperLAN/1 es un encaminamiento ad-hoc. Por ejemplo, si su destino esta fuera de rango, los nodos intermedios automáticamente lo reenvían encontrando la mejor ruta disponible dentro de la red HiperLAN/1 (las rutas son recalculadas automáticamente de manera regular).

HiperLAN/2: En 1997, el ETSI formó el grupo BRAN (Radio De banda ancha Red de Área) para trabajar sobre HiperLAN/2, que fue aprobado en febrero de 2000. HiperLAN/2 es un rediseño de Hiper-LAN/1 y fue el primer estándar en usar OFDM. HiperLAN/2 y IEEE 802.11a son muy similares en su uso de la banda 5GHz y OFDM para obtener tasas de transferencias superiores a 54Mbps. La principal diferencia entre los dos estándares está en la parte de acceso al medio de los sistemas. HiperLAN/2 usa TDM (Multiplexación de División de Tiempo), además de 802.11a/g usa CSMA/CD.

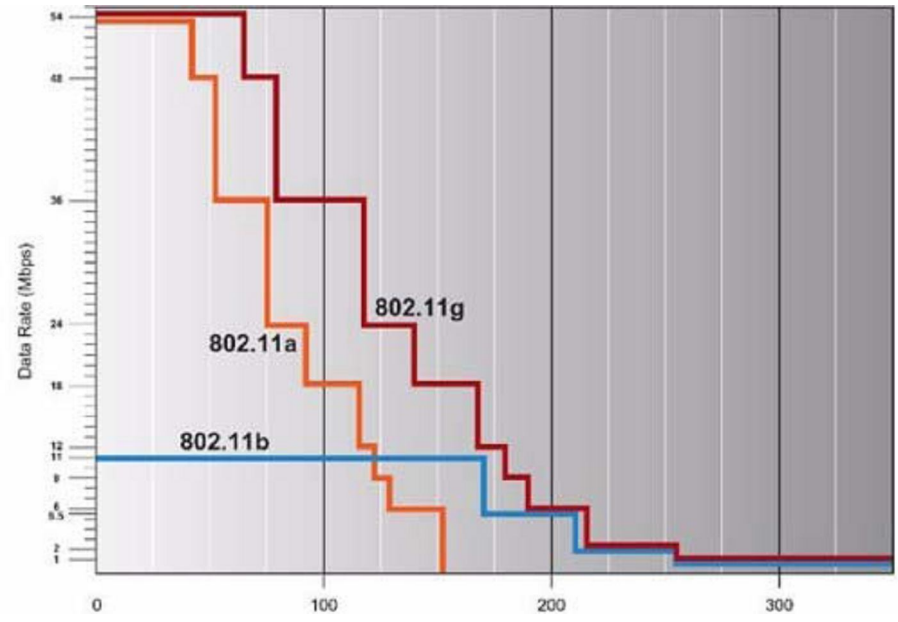
HomeRF. Etiqueta para un grupo industrial que se unió en 1998, para desarrollar un estándar para conectividad inalámbrica entre computadores personales y dispositivos electrónicos. El estándar que resultó es el Compartido Protocolo de Acceso Inalámbrico (SWAP), que permite transmitir voz y datos con una tasa de transferencia sobre 1.6 Mbps.

IEEE 802.11. En el ámbito de las redes WLANs el estándar que más ha destacado es la especificación de la IEEE: 802.11. Liberada en 1997, hoy es la especificación más utilizada ya que brinda a sus usuarios flexibilidad, simplicidad de uso y efectividad de costos. Este estándar especifica los parámetros de dos capas del modelo OSI: la capa física (PHY) y la capa de control de acceso al medio (MAC). La capa MAC tiene tres funciones principales: Controlar el canal de acceso, mantener la calidad de servicio (QoS) y proveer seguridad. Además de que soporta servicios de seguridad para las aplicaciones de las capas superiores tales como autenticación y privacidad, pero la especificación IEEE 802.11 sólo da un método débil de autenticación y para asegurar la privacidad cuenta con una opción llamada Intimidad Equivalente De alambre (WEP) que no ha cumplido con

su propósito. Al inicio, el 802.11 especificaba un bajo índice de transferencia real, hasta de 2Mbps.

El estándar ha sido mejorado en dos diferentes especificaciones: el estándar 802.11b conocido como Wi-Fi, que permite en teoría, funcionalidad inalámbrica comparable con Ethernet con un índice de transferencia real de hasta 11Mbps en la banda comercial y el estándar 802.11a que permite hasta 54Mbps en la banda industrial, científica y médica. La arquitectura de una WLAN IEEE 802.11 consiste, generalmente, de un conjunto de servicios básicos (BSS) que se interconectan a un sistema de distribución (DS) para formar un conjunto de servicios extendidos (ESS) (Figura 6).

Figura 6. Comparativa entre 803.11b, 803.11a y 803.11g (Mbps/pies)



Fuente: Bernier et. al (2005)

2. PROBLEMAS CONCRETOS DE LA SEGURIDAD EXISTENTE EN REDES LAN INALAMBRICAS

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

2.1. PUNTOS OCULTOS

Este es un problema específico de las redes inalámbricas, pues es muy común que los propios empleados de la empresa por cuestiones de comodidad, instalen sus propios puntos de acceso. Este tipo de instalaciones, si no se controlan, dejan grandes huecos de seguridad en la red. El peor de estos casos es la situación en la cual un intruso lo deja oculto y luego ingresa a la red desde cualquier ubicación cercana a la misma. La gran ventaja que queda de este problema es que es fácil su identificación siempre y cuando se propongan medidas de auditorías periódicas específicas para las infraestructuras WiFi de la empresa, dentro del plan o política de seguridad.

2.2. FALSIFICACIÓN DE AP

Es simple colocar un AP que difunda sus SSID, para permitir a cualquiera que se conecte, si sobre el mismo se emplean técnicas de “Phishing”, se puede inducir a creer que se está conectando a una red en concreto. Existen varios productos ya diseñados para falsificar AP, en la terminología WiFi se los suelen llamar “Granuja AP” o Falsificación AP”, el más común es un conocido escritura en Perl denominado justamente “FakeAP”, que envía Faros con diferentes ESSID y diferentes direcciones MAC con o sin empleo de WEP.

2.3. DEFICIENCIAS EN WEP (Características lineales de CRC32)

Esta característica fue demostrada en teoría por Nikita Borisov, Ian Goldberg y David Wagner. El ICV permite verificar la integridad de un mensaje, por lo que, el receptor aceptará el mensaje si su ICV es válido. Esto presenta dos problemas:

- El CRC es independiente de la clave empleada.
- Los CRC son lineales CRC (m € k) = CRC (m) € CRC (k). En virtud de esta linealidad, se puede generar un ICV válido. Un atacante debe interceptar un mensaje (conocido o no) y modificarlo en forma conocida para generar un mensaje m, operando sobre el mismo obtendrá un paquete que será aceptado por el receptor.

2.4. ICV INDEPENDIENTE DE LA LLAVE

Esta característica fue demostrada en teoría por David Wagner. Nuevamente se trata el ICV, el cual se calcula previamente a comenzar el

proceso criptográfico, por lo tanto no depende de la clave ni del IV. Esta debilidad da lugar a que conocido el texto plano de un solo paquete encriptado con WEP, sea posible inyectar paquetes en la red.

2.5. TAMAÑO DE IV DEMASIADO CORTO

El IV tiene 24 bits de longitud (224 = 16.777.216) y viaja como texto plano. Un punto de acceso que opere con grandes volúmenes de tráfico comenzará a repetir este IV a partir de aproximadamente 5 horas. Esta repetición hace que matemáticamente se pueda operar para poder obtener el texto plano de mensajes con IV repetido. El estándar especifica que el cambio de IV es opcional, siendo un valor que empieza con cero y se va incrementando en uno.

2.6. DEFICIENCIAS EN EL MÉTODO DE AUTENTICACIÓN

Si un atacante captura el segundo y tercer mensaje de administración en una autenticación mutua. El segundo posee el desafío en texto plano y el tercero contiene el mensaje criptografiado con la clave compartida. Con estos datos, posee todos los elementos para autenticarse con éxito sin conocer el secreto compartido.

2.7. DEBILIDADES EN EL ALGORITMO LLAVE QUE PROGRAMA de RC4

Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron en Agosto del 2001 la demostración teórica de la vulnerabilidad más devastadora de las existentes hasta ahora en la encriptación WEP. Adam Stubblefield, un

trabajador de AT&T Labs, fue la primera persona que implementó este ataque con éxito.

Demostraron que usando sólo la primera palabra de un keystream, podían obtener información de la clave secreta compartida. Se buscan IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición "*condición resuelta"* o condición resuelta. El número de paquetes que se necesitan recolectar antes de descubrir un byte de la llave varía en función que en que valor se encuentre el contador de IV's de las tarjetas que se estén monitorizando. Hay 9.000 IV's débiles en los 16 millones de IV's posibles.

Algunas llaves requieren que sean capturados incluso más de 4000 paquetes resueltos. Se puede adivinar la llave después de recolectar de 5 a 10 millones de paquetes encriptados. Poco después de que el trabajo realizado por estos tres autores y la vulnerabilidad práctica de Stubblefield fuera publicado, aparecieron dos herramientas en Internet que implementan totalmente el ataque:

- Wepcrack
- Airsnort

2.8. DEBILIDAD EN WPA

Un estudio realizado por Robert Moskowitz, director de ICSA Labs, indica que el sistema utilizado por WPA para el intercambio de la información utilizada para la generación de las claves de cifrado es muy débil. Según este estudio, WPA en determinadas circunstancias es incluso más inseguro que WEP. Cuando las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los

20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves.

Sobre este tráfico, realizando un ataque de diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red. Es decir, a diferencia de WEP en que es necesario capturar un volumen significativo de tráfico para poder identificar las claves, en WPA únicamente capturando el tráfico de intercambio de claves es posible realizar este ataque de diccionario. Esto no es un problema nuevo, pues fue apuntado durante la verificación inicial del protocolo. Es solo una muestra que una implementación inadecuada puede afectar negativamente cualquier sistema de cifrado. Es claro entonces que el problema solo es explotable bajo una serie de circunstancias muy concretas. Este problema puntual no es, en absoluto, una indicación de la debilidad de WPA. Únicamente es indicador de la necesidad de utilizar claves convenientemente largas y que incluyan caracteres especiales.

2.9. DEFICIENCIAS EN LA ENCRIPTACIÓN WEP

2.9.1. Características lineales de CRC32. Esta vulnerabilidad fue demostrada teóricamente por Nikita Borisov, Ian Goldberg y David Wagner (Universidad de Berkeley).

Como ya se ha mencionado anteriormente, el campo ICV (Valor de Comprobación de Integridad) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje. Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (Comprobación de Redundancia Cíclica) de

32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

- Los CRCs son independientes de la llave utilizada y del IV.
- Los CRCs son lineales:

$$\mathbf{CRC\ (m \oplus k) = CRC\ (m) \oplus CRC\ (k)}$$

Debido a que los CRCs son lineales, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es lineal y esto permite hacer el '*tirando de bit"* como veremos a continuación:

-Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m':

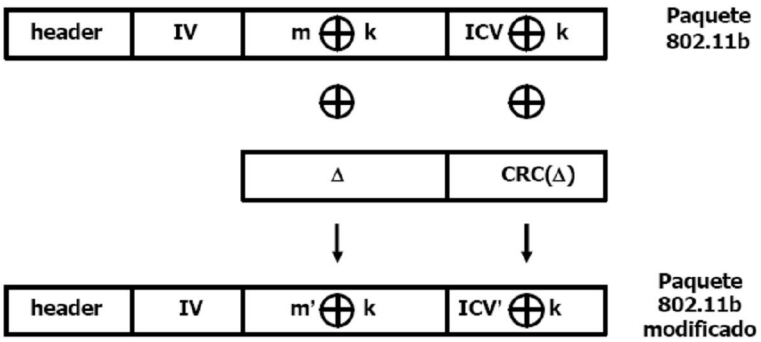
$$\mathbf{m' = m \oplus \Delta}$$

-Como el CRC-32 es lineal, puede generar un nuevo ICV' a partir del ICV de m:

$$\mathbf{IC' = IC \oplus h\ (\Delta)}$$

-ICV' será valido para el nuevo ciphertext c'

$$\mathbf{c' = c \oplus \Delta = k \oplus (m \oplus \Delta) = k \oplus m'}$$



2.9.2. MIC Independiente de la llave. Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de Berkeley). Conocida en inglés como "Carencia de keyed MIC": Ausencia de mecanismo de chequeo de integridad del mensaje (MIC) dependiente de la llave. El MIC que utiliza WEP es un simple CRC-32 calculado a partir del payload, por lo tanto no depende de la llave ni del IV. Esta debilidad en la encriptación da lugar a que conocido el plaintext de un solo paquete encriptado con WEP sea posible inyectar paquetes a la red.

Esto es posible de la siguiente manera:

-El atacante captura un paquete **c = m ⊕ k** donde m es conocido (por ejemplo, el atacante envía un e-mail a la víctima).

-El atacante recupera el flujo pseudo-aleatorio **k = c ⊕ m** para el IV concreto del paquete.

-Si el atacante quiere inyectar un mensaje m', debe realizar lo siguiente:

ICV' = CRC32 (m')

- El atacante ya puede ensamblar la parte encriptada del paquete:

c = (m'ICV') ⊕ k

-El atacante obtiene un paquete válido y listo para ser inyectado a la red:

2.9.3. Tamaño de IV demasiado corto. Otra de las deficiencias del protocolo viene dada por la corta longitud del campo IV en las tramas 802.11b. El vector de inicialización (IV) tiene sólo 24 bits de longitud y aparece en claro (sin encriptar), matemáticamente sólo hay 2^24 (16.777.216) posibles valores de IV. Aunque esto pueda parecer mucho, 16 millones de paquetes pueden generarse en pocas horas en una red wireless con tráfico intenso.

2.9.4. Reutilización de IV. Esta vulnerabilidad fue demostrada teóricamente por David Wagn0er (Universidad de Berkeley). Se basa en que WEP no utiliza el algoritmo RC4: el Vector de Inicialización se repite frecuentemente. Se pueden hacer ataques estadísticos contra cyphertexts con el mismo IV. Si un IV se repite, se pone en riesgo la confidencialidad. El estándar 802.11 especifica que cambiar el IV en cada paquete es opcional. El IV normalmente es un contador que empieza con valor cero y se va incrementando de uno en uno, por lo tanto:
-Rebotar causa la reutilización de IV's, solo hay 16 millones de IV's posibles, así que después de interceptar suficientes paquetes, seguro que hay IV's repetidos. Un atacante capaz de escuchar el tráfico 802.11 puede descifrar ciphertexts interceptados incluso sin conocer la clave.

2.9.5. Deficiencias en el método de autenticación Shared Key. El método de autenticación de Llave Compartida descrito anteriormente se puede explotar fácilmente mediante un ataque pasivo:

El atacante captura el segundo y el tercer mensajes de dirección de una autenticación mutua (texto De autenticación y Respuesta De autenticación). El segundo mensaje contiene el texto no muy claro, y el tercer mensaje contiene el texto encriptado con la clave compartida. Como

el atacante conoce el texto aleatorio (plaintext, P), el texto encriptado (cyphertext, C), y el IV público, el atacante puede deducir el flujo pseudo-aleatorio (keystream) producido usando WEP utilizando la siguiente ecuación:

$$WEP_{PR}^{K,IV} = C \oplus P$$

El tamaño del keystream será el tamaño de la trama de autenticación, ya que todos los elementos de la trama son conocidos: número de algoritmo, número de secuencia, código de estado, elemento id, longitud, y el texto de desafío. Además, todos los elementos excepto el texto de desafío son los mismos para todas las Respuestas De autenticación.

El atacante tiene por tanto todos los elementos para autenticarse con éxito sin conocer la clave secreta compartida K. El atacante envía un Petición De autenticación al AP con el que se quiere asociar. El AP contesta con un texto de desafío en claro. El atacante entonces, coge el texto de desafío aleatorio, R, y el flujo pseudo-aleatorio WEPk, IV PR y genera el cuerpo de una trama Authentiation Response válido, realizando una operación XOR con los dos valores.

El atacante entonces debe crear un nuevo ICV valido aprovechando la vulnerabilidad de características lineales de CRC32. Una vez creado el nuevo ICV, el atacante acaba de completar la trama de Authentication Response y la envía, de esta manera se asocia con el AP y se une a la red. Con este proceso el atacante sólo esta autenticado, pero todavía no puede

utilizar la red. Como el atacante no conoce la clave compartida, para poder utilizar la red debe implementar algún ataque al protocolo WEP.

3. IDENTIFICACION Y SOLUCION DE PRINCIPALES PROBLEMAS DE SEGURIDAD EN REDES LAN INALAMBRICAS

El acceso tan flexible y rápido sin necesidad de usar cables, es motivo por el que las redes inalámbricas han tenido tanto desarrollo, pero en consecuencia resulta un problema grande en lo que a seguridad se refiere.

Existen diferentes métodos para garantizar seguridad dentro de una comunicación inalámbrica como: filtrado de direcciones MAC, uso del protocolo WEP (Intimidad Equivalente De alambre), conexión a través de CNAC (Control de Acceso de Red Cerrado), entre otros. Estos métodos aunque intentan garantizar niveles de seguridad dentro de la red a diferentes niveles del modelo OSI, en la mayoría de los casos requieren implementar otros mecanismos para elevar los niveles de seguridad de la red, dentro de los cuales se puede mencionar: VPNs, implementar seguridad a nivel de la capa de aplicación usando seguridad basada en criptografía, entre otros.

3.1. FILTRADO DE DIRECCIONES MAC

Este método consiste en la creación de una tabla de acceso en cada uno de los puntos de acceso (AP) de la WLAN. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar a una determinada WLAN. Como toda tarjeta de red esta posee una dirección MAC única, que permite autenticar el equipo. Este método tiene como ventaja su sencillez, por lo que se puede usar para

redes relativamente pequeñas. No obstante, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes, entre las que se tiene:

- No es un sistema escalable y flexible, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

- El formato de una dirección MAC no es amigable (esta representado en 48 bits en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.

- Las direcciones MAC viajan sin cifrar por el aire. Un intruso podría obtener direcciones MAC de tarjetas autorizadas en la red empleando un sniffer y luego asignarle una de estas direcciones a su computador, empleando programas como: AirJack6 o WellenReiter, haciéndose pasar por un usuario válido.

3.2. PROTOCOLO WIRED EQUIVALENT PRIVACY (WEP)

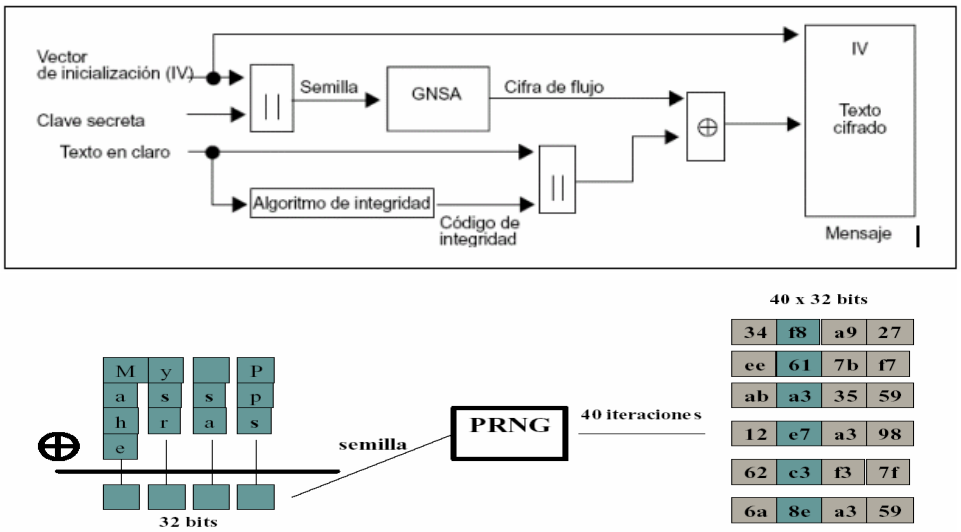
Este protocolo forma parte de la especificación 802.11[4] creado con la finalidad de proteger datos transmitidos en una comunicación inalámbrica mediante el uso de mecanismos de cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la mayoría de los dispositivos inalámbricos[5].

[4] Randall K. Nichols, Panos C. Lekkas. Seguridad para comunicaciones inalámbricas. McGraw-Hill, 2003. Primera edición. pp 187-420.

[5]Comer D E. Internetworking with TCP/IP. Vol. I: Principles, Protocols and Architecture. Prentice-Hall, USA 1991. Segunda Edición.

WEP cifra de la siguiente manera (ver figura 7):

Figura 7. Proceso de cifrado WEP.



- A la trama en claro se le calcula un código de integridad (Valor de Comprobación de Integridad, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta vulnerabilidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama (Figura 7).

- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudoaleatorios. El generador RC4 es capaz de generar una secuencia seudoaleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).

- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.

- El IV y la trama se transmiten juntos.

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.

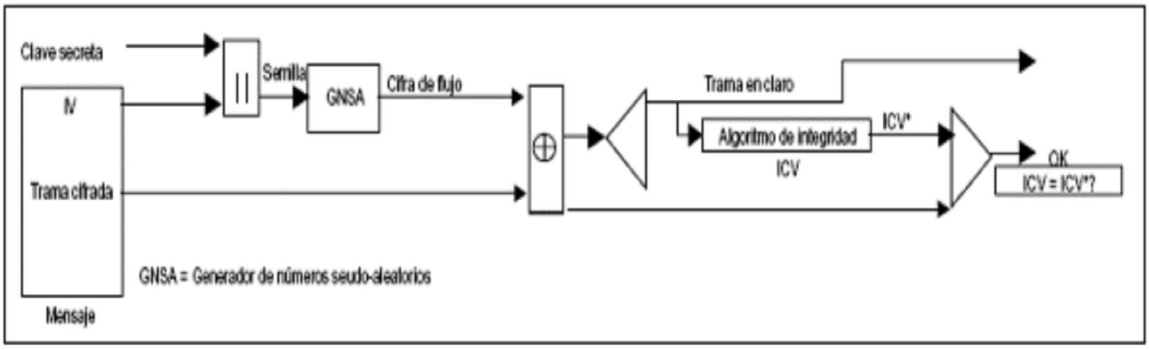
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión. Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrada, obteniéndose de esta manera la trama en claro y el ICV.

- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.

- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

WEP resuelve aparentemente el problema de la confidencialidad en la comunicación inalámbrica. Sin embargo, existen tres situaciones que hacen que WEP no sea seguro. Figura 8.

Figura. 8 Proceso de descifrado de WEP.



- En casi todas las redes de área local inalámbricas establecidas se emplea a WEP con claves de cifrado estáticas. Lo que hace posible que un atacante acumule grandes cantidades de tramas cifradas con la misma clave y pueda intentar un ataque por fuerza bruta.

- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2 a la 24 IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener las tramas en claro mediante un ataque estadístico. Con la trama en claro y su

respectivo cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen herramientas gratuitas que facilitan el trabajo de romper la clave secreta de enlaces protegidos con WEP como son: **WEPCrack**, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer o bien AirSnort hace lo mismo, pero integra las funciones de sniffer y analizador de claves y por tanto es más fácil de usar. **AirSnort** captura paquetes pasivamente y obtiene la clave WEP cuando ha capturado suficientes datos.

3.3. CNAC (Closed Network Access Control)

Consiste en usar el identificador de la red de área local inalámbrica (SSID, Servidor Pone ID) como contraseña para acceder a la red, tratando de ser un mecanismo de autenticación. Este identificador de red es fácil de conseguir ya que es enviado por los clientes al asociarse o autenticarse en el punto de acceso. Por lo que tampoco garantiza que usuarios no autorizados tengan acceso a la red.

3.4. TKIP (Protocolo de Integridad Temporal de Clave)

Las deficiencias presentadas por RC4 y WEP, se están tratando de solucionar en la actividad de cifrado, a través del protocolo **de Integridad**

Temporal de Clave. Propuesta que apareció a finales de 2002, también basada en RC4, pero propone tres mejoras importantes:

-**Combinación de clave por paquete:** La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Llave Precompartida). Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.

-**VI (Vector de inicialización)** de 48 bits: Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones.

-**MIC (Comprobación de Integridad de Mensaje):** Se plantea para evitar ataques inductivos o de hombre del medio. Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y genera una alerta, que indica una posible falsificación del mismo.

3.5. WPA (WiFi Acceso Protegido)

Microsoft ofrece otra alternativa que inicialmente denominó **SSN** (Red de Seguridad simple), el cual es un subconjunto de 802.11i y al mismo tiempo una implementación de **TKIP** al estilo Microsoft. SSN lo adoptó 802.11i renombrándolo como **WPA,** en el año 2004 aparece **WPA2** que es la segunda generación del WPA. Este ya proporciona encriptación con AES (que se menciona a continuación), un alto nivel de seguridad en la autentificación de usuarios y está basado en la norma IEEE 802. 11i y forma parte de ella.

Aunque la WPA impulsa la seguridad WLAN, muchos la consideran una solución temporal pues la solución de 802.11 se orienta hacia el Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (Counter-Mode/CBC-Mac Protocolo, CCMP), que también forma parte de la norma 802.11i.

Se trata de un nuevo modo de operación para cifrado de bloques, que habilita una sola clave para ser empleada tanto en autenticación como para criptografía. Se trata de un verdadero "Mix" de funciones, y su nombre completo proviene el "Counter mode" (CTR) que habilita la encriptación de datos y el Bloque de Cifra que Encadena Código de Autenticación de Mensaje (CBC-MAC) para proveer integridad, y de ahí su extraña sigla CCMP.
El protocolo CCMP usa la Norma de Encriptación Avanzada (AES) para proporcionar encriptación más fuerte. Sin embargo, AES no está diseñada para ser compatible con versiones anteriores de software. A pesar de todos los esfuerzos realizados, muchas entidades siguen considerando a TKIP y WPA como métodos insuficientes de seguridad, el mayor exponente de esta posición es FIPS (Estándar de Proceso de Información federal), que excluye a RC4 en las comunicaciones confidenciales. Su publicación FIPS-197 de finales del 2001, define al estándar AES (Avanzado Encriptación Estándar) con clave mínima de 128 bits, como el aplicable a niveles altos de seguridad.

La WiFi Alliance propone dos tipos de certificación para los productos, cuyas características se presentan a continuación:

- **Modelo Empresas:**

• WPA: Autentication: IEEE 802.1x/EAP. Encriptación: TKIP/MIC.
• WPA2: Autentication: IEEE 802.1x/EAP. Encriptación: AES-CCMP.

- **Modelo personal (SOHO/personal):**

• WPA: Autentication: PSK. Encryptation: TKIP/MIC.
• WPA2: Autentication: PSK. Encryptation: AES-CCMP.

3.6. SEGURIDAD EN LA INFORMACIÓN

El concepto de seguridad en la información es más amplio que la simple protección de los datos a nivel lógico. Para proporcionar seguridad real se deben tener en cuenta múltiples factores, tanto internos como externos.

En primer lugar hay que caracterizar el sistema que va albergar la información para poder identificar las amenazas y en este sentido se puede hacer la siguiente subdivisión:

Sistemas aislados: Son los que no están conectados a ningún tipo de red. De unos años a esta fecha se han convertido en minoría, debido al auge que ha experimentado internet.

Sistemas interconectados: Hoy en día casi cualquier computador pertenece a alguna red, enviando y recibiendo información del exterior casi constantemente. Lo que hace que las redes de computadores sean cada vez más complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

Es por ello que el objetivo principal de cualquier comunicación y administración de datos confiable es cumplir con los principios de la seguridad computacional, que se resumen en los siguientes servicios[6]:

Confidencialidad: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados, es decir se refiere a que la información sólo pueda ser leída por personas autorizadas.

Integridad: Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados. Es decir se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Autenticación: Es el proceso de verificar y asegurar la identidad de las partes involucradas, es decir se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

No repudio: Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente este proceso se lleva a cabo a través de la autenticación. Se refiere a que no se pueda negar la autoría de un mensaje enviado.

Cuando se diseña un sistema de seguridad, gran cantidad de problemas pueden ser evitados si se puede comprobar la autenticidad, garantizar la confiabilidad, asegurar integridad y el no rechazo de un mensaje. La

[6] Meneses A, Van Oorschot P and Vanstone S. Handbook of Applied Cryptography. CRC Press, New York 2001. Quinta Edición.

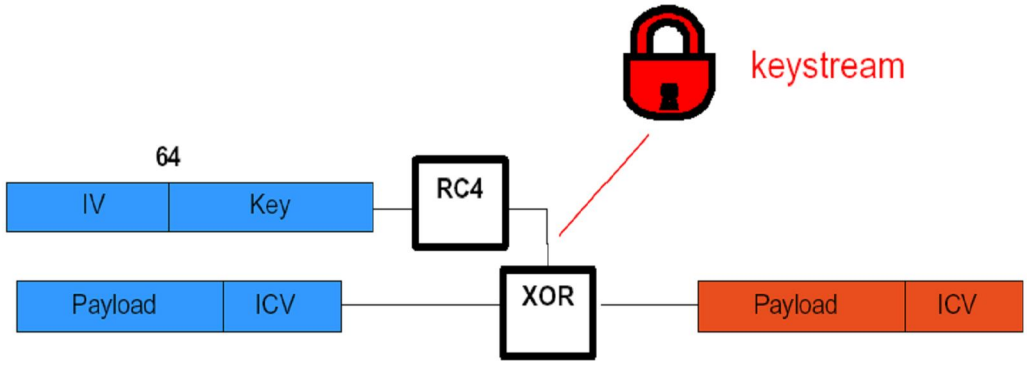
criptografía simétrica y asimétrica conjuntamente con otras técnicas, permiten en alto porcentaje lograr satisfactoriamente resolver los problemas planteados anteriormente.

3.7 CRIPTOGRAFÍA CIFRADO

La palabra criptografía proviene del griego ***kryptos***, que significa ocultar y ***gráphein***, escribir, es decir, escritura oculta[7]. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder ocultar el mensaje (cifrar o encriptar, Figura 9), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje oculto (descifrar o descencriptar, Figura 10).

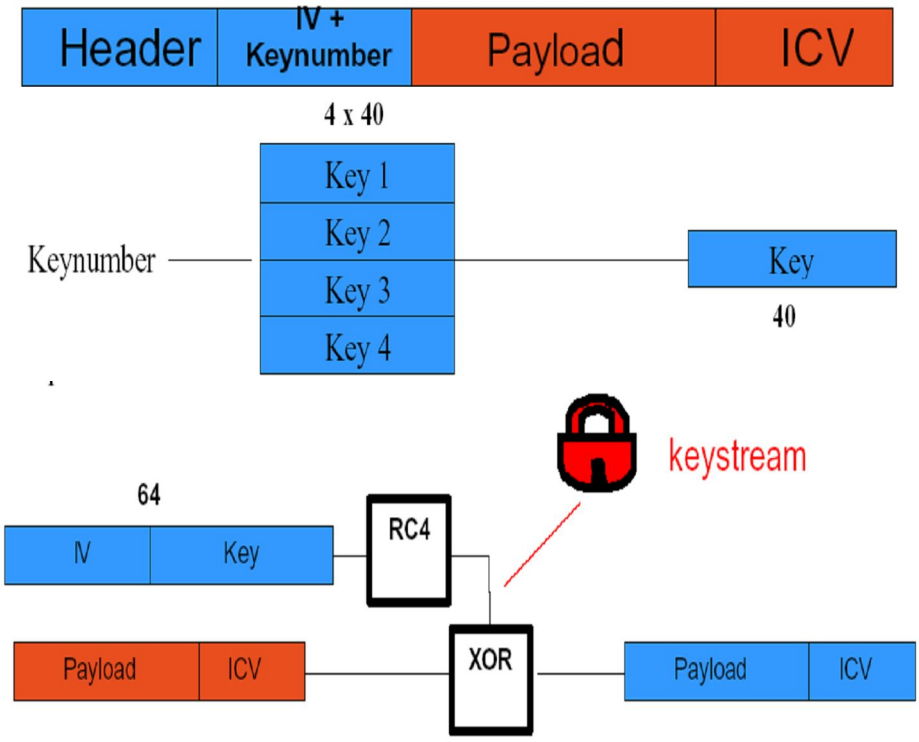
La criptografía se divide en dos grandes ramas, la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica.

Figura 9. Modo de cifrado



[7]Manuel J. Lucena López. Criptografía y seguridad en computadores. http://www.di.ujaen.es/ mlucena. 2003.

Figura 10. Modo de descifrar



3.7.1. Criptografía simétrica. Se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente (clave simétrica). La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar. Este tipo de criptografía se conoce también como criptografía de clave o de llave privada. La criptografía simétrica ha sido la más usada en toda la historia, esta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computador. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar (Figura 11).

Figura 11: Esquema e cifrado simétrico.

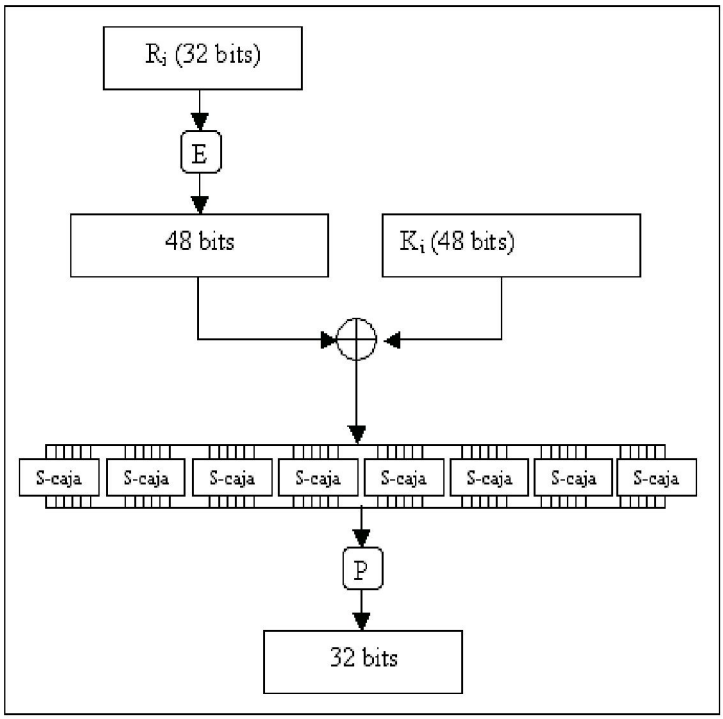
3.7.1.1. DES. Es el algoritmo simétrico mas extendido mundialmente, se basa en el algoritmo LUCIFER[8], desarrollado por IBM a principios de los setenta y adoptado como estándar por el gobierno de EE.UU. para comunicaciones no clasificadas en 1976.

El algoritmo DES codifica bloques de 64 bits empleando claves de 56 bits. Es una red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio ***(P_i)*** y otra que se aplica al final ***(P_f)***, tales que $P_i = P^{-1}_f$.

La función ***f*** (figura 12) se compone de una permutación de expansión ***(E),*** que convierte el bloque de 32 bits correspondiente en uno de 48 bits. Después realiza un or-exclusivo con el valor K_i, también de 48 bits, aplica ocho S-Cajas de 6*4 bits y efectúa una nueva permutación ***P***.

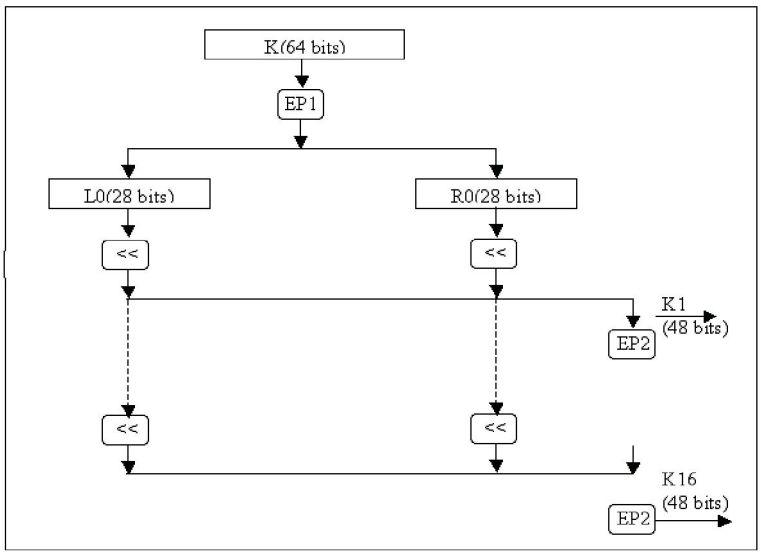
[8] Ibíd. Lucena M.

Figura 12: Esquema de la función f del algoritmo DES.



Se calcula un total de 16 valores de K_i (figura 13), uno para cada ronda, efectuando primero una permutación inicial ***EP1*** sobre la clave de 64 bits, llevando a cabo desplazamientos a la izquierda de cada una de las dos mitades de 28 bits resultantes y realizando finalmente una elección permutada ***(EP2***) de 48 bits en cada ronda, que será la K_i. Los desplazamientos a la izquierda son de dos bits, salvo para las rondas 1, 2, 9 y 16, en las que se desplaza solo un bit. Nótese que aunque la claves para el algoritmo DES tiene en principio 64 bits, se ignoran ocho de ellos un bit de paridad por cada byte de la clave, por lo que en la práctica se usan solo 56 bits.

Figura 13: Calculo de las Ki para el algoritmo DES.



Para descifrar basta con usar el mismo algoritmo (ya que $P_i = P^{-1}{}_f$) empleando las K_i en orden inverso.

3.7.1.2. TDES. Algoritmo que surge con la necesidad de elevar los índices de seguridad del algoritmo DES. Consiste en aplicar varias veces el algoritmo DES con diferentes claves al mensaje original. Se puede hacer ya que DES no presenta estructura de grupo. Triple-DES corresponde a la siguiente ecuación:

$$C = E_{K3}\,(E^{-1}{}_{K2}\,(E_{K1}\,(M))\,)$$

Es decir, se codifica con la subclave K_1, y se decodifica con K_2 y se vuelve a codificar con K_1. La clave resultante es la concatenación de K_1 y K_2, con una longitud de 112 bits. Es decir TDES consiste en aplicar 3 veces DES de la siguiente manera:

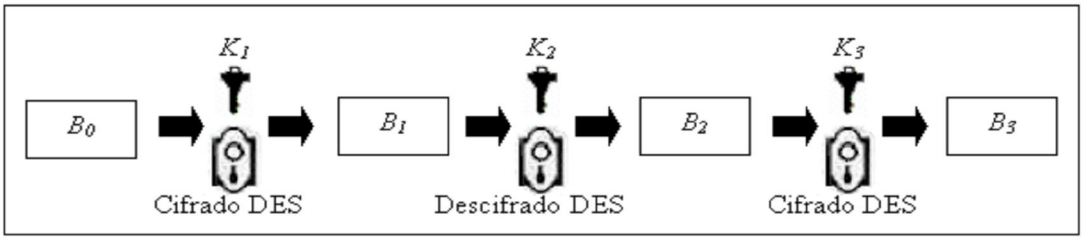
La primera vez se usa una clave K_1 junto con el bloque B_0, en modo de cifrado, obteniendo el bloque B_1.

La segunda vez se toma a B_1 con la clave K_2, diferente a K_1 de forma inversa, en modo de descifrado.

La tercera vez a B_2 con una clave K_3 diferente a K_1 y K_2 en modo cifrado (figura 14), es decir, aplica una relaccion de 1 a la 16 a B_0 con la clave K_1, después aplica de la 16 a la 1, a B_1 con la clave K_2, finalmente aplica una vez mas de la 1 a la 16 a B_2 usando la clave K_3, obteniendo finalmente a B_3.

En cada una de estas tres veces aplica el modo de operación más adecuado.

Figura 14: Esquema de cifrado de TDES



3.7.1.3. AES (Algoritmo Rijndael). En octubre de 2000 el NIST (Instituto Nacional para Standars y tecnología) anunció oficialmente la adopción del algoritmo Rijndael[9], como nuevo estándar avanzado de cifrado (AES) para su empleo en aplicaciones criptográficas no militares, culminando así un proceso de mas de tres años, encaminado a proporcionar a la comunidad

[9] Ibíd. Lucena M

internacional un nuevo algoritmo de cifrado potente, eficiente y fácil de implementar. El cual sustituiría a DES.

AES es un sistema de cifrado por bloques, diseñado para manejar longitudes de clave y de bloque variables, ambas comprendidas entre los 128 y los 256 bits. Realiza varias de sus operaciones internas a nivel de byte, interpretando estos como elementos de un cuerpo de Galois GF (2^8). El resto de sus operaciones se efectúan en términos de registros de 32 bits, sin embargo, en algunos casos, una secuencia de 32 bits se toma como un polinomio de grado inferior a 4, cuyos coeficientes son a su vez polinomios en GF (2^8).

AES tiene definido cada ronda como una composición de cuatro funciones invertibles formando tres capas, diseñadas para proporcionar resistencia frente a criptoanálisis lineal y diferencial. Cada una de las funciones tiene un propósito preciso:

- La capa de mezcla lineal: funciones desplazar fila (ShiftRows) y mezclar columnas (Mix Column), permiten obtener un alto nivel de difusión a lo largo de varias rondas.

- La capa no lineal: función ByteSub, consiste en la aplicación paralela de S-Cajas con propiedades optimas de no linealidad.

- La capa de adición de clave: la función AddRounKey es un simple or-exclusivo entre el estado intermedio y la subclave correspondiente a cada ronda.

3.7.2. Criptografía asimétrica. Es aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Hellman[10], proponen una forma para hacer esto, sin embargo no fue hasta que el popular método de Rivest Shamir y Adleman RSA publicado en 1978[11], cuando toma forma la criptografía asimétrica, su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

3.7.2.1. RSA. El algoritmo RSA debe su nombre a las iniciales de sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman. Este sistema de cifrado basa su seguridad en la conjetura matemática que sostiene que el problema de factorizar números enteros en sus factores primos tiene una complejidad computacional prohibitiva para el estado del arte de la tecnología de hoy en día y los tamaños en bits de los números utilizados. Las llaves pública y privadas $(K_{pub}; K_{priv})$ se calculan a partir de un número que se obtiene como producto de dos primos grandes.

El proceso para generar dicho par de llaves es el siguiente:

1. Se elige de manera aleatoria dos números primos grandes, ***p*** y ***q.***

2. Se calcula el producto $n = pq$

3. Se elige ahora un número e primo relativo con $(p - 1)(q - 1)$

[10] Diffie W. and Hellman M. New directions in cryptography. IEEE Trans. Information Theory, pages 644–654, 1976. IT-22(6).November 1976.

[11] RSA Laboratories. http://www.rsasecurity.com/rsalabs/.

4. La llave pública será ***(e; n).*** Nótese que ***e*** debe tener inversa módulo ***(p - 1)(q - 1)*** para garantizar que existirá un número ***d***, tal que $de \equiv 1 \bmod$ ***((p - 1)(q - 1))*** es decir, que ***d*** es el inverso de e mod ***(p - 1)(q - 1)***

5. La llave privada será ***(d; n)***

Por lo que:
$K_{pub} = (e; n)$ y $K_{priv} = (d; n)$

Para poder garantizar un margen de seguridad aceptable en transacciones comerciales electrónicas, diferentes estándares recomiendan usar RSA con pares de llaves públicas y privadas con un tamaño no menor a 1024 bits.

3.7.3. Criptografía de curvas elípticas (CCE). Las curvas elípticas constituyen un formalismo matemático conocido y estudiado desde hace más de 150 años. Las primeras propuestas de uso de las curvas elípticas en la criptografía fueron hechas por Neal Koblitz y Víctor Millar, de manera independiente, en 1985. La criptografía de curvas elípticas (CCE) fundamenta su seguridad en el alto grado de dificultad que supone resolver el problema del logaritmo discreto en el grupo abeliano formado por curvas elípticas definidas sobre campos finitos. De forma general, una curva elíptica $E(F_q)$ se define como el conjunto de puntos que satisface la ecuación:

$$E: y^2 = x^3 + ax + b$$

Donde ***a*** y ***b*** están en un campo finito apropiado F_q de orden ***q***, el cual puede ser el grupo de los números racionales, números complejos, enteros módulo ***n***, campos de Galois, etc. Los coeficientes ***a*** y ***b*** caracterizan de manera unívoca cada curva. Se define también un punto en el infinito,

denotado como ***O***, a un punto imaginario situado por encima del eje de las abscisas a una distancia infinita, y que por lo tanto no tiene un valor concreto. Existe en el grupo la suma y una operación conocida como multiplicación escalar:

Si ***k*** es un entero y ***P € E*** (F_q) es un punto, entonces k_P es el punto obtenido al sumar ***k*** copias de ***P***. El elemento neutro es ***O***. Las curvas elípticas definidas en un Campo de Galois G_F ***(P)*** siendo ***P*** un número primo, forman un grupo donde todos los elementos, con excepción del cero, tienen inversa, por lo que se puede sumar, restar, multiplicar y dividir. Los puntos de estas curvas cumplen la ecuación:

$$y^2 = x^2 + ax + b \ (\text{mod } P)$$

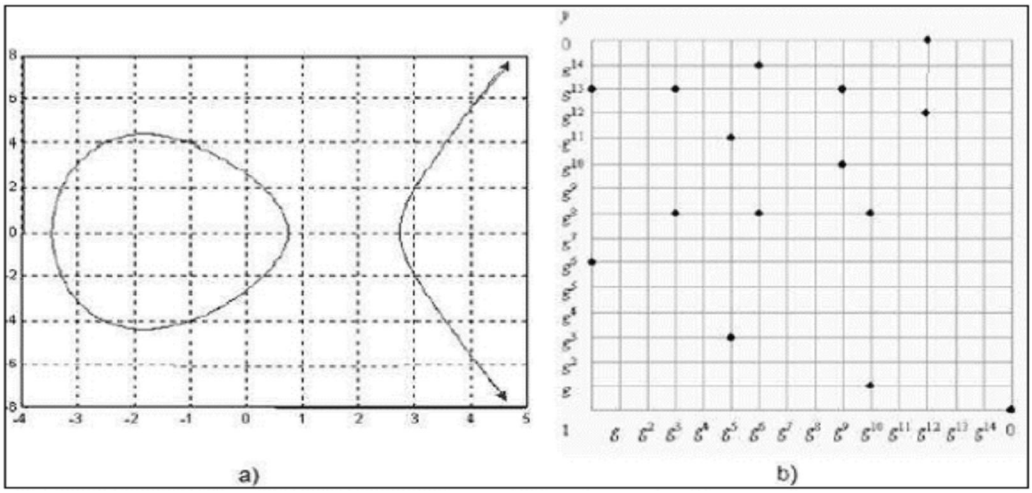
Definiendo de esta forma el grupo **E (GF (P))**[12]**.** En la figura 15 se muestran curvas elípticas definidas en el conjunto ***R***, y en el campo ***F*** (2^4). Tómese un punto ***G*** cualquiera de una curva elíptica ***E.*** Se denominará (***G***) al conjunto {***O, G, 2G***,...,}. En ***E (GF (P)) y E (GF*** (2^m)***)*** los conjuntos de esta naturaleza deberán necesariamente ser finitos, ya que el número de puntos de la curva es finito. Por lo tanto, si se dispone de un punto ***Q € (G)***, debe existir un número entero ***k*** tal que ***kG = Q***. El problema de logaritmo discreto para las curvas elípticas consiste en hallar el número ***k*** a partir de ***G*** y ***Q***.

Debido a la enorme complejidad computacional que dicho problema matemático representa, es posible obtener con **CCE** niveles de seguridad similares a los proporcionados por otros sistemas de cifrado al precio de operaciones de campos finitos muchos menores a las requeridas por los

[12]Ibíd Meneses A

otros esquemas. Las operaciones sobre campos finitos menores conducen al uso de llaves públicas y secretas también menores lo que a su vez tiene como resultado una mayor velocidad, y menores requerimientos de memoria y de poder de cómputo en las implementaciones de los algoritmos que conforman al esquema.

Figura 15: Gráficas de curvas elípticas: a) $y^2 = x^3 + 10x + 7$ sobre R; b) $y^2 + xy = x^3 + g^4x^2 + 1$ sobre $F(2^4)$.



3.8. OTROS ALGORITMOS ASIMÉTRICOS

3.8.1. Algoritmo de Diffe-Hellman. Es un algoritmo asimétrico, que se emplea fundamentalmente para acordar una llave común (también conocida como llave de sesión) entre dos interlocutores, a través de un canal de comunicación inseguro. La ventaja de este sistema es que no son necesarias llaves públicas en el sentido estricto, sino una información compartida por los dos comunicantes. Matemáticamente el algoritmo de cifrado de Diffe-Hellman se basa en las potencias de los números y en la función modular.

Sean ***A*** y ***B*** los interlocutores en cuestión. En primer lugar, se calcula un número primo ***p*** y un generador α de Z^*_p, con $2 \leq \alpha \leq p - 2$. Esta

información es pública y conocida por ambos. El algoritmo queda de la siguiente manera:

1. ***A*** escoge un número aleatorio ***x,*** comprendido entre 1 y ***p*** - 2 y envía a ***B*** ***e***l valor α^{x} (mod ***p***).

2. ***B*** escoge un número aleatorio ***y***, análogamente al paso anterior, y envía a ***A*** el valor α^{y} (mod ***p).***

3. ***B*** recoge α^{x} y calcula ***K*** = $(\alpha^{x})^{y}$ (mod ***p)***

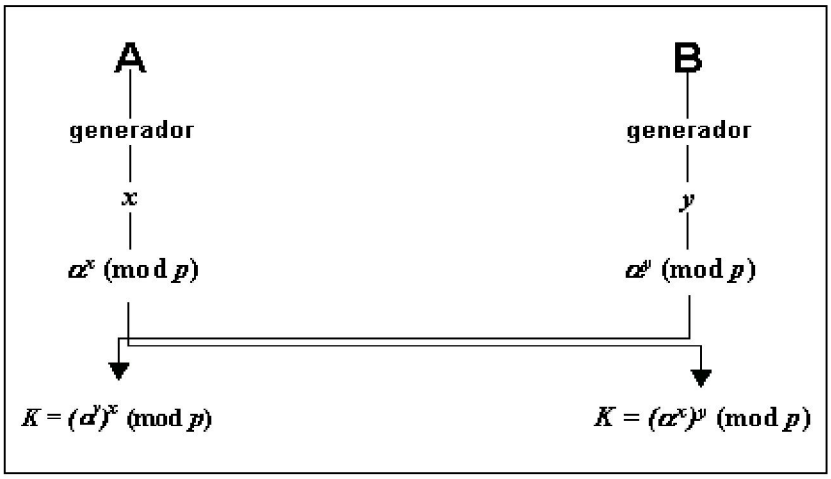
4. ***A*** recoge α^{y} y calcula ***K*** = $(\alpha^{y})^{x}$ (mod ***p***)

Puesto que ***x e y*** no viajan por la red, al final ***A*** y ***B*** acaban compartiendo el valor de ***K,*** sin que nadie que capture los mensajes transmitidos pueda repetir el cálculo. (Figura 16)

3.8.2. Acuerdo de llaves con CE. El problema del logaritmo discreto es la base para la seguridad de muchos sistemas criptográficos incluyendo al de curvas elípticas. La criptografía de curvas elípticas utiliza al grupo de puntos definidos en una curva elíptica sobre un campo finito para obtener una variante del algoritmo para el acuerdo de llaves convencional Diffe-Hellman, **ECDH[13].**

[13] Zuccherato R. and Adams C. Using Elliptic Curve Diffie-Hellman in the SPKM GSS API. 1999.

Figura 16: Diffie-Hellman.

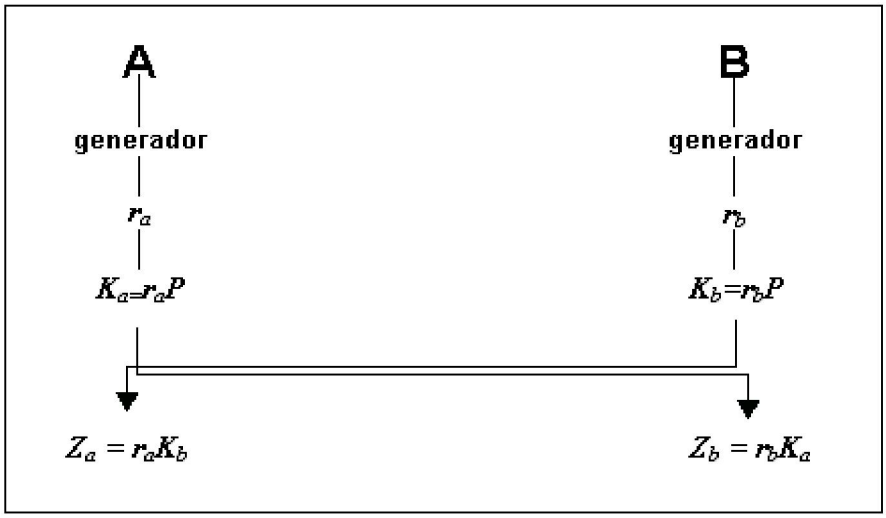


La generación de llaves de sesión utilizando **ECDH** requiere ciertos parámetros de las curvas elípticas: la curva a ser utilizada, el punto generador ***(P),*** el orden de ***P, (n)*** y otros más. Los interlocutores ***A*** y ***B***, generan cada uno, un entero aleatorio r_a y r_b, dentro del intervalo [1, n-1], calculando la llave pública de **ECDH** $Ka = r_aP$ y $K_b = r_bP$. Esta llave pública es enviada a la contraparte, entonces cada entidad calcula el punto $Z_b = r_bK_a$ y $Z_a = r_aK_b$. Los puntos Z_a y Z_b serán utilizados como la llave de sesión[14].

[14] Zuccherato R. and Adams C. Using Elliptic Curve Diffie-Hellman in the SPKM GSS API. 1999.

Este proceso se muestra en la figura 17.

Figura 17: Diffie-Hellman para Curvas Elípticas



4. MEDIDAS DE SEGURIDAD EN WIFI

Para lograr que una WLAN sea segura los conocedores del tema recomiendan:

a. Emplear las mismas herramientas que los intrusos: realizar la misma actividad, pero en beneficio propio, es decir realizar controles periódicos con “Netstumbler”, escuchar tráfico e intentar obtener información trivial con “Kismet” o “AirSnort”, medir potencias irradiadas con cualquier tarjeta desde los perímetros de la red.

b. **Mejorar la seguridad física**.

c. Cancelar puertos que no se emplean.

d. Limitar el número de direcciones MAC. Esta actividad se realiza por medio de ACLs (Control de Lista de Acceso) en los AP, en las cuales se especifica (a mano) las direcciones MAC de las tarjetas a las que se les permitirá el acceso, negando el mismo a cualquiera que no figure en ellas. Cabe aclarar que es muy fácil falsificar una dirección MAC (Ej: en los SSOO Linux es simplemente el comando "ifconfig").

e. Ya no se menciona el tema de cancelar las tramas Beacon en los AP, pues cualquier sistema de escucha, por más que no capture la trama Beacon, al capturar la trama PROVE REQUEST del cliente, o la trama PROVE RESPONSE del AP, en ellas también viaja el ESSID.

f. Satisfacer la demanda. Si se están empleando AP no autorizados por parte de los empleados, es porque les resulta útil, por tanto, se pueden adoptar las medidas para que se implanten, pero de forma segura y controlada, de otra forma, seguirán apareciendo, de forma clandestina.

g. **Controlar el área de transmisión.** Muchos puntos de acceso inalámbrico permiten ajustar el poder de la señal, se debe colocar los puntos de acceso tan lejos como sea posible de las paredes y ventanas exteriores, debe probarse el poder de la señal para que solo el usuario autorizado pueda conectarse a estos sitios, luego se debe cambiar la contraseña predeterminada en todos los puntos de acceso, utilizando una contraseña fuerte para proteger todos estos puntos.

h. Implementar la autenticación de usuario. Mejorar los puntos de acceso para usar las implementaciones de las normas WPA y 802.11i.

i. **Proteger la WLAN con la tecnología "VPN Ipsec" o tecnología "VPN clientless".** Esta es la forma más segura de prestar servicios de autenticación de usuario e integridad y confidencialidad de la información en una WLAN. La tecnología adicional VPN no depende del punto de acceso o de la tarjeta LAN inalámbrica; por consiguiente, no se incurren en costos adicionales de hardware puesto que las normas de seguridad inalámbrica continúan evolucionando.

j. Activar el mayor nivel de seguridad que soporta su hardware. Incluso en equipos de modelo anterior que soporta únicamente WEP, es recomendable activarlo. En lo posible, utilizar por lo menos una WEP con un mínimo de encriptación de 128 bits.

k. Instalar firewalls personales y protección antivirus en todos los dispositivos móviles. La Alianza WiFi recomienda utilizar la política de seguridad de redes corporativas para imponer su uso continuo.

4.1. PASOS PARA ASEGURAR UNA RED INALÁMBRICA

Paso 1, Se debe activar el protocolo WEP. Parece obvio, pero en la práctica no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o despiste de los mismos no tienen el WEP activado. WEP no es completamente seguro, pero es mejor que nada.

Paso 2, Seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No se debe usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por unos.

Paso 3, Uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que expondría a mayores amenazas el sistema. Además el uso del SKA obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo que añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

Paso 4, Desactivar el DHCP y activar el ACL. Se debe asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no se permitirá la inclusión de nuevos dispositivos a la red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

Paso 5, Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial preconfigura el suyo en sus dispositivos, por ello es fácil descubrirlo. Debe cambiarse por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debe modificarse a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

Paso 6, Hacer uso de Las Redes Privadas Virtuales, pues estas dan un extra de seguridad que va a permitir la comunicación entre dispositivos con una gran seguridad. En lo posible añadir el protocolo IPSec.

Paso 7, Aislar el segmento de red formado por los dispositivos inalámbricos de la red convencional. Es aconsejable montar un firewall

que filtre el tráfico entre los dos segmentos de red. Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos wireless realmente seguros. También, en este sentido hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de estas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad.

5. CASOS PRACTICOS DE ATAQUES A REDES LAN INALAMBRICAS

5.1. ATAQUES AL WEP

Numerosos ataques sobre WEP han sido publicados entre los más analizados se tienen:

5.1.1. El Ataque FMS. ***Fluhrer, Mantin y Shamir*** publicaron[15] el primer ataque de recuperación sobre WEP en 2001. Su ataque se basó en las siguientes ideas: Un atacante que escuche pasivamente el tráfico de una red protegida con WEP puede grabar un montón de paquetes cifrados incluyendo los vectores de inicialización usados por dichos paquetes. Debido a que los primeros octetos de la mayoría de paquetes son predecibles fácilmente, el atacante es capaz de recuperar los primeros octetos de los keystreams empleado para cifrar estos paquetes. Todos los octetos siguientes de una clave por paquete son los mismos para todos los paquetes, pero son inicialmente desconocidos para el atacante.

[15] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Debilidades en el algoritmo de programación de clave de RC4. En Serge Vaudenay y Amr M.Youssef, editores, Selected Areas in Cryptography 2001, vol.2259 de Lecture Notes in Computer Science, pgs.1-24 Springer, 2001

Asumiendo que un atacante conoce los primeros l bytes de una clave RC4 usada para generar un keystream X. Podrá simular los primeros l pasos del RC4-KSA y conocer Sl y jl. En el paso siguiente del RC4-KSA, jl+1 = jl+K[l]+Sl[l] y Sl[l] es intercambiada con Sl [jl+1].

Si el atacante pudiese revelar Sl+1[l], podría fácilmente recuperar K[l] calculando la diferencia entre Sl-1 [Sl+1[l]]-jl-Sl[l]. Fluhrer, Mantin y Shamir utilizaron el siguiente truco para revelar este valor:

Asume que las siguientes condiciones permanecen después de los primeros l pasos del RC4-KSA:

1. $S_l[1] < l$
2. $S_l[1] + S_l[S_l[1]] = l$
3. $S_l^{-1}[X[0]] \neq 1$
4. $S_l^{-1}[X[0]] \neq S_l[1]$

En el siguiente paso del RC4-KSA, un valor k=Sl [jl+1] será intercambiado con Sl+1[l]. Si j cambia aleatoriamente para el resto del RC4-KSA, los valores S [1], S [S[1]], y S[l] no serán alterados con una probabilidad de aproximadamente (1/e)3 durante el restante RC4-KSA.

Cuando se produce el primer octeto de salida por el RC4-PRGA, j tomará el valor Sn [1], y Sn[1] y Sn[j] se intercambian. Tras el intercambio, S[1]+S[S[1]]=l todavía permanece y el primer octeto de salida del RC4-PRGA X[0] será S[l]. Si las condiciones 3 o 4 no se mantuvieran, esto indicaría que S[1] o S[S[1]] han sido alterados. En pocas palabras, si estas cuatro condiciones se mantienen, la función:

$$\mathcal{F}_{fms}(K[0], \ldots, K[l-1], X[0]) = S_l^{-1}[X[0]] - j_l - S_l[l]$$

Tomará el valor de K[l] con una probabilidad de alrededor $(1/e)^3$ aproximadamente 5%. Es decir, el conjunto de condiciones unidas en esta función como una correlación para RC4. ***Fluhrer, Mantin y Shamir*** se referían a estas condiciones (o al menos a las dos primeras) como la condición resuelta.

Un ataque de recuperación completa de la clave WEP se puede construir usando esta correlación. Un atacante captura paquetes de una red protegida con WEP y recupera el primer octeto de keystream usado para cifrar esos paquetes adivinando el primer octeto de texto plano. Hay también varias técnicas activas para generar trafico en una red protegida con WEP incluso sin clave, lo que permite la recuperación de más de los primeros 1000 octetos de keystream por paquete. Seleccionan los paquetes donde la condición resuelta permanece y calcula Ffms para esos paquetes. Cada resultado de Ffms puede verse como un voto para el valor de Rk[0]. Después de haber capturado suficientes paquetes, el atacante toma una decisión respecto al valor de Rk[0] basada en el número de votos generados por Ffms.

Si la decisión fue correcta, el atacante conoce el primer l=4 octetos de todas las claves por paquete y puede continuar con Rk[1]. Nótese que todos los paquetes necesitan reevaluarse en cuanto la condición resuelta permanece, ya que esta comprobación depende del valor de Rk[0]. Una vez se hayan determinado todos los octetos de Rk, el atacante comprueba que la clave resultante sea correcta utilizando un número de descifrados de prueba. Si la clave es correcta, el atacante lo ha conseguido. Si la clave resultante es incorrecta, el atacante busca una decisión para Rk[i], donde un valor alternativo para Rk[i] seria también muy deseable. El atacante corrige la decisión el árbol de decisiones a profundidad i y continúa el ataque con la decisión alternativa.

Aunque la probabilidad de suceso del 5% de Ffms parece impresionante, el ataque necesita entre 4.000.000 y 6.000.000 de paquetes para conseguir una probabilidad que exista al menos el 50%, dependiendo del entorno exacto y de la implementación[16]. La razón para esto es que la condición resuelta permanece solamente para un pequeño número de vectores de inicialización elegidos aleatoriamente.

5.1.2. El ataque KoreK. En 2004, una persona bajo el seudónimo de KoreK[17] emuló la implementación de una avanzada herramienta de crackeo WEP en un foro de internet. KoreK utilizo 16 correlaciones adicionales entre los primeros l octetos de una clave RC4, los primeros dos octetos del keystream generado, y el siguiente octeto de la clave K[l]. La mayoría de estas correlaciones habían sido encontradas por el propio KoreK, unas pocas habían sido discutidas en público con anterioridad. KoreK asignó nombres como A_u15 o A_s13 a estos ataques, el ataque FMS original es llamado A_s5_1 para este caso particular.

Prácticamente todas las correlaciones encontradas por KoreK usaban el planteamiento que el primer o segundo octeto del keystream revelan el valor de jl+1 bajo ciertas condiciones, si 2-4 valores en S tienen una constelación especial y no cambian durante el restante RC4-KSA después del paso l+1. Una excepción interesante es la correlación A_neg, la cual no vota por un cierto valor de K[l]. En vez de esto un valor puede excluirse de

[16] Stubblefield A, Ioannidis J, y Rubin A. Un ataque de recuperación de clave sobre 802.11b WEP. ACM Transactions on Information and System Security,7(2):319-332. May 2004

[17] KoreK, Siguiente generación de ataques WEP? http://www.netstumbler.org/showpost.php?p=93942&postcount=35 ,2004

la lista de posibles candidatos para K[l], lo que puede verse como un voto negativo para K[l].

La estructura completa del ataque es el mismo árbol basado en decisiones aproximadas que para el ataque FMS. El número de paquetes capturados se reduce de alrededor de 700.000 para una probabilidad de suceso del 50%. De nuevo, la exactitud de los números depende del entorno exacto, de la implementación y parámetros usados para el ataque. Un factor importante es que si los vectores de inicialización son generados por un algoritmo PRNG o si son generados secuencialmente por un contador.

5.1.3. El ataque PTW. En 2007, una nueva generación de ataques WEP fueron publicados[18] por Tews, Weinmann y Pyshkin. Su ataque introdujo dos nuevos conceptos:

1. Todas las correlaciones previas utilizadas requerían que 2-4 valores en S no cambien durante el restante RC4-KSA. También tenían un montón de condiciones previas que necesitaban mantenerse para usar la correlación. Con lo cual, solamente un pequeño número de paquetes podría usarse para votar un cierto octeto de la clave.

En 2005, Klein mostró[19] que l-X [l-1] toma el valor de S[l] con una probabilidad de 2/n. Si Sl[l] permanece inalterado hasta que se produzca X [l-1], la función:

$$\mathcal{F}_{Klein}(\mathsf{K}[0],\ldots,\mathsf{K}[l-1],\mathsf{X}[l-1]) = \mathsf{S}_l^{-1}[l-\mathsf{X}[l-1]] - (\mathsf{S}_l[l]+j_l)$$

[18] Tews E, Weinmann R-P, y Pyshkin A. Rompiendo wep de 104 bits en menos de 60 segundos. En Sehun Kim, Moti Yung y Hyung-Woo Lee, editores, WISA, vol.4867 de Lecture Notes in Computer Science, pgs.188-202. Springer,2007

[19] Klein A. Ataques al cifrado de flujo RC4. Designs, Codes and Cryptography,48(3):269-289,2008.

Toma el valor de K[l] con una probabilidad de 2/n. Este resultado es también conocido como la correlación Jenkins[20]. Sl[l] permanece inalterado con una probabilidad de aproximadamente 1/e. Si Sl[l] ha sido modificado antes de que se produzca X [l-1], FKlein toma un valor mas o menos aleatorio. En total, esto resulta en la siguiente probabilidad de que FKlein tome el valor de K[l]:

$$\left(\left(\frac{1}{e}\right)\frac{2}{n}\right)+\left(\left(1-\frac{1}{e}\right)\frac{1}{n}\right)\approx\frac{1.37}{n}$$

Esta correlación no hace requerimientos al estado interno de RC4 o del keystream, por lo que se puede usar cada paquete.

2. El segundo concepto nuevo es un cambio en la estructura del ataque. Hasta ahora, cada ataque de recuperación de clave tenía una estructura basada en un árbol de decisiones y se usaba algún tipo de estrategia para la primera búsqueda para determinar la clave octeto por octeto.

Asumiendo que un atacante conoce los primeros l octetos de una clave RC4 y consigue recuperar k=Sl+2[l+1] en lugar de Sl+1[l]. Ahora Sl+1-1[k]-Sl+1[l+1]-Sl[l]-jl=K[l]+K [l+1] permanece y un atacante habría recuperado el valor de K[l]+K [l+1]. Con una probabilidad muy alta Sl+1-1[k]=Sl-1[k] y Sl+1[l+1]=Sl[l+1] permanece y Sl-1[k]-Sl+1[l+1]-Sl[l]-jl toma el valor de K[l]+K[l+1].

Estas correlaciones entre los primeros l octetos de una clave RC4, el keystream generado, y a los siguientes i octetos de la clave una correlación se llamaran multiocteto y se escribirá o1 para la suma. Tews, Weinmann y Pyshkin modificaron FKlein para votar por la suma de los siguientes m octetos de clave por cada m {1,...,13}. Esto resulta en la siguiente función:

[20] Jenkins R. Isaac y RC4 http://burtleburtle.net/bob/rand/isaac.html ,1996.

$$\mathcal{F}_{ptw_m}(\mathsf{K}[0],\ldots,\mathsf{K}[l-1],\mathsf{X}[l+m-2])$$
$$=\mathsf{S}_l^{-1}[l+m-1-\mathsf{X}[l+m-2]]-\left(\sum_{a=l}^{l+m-1}\mathsf{S}_l[a]\right)$$

La cual depende solamente de los primeros 3 octetos de la clave por paquete (IV) y vota por oi en lugar de Rk[i]. El ataque PTW actualmente funciona así: Primero un atacante captura paquetes y recupera sus keystreams como con los ataques FMS y KoreK. El atacante conoce los primeros l=3 octetos de todas las claves por paquete. Ahora evalúa Fptwm para cada paquete y cada m {1,...,13} y consigue votos para o0...o12. Después de que todos los paquetes se hayan procesado, la clave raíz resultante se calcula usando Rk[0]=o0 y Rk[i]=oi-oi-1. Si la clave es correcta, se toma una decisión alternativa para uno de los valores oi y la clave se actualiza usando solamente 12 únicas substracciones sin necesidad de reevaluar todos los paquetes. El ataque necesita solo alrededor de 35.000 a 40.000 paquetes para el 50% de probabilidad de suceso, lo que podría ser recolectado en menos de 60 segundos en una red rápida. Solo se necesitan unos pocos segundos de tiempo de CPU para ejecutar el ataque.

Han sido propuestas algunas modificaciones al ataque PTW[2122] las cuales reducen el número de paquetes necesarios o permitir el uso del ataque PTW en algunos casos especiales donde la recuperación de flujos de clave completos es difícil.

[21] Yuko Ozasa, Yoshiaki Fujikawa, Toshihiro Ohigashi, Hidenori Kuwakado y Masakatu Morii. A study on the Tews, Weinmann, ataque Pyshkin contra WEP. En IEICE Tech. Rep., vol.107 de ISEC2007-47,pgs.17-21,Hokkaido,July 2007. Thu,Jul 19,2007 - Fri, Jul 20: Future University-Hakodate (ISEC, SITE, IPSJ-CSEC)

[22] Vaudenay S y Vuagnoux M. Ataques solo-pasivos de recuperación de clave sobre RC4. En Selected Areas in Cryptography 2007, Lecture Notes in Computer Science, Springer.2007

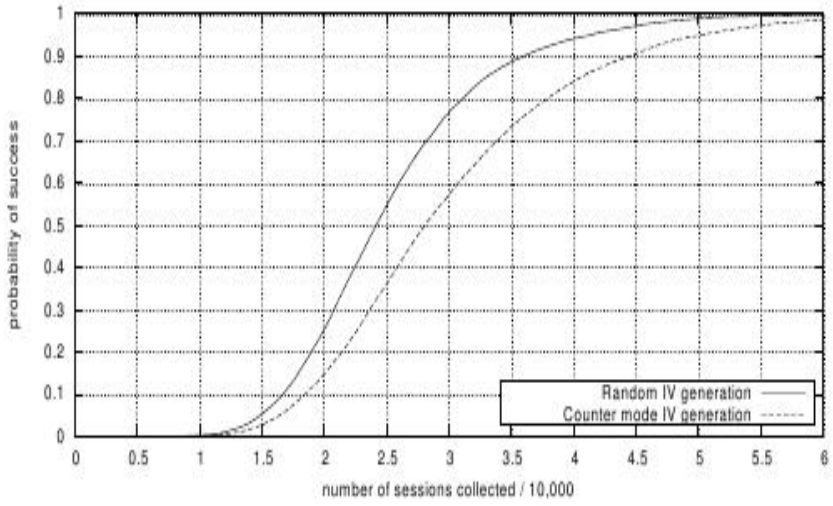
5.1.4. El ataque Chopchop. El ataque Chopchop[23] permite a un atacante descifrar interactivamente los últimos m bytes de texto plano de un paquete cifrado enviando m-128 paquetes de promedio a la red. El ataque no revela la clave raíz y no se basa en ningunas propiedades especiales del cifrado de flujo RC4. Es posible resumir el ataque chopchop de la forma siguiente:

Antes del cifrado, se añade un chequeo de comprobación CRC32 de cuatro octetos llamado ICV a los datos del paquete. Un paquete con el cheksum P puede representarse como un elemento del anillo polinomico F2 [X]. Si el checksum es correcto, P mod PCRC=PUNO permanece, donde PUNO es un polinomio conocido y PCRC es un polinomio conocido también, el cual es irreducible. Podemos escribir P como QX8+R. Aquí R es el último octeto de P y Q son todos los octetos restantes. Cuando el paquete (cifrado) es truncado por un octeto, Q probablemente tendrá un checksum incorrecto.

Asumiendo que el atacante conoce R. Añadiendo PUNO+(X8)-1(PUNO+R) a Q corrige el checksum de nuevo. Por ejemplo si un cliente no esta autenticado, y un punto de acceso recibe un paquete de este cliente, el punto de acceso generará un mensaje de error. Paquetes con un checksum incorrecto son descartados silenciosamente. Un atacante puede usar esto para descifrar interactivamente paquetes. El atacante selecciona un paquete capturado para descifrado. Trunca el paquete por un octeto, adivina R, corrige el checksum y envía el paquete al punto de acceso para saber si suposición de R ha sido correcta. Si ha adivinado R correctamente, el atacante ahora conoce el último octeto de texto plano y puede continuar con el segundo ultimo octeto. Si la suposición ha sido incorrecta, realiza una adivinación adicional para R. Después de unas 256 suposiciones y un promedio de 128, ha adivinado el valor correcto de R.

[23] Ibíd KoreK

5.1.5. Un ataque mejorado sobre WEP. Desafortunadamente, después del lanzamiento del ataque PTW, se siguió prestando poca atención al viejo ataque KoreK. Comparado al ataque PTW, el ataque KoreK tenía la desventaja de que solamente necesita los primeros dos octetos de todos los paquetes capturados. Normalmente, la recuperación de los primeros dos octetos del flujo de clave es mucho más fácil que recuperar los primeros 15 o 31 octetos. Una agradable excepción es el trabajo hecho por Vaudenay y Vuagnoux[24], quienes mostraron que la correlación utilizada en el ataque PTW puede también rescribirse para votar por oi en lugar de Rk[i]. Esta correlación es una de las 17 utilizadas en el ataque KoreK.



[24] Ibíd Vaudenay S y Vuagnoux M.

Para mejorar el rendimiento del ataque PTW, se comienza reescribiendo todas las correlaciones utilizadas por KoreK para votar por oi en lugar de Rk[i]. Sorprendentemente, fue posible modificar exitosamente casi todas las correlaciones usadas por KoreK, con unas pocas excepciones:

Las correlaciones A_4_s13, A_4_u5_1, y A_4_u5_2 en el ataque KoreK original podían usarse solamente para votar por Rk[1] cuando Rk[0] es conocido. Usando estas correlaciones para Rk[2], Rk[3] o cualquier otro octeto de la clave más allá de Rk[1] no ha sido implementado por KoreK. La modificaciones de estas correlaciones resulta en nuevas correlaciones las cuales solamente votan por oi, incluso con Rk[0] ó o0 desconocidos.

KoreK asignó etiquetas con comentarios a algunas correlaciones. La correlación A_u5_3 es la única etiquetada con el comentario 'no buena'. Cuando intentamos modificar A_u5_3 para votar oi, la resultante correlación no produjo resultados útiles. La correlación A_neg fue utilizada por KoreK para excluir valores de ser Rk[i]. La modificación de esta correlación resulta en una nueva correlación que excluye valores de ser oi con alta probabilidad. Para implementar esta característica adicional, un peso negativo se asigna a esta correlación. Otra extensión interesante del ataque PTW fue sugerida por Yuko Ozasa et al (2007) y Serge Vaudenay y Martin Vuagnoux (2007) independientemente. Primero mostraron que es posible obtener cuatro veces más votos para o13 que para todos los demás valores de oi. Esto hace mucho más fácil para un atacante decidir el valor de o12 que todos los demás valores de oi. Segundo, encontraron que la correlación usada en el ataque PTW puede fácilmente modificarse para votar por el valor de o12+oi, incluso cuando el valor de o12 es desconocido por el momento.

Después que el atacante haya decidido el valor de o12, puede obtener votos adicionales para cada oi, substrayendo el valor de o12 de esos votos. Para usar estas correlaciones adicionales, un atacante necesita los octetos de flujo de clave X [15] a X [30], que a veces también se pueden recuperar. Usando todas estas ideas, es posible modificar una implementación del ataque PTW, resultando en una nueva herramienta de crackeo WEP, que claramente necesita menos paquetes que previas implementaciones del ataque PTW. Decidimos usar la misma estrategia de ranking de claves utilizada en el ataque PTW original. Esta limita el número de claves que la implementación prueba antes de fallar a 2^20. El mismo límite ha sido usado por publicaciones previas sobre ataques WEP, por lo que sería fácil comparar este ataque con los anteriores.

Este tipo de ataque puede ser prevenido considerando un tiempo de renovación de clave muy corto, por ejemplo 120 segundos o menos. En 120 segundos, el atacante puede solamente descifrar partes del valor ICV al final del paquete. Alternativamente deshabilitando el envío de frames de reportes de fallo MIC en los clientes también podría prevenir el ataque. La mejor solución seria deshabilitar TKIP y utilizar CCMP solamente en la red.

5.1.6. Ataque de fuerza bruta. La semilla de 32 bits que utiliza el PRNG es obtenida a partir de la passphrase. La passphrase normalmente contiene caracteres ASCII, por lo cual el bit más alto de cada carácter siempre es cero. El resultado de la operación XOR de estos bits también es cero y esto provoca una reducción de la entropía de la fuente, es decir, las semillas sólo podrán ir desde 00:00:00:00 hasta 7F:7F:7F:7F en lugar de hasta FF:FF:FF:FF.

El uso del PRNG con esta semilla también reduce la entropía. De la semilla de 32 bits sólo utilizan los bits del 16 al 23. El generador lineal congruente (LGC: generador lineal congruential) de módulo 2^32, lo que provoca que los bits mas bajos sean “menos aleatorios” que los altos, es decir, el bit 0 tiene una longitud de ciclo de 2^1, el bit 1 de 2^2, el bit 2 de 2^3, etc. La longitud de ciclo del resultado será por tanto 2^24. Con esta longitud de ciclo sólo las semillas que vayan de 00:00:00:00 a 00:FF:FF:FF producirán llaves únicas.

Como las semillas sólo llegan hasta 7F:7F:7F:7F y la última semilla que tiene en cuenta el PRNG es 00:FF:FF:FF, sólo se requiere considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F por lo que la entropía total queda reducida a 21 bits. El conocimiento de estos datos permite hacer ataques de fuerza bruta contra la encriptación WEP generando llaves de forma secuencial utilizando las semillas desde 00:00:00:00 hasta 00:7F:7F:7F. Utilizando este proceso, un procesador PIII a 500MHZ tardaría aproximadamente 210 días en encontrar la llave, aunque se puede usar computación en paralelo para obtener la llave en un tiempo más razonable.

También existe la posibilidad de utilizar un diccionario para generar sólo las semillas de las palabras (o frases) que aparezcan en el diccionario, con lo que si la passphrase utilizada está en el diccionario se conseguirá reducir sustancialmente el tiempo necesario para encontrarla.

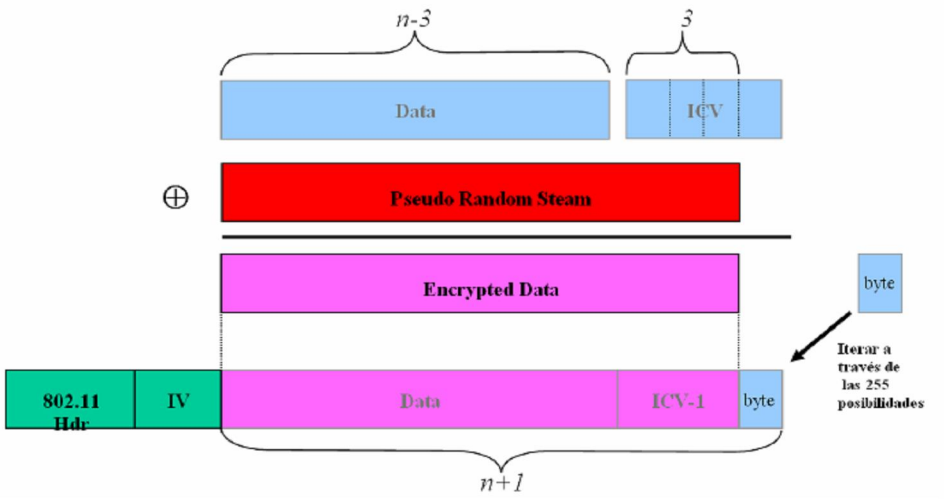
5.1.7. Ataque Inductivo Arbaugh. Demostrado teóricamente por William A. Arbaugh (Universidad de Maryland), basado en explotar la vulnerabilidad de MIC independiente de la llave aprovechando también la redundancia de información producida por el CRC. Para realizar el ataque

hay que conocer parte del plaintext que viaja encriptado en una trama, que puede ser obtenidas por ejemplo identificando mensajes "*DHCPDISCOVER*" de los conocidos que la cabecera IP tendrá como origen 0.0.0.0 y como destino 255.255.255.255 y tienen longitud fija.

Una vez identificada la trama con el mensaje "*DHCPDISCOVER*" se realiza un XOR del plaintext conocido con el cyphertext que se ha recibido, obteniendo así n (en este caso 24) bytes del keystream para el IV concreto del paquete.

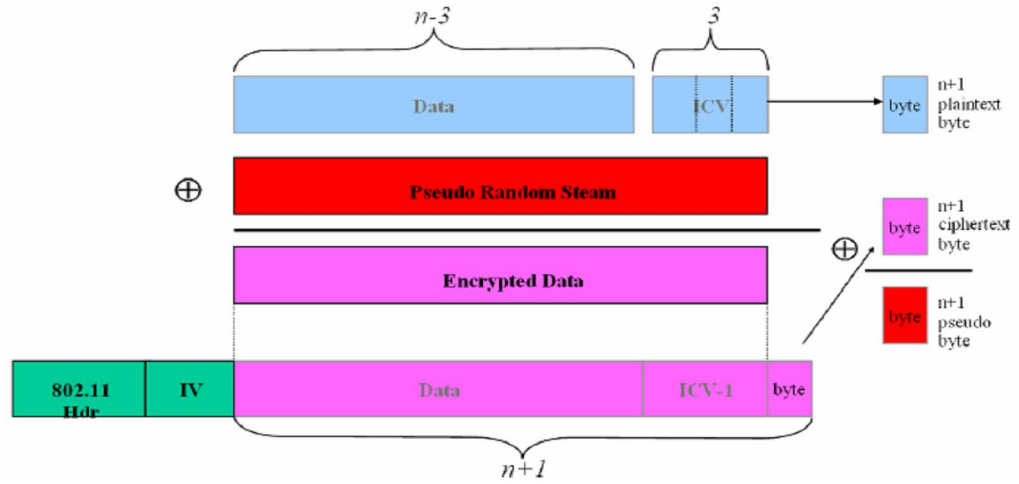
Una vez se tiene los 24 bytes conocidos del keystream hay que generar un paquete de tamaño n-3, es decir 24-3 = 21 bytes de longitud. Este paquete debe ser algo de lo que se pueda esperar una respuesta, por ejemplo un pin o un ARP Request.

Se calcula el ICV del paquete generado y son añadidos sólo los primeros 3 bytes del ICV calculados. Se realiza un XOR con el resto del keystream añadiendo el último byte del ICV en el byte n+1 (al final del paquete) tratando de adivinar el siguiente byte del keystream tal y como se muestra en la figura:



Una vez generado el paquete completo este es enviado, y se espera una respuesta (echo reply, ARP reply...), si no hay respuesta se deben ir probando las 255 posibilidades restantes modificando el último byte (n+1). Si hay respuesta se afirma que el byte n+1 era el último byte del ICV, así que tirar un plaintext que concuerda con el cyphertext y que a su vez brinda el byte n+1 del keystream que es el que interesa. Realizando este proceso repetidas veces obtendremos el keystream completo.

Asumiendo que un atacante puede realizar aproximadamente 100 pruebas por segundo, tardaría una media de 36 minutos en encontrar un keystream completo de 1500 bytes valido para un IV determinado. Una vez se logra tener el keystream entero, los 224 – 1 restantes son fáciles de obtener.



El atacante tiene que volver a generar un paquete del cual se le devuelva una respuesta, (lo mejor es enviar broadcast pins, así se reciben múltiples respuestas por cada paquete enviado). El atacante conoce el plaintext de la respuesta y el que responde cada vez enviará el paquete con un IV diferente, así es posible construir una tabla de keystreams completos para cada IV que el atacante puede utilizar para descifrar el tráfico encriptado con WEP en tiempo real.

El atacante necesita almacenar 1500 bytes de keystream por cada IV, por lo que la tabla ocuparía 2^{24}x1500 = 24GB y tardaría una media de 30 horas en construir la tabla. Si el ataque se realiza en paralelo 4 hosts atacantes tardarían 7,5 horas y 8 hosts atacantes 3.75 horas.

Cuando el atacante recibe un paquete mira en la tabla a que keystream corresponde el IV recibido y hace un XOR del keystream con el cyphertext del paquete para obtener el plaintext.

5.2 ATAQUES A REDES WIRELESS

Vista la manera, romper la encriptación WEP ya no debería ser un problema, por eso en la implementación de los ataques que se mencionarán a continuación no se hablará de WEP ya que si la WLAN que se esta "auditando" tiene encriptación WEP ya se conocen las herramientas necesarias para obtener la clave y por tanto, se podrá realizar los distintos ataques tanto si existe encriptación WEP como si no.

5.2.1. Romper ACL's basados en MAC. Una de las medidas más comunes que se utilizan para asegurar una red wireless es restringir las máquinas que podrán comunicarse con el Punto de Acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar. Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacerse pasar por uno de los equipos que si que tienen acceso a la red.

Para llevar a cabo el ataque basta con esnifar durante un momento el tráfico y fijarse en la MAC de cualquiera de los clientes, sólo hace falta que ponerse su misma MAC y ya se habrá saltado la restricción. Esto es sencillo de implementar, por ejemplo en el sistema operativo Linux se puede realizar con el comando *ifconfig* dependiendo del tipo de tarjeta que se tenga. También existen otras utilidades para cambiar la MAC como por ejemplo *setmac*. Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC se puede tener problemas, aunque generalmente en las redes wireless esto no suele ser un problema muy

grave ya que el Punto de Acceso no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas formas, si se prefiere es posible "anular" a la máquina que se le ha "robado" la dirección MAC. Para hacer esto, se debe implementar un ataque de Denegación de Servicio, como el que se describe a continuación.

5.2.2. Ataque de Denegación de Servicio (DoS). Para realizar este ataque basta con esnifar durante un momento la red y ver cual es la dirección MAC del Punto de Acceso. Una vez conocida su MAC, le es asignada al equipo sniffer y este actúa como si fuera el AP. Lo único que se debe hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (marcos de dirección) de desasociación o desautenticación. Si en lugar de un solo cliente se quiere denegar el servicio a todos los clientes de la WLAN, se envía estas tramas a la dirección MAC de broadcast.

Existen varias herramientas para realizar este ataque, las más comunes para el sistema operativo Linux son:

- *wlan-jack*: perteneciente a las utilidades air-jack, presentadas en la concentración Black Hat 2002 en Las Vegas.

- *dassoc*: envía tramas de desasociación, herramienta desarrollada por @stake (antes L0pht).

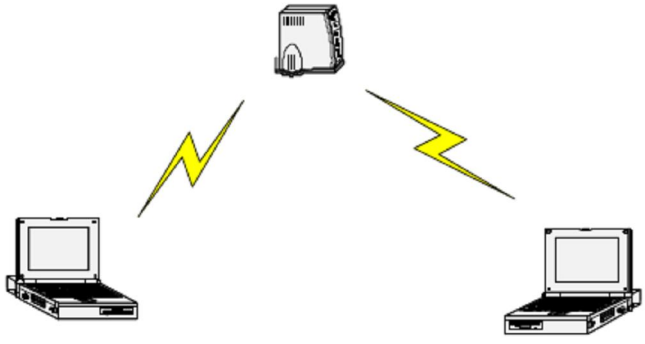
5.2.3. Descubrir ESSID ocultos. Para que un cliente y un AP se puedan comunicar, ambos deben tener configurado el mismo ESSID, es decir, deben pertenecer a la misma red wireless. Una medida de seguridad

bastante común es “ocultar” el ESSID, es decir, hacer que el AP no mande BEACON FRAMES, o en su defecto no incluya el ESSID en éstos.
En este caso, para descubrir el ESSID se deberá esnifar y esperar a que un cliente se conecte, y así poder ver el ESSID en la trama PROVE REQUEST del cliente (en el caso de que no se manden BEACON FRAMES), o en la trama PROVE RESPONSE del AP. Pero también es posible “provocar” la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de mandarlas repetidamente, es decir, nos ponemos la dirección física del AP y mandamos una trama DEAUTH o DISASSOC a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse o autenticarse, con lo que es posible ver el ESSID en los marcos de dirección..

Para implementar el ataque se puede usar la herramienta essid-jack, que también pertenece al paquete de utilidades air-jack para Linux

5.2.4. Ataque Man in the middle. El ataque de Man in the middle, también conocido como Monkey in the middle (figura 18) consiste en convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.

Figura 18. WLAN antes del ataque

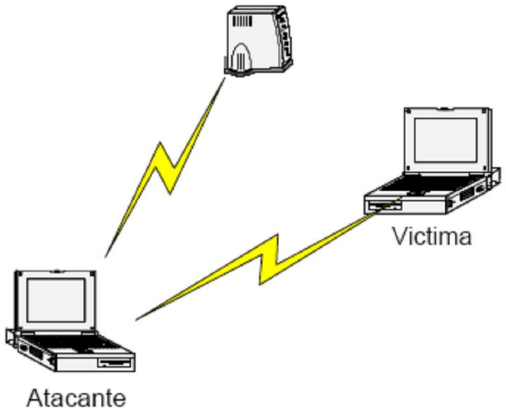


Para realizar este ataque, primero se debe esnifar para obtener:

-El ESSID de la red (si esta ocultado, usaremos el método anterior)
-La dirección MAC del AP
-La dirección MAC de la víctima
Una vez conocidos estos datos, se utiliza el mismo método que en el ataque DoS, para desautenticar a la víctima del AP real, es decir, el atacante spoofea su MAC haciéndose pasar por el AP y manda tramas DEAUTH a la víctima. La tarjeta wi-fi de la víctima empezará entonces a escanear canales en busca de un AP para poderse autenticar, y ahí es donde entra en juego el atacante.

El atacante hace creer a la víctima que él es el AP real, utilizando la misma MAC y el mismo ESSID que el AP al que la víctima estaba autenticada anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta wi-fi del atacante debe estar en modo **master**. Por otra parte, el atacante debe asociarse con el AP real, utilizando la dirección MAC de la víctima. De esta manera se logra insertar al atacante entre la víctima y el AP, en la figura 19 se ve como queda la WLAN después de realizar el ataque.

Figura 19. WLAN después del ataque

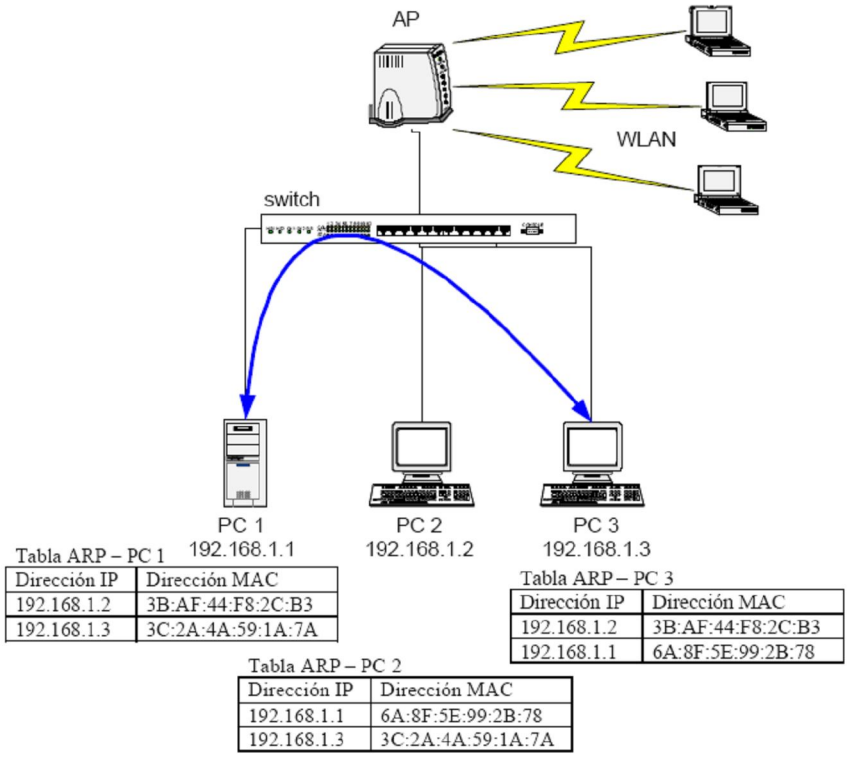


De esta manera todos los datos que viajan entre la víctima y el AP pasan a través del atacante. Como el ataque ha sido realizado a nivel de enlace (nivel 2), el atacante puede ver, capturar e incluso modificar las tramas en los niveles superiores del modelo OSI.

Es muy fácil implementar este tipo de ataques utilizando el driver air-jack con la herramienta monkey-jack. Hay que tener en cuenta que muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, esto como ya se ha visto es incierto para las redes wireless y por tanto el uso de según que tipo de solución podría no ser adecuado para estas redes. Se debe tener cuidado sobre todo en implementaciones de VPN que no realizan las comprobaciones necesarias de autenticación para protegerse de ataques Man in the middle en redes wireless.

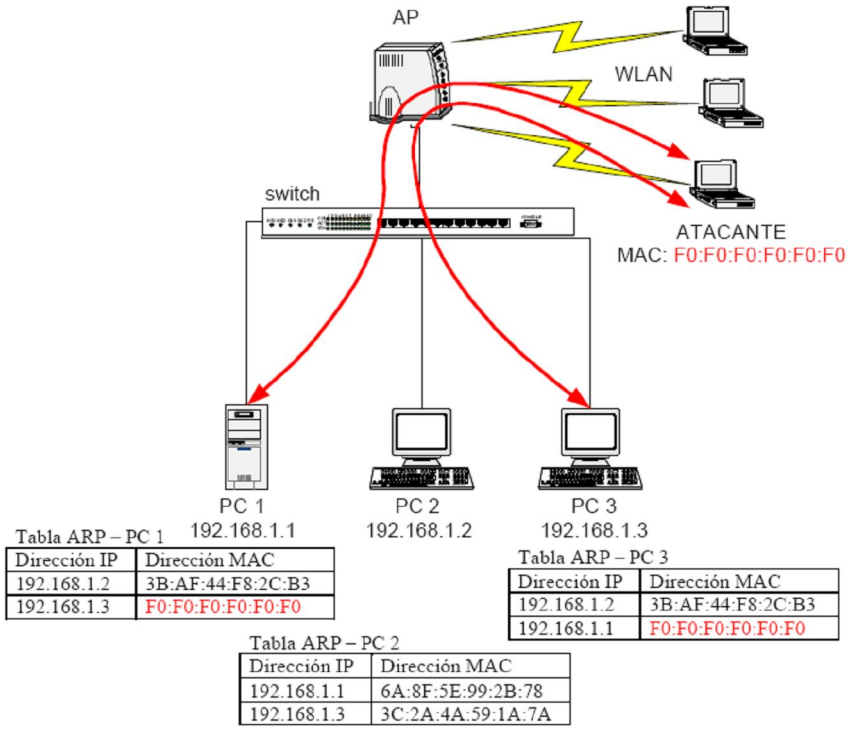
5.2.5. Ataque ARP poisoning. El ARP cache poisoning (figura 20) es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las víctimas, limitando su efectividad a redes conectadas con switches, hubs y bridges, pero no routers. La mayoría de los Puntos de Acceso 802.11b actúan como bridges transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red wireless hacia la LAN donde está conectado el AP y viceversa. Esto permite que se ejecuten ataques de ARP cache poisoning contra sistemas que están situados detrás del Punto de Acceso, como por ejemplo servidores conectados a un switch en una LAN a los que se pueda acceder a través de la WLAN.

Figura 20. Antes del ataque ARP poisoning



El servidor PC 1 se comunica con PC 3 a través del switch, si un atacante desde la WLAN envenena la tabla de ARP's de PC 1 y de PC 3 podrá realizar un ataque del tipo Man in the Middle situándose entre los dos hosts de la red con cables. Así es como se efectuaría la comunicación después del ataque:

Figura 21. Después del ataque ARP poisoning



El atacante manda paquetes *ARP REPLY* a PC 2 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue "envenenar" la caché de ARP's de PC 2. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC 2 la tiene también su propia MAC. Como ARP es un protocolo *stateless*, PC 1 y PC 2 actualizan su caché de acuerdo a la información que el atacante ha inyectado a la red. Como el switch y el AP forman parte del mismo dominio de broadcast, los paquetes ARP pasan de la red wireless a la red con cables sin ningún problema.

Para realizar el ataque ARP Poisoning, existen múltiples herramientas en Internet, ya que este ataque no es específico de las redes wireless, la más famosa es el sniffer Ettercap. Este ataque puede ser frenado creando dos VLAN's en el switch, una para la boca a la que está conectado el AP y la

otra para el resto de máquinas. Otra forma de frenarlo sería utilizando tablas de ARP estáticas.

6. CONCLUSION

Una vez realizada la revisión exhaustiva y rigurosa de la información existente en medios escritos, digitales entre otros, se obtuvieron unos resultados que permiten presentar el siguiente conjunto de conclusiones:

En referencia al método utilizado para el desarrollo del presente, la monografía logra exponer claramente temas a nivel académico. Adicionalmente permite determinar la habilidad para hacer investigaciones académicas de los futuros profesionales además de disciplinarnos en el manejo de gran cantidad de información.

En cuanto a las prácticas realizadas con varios dispositivos Wifi en el laboratorio de la Universidad Tecnológica de Bolívar pudimos identificar y dar solución a los principales problemas de seguridad en redes wifi, implementando los diferentes protocolos relacionados con la seguridad como: WEP, WPA y el método de filtrado de direcciones MAC. Además probamos las vulnerabilidades que se presentan con los métodos antes mencionados, al efectuar un ataque de recuperación de clave de red utilizando diferentes programas sniffers que permiten auditar una red objetivo.

También logramos generar un ambiente óptimo de seguridad conociendo las debilidades que evidenciamos cuando realizamos ataques a redes específicamente en modo de encriptación WEP, donde utilizamos una tarjeta PCMCIA en modo monitor y el programa Aircrack-ng, lo que nos permitió capturar un sin número de paquetes y varios Ivs que son los que permiten que el sniffer genere la clave de red con éxito. Adicional a esto

encontramos varios inconvenientes en los que podemos puntualizar la conexión fallida del archivo Aircrack-ng GUI.exe contenido en el programa Aircrack-ng-1.0-rc1-win, motivo por el cual no logramos obtener la clave de red.

Los resultados obtenidos en cuanto al tema de seguridad en redes LAN permiten concluir que las redes Wi-Fi son bastante vulnerables por tanto los hackers pueden violarlas con gran facilidad. De igual manera que la seguridad de los sistemas informáticos es una tarea difícil de efectuar, ya que implica de gran experiencia de los diseñadores del sistema y de mayores recursos computacionales. Recientemente, ha habido numerosas investigaciones dedicadas a brindar mayor seguridad a sistemas de cómputo, sin embargo, siempre existen vulnerabilidades en el sistema que impiden garantizar totalmente seguridad de un sistema.

Otro punto a destacar en cuanto a seguridad es que el constante desarrollo tecnológico, es difícil siempre proporcionar un óptimo nivel de seguridad, ya que el hardware y el software están siempre en constante mejora.

Por otro lado, en muchos sistemas de cómputo, la seguridad no siempre es considerada como el factor más importante en el diseño. La nueva tendencia del desarrollo tecnológico, en el cual se encuentran las PDAs y las redes de área local inalámbricas, es de gran utilidad ya que proveen movilidad, flexibilidad, sin embargo presentan problemas a la seguridad debido a que están basadas en una plataforma abierta poco segura y muy vulnerable a ataques externos.

Para el caso de las redes de área local inalámbricas, por el simple hecho de usar como medio de transmisión la radio frecuencia (RF), las vuelve

vulnerables. Es decir, el canal de comunicación es inherentemente inseguro y puede ser atacado de manera pasiva comprometiendo la confidencialidad de los datos, o bien de manera activa en la cual un intruso puede enviar, recibir, alterar o falsificar mensajes. Sin embargo se puede decir que la seguridad es un atributo que no se puede cubrir de manera total, sino de forma parcial solamente.

7. RECOMENDACIONES

Estimular a los alumnos de las carreras o programas a fines a consultar el presente documento con fines informativos, dado que contiene una amplia revisión literaria sobre el tema propuesto y les permite tener un amplio conocimiento tanto de las debilidades como de las posibilidades de fortalecerlas en el campo de la seguridad en redes LAN.

Dar continuidad a la presente investigación, para poder afianzar el tema de la seguridad en redes LAN ya que este es de permanente actualización y desarrollo y exige permanente innovación en lo referente a mecanismos que brinden seguridad a los sistemas.

Promocionar esta investigación ya que además de los estudiantes puede ser útil a docentes, profesionales y en general a todos los interesados en el tema de la seguridad de redes LAN.

Los estudiantes que deseen seguir investigando les recomendamos seguir:
En los casos prácticos de ataques a redes LAN inalámbricas, más específicamente el ataque en modo de encriptación WEP, que se realizó con

el programa Airodump-ng ya que se presentan problemas en cuanto a su culminación.

BIBLIOGRAFIA

Comer D E. Internetworking with TCP/IP. Vol. I: Principles, Protocols and Architecture. Prentice-Hall, USA 1991. Segunda Edición.

Diffie W. and Hellman M. New directions in cryptography. IEEE Trans. Information Theory, pages 644–654, 1976. IT-22(6).November 1976.
Ganz A, Ganz Z, y Wongthavarawat K. Multimedia Wireless Networks: Technologies, Standards and QoS. Prentice Hall, USA 2003.

González N, L. Seguridad en redes inalámbricas para sistemas multimedia de tiempo real. Disponible en: http://www.netstumbler.org/showpost.php?p=93942&postcount=35,2004 Consultado octubre de 2008.

Jenkins R. Isaac y RC4 Disponible en: http://burtleburtle.net/bob/rand/isaac.html, Consultado octubre de 2008.

Klein A. Ataques al cifrado de flujo RC4. Designs, Codes and Cryptography,48(3):269-289,2008.

Kore K, Siguiente generación de ataques WEP?
Manuel J. Lucena López. Criptografía y seguridad en computadores. http://www.di.ujaen.es/ mlucena. 2003. Consultado octubre de 2008.

Meneses A, Van Oorschot P and Vanstone S. Handbook of Applied Cryptography. CRC Press, New York 2001. Quinta Edición.

Randall K. Nichols, Panos C. Lekkas. Seguridad para comunicaciones inalámbricas. McGraw-Hill, 2003. Primera edición. pp 187-420.

RSA Laboratories. http://www.rsasecurity.com/rsalabs/ Consultado octubre de 2008.

Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Debilidades en el algoritmo de programación de clave de RC4. En Serge Vaudenay y Amr M.Youssef, editores, Selected Areas in Cryptography 2001, vol.2259 de Lecture Notes in Computer Science, pgs.1-24 Springer, 2001

Stubblefield A, Ioannidis J, y Rubin A. Un ataque de recuperación de clave sobre 802.11b WEP. ACM Transactions on Information and System Security,7(2):319-332. May 2004

Tews E, Attacks on the wep protocol. Cryptology Print Archive, Report 2007/471,2007 http://eprint.iacr.org Consultado octubre de 2008.

Tews E, Weinmann R-P, y Pyshkin A. Rompiendo wep de 104 bits en menos de 60 segundos. En Sehun Kim, Moti Yung y Hyung-Woo Lee, editores, WISA, vol.4867 de Lecture Notes in Computer Science, pgs.188-202. Springer,2007

Vaudenay S y Vuagnoux M. Ataques solo-pasivos de recuperación de clave sobre RC4. En Selected Areas in Cryptography 2007, Lecture Notes in Computer Science, Springer.2007

Vega B A y Martínez D. Seguridad Wifi. Asignatura: Redes y Sistemas de Radio Curso 2004/2005.

Yuko Ozasa, Yoshiaki Fujikawa, Toshihiro Ohigashi, Hidenori Kuwakado y Masakatu Morii. A study on the Tews, Weinmann, ataque Pyshkin contra WEP. En IEICE Tech. Rep., vol.107 de ISEC2007-47,pgs.17-21,Hokkaido,July 2007. Thu,Jul 19,2007 - Fri, Jul 20: Future University-Hakodate (ISEC, SITE, IPSJ-CSEC)

Zuccherato R. and Adams C. Using Elliptic Curve Diffie-Hellman in the SPKM GSS API. 1999.

GLOSARIO

A

ARPANET: Advanced Research Projects Agency Network.

Alohanet: un sistema de redes de ordenadores.

AES (Advanced EncriptionStandard): (Estándar de Cifrado Avanzado) Algoritmo de cifrado de 128, 192 y 256 de longitud de clave promovido por el NIST (National Institute of Standards and Tecnology) en 1996 y llamado a ser el sustituto del estándar DES.

Ancho de banda: Capacidad de un medio para transmitir la señal. Generalmente se mide en bits por segundo (bps)[Cyberdisk].

B

B: Símbolo del byte

Bahía (bay): Espacio que en los ordenadores personales sirve para alojar y servir de soporte físico a los dispositivos de almacenamiento.

Bps: ('bits por segundo') Unidad de medida de la velocidad de transmisión por una línea de telecomunicación.

Bridges (Puentes): Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

Broadcasts: Es la distribución de audio y/o señales de vídeo que transmiten los programas.

C

Capacidad de disco: Es la cantidad de almacenamiento que puede tener el disco.

Concentradores (Hubs): Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.

D

Diseño: Proceso de creación y desarrollo.

Dispositivos: En informática, se utiliza para referirse a los componentes de la computadora.

DES (Data EncryptionStandard) (Estándar de Cifrado de Datos) Algoritmo de cifrado de 56 bits de longitud de clave promovido por el Gobierno de los EE.UU.

Dominio (domain) : Recursos de una red bajo un único puesto de control.

1. En TCP/IP, sistema de nombres usado en las redes jerárquicas mediante el cual grupos de anfitriones (hosts) son administrados por separado dentro de una estructura jerárquica en árbol.
2. En Internet, sistema de nombres separados por puntos que sirven como nemotécnico de las direcciones IP.[Cyberdisk].

DoD: Departamento de Defensa americano con ordenadores conectados punto a punto.

E

Estándar IEEE 802.11: Especifica una interfaz aérea entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos.

Ethernet: Actualmente es el protocolo más sencillo y es de bajo costo. Utiliza la topología de "Bus" lineal.

F

Flujo de la red: Como un grafo dirigido.

FAQ: (Frequently Asked Questions).

FTP (File TransferProtocol): Protocolo que permite la transferencia de ficheros, a través de la red Internet, de ordenador a ordenador. La conexión es directa y se utiliza para carga o descarga de los mismos. No hay que confundir este tipo de transferencia con otras posibles, como, por ejemplo, la de envío de ficheros a través del correo electrónico.

Firewall (Cortafuegos): Sistema, hardware y software, de seguridad, situado entre una red privada y la red Internet para proteger a aquella de las intromisiones o ataques que puedan venirle a través de esta.

H

Hácker: Experto en informática y programación que disfruta explorando nuevas posibilidades.

I

Internet: Conjunto de redes interconectadas entre sí que permite la comunicación entre ellas mediante la utilización del protocolo TCP/IP. Se usa en masculino, femenino, con o sin artículo determinado.

Intranet: Red interna de las instituciones que utiliza los mismos mecanismos que la red Internet, especialmente los relacionados con el mundo WWW, para distribuir la información corporativa. Las intranets

suele estar montadas sobre redes propias, protegidas del exterior mediante sistemas cortafuegos, o también pueden montarse intranets virtuales aprovechando la propia Internet. Una intranet virtual consiste en restringir, mediante distintos mecanismos de seguridad: contraseñas, direcciones IP, o tipo de usuario, el acceso a ciertos servidores y servicios.

L

LAN: Redes de Área Local.

M

Memoria: Guardar datos que la computadora no este usando.

MIPS: Microprocessor without Interlocked Pipeline Stages.

MAC (Control de Acceso al medio): Una serie de computadoras.

Modelo OSI: Es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas.

MIT: Instituto Tecnológico de Massachusetts.

N

Network: Red, Conjunto de redes de comunicaciones, ordenadores y software que permite comunicar (transmitir información) los distintos sistemas entre sí.

NSA: Agencia Nacional de Seguridad de EEUU.

P

PC's: Sistema personales de comunicación.

Q

(QoS): niveles de calidad de servicio de la aplicación multimedia.

R

Red de Área Local Inalámbrica: El término suele utilizarse más para referirse a aquellas redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables.

Red: Una red consiste en un conjunto de puntos y un conjunto de líneas que unen ciertos pares de puntos. Los puntos se llaman nodos (o vértices). Las líneas se llaman arcos (o ligaduras, aristas o ramas).

Routers (Encaminadores): Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor, permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

S

Seguridad: Forma de asegurar los recursos del sistema informático de una organización sean utilizados de la manera más segura.

SSL: Secure Sockets Layer.

Stack: Es una lista ordinal o estructura de datos en la que el modo de acceso a sus elementos es de tipo LIFO.

Switch o (HUB): Es el dispositivo encargado de gestionar la distribución de la información del Servidor (HOST), a la Estaciones de Trabajo y/o viceversa. Las computadoras de Red envía la dirección del receptor y los datos al HUB, que conecta directamente los ordenadores emisor y receptor.

Sistema operativo (SO): Programas que controlan los recursos del sistema y sirven de intermediarios entre las aplicaciones y dichos recursos. El Windows 95, UNIX, Linux, etc, son sistemas operativos.

SSL (SecureSockets Layer): (Capa de conexión segura) Estándar de factor promovido por Netscape y bastante aceptado en Internet. Proporciona en el nivel de transporte enlaces seguros entre clientes y servidores sobre TCP/IP.

T

Telnet: Servicios de terminal remoto. Protocolo estándar que permite la conexión por medio de la red Internet a un sistema dado desde un terminal ubicado en cualquier punto. Este tipo de conexión suele emplearse para acceder a ordenadores que disponen de recursos especiales (bibliotecas), o a los ordenadores centrales y bases de datos locales de la propia organización, cuando se está fuera de la misma.

Token Ring: El protocolo de red IBM es el Token ring, el cual se basa en la topología de anillo.

TCP/IP: Se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

V

VPN (Virtual Private Netowork): (Red PrivadaVirtual) Tunel seguro sobre redes IP.

W

WAP (Wireless ApplicationProtocol): Protocolo inalámbrico de aplicaciones. Permite la comunicación entre dos teléfonos celulares (móviles) al revés de Internet y la conexión de cada uno de ellos a Internet.

WEP (Wired Equivalent Privacy): Privacidad Equivalente a Cableado usa el algoritmo de cifrado RC4 para la confidencialidad mientras que el CRC-32 proporciona la integridad.

WLAN: Redes de Área Local Inalámbricas.