ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB

CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM

REDES DE COMPUTADORES

CARLOS ANDERSON ANDRADE DUARTE

A EVOLUÇÃO DOS PROTOCOLOS DE SEGURANÇA DAS REDES SEM FIO: DO WEP AO WPA2 PASSANDO PELO WPA

VILA VELHA - ES

2010

CARLOS ANDERSON ANDRADE DUARTE

A EVOLUÇÃO DOS PROTOCOLOS DE SEGURANÇA DAS REDES SEM FIO: DO WEP AO WPA2 PASSANDO PELO WPA

Monografia apresentada ao Curso de Pós-Graduação em Redes de Computadores da Escola Superior Aberta do Brasil como requisito para obtenção do título de Especialista em Redes de Computadores, sob orientação do (a) Prof. (a) Dr (a) _____

VILA VELHA - ES

2010

CARLOS ANDERSON ANDRADE DUARTE

A EVOLUÇÃO DOS PROTOCOLOS DE SEGURANÇA DAS REDES SEM FIO: DO WEP AO WPA2 PASSANDO PELO WPA

Monografia aprovada em de ___ _ de 2010

Banca Examinadora

_____

_____

_____

VILA VELHA - ES

2010

AGRADECIMENTO

A DEUS por ser a razão da minha existência... Ao meu amor Cintia pelo apoio e compreensão, a meus pais e aos nossos dois futuros filhos que estão por vir e que me deram a alegria de me tornar pai durante a realização deste trabalho.

RESUMO

Palavras-Chave: WEP, WPA e WPA2

Neste trabalho de monografia eu iniciei descrevendo a família de protocolos 802.11x que é o padrão que define as métricas de segurança em redes sem fio e também apresentando alguns conceitos básicos sobre essas redes. Depois comecei a descrever os protocolos de segurança das redes wireless, iniciando pelo WEP que foi o primeiro passo dado, mas a conclusão a que cheguei é que foram encontradas muitas vulnerabilidades e falhas neste protocolo. Depois descrevi o WPA que foi o protocolo desenvolvido a seguir e tinha, na época, a perspectiva de ser uma solução para o problema da segurança, corrigindo as falhas e vulnerabilidades encontradas no WEP. Mas o que aconteceu é que o WPA também apresentou falhas, bem menos que o WEP, é verdade, além de resultar em uma queda de desempenho e estabilidade nas redes que o usavam. Por isso surgiu então o WPA2 que também foi estudado neste trabalho e que até hoje é o protocolo mais utilizado em se tratando de redes sem fio.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

No mundo atual, as redes sem fio estão cada vez mais difundidas e usadas pela sua praticidade e desempenho adquiridas ao longo da última década. A informação tornou-se o bem mais valioso de qualquer organização inserida na sociedade da informação e mantê-la segura é um grande desafio.

O acesso a uma informação pode definir o sucesso ou o fracasso de uma organização, bem como sua capacidade competitiva frente ao mercado. Torna-se então fácil entender o porquê de tanta preocupação com a segurança dessas organizações.

Um grande aumento do número de redes sem fio WLAN's (Wireless Local Area Network´s) utilizadas por usuários caseiros, instituições, universidades e empresas pôde ser observado ao longo dos últimos anos. Esta crescente utilização trouxe consigo não só mobilidade e praticidade para seus usuários, mas também uma maior preocupação com a segurança. É exatamente essa preocupação com a segurança nessas redes que vem fazendo com que os protocolos de segurança sejam criados, desenvolvidos e atualizados cada vez mais.

A primeira barreira de segurança adotada foi o WEP (Wired Equivalent Privacy), o primeiro protocolo de segurança, que conferia no nível de enlace (nível 2 do modelo OSI), uma certa segurança para as redes sem fio semelhante à segurança das redes com fio.

Após vários testes realizados com este protocolo algumas vulnerabilidades e falhas fizeram com que o WEP perdesse quase toda a sua credibilidade. Nele a mesma chave é usada por todos os usuários de uma mesma rede, gerando uma repetição de seqüência de RC4 (algoritmo) extremamente indesejável, pois dá margem a ataques bem-sucedidos e conseqüente descoberta de pacotes por eventuais intrusos.

Para sanar as falhas e limitações do WEP surge o WPA (Wi-Fi Protected Access). O WPA corrigiu vários erros do WEP, mas ainda foram encontradas falhas, além de seu desempenho ter uma queda significativa em termos de estabilidade, por isso, surgiu o WPA2 com a promessa de ser a solução definitiva de segurança e estabilidade para as redes sem-fio do padrão Wi-Fi.

1.1 PROBLEMA

O maior bem de uma empresa inserida na sociedade da informação são seus dados e seu capital intelectual que gera seu conhecimento, sendo assim, existe um grande esforço e preocupação com a segurança desses dados.

Impedir o acesso indevido a essas informações é uma constante preocupação de todos os setores envolvidos no processo desde fabricantes a usuários.

A tecnologia sem fio surgiu no mercado para prover a esses usuários a mobilidade que a tecnologia cabeada não era capaz de fornecer. O aumento de sua utilização cresce proporcionalmente com a redução dos custos de aquisição dos equipamentos voltados para essa tecnologia. Junto com seu uso cresce também a preocupação com a segurança.

Essa preocupação iniciou com o surgimento do WEP que foi o primeiro protocolo de segurança criado. O WEP apresentou falhas, então foi criado o WPA com a intenção de saná-las, mas não conseguiu atingir seu objetivo. Por isso foi criado o WPA2 que até hoje é o protocolo de segurança mais usado nas redes wireless.

Como ocorreu esse processo de criação e evolução dos protocolos de segurança das redes sem fio, padrão 802.11?

1.2 JUSTIFICATIVA

Esse tema foi escolhido pela crescente popularização das redes sem fio no mercado atual. Este fato vem causando grandes inquietações sobre a segurança nesse tipo de tecnologia. As dúvidas tornam-se ainda maiores em se tratando de informações coorporativas trafegando nesse ambiente.

Garantir a segurança nesse tipo de rede é uma preocupação dos fabricantes, visto que seus clientes querem e necessitam dessa tecnologia, mas sem abrir mão do nível de segurança das redes cabeadas.

Sendo assim, discutir esse assunto torna-se extremamente interessante para melhor conhecermos os avanços que foram feitos na área de segurança das redes wireless.

1.3 OBJETIVO GERAL

O objetivo dessa monografia é descrever as formas de funcionamento dos padrões de segurança em redes sem fio expondo-os e comparando-os, tratando de suas limitações, seus benefícios, e especificando as vantagens e desvantagens de cada um.

1.4 OBJETIVOS ESPECÍFICOS

- Descrever os principais conceitos wireless;

- Descrever as definições do 802.1x - o padrão que define as métricas de segurança em redes sem fio.

- Caracterizar os padrões de segurança de uma rede sem fio;

- Descrever como funciona e as limitações e vantagens do WEP, WPA e WPA2;

1.5 DELIMITAÇÃO DO TRABALHO

Este trabalho trata da evolução dos protocolos de segurança das redes sem fio. Do WEP que foi o primeiro protocolo criado ao WPA2 que é o protocolo mais utilizado hoje em dia passando pelo WPA.

Descreverei as formas de funcionamento desses protocolos de segurança em redes sem fio expondo-os e descrevendo-os, tratando de suas limitações, suas vulnerabilidades e especificando as vantagens e desvantagens de cada um.

1.6 METODOLOGIA

Neste estudo irei coletar informações, conceitos e definições sobre os protocolos de segurança das redes sem fio através de pesquisa bibliográfica em livros, revistas especializadas, artigos e sites específicos.

Depois apresentarei essas informações e os conceitos coletados de uma forma bem organizada e clara, para descrever como foi o processo de evolução dos protocolos de segurança das redes sem fio.

2 CONCEITOS WIRELESS

2.1 ARQUITETURA IEEE 802.11X - PADRÕES WIRELESS

O IEEE (*Institute of Electrical and Electronics Engineers*) é o órgão responsável pela padronização nas áreas de informática e engenharia elétrica, além de publicar uma série de jornais e promover diversas conferências sobre essas áreas durante o ano (TANENBAUM, 2003).

A família 802.11 (como é popularmente conhecido os padrões das redes wireless), surgiu após o comitê do IEEE receber a tarefa de padronizar as redes sem fio. Esse padrão recebeu o nome de 802.11 e é conhecido também como WiFi. De acordo com Tanenbaum (2003), essa padronização foi necessária, pois quando surgiram os notebooks, as pessoas sonhavam em entrar no escritório e conectá–los automaticamente na internet. Por isso diversos grupos começaram a trabalhar para alcançar esse objetivo. Desse trabalho surgiu rapidamente a comercialização de redes sem fio por várias empresas. O problema é que dificilmente duas delas eram compatíveis. Com essa proliferação de padrões um computador com um rádio da marca X não funcionaria em uma sala equipada com uma estação-base da marca Y.

Esse padrão deveria funcionar na presença de uma estação-base, onde todo o tráfego passaria pela estação-base (ponto de acesso), e deveria funcionar também na ausência de uma estação-base. Neste caso, cada computador transmitiria uns para os outros (interligação *ad hoc*).

2.1.1 Protocolo 802.11a

O protocolo 802.11a fornece transmissões a uma velocidade nominal de enlace, incluindo sinais de modulação, cabeçalhos de pacotes e correção de erros, de 54 Mbps na banda de 5GHz, sendo sua velocidade real de 24 a 27 Mbps. Trabalha com o OFDM (*Orthogonal Frequency Division Multiplexing*) e com 8 (oito) canais de rádio sendo, por isso, mais resistente à interferências. Por utilizar uma freqüência mais alta, seus transmissores também possuem um alcance mais curto, sendo necessário usar mais pontos de acesso para cobrir a mesma área.

2.1.2 Protocolo 802.11b

Esse padrão aplica-se a *Wireless LAN's* e fornece uma transmissão de 11 Mbps na freqüência de 2,4 GHz. Embora seja mais lento que o 802.11a, possui um alcance sete vezes maior, sendo também chamado de 802.11 *High Rate* ou **Wi-Fi** (D-LINK, 2002).

Trabalha com o DSSS (*Direct Sequence Spread Spectrum*) e com 11 canais de rádio, possuindo um alcance de 15 a 100 metros. O número de estações de trabalho que podem ser conectadas a cada ponto de acesso é ilimitado, mas assim como nas redes Ethernet, quanto maior o número de estações conectadas menor a velocidade da rede, já que apenas uma pode transmitir de cada vez (D-LINK, 2002).

2.1.3 Protocolo 802.11g

Esse padrão é uma versão aperfeiçoada do 802.11b. Foi aprovado pelo IEEE em novembro de 2001. Sua velocidade nominal é de 54 Mbps. Utiliza o OFDM do padrão 802.11a, mas opera na banda de 2,4 GHz de freqüência, como o 802.11b, sendo, portanto compatíveis. Essa compatibilidade é uma grande vantagem sobre o padrão 802.11a que também transmite a 54 Mbps, mas é incompatível devido à sua faixa de transmissão (TANENBAUM, 2003).

Em uma rede mista (com tecnologia do padrão 802.11g e do 802.11b), a velocidade da transmissão pode chegar a 54 Mbps (entre uma estação e um ponto de acesso 802.11g), mas no momento em que um ponto que opere no padrão 802.11b comece a transmitir essa taxa tende a cair para níveis próximos aos da rede 802.11b.

2.1.4 Protocolo 802.11n

O IEEE aprovou oficialmente a versão final do padrão para redes sem fio 802.11n em Setembro de 2009. As principais especificações técnicas do padrão 802.11n incluem:

- Taxas de transferências disponíveis: de 65 Mbps a 600 Mbps;
- Método de transmissão: MIMO-OFDM;
- Faixa de freqüência: 2,4 GHz e/ou 5 GHz.

A tecnologia n proporciona redes *Wi-Fi* mais rápidas, com maior alcance e mais seguras, de tal sorte que se tornam perfeitas para o streaming de conteúdo em alta definição (HD), melhor desempenho de aplicações em redes sem fio (como serviços de *VoIP*) e também uso mais eficiente da bateria de computadores portáteis, já que chips compatíveis com o novo protocolo consomem menos energia.

2.1.5 Protocolo 802.16

O padrão 802.11 foi criado especialmente visando fornecer comunicações sem fio com alta largura de banda garantindo velocidade de transmissão e principalmente mobilidade para seus usuários. Contudo, a necessidade de um novo padrão surgiu ao interligarmos pontos fixos e mais distantes uns dos outros. Nascia assim o padrão 802.16. Como foi projetado principalmente para interligar edifícios, a mobilidade não é relevante (TANENBAUM, 2003).

Aqui as distâncias envolvidas podem ser medidas em quilômetros. Isso significa que a potência envolvida na estação base pode variar muito de estação para estação. Isso afeta a relação sinal/ruído, que por sua vez define vários esquemas de modulação. Por ser uma comunicação aberta sobre uma área considerável a segurança é essencial e obrigatória (TANENBAUM, 2003).

Por trabalhar com um número maior de usuários do que o 802.11, o que implica em maior necessidade de largura de banda, opera na faixa de freqüências de 10 a 66 GHz. Suas ondas são milimétricas, portanto o tratamento de erros nesse padrão merece mais cuidados do que no 802.11, já que esse tipo de onda é fortemente absorvido pela água (TANENBAUM, 2003).

2.2 COMPONENTES DE UMA REDE WIRELESS

Segundo o IEEE 802.11 a arquitetura adotada para as redes sem fio (*Wireless Lan´s*) baseia-se na divisão da área coberta pela rede em células. Essas células são chamadas de BSA (*Basic Service Área*). Um sistema de distribuição é utilizado para

interligar múltiplas BSA´s possibilitando a construção de redes cobrindo áreas maiores que uma célula (SOARES, 1995).

Abaixo estão descritos os equipamentos utilizados para transmissão entre as estações de uma rede Wireless.

2.2.1 Access point

Os AP´s (*Access Point´s*) ou pontos de acesso são estações especiais responsáveis pela captura das transmissões realizadas pelas estações de trabalho de sua BSA, destinadas a outras BSA´s. Para retransmitir os dados capturados de suas BSA´s os AP´s se utilizam do sistema de distribuição (que pode ser baseado em outro meio de transmissão como os fios metálicos ou fibra ótica) (SOARES, 1995).
Segundo SOARES (1995), as funções básicas dos *Access Point´s* são:

> Autenticação, associação e reassociação: Essas funções permitem que as estações continuem conectadas à infra-estrutura mesmo quando estão se movimentando entre as BSA´s. Para tanto as estações realizam movimentos de varredura para determinar qual é o melhor ponto de acesso e passam a acessar o sistema de distribuição através desse AP. Para realizar essa escolha a potência do sinal e a qualidade da recepção dos quadros enviados pelos AP´s são analisados.
>
> Gerenciamento de Potência: Possibilita a economia de energia, ao verificar que uma determinada estação encontra-se operando com a função de recepção desabilitada (modo power save) o AP armazena temporariamente os quadros a ela endereçados. As estações e o AP operam com relógios sincronizados e “periodicamente as estações ligam seus receptores e o AP transmite quadros anunciando tráfego, para que as estações possam se preparar para receber os quadros armazenados no AP a elas endereçados”.
>
> Sincronização: garante que as estações associadas a um AP sejam sincronizadas por um relógio comum. Através de um envio periódico de quadros que são usados pelas estações para atualizar seu relógio essa sincronização é implementada. Esses quadros ou beacons carregam o valor do relógio do AP.

Figura 1 – Exemplo de Access Point
Fonte: Tcninfo (2010)

2.2.2 Adaptadores

Os adaptadores são as placas de rede sem fio, elas podem ser de três tipos de acordo com a sua conexão ao computador: PCI, USB e PCMCIA. Essas placas possuem uma pequena antena integrada, mas também podem ter conexão para uma antena externa caso precisem de maior alcance. (D-LINK, 2002).

Figura 2 – Exemplo de Placa de Rede Wireless (Adaptadores)
Fonte: Tcninfo (2010)

2.2.3 Antenas

Antenas são equipamentos utilizados para captar ou irradiar ondas eletromagnéticas. Aumentam a área de influência/cobertura dos dispositivos sem fio, de maneira que podemos alcançar centenas de metros sem problemas. Com uma antena apropriada podemos maximizar o raio de cobertura das *Wireless LAN´s*: com antenas parabólicas de alto ganho foi estabelecida comunicação entre dispositivos Wireless a mais de 70 Km (D-LINK, 2002).

A decisão sobre qual antena usar envolve muitos fatores, tais como:

- Área de cobertura;
- Distância máxima;
- Localização Indoor;

- Localização Outdoor e
- Altura na localização da antena.

2.2.3.1 omni-direcionais

Dão cobertura com um diagrama de irradiação circular (360º). Supõe-se que oferecem serviço por igual independentemente de sua colocação, mas uma vez que as freqüências nas quais estamos trabalhando são próximo às de microondas, os diagramas não são mais circulares, mas sim ovais (D-LINK, 2002).

Figura 3 – Exemplo de Antena Omni-direcional
Fonte: Ngsat (2010)

2.2.3.2 direcionais

Uma antena direcional fornece um padrão de irradiação muito forte em uma direção específica, focalizando a irradiação da energia para fornecer uma maior distância de cobertura. Dentre as antenas direcionais estão as antenas Yagi, Patch e Parabólica. (D-LINK, 2002).

São direcionais e só emitem/recebem com uma largura de banda definida pela construção da antena (D-LINK, 2002).

Figura 4 – Exemplo de Antena Direcional
Fonte: Tcninfo (2010)

2.3 CSMA/CA

Devido à complexidade inerente do ambiente sem fio o protocolo da subcamada MAC do 802.11 é bastante diferente do protocolo da Ethernet. O CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) é um protocolo utilizado para evitar colisões nas transmissões sem fio (SOARES, 1995).

Nesse protocolo são usadas tanto a detecção do canal físico quanto do canal virtual. Admite dois modos de operação. No primeiro modo, se uma estação quer transmitir, ela escuta o canal e ela começará a transmitir se ele estiver ocioso. Durante a transmissão ela não escuta o canal, mas emite seu quadro inteiro, que não possui garantia nenhuma de chegar ao seu destino devido à possibilidade de interferência no receptor (TANENBAUM, 2003).

Caso o canal esteja ocupado, a estação só começará a transmitir quando o canal ficar inativo. Ocorrendo uma colisão, as estações envolvidas esperarão um tempo aleatório e tentarão novamente mais tarde (TANENBAUM, 2003).

O seu outro modo de operação se baseia no MACAW e lida com a detecção de canal virtual.

2.4 TOPOLOGIAS

Segundo Soares (1995), a arquitetura adotada pelo projeto IEEE 802.11 para as redes sem fio baseia-se na divisão da área coberta pela rede em células. As células são chamadas BSA (*Basic Service Área*). Um grupo de estações que se comunica em uma BSA, constitui um BSS (*Basic Service Set*). O tamanho da BSA (célula) depende das características do ambiente e dos transmissores/receptores usados nas estações. Para permitir a construção das redes cobrindo áreas maiores que uma célula, múltiplas BSA´s são interligadas através de um sistema de distribuição que pode ser uma rede baseada em outro meio de transmissão, por exemplo, fios

metálicos ou fibra ótica via AP (Access Point ou pontos de acesso). Os AP´s são responsáveis pela captura das transmissões realizadas pelas estações de sua BSA, destinadas a estações localizadas em outras BSA´s, retransmitindo-as, usando o sistema de distribuição.

Uma ESA (*Extended Service Área*) é um conjunto de BSA´s interligadas por um sistema de distribuição através de *Access Points*. Um ESS (*Extended Service Set*) é um conjunto de estações formado pela união dos vários BSS´s conectados por um sistema de distribuição. ESS-ID é a identificação de cada ESS. Dentro de cada ESS, cada BSS é identificado por um BSS-ID. Esses dois identificadores formam o Network-ID de uma rede sem fio 802.11 (SOARES, 1995).

Uma rede local sem fio é constituída por um ESS formado pela interconexão de múltiplos BSS´s (SOARES, 1995).

2.4.1 Ibss

No "*Independent Basic Service Set*" (IBSS) é uma rede análoga a uma rede ponto a ponto. Várias estações sem fio se comunicam diretamente entre si sobre uma base *ad-hoc* ponto a ponto. Não estão conectados a uma rede maior e abrange uma área limitada.

2.4.2 Bss

Um BSS (*Basic Service Set*) nada mais é do que um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA. Fornece uma área

de cobertura onde as estações do BSS se encontram totalmente conectadas. Uma estação pode mover-se livremente dentro do BSS, mas não pode se comunicar diretamente com outras estações se abandona o BSS. Baseia-se em um AP que atua como servidor lógico para uma célula WLAN. As comunicações entre dois nós A e B vão de A ao AP e do AP ao nó B. Além disso, é necessário um AP para realizar as funções de *bridging* e conectar múltiplas células WLAN ou canais, e para conectar células WLAN a redes cabeadas (D-LINK, 2002).

2.4.3 Ess

O "*Extended Service Set*" (ESS) trabalha com múltiplas células BSS conectadas por *backbones* de cabo ou sem fio utilizando o mesmo canal ou canais diferentes para aumentar o desempenho agregado.

3 WEP

3.1 A SEGURANÇA NO PROTOCOLO 802.11

O alcance das redes 802.11 é freqüentemente de algumas centenas de metros, dessa forma invadir uma rede desse tipo se torna muito fácil a qualquer um que tenha o equipamento certo e que se depare com uma rede desprotegida. Um notebook com uma placa de rede sem fio é capaz de captar sinais dentro de carro em um estacionamento de uma empresa que não tenha feito às devidas configurações de segurança de sua rede (TANENBAUM, 2003).

Visando tornar os equipamentos cada vez mais amigáveis ao usuário os fabricantes cada vez mais disponibilizam no mercado os *plug-and-play* - equipamentos tão fáceis de usar que praticamente não necessitam de configuração alguma. Em geral é só conectá-lo a rede elétrica e o mesmo começará a operar imediatamente. Dessa forma, o usuário muitas vezes nem toma conhecimento da necessidade de alteração das configurações de segurança do equipamento e deixa sua rede completamente desprotegida (TANENBAUM, 2003).

Caso a segurança não seja habilitada, estes sinais podem ser prontamente interceptados por receptores que estejam por perto.

O Wi-Fi Alliance é uma instituição formada por várias indústrias para indicar uma certificação de interoperabilidade a um produto *wi-fi* - o *Wi-Fi CERTIFIED*. Ele recomenda que os gerentes e usuários de uma rede doméstica ou pequena planejem o nível de segurança que vão querer e uma avaliação de risco para selecionar a segurança apropriada de acordo com a sensibilidade de seus dados e a probabilidade de um ataque. Segurança é uma decisão pessoal: Para a maioria das casas ou ambientes de SOHO onde o WLAN serve principalmente entretenimento,

pesquisa, e necessidades pessoais e empresariais de uma natureza menos sensível, o WEP provê segurança adequada para intimidar o intruso casual. Principalmente se for usado com um firewall e software de anti-vírus (WI-FI Alliance, 2010).

Redes empresariais grandes requerem tipicamente um nível muito mais alto de segurança. Isto implica na utilização de níveis avançados que podem ser alcançados com tecnologias de segurança amplamente disponíveis hoje. Escolher uma solução de segurança apropriada requer uma compreensão de como WLANs trabalham e o que as faz vulneráveis (WI-FI Alliance, 2004).

O protocolo WEP foi o primeiro adotado para segurança de redes sem-fio, que conferia no nível de enlace (nível 2 do modelo OSI) certa segurança semelhante à segurança das redes a cabo. O padrão WEP tem muitas falhas e é relativamente simples de quebrar, mas mantém a camada de proteção básica que deve sempre estar ativa.

O padrão 802.11 trata de um protocolo de segurança do nível de enlace de dados, o WEP (*Wired Equivalent Privacy*), teoricamente esse protocolo foi projetado para assegurar às redes sem fio uma segurança equivalente a de uma rede cabeada. Ele visa fornecer às redes sem fio a mesma privacidade das redes com fios.

Quando a segurança no 802.11 é ativada, cada estação tem uma chave secreta compartilhada com a estação base. O padrão não especifica como as chaves são distribuídas. Uma vez estabelecidas essas chaves permanecem estáticas por meses ou anos (TANENBAUM, 2003).

Ao ser habilitado o WEP protege somente os dados de usuário do pacote e não os cabeçalhos, para que outras estações possam escutar os dados de controle necessários pra manter a rede. No entanto, as demais estações não serão capazes de decodificar os dados de usuário (D-LINK, 2002).

A privacidade oferecida pelo WEP se baseia em chaves criptográficas simétricas de 40 bits e um vetor de inicialização público de 24 bits (IV – *Initialization Vector*). Para se conectar à essa rede a estação deve conhecer a chave atual, dessa forma um usuário indesejado somente poderá acessar seus dados se conseguir quebrar a criptografia do WEP (D-LINK, 2002).

O WEP pode ser utilizado entre o Ponto de Acesso (AP – *Access Point*) e os clientes da rede (modo com infra-estrutura), ou na comunicação direta entre clientes (modo *ad-hoc*). A criptografia WEP só é aplicada ao tráfego do canal de comunicação sem fio e, portanto, o tráfego roteado para fora da rede sem fio não possui criptografia WEP, como podemos ver na figura 5 abaixo.

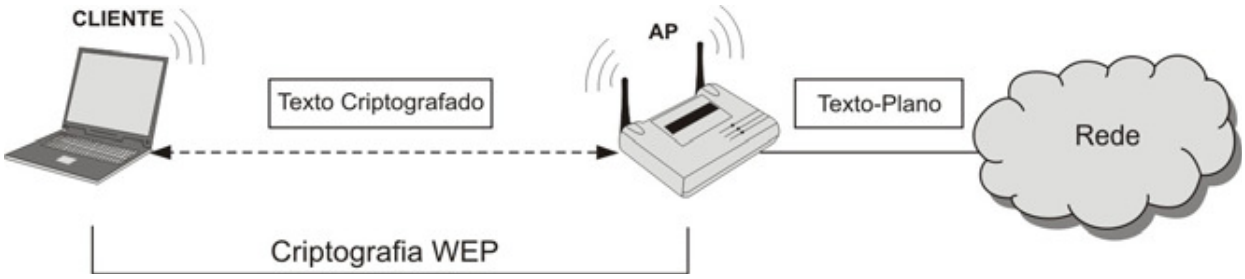

Figura 5 – Funcionamento do WEP
Fonte : Unibratec (2010)

3.1.1 A criptografia no WEP e o algoritmo RC4

A criptografia do WEP utiliza uma cifra de fluxo baseada no algoritmo RC4. O algoritmo RC4 foi projetado por Ronald Rivest e se manteve secreto até vazar e publicado na internet em 1994. Esse algoritmo gera um fluxo de chaves que sofre uma operação XOR com um texto simples para formar o texto cifrado (TANENBAUM, 2003).

É Utilizado um método onde cada carga útil de pacote é codificada. Essa carga útil é verificada através do polinômio CRC-32 e o total de verificação é anexado a carga útil para formar o texto simples que será usado no algoritmo de criptografia. Logo depois esse texto simples sofre uma operação XOR com um bloco de fluxo de chaves de tamanho igual (TANENBAUM, 2003).

O algoritmo consiste em utilizar um *array* que a cada utilização tem os seus valores permutados e misturados com a chave. Esta chave, utilizada na inicialização do *array*, pode ter até 256 bytes (2048 bits).

3.1.2 Diagrama de cifragem e decifragem WEP

O resultado do processo descrito acima é o texto cifrado. O IV usado para iniciar o RC4 é enviado com o texto cifrado. Ao obter o pacote o receptor extrai a carga útil criptografada, gera então o fluxo de chaves a partir da chave secreta compartilhada e o IV que acabou de receber, e depois efetua uma operação XOR do fluxo de chaves com a carga útil para recuperar o texto simples. E finalmente ele pode conferir o total de verificação para ver se o pacote foi adulterado ou não (TANENBAUM, 2003).

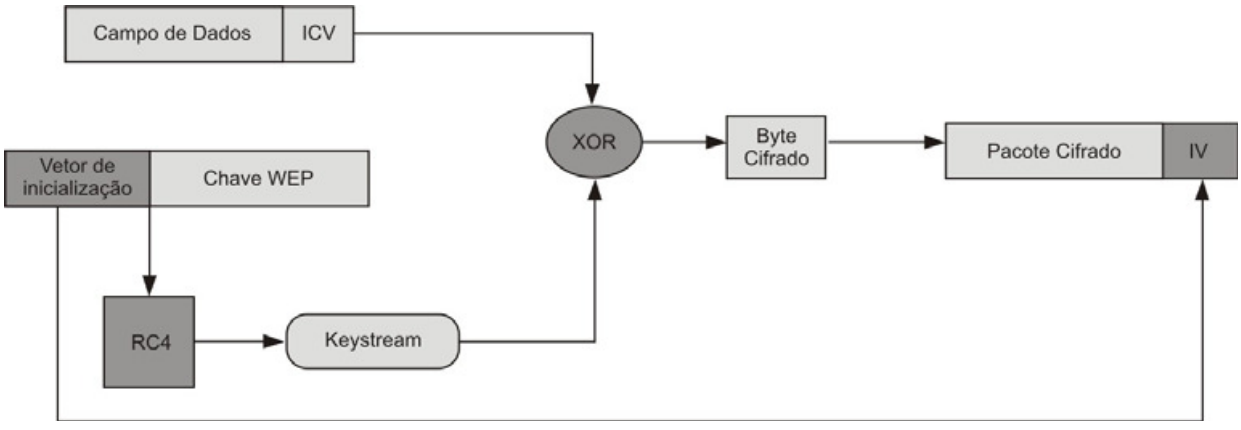

Figura 6 – Encapsulamento WEP
Fonte: Unibratec (2010)

3.2 USO DE SSID

O SSID, *Service Set Identifier*, é o nome designado para uma rede de área local sem fio especifica (WLAN) (D-LINK, 2002).

O padrão 802.11 desde seu princípio forneceu alguns mecanismos de segurança básicos para impedir que sua liberdade aprimorada seja uma possível ameaça. Para tanto, os pontos de acesso podem ser configurados com um identificador do conjunto de serviços (SSID). A placa NIC também deve conhecer este SSID para associá-lo ao AP e assim passar para a transmissão e recepção de dados na rede (D-LINK, 2002).

Esta segurança é muito fraca pelos seguintes motivos:

- Todas as placas NIC e todos os AP´s conhecem perfeitamente o SSID;
- O SSID é enviado por ondas de maneira transparente (Inclusive é sinalizado pelo AP);
- A placa NIC ou o controlador podem controlar localmente caso a associação do SSID desconhecido ser permitida.

Embora este esquema possa apresentar outros problemas, isto é suficiente para deter o intruso mais despreocupado.

Cada fabricante utiliza um valor default para esta opção, mas devemos alterá-la para um valor alfanumérico qualquer que seja difícil de adivinhar. Geralmente estará

disponível no utilitário de configuração do ponto de acesso a opção “broadcast SSID”. Ao ativar esta opção o ponto de acesso envia periodicamente o código SSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber previamente o código. Ativar esta opção significa abrir mão desta camada de segurança, em troca de tornar a rede mais “*plug-and-play*”. Você não precisará mais configurar manualmente o código SSID em todos os micros. Apenas o SSID, oferece uma proteção muito fraca. Mesmo que a opção broadcast SSID esteja desativada, já existem *sniffers* que podem descobrir rapidamente o SSID da rede monitorando o tráfego de dados (D-LINK, 2002).

3.2.1 Autenticação open system

A autenticação *Open System*, também chamada de autenticação nula, é a forma de autenticação mais simples nas redes IEEE 802.11. As estações que solicitarem autenticação com esse mecanismo serão autenticadas, exceto caso uma estação se recuse a autenticar alguma estação em particular. O mecanismo envolve dois passos:

1. A estação solicitante declara sua identidade e solicita autenticação.
2. A estação solicitada informa o resultado da autenticação.

Se o resultado da autenticação for “*successful*”, as estações estarão mutuamente autenticadas.

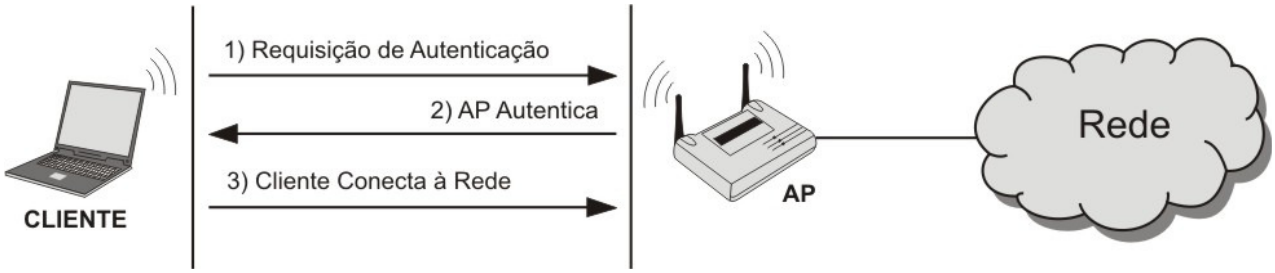

Figura 7 – Autenticação WEP – Sistema Aberto (*Open System*)
Fonte: Unibratec (2010)

3.2.2 Autenticação shared key

A autenticação *Shared Key* envolve estações que compartilhem uma chave secreta. Não há necessidade de transmitir a chave secreta de forma aberta, mas o mecanismo de privacidade WEP é necessário. A chave secreta deve ser entregue às estações participantes através de um canal seguro independente do IEEE 802.11.

No modo *Shared Key*, a estação que inicia a autenticação é referenciada como *requester* e a outra é chamada responder. Esta forma de autenticação envolve quatro passos:

I. *Requester* envia uma mensagem {*authentication request*} ao responder (AP) solicitando autenticação por *shared key*.
II. Responder responde com uma mensagem {*authentication response*} contendo um desafio (*challenge*).
III. *Requester* cifra o desafio com sua chave WEP e o devolve em uma nova mensagem {*authentication request*}.
IV. Se o responder decifrar o authentication *request* e obter o desafio original, ele responde com um *authentication response* concedendo acesso ao requester.

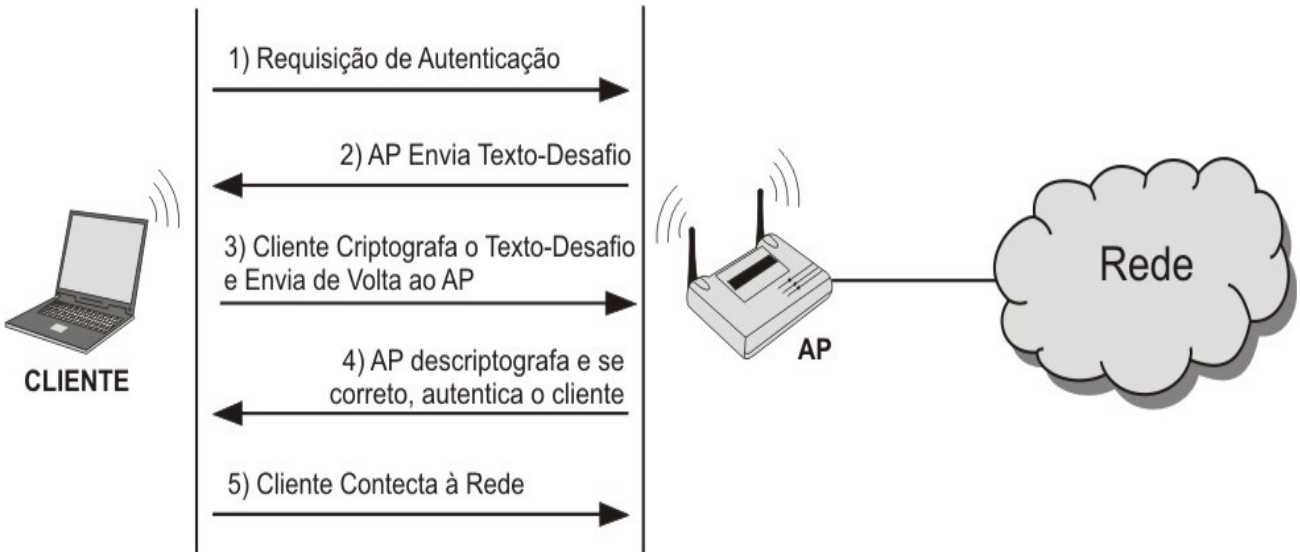

Figura 8 – Autenticação WEP Chave Compartilhada (*Shared Key*)
Fonte Unibratec (2010)

3.3 FILTRO DE MAC

Uma outra forma de segurança adicional é o filtro de MAC. Um endereço MAC baseado em ACL´s (*Access Control Lists*) ao ser utilizado fará com que somente os dispositivos registrados possam acessar a rede. Habilitar o filtro através de endereços MAC é como adicionar outra tranca a porta principal, e quanto mais barreiras um hacker encontrar, mais rapidamente desistirá de invadir nossa rede.

3.4 VULNERABILIDADES DO WEP

Vulnerabilidades são as falhas ou falta de segurança nas quais pessoas mal intencionadas possam invadir, subtrair, acessar ilegalmente, adulterar e destruir informações confidenciais.

Segundo a WI-FI Alliance (2004), depois de realizados vários estudos e testes com este protocolo, foram encontradas vulnerabilidades e falhas que tiraram quase toda a credibilidade do WEP. O primeiro ataque prático em WEP foi identificado por Scott Fluhrer, Itsik Mantin e Adi Shamir.

Uma das principais falhas existentes no protocolo WEP é a possibilidade de quebra de seu algoritmo. De acordo com ENGST e FLEISHMAN (2005), o protocolo WEP seria como uma porta trancada, impedindo que invasores consigam entrar na rede sem fio. Através da utilização de uma “chave segredo”, ou uma chave cifrada, o WEP cifra todos os dados que circulam na rede, impedindo a espionagem dos invasores.

O problema é que esta chave deve ser compartilhada por todos na rede, pois tanto um lado como o outro da comunicação precisa conhecer essa chave para o processo de cifragem e decifragem. Isto, principalmente num ambiente muito amplo e com muita mobilidade é um grande problema, por mais seguro que seja a distribuição dessa chave, pois, muitas pessoas precisarão conhecer essa chave além dos dispositivos e equipamentos que podem ser atacados para a obtenção da mesma.

Por esta chave ser a mesma para todos os usuários, cada pacote deve ter um vetor de inicialização diferente para evitar a repetição de uma mesma seqüência RC4, pois o RC4 é composto da chave secreta de 40 (que é o padrão) ou 104 bits mais o vetor de inicialização de 24 bits.

Entretanto, como o vetor possui o tamanho de apenas 24 bits, o período de troca fica restrito ao número de pacotes que são enviados e recebidos na transmissão. É

possível que um invasor realize operações de análise estatística dos quadros cifrados com a mesma chave durante o período de repetição.

Uma das recomendações na época era realizar a troca das chaves secretas periodicamente para aumentar a segurança da rede. Só que essa troca, quando feita, era realizada de maneira pouco prática, pois era feita manualmente o que se tornava inviável em redes com grande número de usuários.

Outra grande falha do WEP é a possibilidade de um invasor poder alterar um bit da mensagem cifrada sem precisar ter o conhecimento do seu conteúdo ou a chave quando utiliza uma autenticação do tipo *Shared Key*.

A utilização do algoritmo CRC-32 para detectar possíveis erros de transmissão que por ventura tenham modificado o conteúdo dos dados, também é considerado uma falha, pois, quando o CRC foi projetado não pensou-se em segurança, mas apenas em detectar alterações ocorridas devido à ruídos inerentes do canal de comunicação. Então, o CRC tem uma função linear, que não é segura quanto à criptografia. Com isso, um possível invasor pode identificar os bits do CRC, alterar qualquer outro bit na mensagem e recalcular o *checksum* para que o mesmo possa ser aceito pelos equipamentos na rede sem que se perceba que a mensagem foi alterada.

4 WPA (WI-FI PROTECTED ACCESS)

Devido a todos os problemas (falhas e vulnerabilidades) detectados no protocolo WEP, um grupo de membros da Wi-Fi Alliance e do IEEE se empenharam em desenvolver um novo protocolo que resolvesse algumas das vulnerabilidades apresentadas pelo WEP. Surgia então no ano de 2002, a primeira versão do WPA (*Wi-Fi Protected Access*) que também foi chamado de WEP2 ou TKIP (*Temporal Key Integrity Protocol*). (WI-FI Alliance, 2010).

O WPA nasceu então para aumentar gradativamente o nível de proteção de dados e controle de acesso para redes sem fio. É um padrão baseado em um subconjunto de IEEE 802.11i e, como foi dito anteriormente, veio para substituir o WEP depois que diversas falhas e vulnerabilidades foram detectadas nesse primeiro protocolo. Foi projetado para rodar em qualquer hardware que fosse baseado no padrão antigo (WEP). Quando corretamente instalado, fornece aos usuários de LAN´s sem fios um nível alto de segurança para os dados por eles transmitidos.

Nesse padrão somente usuários autorizados podem ter acesso à rede. O WPA utiliza o Protocolo de Integridade Fundamental Temporal (TKIP) (WI-FI Alliance, 2010).

4.1 TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

O TKIP é um protocolo de chave temporária criado em 2002 e faz parte do padrão WPA. Foi a primeira tentativa de corrigir os problemas apresentados pelo WEP, tanto que ele ainda guarda algumas características apresentadas pelo WEP como a utilização do algoritmo modificado RC4 para embaralhar os dados. Com o TKIP

permitiu-se eliminar os problemas de confidencialidade e integridade apresentados pelo WEP.

No WEP o tamanho padrão de chaves era 64 bits, já o TKIP usa o padrão de tamanho 128 bits que era opcional no WEP. Além disso, dobrou o tamanho do vetor de inicialização que era de 24 bits no WEP para 48 bits.

O TKIP usa uma chave chamada de *Temporal Key*, resultante da combinação entre a chave compartilhada do Ponto de Acesso e do cliente e o endereço MAC da placa de rede wireless do cliente. Cada chave gerada fica diferente e única para cada cliente wireless na rede.

Essa chave é chamada de *Temporal Key* porque ela é alterada de tempo em tempo. O administrador da rede pode informar o tempo de troca ou se não informado ela é trocada a cada 10.000 quadros. Se por acaso um invasor conseguir quebrar essa chave de criptografia do TKIP, ela será útil para ele apenas em um determinado intervalo de tempo, durante o qual a chave é considerada válida.

O TKIP implementa número de seqüência para evitar ataque de repetição e inserção. Já para integridade dos dados ele utiliza o algoritmo MIC - *Message Integrity Checksum* (Michael).

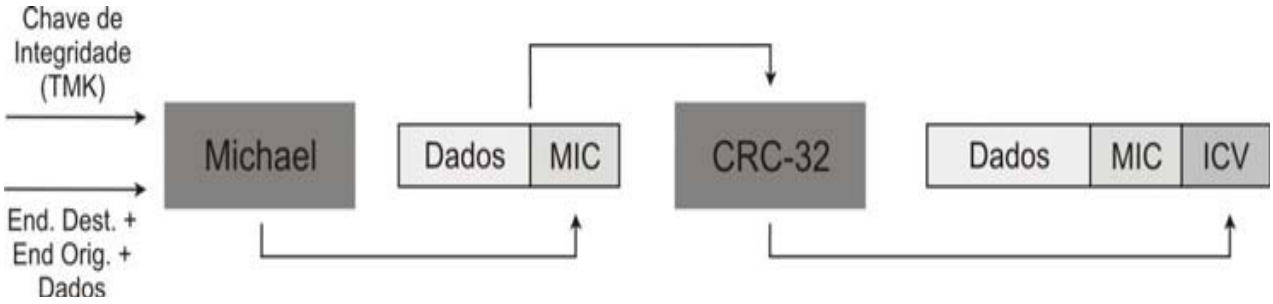

Figura 9 – Integridade WPA
Fonte Unibratec (2010)

4.2 MIC (MESSAGE INTEGRITY CHEC)

O WPA trabalha com o MIC (Message Integrity Chec) ou Cheque de Integridade de Mensagem que é parte do padrão 802.11. Ele evita que um pacote seja alterado durante transmissão em uma rede sem fio. Como uma parte do TKIP, o MIC provê um campo adicional de 8 bytes dentro da especificação 802.11 que protege tanto os dados de carga útil quanto o cabeçalho do pacote de manipulação indesejada. O algoritmo que implementa o MIC é conhecido como Michael Shamir (WI-FI Alliance, 2010).

O MIC é uma tecnologia empregada para impedir um atacante de capturar, e alterar pacotes de dados. O MIC provê uma função matemática forte na qual tanto o receptor quanto o transmissor executam e comparam o MIC. Se o resultado não for semelhante, é entendida a falsificação/alteração dos dados (WI-FI Alliance, 2010).

4.3 EAP (EXTENSIBLE AUTHENTICATION PROTOCOL)

Com o TKIP podemos dizer que tinham resolvido em parte os problemas de confidencialidade dos dados. Então surgiu o 802.1x/EAP para resolver os problemas com autenticação.

O WPA utiliza o EAP (Extensible Authentication Protocol), um protocolo de autenticação genérico, que através de um servidor central de autenticação, autentica cada usuário antes que este tenha acesso à rede. Ele possibilita inúmeras formas de

autenticação, inclusive certificação digital. Sua definição foi feita na RFC 2284, com atualizações no draft 2284bis.

O modo de funcionamento do protocolo EAP é muito simples, mas eficiente. O Objetivo é evitar acessos não autorizados à rede.

Segundo ENGST e FLEISHMAN (2005), o funcionamento do EAP é composto por três elementos: o cliente que é o solicitante, um ponto de acesso à rede que deverá ser o responsável pela autenticação (como se fosse um porteiro, controlando quem pode passar e quem não tem acesso), e um servidor de autenticação, contendo um banco de dados onde as informações de autenticação do cliente serão armazenadas.

Quando o cliente solicita o acesso à rede para o responsável pela autenticação (ponto de acesso), ele confere essas informações do cliente no servidor de autenticação (que contém o banco de dados) e este retorna se as informações estão corretas ou não. Se as informações forem válidas, o ponto de acesso (porteiro) concederá o acesso à rede para o solicitante.

De acordo com ENGST e FLEISHMAN (2005), essas autenticações podem ser uma simples validação de nome de usuário e senha ou um sistema mais rigoroso de controle que verifica a autenticidade de uma assinatura digital, por exemplo.

O protocolo EAP, na sua definição, permite a utilização de uma grande variedade de mecanismos de autenticação, como smart cards, Kerberos, public key, one-time passwords. Como a maioria destes métodos só permitem a autenticação do cliente frente ao servidor, em vários casos é preciso o suporte à autenticação mútua e a utilização de um mecanismo de estabelecimento de chaves de sessão. Isso levou à criação do protocolo EAP-TLS, pois o TLS permite a autenticação mútua e negociação do algoritmo de criptografia e chaves criptográficas antes do protocolo de aplicação transmitir ou receber dados fornecendo privacidade e integridade na comunicação .

4.4 BENEFÍCIOS DO WPA EM RELAÇÃO AO WEP

Trabalha com criptografia dinâmica de chave e autenticação mútua por isso quando comparado ao WEP o WPA oferece aos usuários mais segurança no acesso aos dados e à rede. Mantém usuários indesejáveis afastados, adicionando características avançadas de autenticação e senha e foi projetado como padrão de segurança compatível com múltiplos fabricantes. (D-LINK, 2002).

Cada usuário deve entrar com uma única senha para ativar o WPA. Depois de ativado, a senha irá mudar periodicamente para prevenir a entrada de intrusos na rede. Esta é a diferença para o WEP, que utiliza uma única chave estática para criptografia.

O padrão 802.1x suporta servidores de autenticação, tais como Radius ou LDAP, para reconhecer o usuário em um ambiente empresarial. O padrão WPA ofereceu o primeiro grande passo na direção de se garantir a segurança nas transferências de dados wireless (D-LINK, 2002).

Além disso, permitia trabalhar numa rede híbrida que tenha WEP instalado e para posterior migração para o WPA2 necessitaria de somente atualização de software, pois foi feito para ser compatível com o padrão IEEE 802.11i.

4.5 VULNERABILIDADES DO WPA

O WPA solucionou praticamente todas as vulnerabilidades apresentadas pelo protocolo WEP. Porém, falhas em sua implementação o tornaram vulnerável. O algoritmo de combinação de chaves é fraco. O MIC possui um mecanismo de proteção para evitar ataques de força bruta, porém esse mecanismo acarreta um ataque de negação de serviço (DoS). Quando dois erros de MIC são detectados em menos de um minuto o AP cancela a conexão por 60 segundos e altera a chave de integridade. Portanto, com uma simples injeção de pacotes mal formados é possível fazer um ataque de negação de serviço.

5 WPA2

O WPA corrigiu vários erros do WEP, porém, ainda restou algumas vulnerabilidades como foi visto no capítulo anterior. Além disso, seu desempenho teve uma queda significativa em termos de estabilidade, por isso, houve a necessidade de se criar um outro protocolo que fosse mais seguro ainda que o WPA e que também tivesse um melhor desempenho. Então o WPA2 surgia com a promessa de ser a solução definitiva de segurança e estabilidade para as redes sem-fio do padrão Wi-Fi.

Em setembro de 2004, a Wi-Fi Alliance apresentou o WPA2, a segunda geração de segurança do WPA. Como o WPA, o WPA2 proporciona para empresas e usuários de Wi-Fi um alto nível de garantia para que seus dados permaneçam protegidos e que somente usuários autorizados tenham acesso as suas redes sem fios. O WPA2 está baseado no IEEE final 802.11i, emenda do padrão 802.11, ratificado em junho de 2004. Segundo muitos analistas esse padrão 802.11i era exatamente o que faltava para estimular implementações seguras de redes wireless nas empresas (WI-FI Alliance, 2010).

A principal mudança entre o WPA2 e o WPA é o método criptográfico utilizado. Enquanto o WPA utiliza o TKIP com o RC4, o WPA2 utiliza o *Advanced Encyptation Standart* (AES) em conjunto com o TKIP com chave de 256 *bits*, que é um método muito mais poderoso.

Também como o WPA, o WPA2 usa tecnologia de autenticação IEEE 802.1X/EAP ou tecnologia de PSK. Mas trabalha com um mecanismo novo de encriptação avançado e mais robusto que o TKIP que usa o Counter-Mode/CBC-MAC Protocolo (CCMP) chamado de AES (Advanced Encryption Standard) (WI-FI Alliance, 2010).

Foi adotado como um padrão de governo oficial pelo Departamento norte-americano de Comércio e o Instituto Nacional de Padrões e Tecnologia (NIST). Na sua especificação o padrão 802.11i garante que os dados enviados por essas redes

sejam criptografados e não sejam violados por nenhum tipo de interceptação (SYMANTEC, 2010).

5.1 AES (ADVANCED ENCRYPTION STANDARD)

O AES (Padrão Avançado de Criptografia) fornece suporte a chaves de 128, 192 e 256 bits e satisfaz exigências de fundo público norte-americanas. AES é um bloco cifra, um tipo de cifra de chave simétrica que usa grupos de bits de comprimento fixo - chamados blocos. Uma cifra fundamental simétrica é uma cifra que usa a mesma chave para encriptação e descriptação. A palavra cifra é usada em criptografia para descrever as instruções ou algoritmo usado para codificar e decifrar uma informação (Wi-Fi Alliance, 2010).

Com o AES, bits são codificados em blocos de texto que é calculado independentemente, trabalha com blocos de 128 bits com três tamanhos de chave possíveis 128, 192 e 256 bits como especificado no padrão de AES. Para a implementação de WPA2/802.11i de AES, uma chave de tamanho de 128 bits é usada. A utilização do AES inclui quatro estágios. Esses estágios são repetidos então 10, 12 ou 14 vezes dependendo do tamanho da chave. Para a implementação de WPA2/802.11i de AES, cada círculo é repetido 10 vezes (Wi-Fi Alliance, 2010).

Esse protocolo usa o Counter-Mode/CBC-Mac Protocolo (CCMP). O CCM é um novo modo de operação para um bloco cifra que habilita uma única chave a ser usada para criptografia e autenticação. Os dois modos subjacentes empregados em CCM incluem modo de Contador (CTR) isso alcança criptografia de dados e Bloco de Cifra que encadeiam Código de Autenticação de Mensagem (Cipher Block Chaining Message Authentication Code, CBC-MAC) para prover a integridade dos dados (Wi-Fi Alliance, 2010).

Esse CBC-MAC é usado para gerar um componente de autenticação como resultado do processo de criptografia. Isto é diferente da implementação de MIC anterior na qual é requerido um algoritmo separado para cheque de integridade. Para tornar sua capacidade de criptografia mais avançada, o AES usa um Vetor de Inicialização (IV) de 48 bits (Wi-Fi Alliance, 2010).

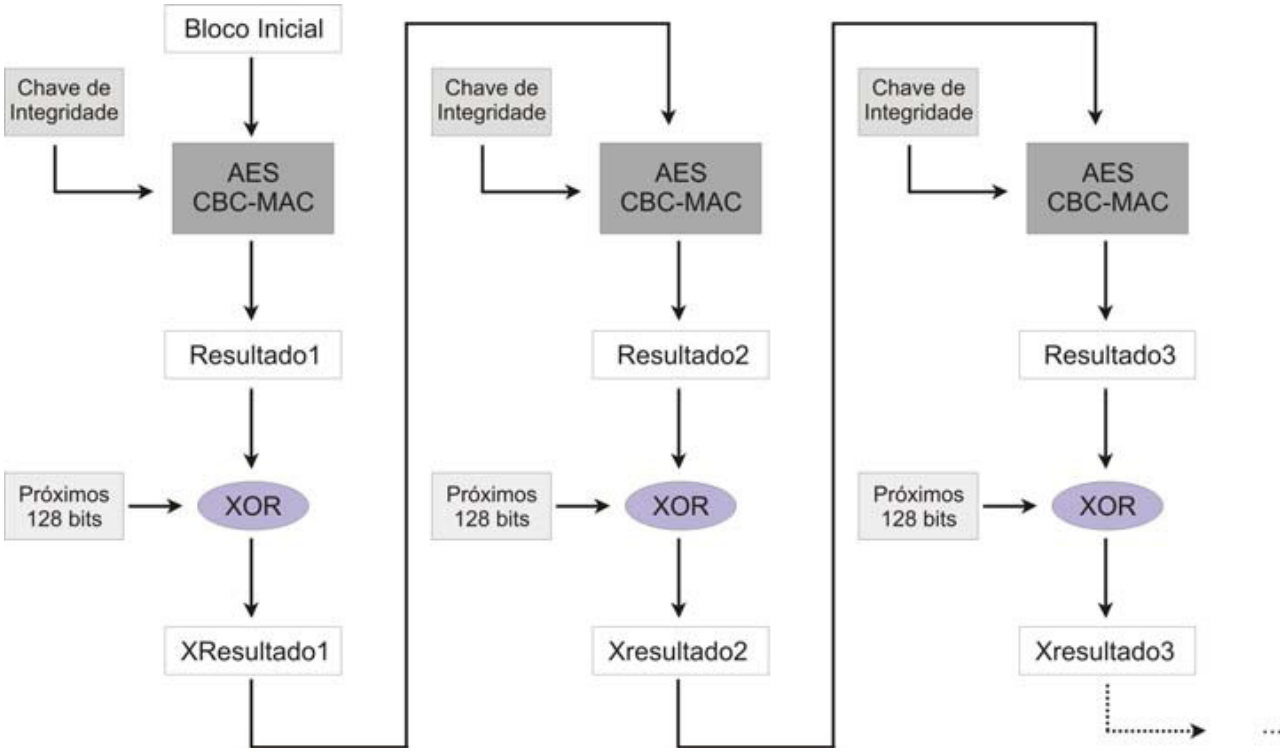

Figura 10 – Integridade WPA2
Fonte Unibratec (2010)

5.2 VULNERABILIDADES WPA2

Atualmente, por possuir um mecanismo de segurança bastante eficiente como foi visto, não foram descobertas muitas vulnerabilidades ou falhas de segurança no protocolo WPA2. Um dos tipos ataques a que ele está sujeito é o de Negação de

Serviço (DoS), pois os quadros de gerenciamento e controle ainda não tem proteção.

Segundo o IDG Now! (2010), especialistas em segurança da AirTight Networks descobriram uma falha de segurança no protocolo de rede sem fio WPA2 que eles chamaram de “Hole 196” ou “Buraco 196”. Ela ganhou esse nome em referência à página 196 do manual de padrões da IEEE. É nessa página que o padrão IEEE trata as chaves usadas pelo WPA2: a PTK (Pairwise Transient Key), que é única para cada cliente e usada para tráfego unidirecional, e a GTK (Group Temporal Key), que é usada para broadcast.

A PTK consegue detectar quando dados e endereços MAC estão sendo forjados. Já a GTK não consegue detectar essa falsificação. De acordo com o IDG Now (2010), os especialistas da AirTight que descobriram essa falha, dizem que essa é a questão central, pois pode deixar um cliente gerar pacotes arbitrários de broadcast, para que outros clientes respondam com informação sobre suas PTKs secretas, que podem ser decodificadas pelos atacantes.

A AirTight disse que bastam 10 linhas extras de código disponível na web para o driver open source Madwifi para fazer um PC com uma placa de rede comum simular o endereço MAC de um Acess Point (AP) e passar-se por gateway para o envio de tráfego. (IDG Now!, 2010).

Segundo a Wi-Fi Alliance (2010), eles se preocupam com a segurança e estão sendo feitos mais estudos sobre os detalhes do “hole 196”. No entanto o atacante pode se utilizar de uma técnica chamada ARP Spoofing, mas que esta é uma vulnerabilidade que existe em redes sem fio, mas nas redes cabeadas também. ARP Spoofing não recupera chaves para redes sem fio usando criptografia WPA2-AES ou WPA-TKIP, ou seja, para que o “Buraco 196″ possa ser explorado, é necessário que o hacker tenha acesso à chave WPA2 e esteja autenticado (logado) na rede, o que é um pouco menos preocupante.

5.3 COMPARANDO WEP, WPA E WPA2

O WPA buscava sanar todas as vulnerabilidades conhecidas do WEP: enquanto o WEP não possui qualquer meio de autenticação de usuário o WPA fornecer esquema de autenticação mútuo que usa IEEE 802.1X/Extensible Protocolo de Autenticação (EAP). Trabalha com TKIP - Protocolo de Integridade Fundamental Temporal com Cheque de Integridade de Mensagem (MIC) (Wi-Fi Alliance, 2010).

Como já foi dito o WPA2 também inclui um novo mecanismo de criptografia avançado que usa o Contador-Mode/CBC-MAC Protocolo (CCMP) chamado de Padrão de Criptografia Avançado (AES) (Wi-Fi Alliance, 2010).

Existem dois modos de trabalharmos com WPA e WPA2: Enterprise and Personal. Em ambos os casos os dois protocolos provêem autenticação e criptografia.

No modo enterprise, cada usuário possui uma chave única para acessar a WLAN. Fornecendo assim um nível alto de privacidade individual. O WPA utiliza o TKIP que emprega um padrão de criptografia que calcula e emite chaves de criptografia para cada pacote de dados comunicado em cada sessão de cada usuário, tornando extremamente difícil quebrar essa barreira. No WPA2, o padrão de criptografia usado é o AES que é mais forte que TKIP, provendo então uma proteção adicional de rede (Wi-Fi Alliance, 2010).

O modo Personal é projetado para casa e escritório de office/home pequeno (SOHO), ou seja, usuários que não têm servidores de autenticação disponível. Usa uma chave pré-compartilhada (PSK) para autenticação em vez de IEEE 802.1X.

Quanto à proteção contra ataques à WLAN o WPA e o WPA2 protegem a rede sem fios de uma variedade de ameaças. O WPA evita as fraquezas de segurança do

WEP original que é o resultado da sua criptografia imperfeita e sua falta de autenticação. Usando TKIP, traz um algoritmo de criptografia maior e com autenticação IEEE 802.1X/EAP. Juntos, TKIP e autenticação mútua separam a rede de Wi-Fi de uma variedade de ameaças quando o modo WPA-Enterprise for usado.

O WPA2 oferece proteção avançada de ataques de rede sem fios através da utilização do AES, criptografia de grau de governo e autenticação IEEE 802.1X/EAP, baseado em um padrão de autenticação mútua mais forte e criptografia avançada para proteger a rede sem fios de uma variedade de ameaças e ataques.

Apesar de ter surgido a descoberta do “hole 196” conforme já descrito, para que essa vulnerabilidade possa ser explorada, é necessário que o invasor tenha acesso à chave WPA2 e seja um usuário autenticado na rede, o que é um pouco menos preocupante.

CONCLUSÃO

Ao compararmos os três protocolos que foram aqui descritos, podemos ver que o WEP realmente oferecia uma segurança muito frágil e concluímos que sua substituição pode ser vista como uma necessidade emergencial para qualquer empresa onde a segurança seja um fator relevante. Uma boa solução neste caso era a adoção do WPA, que sanava algumas falhas do WEP, como por exemplo, o problema das chaves estáticas. Além disso, os equipamentos utilizados pelo WEP eram compatíveis com o WPA necessitando apenas de atualização de software.

Já o WPA2 trabalha com uma criptografia mais forte e com autenticação de usuários permitindo assim um desenvolvimento rápido dos produtos wireless e um estímulo para as implementações de redes locais sem fio.

Quem não tem muita preocupação com a segurança e está à procura de desempenho e estabilidade o protocolo WEP é o indicado.

O protocolo WPA embora tenha se proposto a substituir o WEP, corrigindo seus erros, não foi muito bem aceito, pois uma vez configurado, torna a rede mais lenta ocasionando problemas de performance, além de não ter sanado todos os problemas de segurança.

Já o protocolo WPA2 vem cumprindo bem o seu papel a que foi proposto, proporcionando segurança e estabilidade. É o protocolo mais utilizado atualmente.

Apesar da descoberta do “Hole 196” conforme já descrito, para que essa vulnerabilidade possa ser explorada, é necessário que o invasor tenha acesso à chave WPA2 e seja um usuário autenticado na rede. Quando isso acontece, realmente, por mais seguro que o protocolo possa ser, fica difícil evitar qualquer falha de segurança.

Além disso, qualquer tecnologia só irá funcionar se bem configurada, caso contrário, devido à má configuração dos pontos de acesso e dos softwares-clientes, as invasões continuarão acontecendo. As empresas devem assegurar que seus pontos de acesso wireless sejam configurados de forma segura e não sejam instalados na rede sem a devida autorização.

Dois meios primários de atribuir segurança a uma rede sem fio são criptografia e autenticação e o ideal é que esses métodos trabalhem juntos e complementem um ao outro. Muitas vezes somente os protocolos não são suficientes para garantir o nível de segurança desejado. Então, nestes casos, torna-se necessário configurar outros métodos de segurança para reforçar o bloqueio, como por exemplo, a utilização do filtro de MAC e a desativação do broadcasting de SSID.

Podemos concluir então que, apesar de muitas empresas reclamarem da segurança oferecida pelas redes sem fio, atualmente é possível obter um alto nível de segurança com a adoção das tecnologias certas e com as devidas configurações corretas das mesmas, além de uma boa política de segurança na administração de suas redes.

REFERÊNCIAS

D-LINK. **D-Support for Wireless LAN. D-PR: D-Linker Professional Resellers for wireless.** 2002.

FLEISHMAN, G.; ENGST, A. **Kit do Iniciante em Redes Sem Fio.** 2ª Edição. Editora Makron Books. 2005.

IDG NOW!. **Descoberta falha no protocolo de segurança Wi-Fi WPA2**: 2010. Disponível em: < http://computerworld.uol.com.br/seguranca/2010/07/26/descoberta-falha-no-protocolo-de-seguranca-wi-fi-wpa2> Acesso em 21 de Agosto de 2010.

MOHER, M.; HAYKIN, S. **Sistemas Modernos de comunicação wireless**. São Paulo. Editora Bokman. 1ª Edição. 2008.

MORIMOTO, C. E.; **Redes - Guia Prático**. Porto Alegre. Editora sul Editores. 1ª Edição. 2008.

NGSAT. **Produtos**. Disponível em: < www.ngsat.com.br>. Acesso em 07/08/2010.

OLIVEIRA, L. A. A. **Comunicação de Dados e Teleprocessamento. Uma Abordagem Básica**. Editora Atlas. 3ª Edição. 1993.

PETERSON, LARRY L.; DAVIE, BRUCE S.: **Redes de Computadores**. Rio de Janeiro. Elsevier. 5ª Reimpressão.

REVISTA PCWORLD: **Protocolo 802.11n: por que demorou tanto e o que ele traz de novidade.**. Disponível em: <http://pcworld.uol.com.br/dicas/2009/09/16/protocolo-802-11n-por-que-demorou-tanto-e-o-que-ele-traz-de-novidade/>. Acesso em 06 de Agosto de 2010.

ROSS, J. **O Livro do Wireless**. Editora Alta Books. 1ª Edição. 2009.

SANTOS, I. C. **A evolução do WEP: WPA tratamento especial às vulnerabilidades**. SECURITY HACKER. Editora Escala. Ano 01. Nº 07. Maio/2004

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de Computadores das LANs, MANs e WANs às Redes ATM**. Rio de Janeiro. Editora Campus. 1995.

SYMANTEC. **Uma Atualização sobre a Segurança Wireless.** Disponível em: <http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_4708.html>. Acesso em: 04 de Agosto de 2010.

TANENBAUM, A. S. **Redes de Computadores**. Rio de Janeiro. Editora Campus. 4ª edição. 2003.

TECNINFO. **Produtos para rede em geral**. Disponível em: < www.tcninfo.com.br>. Acesso em 07/08/2010.

UNIBRATEC: **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w**. Disponível em: <http://www.unibratec.com.br/jornadacientifica/diretorio/UFPEAGL.pdf >. Acesso em: 07 de Agosto de 2010.

WI-FI ALLIANCE. **Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise:** 2005. Disponível em: < http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf> Acesso em: 01 de Agosto de 2010.

WI-FI ALLIANCE. **Deploying WPA and WPA2 in the Enterprise**. Disponível em: <http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise > Acesso em: 01 de Agosto de 2010.

WI-FI ALLIANCE. **Security.** Disponível em: <http://www.wi-fi.org/security.php> Acesso em: 01 de Agosto de 2010.

WI-FI ALLIANCE. **Wi-Fi Alliance Responds to ARP Spoofing**: 2010. Disponível em: <http://www.wi-fi.org/news_articles.php?f=media_news&news_id=992> Acesso em: 21 de Agosto de 2010.

WI-FI ALLIANCE. **Wi-Fi Protected Access Security Sees Strong Adoption**. 2004. Disponível em: <http://www.wi-fi.org/news_articles.php?f=media_news&news_id=37> Acesso em 07 de Agosto de 2010.