Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w*

ANDRÉ GUEDES LINHARES PAULO ANDRÉ DA S. GONÇALVES

Universidade Federal de Pernambuco (UFPE) - Centro de Informática (CIn)

Av. Professor Luis Freire s/n – Cidade Universitária - Recife – PE – Brasil

{agl, pasg}@cin.ufpe.br

RESUMO

Este artigo apresenta uma análise dos mecanismos de segurança de redes IEEE 802.11. Os protocolos WEP, WPA e WPA2 são analisados sob os aspectos básicos de segurança: autenticação, integridade e confidência. Para cada protocolo há uma descrição de suas vulnerabilidades conhecidas. Finalmente, é feita uma análise do novo padrão de segurança IEEE 802.11w que se encontra em fase de desenvolvimento. A principal contribuição deste artigo reside na identificação de vulnerabilidades associadas a este novo padrão.

ABSTRACT

In this paper we analyze security mechanisms for wireless LANs IEEE 802.11. We analyze WEP, WPA and WPA2 mechanisms under the following basic security aspects: authentication, integrity and confidentiality. We describe all known vulnerabilities related to each security mechanism presented. Finally, we analyze the new IEEE 802.11w standard, which is currently under development. Our finds reveals that IEEE 802.11w has some weakness.

PALAVRAS-CHAVE

Segurança, IEEE 802.11

1. INTRODUÇÃO

A segurança de redes é freqüentemente tratada pelas camadas mais altas da pilha de protocolos e na maioria das vezes é vista apenas como um problema da camada aplicação. Com o advento das redes locais sem fio (WLANs – *Wireless Local Area Networks*) este paradigma de segurança sozinho se mostra inadequado. Essas redes se baseiam na comunicação via ondas de rádio e, portanto, qualquer um possuindo um receptor de rádio pode interceptar a comunicação. Além disso, qualquer um possuindo um transmissor de rádio pode injetar dados na rede. Assim, as WLANs necessitam de componentes de segurança presentes na camada enlace para proteger o acesso à rede e manter a confidência dos dados que transitam na mesma.

* Este trabalho foi realizado com recursos da FACEPE, CAPES, CNPq, UFPE e FINEP.

Nos últimos anos, houve um grande crescimento na utilização de WLANs, principalmente, as baseadas nos padrões da família IEEE 802.11 [1]. No padrão IEEE 802.11 [2] aprovado em 1999, foi introduzido um protocolo de segurança denominado WEP (*Wired Equivalent Privacy*). O intuito desse protocolo era oferecer às WLANs IEEE 802.11 um nível de privacidade equivalente ao das redes locais (LANs – *Local Area Networks*) Ethernet. Uma LAN geralmente está protegida por mecanismos de segurança físicos (*e.g.* controle de acesso à salas, prédios, etc) que são eficazes em uma área física controlada. Contudo, essa abordagem não é efetiva para as WLANs, pois as ondas de rádio usadas para a comunicação não ficam necessariamente confinadas pelas paredes da área onde se encontram os dispositivos que compõem a rede. Usando criptografia de dados, o WEP consegue uma proteção similar à oferecida por mecanismos de segurança físicos. A criptografia de dados protege as informações que irão transitar pelo canal de comunicação entre o ponto de acesso e os clientes (e vice-versa). Em conjunto com esta medida, outros mecanismos de segurança típicos de LANs podem ser utilizados. Exemplos incluem a proteção através de senhas, filtragem de endereços MAC (*Medium Access Control*) e o uso de redes privadas virtuais (VPNs – *Virtual Private Networks*).

Diversas pesquisas [3, 4, 5, 7] demonstraram problemas significativos de segurança no padrão IEEE 802.11. Em 2003, o WEP foi então substituído pelo WPA (*Wi-Fi Protected Access*) que por sua vez, devido a algumas falhas de implementação, foi substituído, em 2004, pelo padrão IEEE 802.11i ou WPA2 [6]. Atualmente, um grupo de pesquisa do IEEE[1] está trabalhando em um novo padrão de segurança denominado IEEE 802.11w. O intuito é estender o padrão IEEE 802.11i, adicionando proteção aos quadros de gerenciamento que desde o surgimento do padrão IEEE 802.11 até então ficaram desprotegidos e passíveis de serem utilizados em ataques de negação de serviço (DoS- *Deny of Service*) . A figura abaixo ilustra a evolução em ordem cronológica dos mecanismos de segurança que protegem redes WLAN da família 802.11

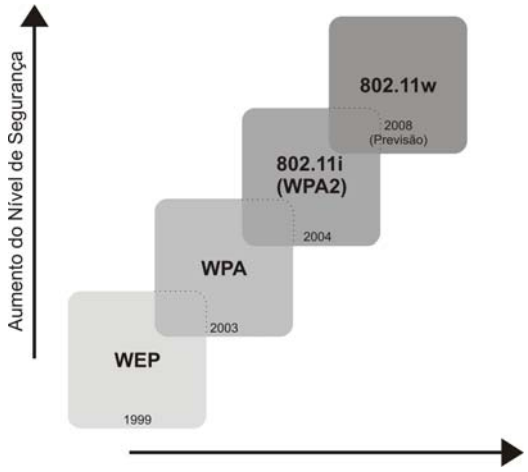

Figura 1 – Evolução dos Mecanismos de Segurança 802.11

[1] **IEEE 802.11 Task Group w -** http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm

O desenvolvimento de bons mecanismos de segurança para redes é, geralmente, baseado em três requisitos mínimos: confidência, autenticação e integridade. A confidência está inerentemente ligada à criptografia dos dados cujo intuito é permitir que somente pessoas previamente autorizadas tenham acesso às informações, decodificando-as, ou seja, apenas pessoas autorizadas conseguem decodificar a mensagem e entender a informação. A autenticação lida com a identificação de pessoas e dispositivos. Somente pessoas e dispositivos autorizados podem ter acesso à rede e aos serviços da mesma. A integridade garante que os dados recebidos pelo receptor sejam os mesmos que foram transmitidos pelo emissor, ou seja, garante que alterações nos pacotes que transitam na rede (*e.g.*, por erros de transmissão inerentes ao meio sem fio ou pela manipulação de dados) sejam facilmente detectadas.

Este artigo apresenta uma análise dos mecanismos de segurança WEP, WPA, WPA2 e IEEE 802.11w propostos para WLANs baseadas nos padrões da família IEEE 802.11. As análises do WEP, WPA e WPA2 são feitas com relação à autenticação de usuários e dispositivos, integridade e confidência de dados. As vulnerabilidades conhecidas de cada um destes mecanismos de segurança também são apresentadas. Por fim, é realizada a análise do IEEE 802.11w. Este artigo contribui identificando pontos falhos deste mecanismo antes mesmo do término de seu desenvolvimento.

Este artigo está organizado da seguinte forma: as Seções 2, 3 e 4 apresentam respectivamente os mecanismos de segurança WEP, WPA e WPA2 , cada qual com as análises e vulnerabilidades associadas. A Seção 5 faz uma análise do padrão IEEE 802.11w e, finalmente, a Seção 6 conclui o trabalho.

2. Wired Equivalent Privacy (WEP)

WEP foi o protocolo de segurança introduzido no padrão IEEE 802.11 em 1999. Ele provê dois métodos de autenticação de dispositivos, utiliza CRC-32 (*Cyclic Redundancy Checks*) para a verificação da integridade de dados e usa o algoritmo de criptografia RC4 (*Ron´s Code #4*) para prevenir a leitura de dados de usuário que transitarão na rede. O WEP pode ser utilizado entre o Ponto de Acesso (AP – *Access Point*) e os clientes da rede (modo com infra-estrutura), assim como na comunicação direta entre clientes (modo *ad-hoc*). Como ilustrado na Figura 2, 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.

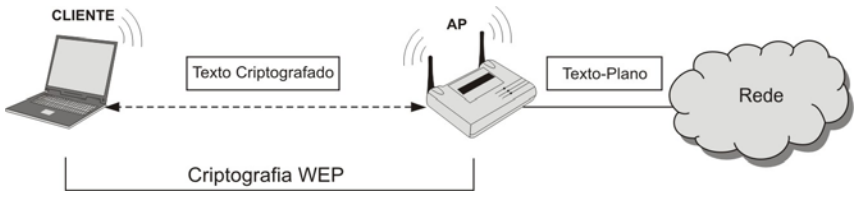

Figura 2 - WEP

2.1 Autenticação

Um dispositivo deve ser autenticado pelo ponto de acesso antes de se associar a ele e poder enviar dados na rede. O padrão IEEE 802.11 define dois tipos de autenticação WEP: Sistema Aberto (*Open System*) e Chave Compartilhada (*Shared Key*).

O ***Sistema Aberto*** permite que qualquer dispositivo se associe à rede. Para isso é necessário informar o SSID (*Service Set Identifier*) da rede (*i.e.* nome da rede). O SSID pode ser adquirido através de pacotes do tipo BEACON. Estes pacotes não possuem criptografia e são enviados periodicamente em *broadcast* pelo Ponto de Acesso. Além do SSID, estes pacotes contêm outras informações sobre a rede como por exemplo, o canal de transmissão, a taxa de transmissão, etc. A figura 3 ilustra o processo de autenticação WEP sistema aberto. O dispositivo envia um pedido de autenticação ao Ponto de Acesso que por sua vez envia uma mensagem informando que o dispositivo foi autenticado. Em seguida, o cliente se associa ao ponto de acesso, conectando-se à rede.

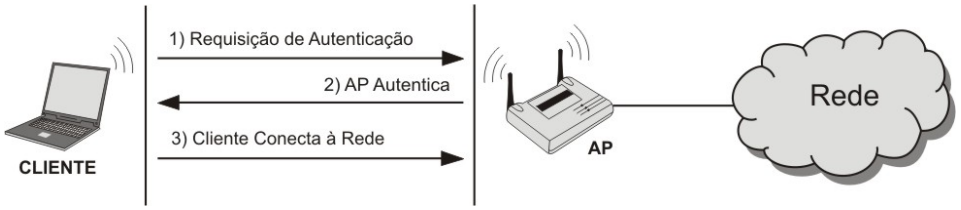

Figura 3 – Autenticação WEP – Sistema Aberto (*Open System*)

A autenticação por ***Chave Compartilhada*** requer que o cliente e o ponto de acesso possuam uma mesma chave. O processo de autenticação por chave compartilhada é apresentado na Figura 4. O cliente envia um pedido de autenticação ao ponto de acesso que em seguida envia ao cliente um texto-plano (sem criptografia). Este texto é chamado de texto-desafio (*challenge text*). O cliente usa sua chave pré-configurada para criptografar o texto-desafio, retornando o resultado ao ponto de acesso. O AP o descriptografa com sua própria chave e compara o texto obtido com o texto-desafio originalmente enviado. Se o texto for o mesmo, o cliente é autenticado, caso contrário o cliente não consegue se associar à rede.

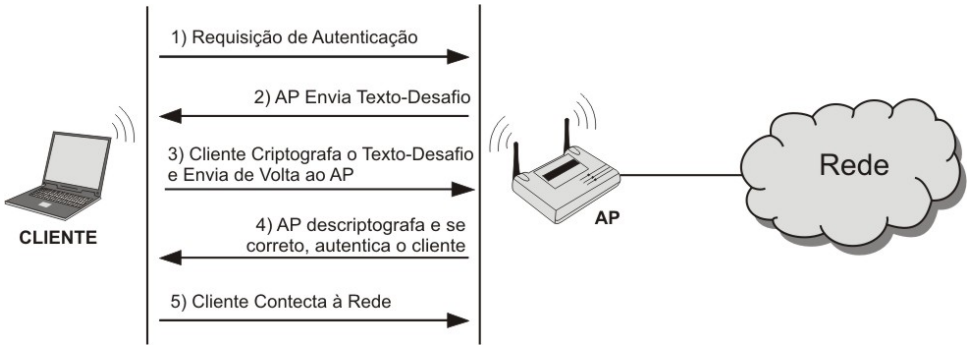

Figura 4 – Autenticação WEP Chave Compartilhada (*Shared Key*)

Ambos os tipos de autenticação WEP podem ser combinados com a filtragem de endereços MAC (*MAC Filtering*). Neste método, o ponto de acesso possui uma lista contendo o endereço MAC de dispositivos que podem ser autenticados. Se o endereço MAC não estiver na lista, não será possível o acesso à rede. Este método não faz parte da especificação IEEE 802.11, mas é disponibilizado por vários fabricantes de equipamentos Wi-Fi (*Wireless Fidelity*)[2] para tentar aumentar o controle de acesso à rede.

2.2 INTEGRIDADE

Para a verificação da integridade de mensagens recebidas, o WEP adiciona à mensagem a ser enviada um ICV (*Integrity Check Value*). O ICV nada mais é que um típico CRC adicionado à mensagem original antes da criptografia ser realizada. Ao receber uma mensagem, um cliente (ou AP) a decodifica e calcula o CRC-32 da mensagem, conferindo-o com o CRC-32 informado no campo ICV. Se forem diferentes, a mensagem é descartada. Este processo é ilustrado na Figura 5.

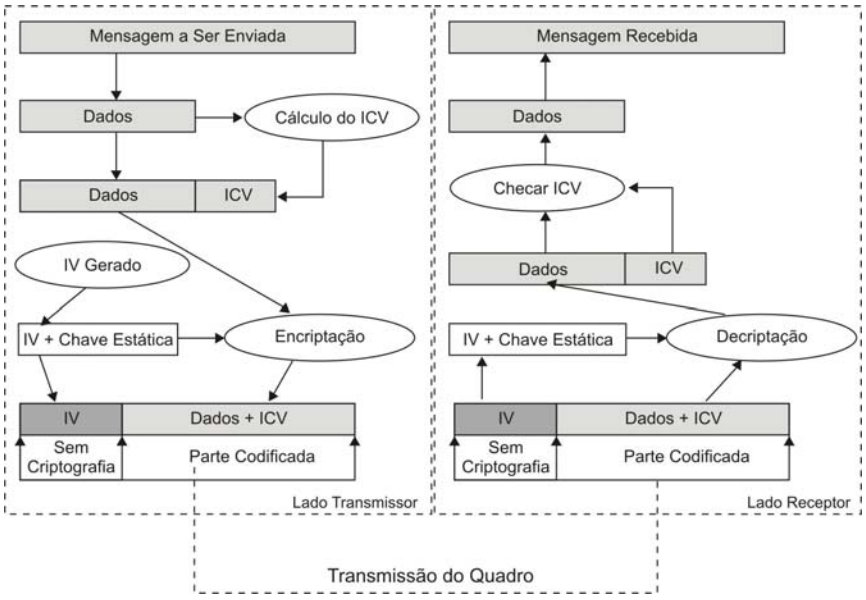

Figura 5 – Integridade WEP

2.3 Confidência

Para tornar as mensagens confidenciais, o WEP utiliza o algoritmo criptográfico RC4. Apenas a mensagem e o ICV são criptografados. O cabeçalho 802.11 é passado em claro. O WEP utiliza um vetor de inicialização (IV – *Initialization Vector*) sendo este uma chave de 24 bits, a princípio, dinâmica. Conforme a norma IEEE 802.11, a chave WEP padronizada de 64 bits a ser utilizada pelo RC4 é formada pelo IV de 24 bits concatenado à chave estática de 40 bits (aquela compartilhada pelos dispositivos).

O RC4 é dividido em dois algoritmos: *Key-Scheduling Algorithm* (KSA) e *Pseudo-Random Generation Algorithm* (PRGA). O KSA é bem simples, ele inicializa um *array* de 256 posições com os valores de 0 a

[2] Termo usado para referir-se genericamente à redes sem fio que utilizam qualquer um dos padrões 802.11.

255. Logo após, executa uma série de *swaps*, permutando o *array*. A permutação é feita de acordo com a chave, chaves diferentes permutam o *array* de formas dirferentes. O PRGA ainda executa um *swap* e gera um byte como saída que será utilizado na operação XOR.

Para a criptografia de cada mensagem com seu respectivo ICV um novo IV deve ser gerado[3] incrementando-o de uma unidade para evitar a repetição de chaves. Uma vez que o RC4 é um algoritmo de criptografia simétrico, a mesma chave deve ser utilizada para o processo de decodificação. Por este motivo, o IV é enviado em claro concatenado à mensagem criptografada conforme a ilustração da Figura 6. Esse processo de criptografia também é chamado de encapsulamento WEP.

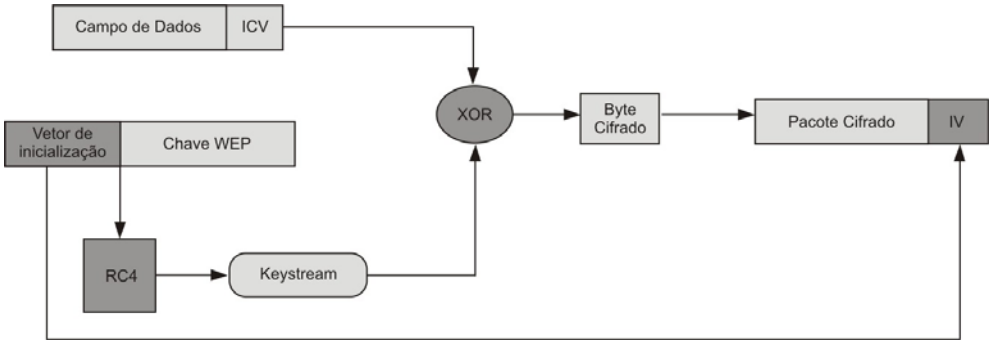

Figura 6 – Encapsulamento WEP

É feito um XOR (OU Exclusivo) entre um byte do pacote e o byte gerado pelo RC4 (*keystream*). O resultado é um outro byte correspondente à cifra do byte do pacote. Esse ciclo é repetido até o último byte do pacote e para cada ciclo deste o RC4 gera um novo *keystream*.

2.4 Vulnerabilidades

Estão listadas abaixo as vulnerabilidades apresentadas pelo protocolo WEP.

Tamanho da Chave **-** originalmente quando o WEP foi lançado, a chave estática WEP era de apenas 40 bits. Chaves com este tamanho podem ser quebradas por força bruta[4] usando-se máquinas atuais. Para solucionar este problema, fabricantes de produtos Wi-Fi lançaram o WEP2 com chave estática de 104 e 232 bits, mantendo o IV de 24 bits. Com isto tornou-se praticamente impossível quebrar, em tempo factível, a chave por meio de força bruta.

Reuso de Chaves **-** os 24 bits do IV permitem pouco mais de 16,7 milhões (2^{24}) de vetores diferentes. Este número de possibilidades é relativamente pequeno. Dependendo do volume de tráfego da rede os IVs se repetirão de tempos em tempos e, portanto, as chaves usadas pelo RC4 também se repetirão. A

[3] Na realidade, o protocolo WEP não especifica como o IV deve ser alterado. Essa questão foi deixada para os fabricantes de dispositivos. Alguns fabricantes iniciam o IV em 0 e o incrementam de uma unidade a cada mensagem criptografada, outros geram o IV de forma randômica para cada mensagem a ser enviada.
[4] Ataques de força bruta consistem em testar todas as combinações de chaves possíveis exaustivamente.

repetição de chaves fere a natureza do RC4 que assim não garante mais a confidência dos dados [8]. Se o IVs forem escolhidos aleatoriamente, a freqüência de repetições pode aumentar significativamente dado o paradoxo do aniversário. De acordo com o paradoxo, após 4823 pacotes há uma probabilidade de 50% de ocorrer uma repetição de IV.

Gerenciamento de Chaves - o WEP não possui um protocolo para gerenciamento de chaves, portanto a chave utilizada pelos dispositivos não pode ser trocada dinamicamente. Isso dificulta a manutenção das redes, principalmente as de grande porte (*e.g.*, as redes corporativas) uma vez que a troca da chave deve ser feita manualmente em cada máquina. Devido a isso, em geral, as chaves não são trocadas com freqüência adequada, contribuindo para a redução da segurança. Visto que o WEP é um mecanismo fortemente baseado no segredo de sua chave é necessário que haja a troca freqüente da mesma.

IV passado em claro - o vetor de inicialização é passado em claro uma vez que o mesmo é necessário para o processo de decodificação. Como o IV é a parte inicial da chave, passa-se em claro uma parte da chave que codificou o pacote. Devido a esta falha, ataques poderosos, como o FMS[5] [5], pôde ser criado.

Protocolo de autenticação Ineficiente - no modo de autenticação por Chave Compartilhada o atacante pode através de uma simples escuta de tráfego ter acesso a um pacote em claro (*e.g.* pacote texto-desafio) e a sua respectiva cifra (pacote codificado). Com estes dados é possível achar os *keystreams* e usá-los para criar uma resposta válida para qualquer texto-desafio. O atacante poderá autenticar-se sem conhecer a chave WEP. O uso de MAC *Filtering* não garante nenhuma segurança ao processo de autenticação, pois existem ataques de MAC *Spoofing* (falsificação de endereço MAC) que facilmente podem se feitos. Um atacante pode rapidamente descobrir um endereço MAC válido, através da escuta de tráfego, e usar o endereço descoberto para burlar o MAC *Filtering*.

Negação de Serviço (DoS – Deny of Service) - é possível forjar pacotes do tipo *De-Authetication* (*i.e.* que invalidam o cliente da rede) e enviá-los em *broadcast* ou diretamente para um cliente específico usando o seu endereço MAC associado. Ferramentas de domínio público como o *void11*[6] e *aircrack*[7] implementam este tipo de ataque. O efeito deste ataque é praticamente instantâneo.

O Algoritmo que Implementa o ICV não é Apropriado – o CRC-32 usado para computar o ICV pode detectar com alta probabilidade alterações na mensagem, servindo à verificação de integridade. Originalmente, o CRC-32 não foi projetado pensando-se em segurança, mas apenas na detecção de alterações ocorridas devido à ruídos inerentes do canal de comunicação. Assim sendo, optou-se fazer o CRC como uma função linear que não é segura em termos criptográficos. Essa propriedade pode ser explorada por um atacante para modificar o conteúdo de um pacote e facilmente corrigir o ICV fazendo o pacote parecer autêntico. Para explorar essa falha, criou-se um ataque chamado *Chopchop* que consiste

[5] Ataque desenvolvido por Fluhrer, Mantin, e Shamir, cujo nome foi dado pelas iniciais de seus criadores.
[6] Void11 - http://www.wirelessdefence.org/Contents/Void11Main.htm
[7] Aircrack - http://www.aircrack-ng.org

em decodificar o pacote sem saber a chave, apenas modificando o ICV.

Problemas do RC4 - Em [5], é demonstrado que o algoritmo KSA do RC4 apresenta uma fraqueza. A partir disso, foi desenvolvido um ataque estatístico que revela a chave WEP estática. Este ataque ficou conhecido como FMS. KoreK[8] otimizou este ataque, aumentando a probabilidade de acerto da chave com um menor número de IVs, diminuindo, assim, o tempo necessário para a quebra da chave. *AirSnort*[9], *WEPCrack*[10] e *Aircrack* são exemplos de ferramentas de domínio público que implementam estes ataques. Em testes realizados em redes com pouco tráfego, levou-se cerca de uma hora para quebrar a chave estática.

Re-injeção de Pacotes – Redes protegidas pelo WEP são passíveis de ataques de re-injeção de tráfego. Este tipo de ataque sozinho não afeta diretamente a segurança da rede. Porém pode ser usado para aumentar o tráfego na rede e assim diminuir o tempo necessário para que ataques como o FMS e o KoreK quebrem a chave WEP.

3. Wi-Fi Protected Access (WPA)

Tendo em vista o grande número de vulnerabilidades apresentadas pelo protocolo WEP, um grupo de trabalho do IEEE 802.11 iniciou pesquisas para o desenvolvimento de um novo padrão de segurança denominado IEEE 802.11i. O intuito primordial era resolver todos os problemas de segurança encontrados no WEP. Enquanto o padrão estava sendo desenvolvido, a *Wi-Fi Alliance*[11], para responder às críticas geradas pelo meio corporativo em relação ao WEP, apresentou em 2003 um padrão denominado *Wi-Fi Protected Access* (WPA) [9]. O WPA é baseado no RC4 e em um subconjunto de especificações apresentadas em uma versão preliminar (*draft)* do IEEE 802.11i.

O WPA introduz diversos mecanismos para resolver os problemas de segurança associados ao WEP:

Regras para o IV e IV estendido de 48 bits – Como os 24 bits de IV utilizado pelo WEP permitiam pouco mais de 16 milhões de IV diferentes, facilitando repetições em um curto espaço de tempo, o WPA introduz um IV estendido de 48 bits. Assim, mais de 280 trilhões (2^{48}) de IVs diferentes são possíveis. Adicionalmente, o WPA introduz regras para a escolha e verificação de IVs para tornar ataques de re-injeção de pacotes ineficazes.

Novo Código de Verificação de Mensagens – O WPA usa um novo campo de 64 bits, o MIC (*Message Integrity Code*), para verificar se o conteúdo de um quadro de dados possui alterações por erros de transmissão ou manipulação de dados. O MIC é obtido através de um algoritmo conhecido como *Michael*.

[8] Hacker bastante conhecido no fórum do netstumbler (www. netstumbler.com)
[9] AirSnort - http://airsnort.shmoo.com
[10] WEPCrack - http://wepcrack.sourceforge.net
[11] Associação internacional sem fins lucrativos formada em 1999 para certificar produtos Wi-Fi baseados no padrão IEEE 802.11. A certificação de produtos Wi-Fi teve início em março de 2000. Um dos principais objetivos é assegurar a interoperabilidade entre todos os equipamentos certificados pela Wi-Fi Alliance.

Distribuição e Derivação de Chaves – O WPA automaticamente distribui e deriva chaves que serão utilizadas para a criptografia e integridade dos dados. Isto resolve o problema do uso da chave compartilhada estática do WEP.

Outras características do WPA são :

- Utiliza o conceito de chaves temporais, no qual há uma hierarquia de chaves. Há uma chave principal, chamada de *Pairwise Master Key* (PMK), de onde se derivam outras chaves como a chave de criptografia de dados e a chave de integridade de dados;
- Trabalha em dois modos distintos de funcionamento. Um destinado a redes domésticas e pequenos escritórios, e outro destinado a redes de grandes instituições (redes corporativas). A principal diferença entre estes dois tipos está na forma de autenticação, pois em redes corporativas é utilizado um servidor de autenticação centralizado (geralmente servidor RADIUS);
- Não tem suporte a redes do tipo *ad hoc* de forma diferente ao WEP;
- Foi projetado para ser implementado através de uma atualização de *software (firmware)* nos equipamentos existentes com o *hardware* utilizado pelo WEP.

3.1 Autenticação

Conforme dito anteriormente, há dois tipos de autenticação no protocolo WPA. Um direcionado para redes corporativas que utiliza um servidor de autenticação 802.1x/EAP, portanto uma infra-estrutura complementar, e um outro, mais simples, projetado para pequenas redes em escritórios e para redes domésticas (redes SOHO – *Small Office/Home Office*). Estes dois tipos de autenticação são denominados WPA Corporativo e WPA Pessoal, respectivamente.

WPA Pessoal – como um usuário comum não é capaz de instalar e fazer a manutenção de um servidor de autenticação criou-se o WPA-PSK (WPA-*Pre Shared Key*) que é uma *passphrase*[12], previamente compartilhada entre o AP e os clientes. Neste caso, autenticação é feita pelo AP. A chave é configurada manualmente em cada equipamento pertencente à rede e pode variar de 8 a 63 caracteres ASCII.

WPA Corporativo - o AP não é responsável por nenhuma autenticação. Tanto a autenticação do usuário quanto do dispositivo é feita por um servidor de autenticação. É utilizada uma infra-estrutura complementar formada por um servidor que usa o protocolo de autenticação 802.1x em conjunto com algum tipo de EAP (*Extensible Authentication Protocol*). O 802.1x é um protocolo de comunicação utilizado entre o AP e o servidor de autenticação. Este protocolo já era largamente utilizado em redes cabeadas e se mostrou também adequado quando integrado às redes sem fio. Quando um cliente solicita uma autenticação, o servidor de autenticação verifica em sua base de dados se as credenciais apresentadas

[12] É basicamente uma sentença ou uma frase que serve como uma senha mais segura ao permitir o uso de um número maior de caracteres.

pelo solicitante são válidas, em caso positivo o cliente é autenticado e uma chave chamada *Master Session Key* (MSK) lhe é enviada. Na maioria das vezes, utiliza-se como servidor de autenticação um servidor RADIUS, mas não é obrigatório. O processo de autenticação é ilustrado na figura 7.

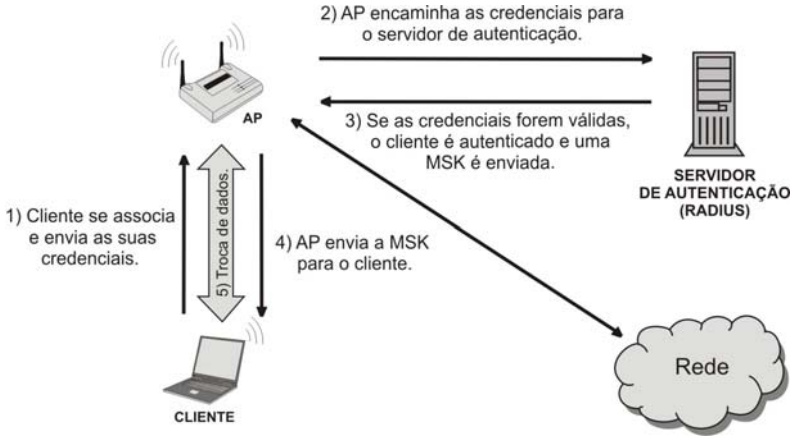

Figura 7 – Autenticação 802.1x/EAP

O EAP é responsável por criar um canal lógico de comunicação seguro entre o cliente (*supplicant*) e o servidor de autenticação, por onde as credenciais irão trafegar. Fisicamente, o cliente se comunica com o AP através do protocolo EAPoL (*Extensible Authentication Protocol over LAN)* e o AP, por sua vez, se comunica com o servidor de autenticação através do protocolo 802.1x, conforme mostra a Figura 8.

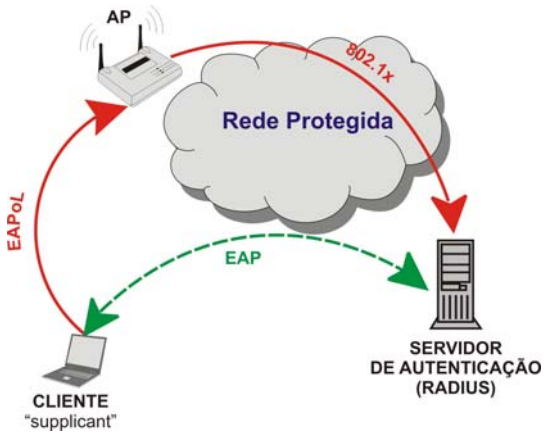

Figura 8 - WPA corporativo

As credenciais podem ser representadas através do binômio usuário/senha, *smart cards*, certificados digitais, biometria, entre outras formas. Atualmente, os tipos de EAP mais utilizados são: EAP-MD5, EAP-TLS (EAP-*Transport Layer Security*), EAP-TTLS (EAP-*Tunneled Transport Layer Security*) e PEAP (*Protected Extensible Authentication Protocol*).

Após a autenticação, inicia-se o processo de derivação da PMK onde as chaves serão estabelecidas, este processo é chamado de *4-Way-Hadshake.* Se a autenticação foi baseada no modo PSK, a chave PMK é a

própria PSK. Se não, a PMK é derivada a partir da MSK que foi compartilhada durante o processo de autenticação 802.1x/EAP. A PMK nunca é usada para encriptação ou integridade. Ela é usada para gerar chaves temporárias *(Pariwise Transient Key - PTK)*. A PTK é um conjunto de chaves, entre elas a chave de criptografia de dados *(Temporal Encryption Key – TEK ou TK)* e a chave de integridade de dados *(Temporal MIC Key - TMK)*. Ao final do *4-Way-Hadshake* é garantido que tanto o cliente quanto o AP possuem a mesma PTK, estando prontos para a troca de dados.

3.2 Integridade

A integridade no WPA é composta por dois valores. Além do ICV, já utilizado pelo WEP, é adicionado ao quadro uma mensagem de verificação de integridade denominada MIC (*Message Integrity Check*). O algoritmo que implementa o MIC denomina-se *Michael*.

O Michael é uma função *hash* não linear, diferentemente do CRC-32. O endereço de destino, de origem, a prioridade (definida atualmente como zero, mas reservada para objetivos futuros, *e.g.* 802.11e), os dados e uma chave de integridade são inseridos no Michael para produzir o MIC. A saída corresponde a 8 bytes que juntamente com o ICV formam a integridade do protocolo WPA. Portanto a integridade é representada por um total de 12 bytes, 8 gerados pelo Michael e 4 pelo CRC-32. A Figura 9 ilustra o processo de integridade no WPA.

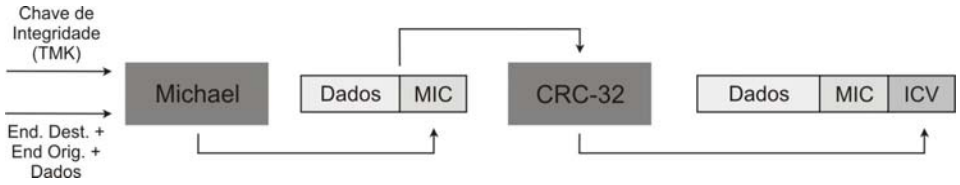

Figura 9 – Integridade WPA

3.3 Confidência

O TKIP (*Temporal Key Integrity Protocol*) soluciona boa parte das vulnerabilidades apresentadas pelo protocolo WEP. O TKIP é baseado no conceito de chaves temporais, ou seja, a chave é usada durante certo tempo e depois é substituída dinamicamente.

No WPA o vetor de inicialização possui 48 bits o que torna praticamente impossível haver reutilização de vetores. Na estrutura do cabeçalho 802.11 o campo reservado para o IV só contém 24 bits, devido a isto criou-se outro campo chamado IV *Extended*, que não faz parte da estrutura do cabeçalho 802.11, para alocar o resto do IV. O IV também é utilizado como um contador de quadros (TSC – TKIP *Sequence Counter*). Quando uma nova chave de criptografia é estabelecida, o TSC é zerado. A cada quadro transmitido, ele é incrementado. Desta forma, quadros com TSC fora de ordem são descartados, evitando-se re-injeções de pacotes.

O processo de codificação do WPA é semelhante ao do WEP (*cf.* Seção 2.3). A principal diferença está na

chave que irá alimentar o RC4. Esta chave é o resultado de um algoritmo de combinação de chave cuja entrada é o vetor de inicialização, o endereço MAC do transmissor e a chave de criptografia de dados. Ao final, a chave gerada pelo algoritmo de combinação de chave e o IV são passados para o RC4 e o processo ocorre conforme visto no WEP (*cf.* Seção 2.3). A Figura 10 ilustra o funcionamento do WPA.

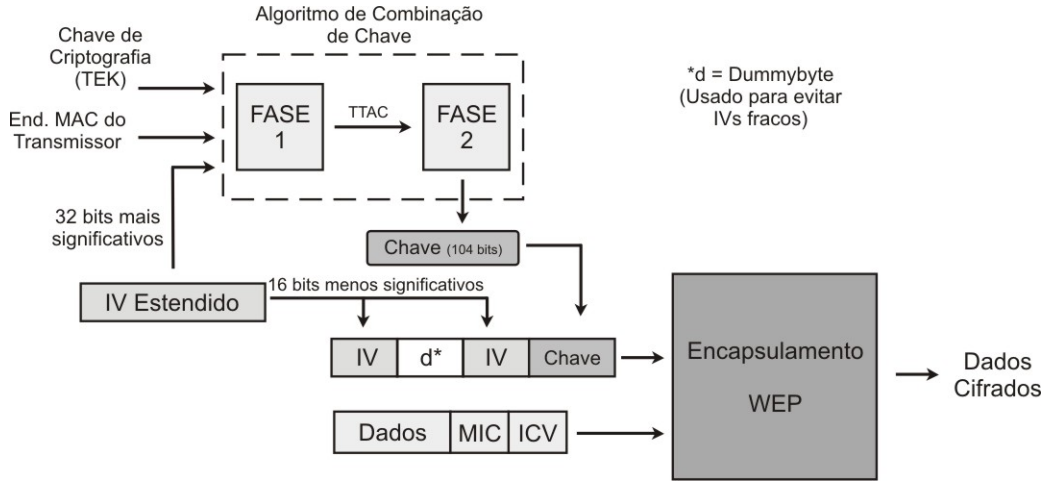

Figura 10 – Mecanismo de funcionamento WPA

3.4 Vulnerabilidades

O WPA solucionou praticamente todas as vulnerabilidades apresentadas pelo protocolo WEP. Porém, falhas em sua implementação o tornaram vulnerável:

Fraqueza no algoritmo de combinação de chave **-** Tendo conhecimento de algumas chaves RC4 (menos de 10 chaves) geradas por IVs, cujos 32 bits mais significativos são os mesmos, um atacante pode achar a chave de criptografia de dados e a chave de integridade [10]. Esse ainda não é um ataque prático, pois possui complexidade de tempo $O(2^{105})$, porém há uma redução significativa se comparado com um ataque de força bruta $O(2^{128})$.

PSK é susceptível a ataques de dicionário **-** Diferentemente do ataque de força bruta, que tenta todas as possibilidades possíveis exaustivamente, o ataque de dicionário tenta derivações de palavras pertencentes a um dicionário previamente construído. Este tipo de ataque, geralmente é bem sucedido porque as pessoas têm o costume de utilizarem palavras fáceis de lembrar e que normalmente pertencem a sua língua nativa. Além do dicionário, informações capturadas durante o *4-Way-Handshake* são necessárias para a quebra da PSK. Um detalhe que não é muito sabido é que se a chave PSK for de mais de 20 caracteres este ataque não funciona em tempo factível.

Negação de Serviço **-** 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. Além disso, o WPA continua sofrendo dos mesmos ataques de negação de serviço que o WEP já sofria, visto que esses ataques são baseados em quadros de gerenciamento.

4. IEEE 802.11i (WPA2)

O padrão IEEE 802.11i, homologado em junho de 2004, foi desenvolvido com o objetivo de prover mais segurança na comunicação, visto que o protocolo de segurança então utilizado (WEP) apresentava diversas vulnerabilidades. O novo método de criptografia utilizado exige um maior poder computacional do NIC (*Network Interface Card*) durante o processo de codificação/decodificação, impossibilitando assim, apenas uma atualização de *firmware*. Parte dos mecanismos apresentados no WPA também é utilizada no WPA2, já que o WPA é baseado em um rascunho do WPA2. Os principais avanços do WPA2 em relação ao WPA são, basicamente, novos algoritmos de criptografia e de integridade.

4.1 Autenticação

O mecanismo de autenticação no WPA2 é, basicamente, o mesmo do WPA, descrito na Seção 3.1. O maior avanço na autenticação é uma preocupação com o *roaming*. Quando um usuário se autentica, há uma série de mensagens trocadas entre o AP e o cliente. Essa troca de mensagens introduz um atraso no processo de conexão. Quando um cliente desloca-se de um AP para outro, o atraso para estabelecer a associação pode causar uma interrupção notória da conexão, principalmente em tráfego de voz e vídeo. Para minimizar este atraso de associação, o equipamento pode dar suporte a PMK *Caching* e *Preauthentication*. O PMK Caching consiste no AP guardar os resultados das autenticações dos clientes. Se o cliente voltar a se associar com o AP, estas informações guardadas são utilizadas para diminuir o número de mensagens trocadas na re-autenticação. Já no *Preauthentication*, enquanto o cliente está conectado a um AP principal, ele faz associações com outros APs cujo o sinal chega até ele. Desta forma, quando há uma mudança de AP não há perda de tempo com a autenticação.

O desenvolvimento desses mecanismos está associado ao contexto de Computação Ubíqua [11, 12, 13, 14]. Esses mecanismos são de suma importância para tecnologias emergentes como VoWi-Fi (VoIP over Wi-Fi) por exemplo.

4.2 Integridade

O protocolo CCMP *(Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol)* é o responsável pela integridade e a confidência do WPA2. O CCMP é baseado no AES *(Advanced Encryption Standard)* que é um *Block Cipher*[13]. O modo de operação do AES implementado pelo WPA2 e o CCM [15] cujas chaves e blocos são de 128 bits.

O CBC-MAC *(Cipher Block Chaining Message Authentication Code)* é responsável pela integridade dos quadros, seu funcionamento é mostrado na Figura 11.

[13] Cifrador que opera com um grupo de bits com tamanho fixo. Em contraste com o *Stream Cipher* (*e.g.* RC4) que cifra bit a bit, o *Block Cipher* cifra um bloco de bits por vez.

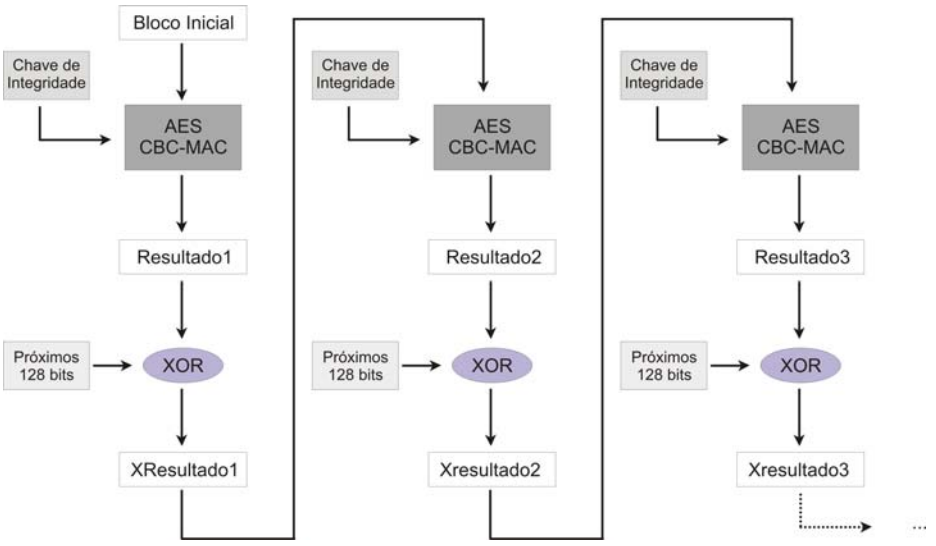

Figura 11 - Integridade WPA2

A caixa “Bloco Inicial” representa os primeiros 128 bits do campo de dados. São passados para o CBC-MAC o bloco e a chave de integridade, e como saída são gerados outros 128 bits, chamado de “Resultado1”. É feito um XOR entre o “Resultado1” e o próximo bloco. Ao resultado do XOR é dado o nome “XResultado1”. O “XResultado1” é passado para o CBC-MAC e, assim, gerado um “Resultado2”. Este procedimento se repete até o último bloco do campo de dados do pacote. No final do processo, dos 128 bits de saída apenas o 64 bits mais significativos vão para o MIC.

4.3 Confidência

O CCMP também é baseado no conceito de chaves temporais, como o TKIP no WPA. Portanto, no WPA2 há uma hierarquia de chaves, onde derivações da PMK geram as chaves temporais de criptografia e integridade. O algoritmo responsável pela criptografia do frame é o AES *Counter Mode* (CTR). A chave de criptografia de dados é simétrica e de tamanho 128 bits. O vetor de inicialização continua com 48 bits.

4.4 Vulnerabilidades

Poucas vulnerabilidades são conhecidas sobre o WPA2 atualmente. Conforme visto anteriormente, o WPA2 possui um bom mecanismo de segurança. Talvez, mais vulnerabilidades ainda não foram descobertas porque os dispositivos que suportam o WPA2 ainda não são largamente utilizados.

As vulnerabilidades conhecidas são:

Negação de Serviço - Visto que todos os mecanismos de segurança existentes até agora não protegem os quadros de gerenciamento e de controle. Portanto, ainda é possível, por exemplo, forjar quadros de gerenciamento do tipo *de-authentication*. Além disso, existem outros ataques como: *RSN Information Element (RSN IE) Poisoning* e *4-Way-Handshake Blocking* [16].

PSK Pequeno **-** Na verdade esta não é uma falha do protocolo, mas, sim, do usuário. PSK com menos de 20 caracteres são susceptível a ataques de dicionário.

5. IEEE 802.11w

O IEEE 802.11i possui melhorias significativas de segurança. Contudo, assim como no WEP e no WPA, toda a segurança é aplicada somente aos quadros de dados (*data frames*) e nenhuma proteção é dada aos quadros de gerenciamento (*management frames*) e de controle (*control frames*) do meio de comunicação sem fio. O Grupo de Trabalho do IEEE 802.11w foi aprovado em março de 2005 com o objetivo inicial de melhorar a segurança das redes IEEE 802.11 através da proteção dos quadros de gerenciamento. Isso se deve a duas razões principais:

1. Os ataques do tipo DoS em redes IEEE 802.11 exploram a falta de proteção nos quadros de gerenciamento. Esses ataques injetam na rede quadros de gerenciamento do tipo d*e-authentication* forjando facilmente pedidos de desassociação da rede de clientes legítimos. Assim, a proteção dos quadros de gerenciamento impediria a realização deste tipo de ataque;
2. Os novos padrões IEEE 802.11v, 802.11k e 802.11r estendem as funcionalidades dos quadros de gerenciamento 802.11 que poderão incluir informações sensíveis como dados sobre recursos de rádio, identificadores baseados em localização e dados para execução de *handoffs*[14] rápidos. Desta forma, torna-se evidente a necessidade de proteção dos quadros de gerenciamento.

Apesar das melhorias de segurança do novo padrão, podemos enumerar as seguintes vulnerabilidades existentes:

1. Antes de tornar o tráfego de gerenciamento confidencial, o IEEE 802.11w assume que o cliente e o ponto de acesso já tenham trocado a chave dinâmica. Isso impede, portanto, a proteção de qualquer quadro de gerenciamento antes do envio da chave o que, em conseqüência, expõe o nome da rede (SSID) e outras informações necessárias para o cliente se conectar à rede;
2. Embora a proteção dos quadros de gerenciamento possa facilitar a identificação de quadros forjados, tornando nula a eficiência de ataques DoS do tipo *de-authentication*, o 802.11w nunca poderá reduzir ataques DoS do tipo *RF-jamming*[15];
3. Uma vez que o Grupo de Trabalho IEEE 802.11w não indicou sua intenção de prover segurança aos quadros de controle, a rede ainda estará exposta a outras formas de ataques. Sem a proteção de quadros de controle, é possível utilizar uma variedade de ataques DoS que exploram técnicas de controle do acesso ao meio de comunicação;
4. Embora esforços estejam sendo feitos com o intuito de permitir que a implantação do 802.11w seja feita através de uma atualização do *firmware* dos equipamentos 802.11i, a manutenção da compatibilidade dos equipamentos com placas de acesso da versão 802.11i ou anteriores será um

[14] A transferência de um cliente de um AP para outro sem a descontinuidade da comunicação.
[15] Interferência deliberada através de ondas de rádio para impedir a recepção de sinais em uma banda de freqüência específica.

problema uma vez que limitará a proteção fornecida pelo novo padrão.

É importante ressaltar que o padrão IEEE 802.11w está previsto para ser concluído em 2008. Assim sendo, tanto o objetivo inicial do grupo quanto os mecanismos de segurança propostos podem mudar drasticamente até a publicação da especificação final.

6. Conclusão

Este artigo apresentou uma análise dos mecanismos de segurança de redes IEEE 802.11. Os protocolos WEP, WPA e WPA2 foram analisados sob os aspectos básicos de segurança: autenticação, integridade e confidência. Para cada protocolo foram descritas suas vulnerabilidades conhecidas. De todas as tecnologias abordadas neste artigo, o WEP, é ainda a mais usada. A indisponibilidade de atualizações de *firmware* de alguns fabricantes e a necessidade de aquisição de novos *hardwares* é o maior fator contra o uso das novas tecnologias (WPA e WPA2), pois isto pode implicar grandes custos, principalmente em redes corporativas onde o número de equipamentos pode ser elevado.

As vulnerabilidades do WEP são muito fáceis de serem exploradas. Qualquer pessoa com certo conhecimento das ferramentas existentes pode atacar uma rede Wi-Fi protegida por WEP, mesmo que não saiba como realmente funciona o ataque. Desta forma, a segurança da maioria das redes Wi-Fi pode ser comprometida. Vimos que o padrão de segurança mais recente (WPA2 ou IEEE 802.11i) também não protege a rede de forma integral, por isso a necessidade do desenvolvimento de um novo padrão, o IEEE 802.11w. Em nossas análises, foi demonstrado que apesar de ainda estar em fase de desenvolvimento, o IEEE 802.11w já apresenta diversas falhas de segurança que precisam ser resolvidas antes da finalização do padrão.

7. Referências

[1] - Shafi, M et al, 1997. Wireless communications in the twenty-first century: a perspective. *Proceedings of the IEEE.* Vol 85, No 10, pp 1622 – 1638.

[2] - IEEE 802.11 WG, 1999. Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specification. *IEEE Computer Society.*

[3] - Borsc, M.e Shinde, H., 2005. Wireless security & privacy. *Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on.* pp 424 – 428.

[4] - Boland, H.e Mousavi, H., 2004. Security issues of the IEEE 802.11b wireless LAN. *Electrical and Computer Engineering, 2004. Canadian Conference on.* Vol 1, pp 333 – 336.

[5] - Fluhrer, S., Mantin, I. e Shamir, A., 2001. Weaknesses in the key scheduling algorithm of RC4. *Eighth Annual Workshop on Selected Areas in Cryptography*. Toronto, Canada.

[6] - IEEE 802.11i WG, 2004. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Computer Society.*

[7] - Shunman, W., 2003. WLAN and it's security problems. *Parallel and Distributed Computing, Applications and Technologies (PDCAT'2003), Proceedings of the Fourth International Conference on.* pp 241 – 244.

[8] – Borisov, N., 2001. Intercepting Mobile Communications: The Insecurity of 802.11. *In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MOBICOM).* pp 180 – 188.

[9] – Wi-Fi Alliance, 2003. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks

[10] - Moen, V., Raddum, H. e Hole, K., 2004. Weaknesses in the Temporal Key Hash of WPA. *Mobile Computing and Communications Review*. Vol 8, pp 76 – 83.

[11] – Weiser, M., 1994. The world is not a desktop. *Interactions*. pp. 7-8.

[12] – Weiser, M., 1993. Hot Topics: Ubiquitous Computing. *IEEE Computer.*

[13] – Weiser, M., 1993. Some Computer Science Problems in Ubiquitous Computing. *Communications of the ACM.*

[14] - Weiser, M., 1991. The Computer for the Twenty-First Century. *Scientific American*. pp. 94-10

[15] – Whiting, D., Housley, R. e Ferguson, N., 2003. Counter with CBC-MAC (CCM). *IETF RFC 3610*

[16] - He, C. e Mitchell, J., 2005. Security analysis and improvements for IEEE 802.11i. *The 12th Annual Network and Distributed System Security Symposium (NDSS'05).* pp 90-110.