Universidade Federal de Pernambuco

Centro de Informática

Graduação em Ciência da Computação

UM ESTUDO SOBRE A SEGURANÇA DE REDES IEEE 802.11

Bruno Gentilini D'Ambrosio

TRABALHO DE GRADUAÇÃO

Recife

10 de junho de 2010

Universidade Federal de Pernambuco

Centro de Informática

Bruno Gentilini D'Ambrosio

UM ESTUDO SOBRE A SEGURANÇA DE REDES IEEE 802.11

Trabalho apresentado ao Programa de Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: *Paulo André da Silva Gonçalves*

Recife

10 de junho de 2010

Dedico este trabalho aos meus pais, por sempre me apoiarem e me instigarem a alcançar patamares cada vez maiores e ao Professor Paulo Gonçalves, por ter me dado a oportunidade de iniciar a minha carreira científica e ter me passado diversos conhecimentos que me fizeram crescer como pesquisador.

AGRADECIMENTOS

Gostaria de agradecer primeiramente à minha família, meus pais Filippo e Regina e todos os outros parentes, que sempre me deram apoio e carinho para que eu seguisse sempre em frente.

Ao meu orientador, o professor *Docteur* Paulo André da Silva Gonçalves, que me ofereceu a oportunidade de trabalhar com pesquisas científicas e sempre acreditou no meu potencial para crescer e fazer trabalhos cada vez melhores.

Aos meus colegas do grupo de pesquisa Bruno de Jesus, Bruno Almeida, Eduardo, Nivia, Hermano, Marcos e Júlio pelos conselhos fornecidos durante as reuniões do grupo e pelo companheirismo durante essa jornada. Agradeço ainda ao Eduardo pela parceria no estudo da segurança das redes IEEE 802.11 e pela ajuda no desenvolvimento dos trabalhos.

Aos meus amigos do Centro de Informática Carlos Frederico, Diego Cesar, Victor Hugo, Telmo, Vinicius, Igor Ryan, Felipe Lapenda, Diogo Salazar, Ítalo Macedo e todos os outros que me forneceram momentos de descontração e apoio durante toda a graduação.

Aos meus grandes amigos Thiago, Fábio, Guilherme, Vanessa, Lara, Andreza, Felype Nery, Márcia Victorino, Marcia Santos, Jacqueline, Marcelo, Sérgio, Nilson Junior, Juliana e todos os outros por me lembrarem que existe vida fora do Centro de Informática e pelo imenso apoio.

Agradeço por fim a Deus por sempre ter me dado forças nos momentos mais difíceis e zelado pela minha saúde e segurança durante toda a minha jornada.

"... E eu cavalgo os ventos

De um novo dia

Alto onde as montanhas alcançam

Encontro novamente meu orgulho e esperança

Renascimento de um homem."

—ANGRA (Rebirth - tradução livre)

RESUMO

As redes sem fio IEEE 802.11, comumente conhecidas como *Wi-Fi*, têm sido amplamente utilizadas tanto em residências quanto em ambientes comerciais e empresariais. Essas redes têm como um de seus principais problemas a segurança, visto que os dados que trafegam nessas redes são transmitidos através de ondas eletromagnéticas e podem ser facilmente capturados. Este trabalho apresenta um estudo aprofundado dos mecanismos de autenticação, integridade e confidência dos protocolos WEP, WPA, IEEE 802.11i (WPA2) e IEEE 802.11w, os quais são os protocolos de segurança existentes para as redes IEEE 802.11. Também são analisadas as vulnerabilidades de cada protocolo e os ataques desenvolvidos contra os mesmos. Além disso, é proposto e avaliado um mecanismo de segurança que protege o protocolo WPA contra os ataques baseados na previsibilidade de dados de determinados tipos de pacotes, sendo esta a maior contribuição deste trabalho.

Palavras-chave: Segurança, IEEE 802.11, Protocolos, Mecanismos de Defesa, Ataques, Vulnerabilidades

ABSTRACT

The IEEE 802.11 wireless networks, commonly known as Wi-Fi networks, have been widely used both have been widely used both in homes and in commercial and business environments. These networks have as one of its main problems the security, since the data that travels over these networks are transmitted via electromagnetic waves, which can be easily captured. In this work we present a study of the mechanisms of authentication, integrity and confidentiality used by the protocols WEP, WPA, IEEE 802.11i (WPA2) and IEEE 802.11w, which are the existing security protocols for IEEE 802.11 networks. We also analyzed the vulnerabilities of each protocol and the attacks developed against them. Furthermore, we propose and evaluate a defense mechanism that protects the WPA protocol against attacks based on the predictability of certain types of data packets. The proposed mechanism is the major contribution of this work.

Keywords: Security, IEEE 802.11, Protocols, Defense Mechanisms, Attacks, Vulnerabilities

SUMÁRIO

LISTA DE FIGURAS

GLOSSÁRIO

AES *Advanced Encryption Standard*. 20

AP *Access Point* ou Ponto de Acesso. 14

ARP *Adress Resolution Protocol*. 24

BIP *Broadcast/multicast Integrity Protocol*. 22

CBC-MAC *Cipher Block Chaining Message Authentication Code*. 20

CCM *Counter with CBC-MAC*. 20

CCMP *Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*. 20

CRC-32 *Cyclic Redudancy Check 32* ou Algoritmo de Verificação de Redundância Cíclica 32. 6

CTR *Advanced Encryption Standard Counter-Mode*. 20

DoS *Denial of Service* ou Negação de Serviço. 2

EAP *Extensible Authentication Protocol*. 14

EAPOL *Extensible Authentication Protocol over LAN*. 15

FMS *Fluhrer, Mantin e Shamir*, são os sobrenomes dos criadores do ataque FMS. 10

GTK *Group Temporal Key*. 28

HMAC *Hash-based Message Authentication Code* ou Código de Autenticação de Mensagens Baseado em Funções *Hash*. 27

ICV *Integrity Check Value* ou Valor de Checagem de Integridade. 6

IEEE *Institute of Electrical and Electronics Engineers*. 1

IGTK *Integrity Group Temporal Key*. 22

IPN *IGTK Packet Number*. 22

IPv4 *Internet Protocol version 4*. 18

IV *Initialization Vector* ou Vetor de Inicialização. 6

KSA *Key-Scheduling Algorithm*. 7

MAC *Medium Access Control*, ou Camada de Controle de Acesso ao Meio. 12

MD5 *Message-Digest Algorithm 5*. 27

MIC *Message Integrity Check*. 16

MSK *Master Session Key*. 14

PMK *Pairwise Master Key*. 14

PRGA *Pseudo-Random Generation Algorithm*. 7

PSK *Pre-Shared Key* ou Chave Pré-Compartilhada. 14

PTK *Pairwise Transient Key*. 16

PTW *Pyshkin, Tews e Weinmann*, são os sobrenomes dos criadores do ataque PTW. 10

QoS *Quality of Service*. 25

RC4 *Ron's Code 4* ou *Rivest Cypher 4*. 6

SHA-1 *Secure Hash Algorithm 1*. 27

SSID *Service Set Identifier* ou Identificador de Rede. 4

TEK *Temporary Encription Key*. 16

TK Outro nome para a TEK. 16

TKIP *Temporary Key Integrity Protocol*. 17

TLS *Transport Layer Security*. 27

TMK *Temporal MIC Key*. 16

TSC *TKIP Sequence Counter*. 17

WEP *Wired Equivalent Privacy*. 2

Wi-Fi *Wireless Fidelity*. 1

WPA *Wi-Fi Protected Access*. 2

WPA-PSK WPA utilizando o modo de autenticação por chave pré-compartilhada. 14

WPA2 *Wi-Fi Protected Access 2* ou IEEE 802.11i. 2

CAPÍTULO 1

INTRODUÇÃO

Os avanços tecnológicos das redes de computadores culminaram no desenvolvimento de redes que dispensam o uso de cabos, as quais são conhecidas como redes sem fio. Existe uma diversidade de tecnologias de redes sem fio cujas diferenças incluem a faixa de frequência utilizada, o alcance das antenas transmissoras, os protocolos de gerenciamento, roteamento e transmissão utilizados, entre outros. Dentre as tecnologias mais promissoras para redes públicas de acesso sem fio à Internet (*hotspots*) e redes locais sem fio internas de prédios, casas, aeroportos e escritórios encontra-se o IEEE 802.11 ou Wi-Fi (*Wireless Fidelity*) [1, 2, 3].

Um dos maiores problemas para o uso de qualquer tipo de rede sem fio é a segurança, visto que o tráfego de informações não possue a proteção e o isolamento que o meio físico das redes cabeadas fornece. A falta de isolamento e direcionamento das ondas eletromagnéticas, as quais são responsáveis pela transmissão das informações em redes sem fio, permite que as informações transmitidas pelas mesmas possam ser facilmente capturadas. Assim sendo, se faz necessário o uso de protocolos de segurança na camada enlace dessas redes.

1.1 MOTIVAÇÃO

As redes sem fio começaram a ser desenvolvidas no início da década de 70 por *Normam Abransom*, professor da universidade do Havaí, com o objetivo de intercomunicar ilhas da região sem o uso do telefone. No início da década de 90, a tecnologia já estava bastante difundida, mas ainda não havia uma padronização, o que dificultava a comunicação entre dispositivos de diferentes desenvolvedores. Nessa época, já existia a preocupação com

a segurança desse tipo de rede, mas a falta de um padrão impedia que um protocolo específico fosse adotado.

Em 1997 o grupo de trabalho IEEE 802.11 lançou o padrão de mesmo nome, o qual foi rapidamente adotado e ficou popularmente conhecido como *Wireless Fidelity* (Wi-Fi). No entanto, inicialmente, o padrão não possuía mecanismos de segurança bem definidos, o que levou o IEEE a desenvolver em caráter emergencial o primeiro protocolo de segurança para redes IEEE 802.11: o WEP (*Wired Equivalent Privacy*) [1]. O WEP não foi desenvolvido por uma equipe especializada em segurança, o que levou ao surgimento de diversas vulnerabilidades. Em 2001, foi publicado os primeiro trabalho [4] mostrando um ataque capaz de recuperar a chave de segurança do WEP. Isso levou o IEEE a criar o grupo de trabalho IEEE 802.11i com o objetivo de desenvolver o sucessor do protocolo WEP.

Enquanto o IEEE 802.11i não era finalizado a *Wi-Fi Alliance* utilizou um rascunho (*draft*) do IEEE 802.11i para desenvolver o WPA (*Wi-Fi Protected Access*) [5], o qual foi lançado em 2003. A grande vantagem do WPA em relação ao IEEE 802.11i é que o primeiro poderia ser implementado como uma atualização de *firmware* dos equipamentos que utilizavam o WEP e o segundo necessitava de *hardwares* com mais desempenho para funcionar.

Em 2004 foi aprovado o IEEE 802.11i [3], que ficou conhecido como WPA2 (*Wi-Fi Protected Access 2*). Apesar de corrigir grande parte das falhas presentes nos protocolos anteriores, o WPA2 ainda é vulnerável à ataques do tipo DoS (*Denial of Service*) por não fornecer proteção aos seus quadros de gerenciamento. Essa vulnerabilidade só foi resolvida pelo IEEE 802.11w [6], cuja especificação foi aprovada no final de 2009.

A segurança das redes IEEE 802.11 continua sendo estudada, visto que existe um grande potencial de surgimento de ataques aos protocolos mais recentes. Essa afirmação é comprovada pelos recentes ataques *Beck-Tews* [7] e *Ohigashi-Morii* [8], que conseguem burlar o mecanismo de checagem de integridade do protocolo WPA, contra o qual ainda não existia nenhum ataque relevante.

1.2 OBJETIVOS

Este trabalho de graduação tem como objetivos gerais o estudo dos protocolos de segurança existentes para as redes IEEE 802.11 e a proposição e avaliação de um mecanismo de defesa contra os ataques ao protocolo WPA baseados na previsibilidade dos dados de determinados tipos de pacotes que trafegam na rede. Para alcançar o objetivo geral, são definidos os seguintes objetivos específicos:

1. Estudo dos mecanismos que compõe os protocolos WEP, WPA, IEEE 802.11i (WPA2) e IEEE 802.11w;
2. Análise das vulnerabilidades dos quatro protocolos;
3. Estudo dos ataques baseados na previsibilidade dos dados;
4. Desenvolvimento do mecanismo;
5. Avaliação da eficiência e dos impactos da utilização do mecanismo nas redes IEEE 802.11.

1.3 ORGANIZAÇÃO DO TRABALHO DE GRADUAÇÃO

O Capítulo 2 descreve o funcionamento do protocolo WEP, destacando os mecanismos de autenticação, integridade e confidência utilizados pelo protocolo. Além disso, também são analisadas as vulnerabilidades do protocolo e os ataques desenvolvidos contra o mesmo. O Capítulo 3 descreve tanto o funcionamento como as vulnerabilidades dos protocolos WPA, IEEE 802.11i (WPA2) e IEEE 802.11w. O Capítulo 4 propõe e avalia um mecanismo de defesa para o protocolo WPA contra os ataques baseados na previsibilidade de determinados tipos de pacotes que trafegam na rede. Por fim, o Capítulo 5 analisa os resultados apresentados e indica os possíveis trabalhos futuros a partir do estudo realizado.

CAPÍTULO 2

WIRED EQUIVALENT PRIVACY (WEP)

Quando foram introduzidas no mercado as redes IEEE 802.11 não possuíam qualquer tipo de segurança, o que gerou desconfiança nas empresas usuárias após um curto período de utilização. Por conta disso, no final da em 1999 foi desenvolvido de forma emergencial o primeiro protocolo de segurança para esse tipo de rede, o WEP (textitWired Equivalent Privacy) [1]. A proposta inicial do protocolo WEP era garantir às redes sem fio o mesmo nível de segurança das redes cabeadas. No entanto, a falta de conhecimento da equipe de desenvolvimento sobre a área de segurança acarretou o aparecimento rápido de diversas falhas, as quais transformaram o protocolo em um alvo fácil para diversos ataques [4, 9, 10, 11, 12]. Este capítulo apresenta os mecanismos de autenticação, integridade e confidência do WEP, bem como as vulnerabilidades existentes no protocolo e os ataques relacionados às mesmas.

2.1 AUTENTICAÇÃO

Para iniciar a comunicação com uma rede IEEE 802.11, o dispositivo do usuário deve realizar o procedimento de autenticação com o ponto de acesso. A especificação do protocolo WEP prevê dois modos possíveis de autenticação, sendo o primeiro conhecido como autenticação por Sistema Aberto (*Open System*) e, o segundo, como autenticação por Chave Compartilhada (*Shared Key*).

A Figura 2.1 ilustra o modo de autenticação por Sistema Aberto. Esse modo de autenticação permite que qualquer cliente tenha acesso livre a rede. Para se autenticar, basta que o dispositivo do cliente informe ao ponto de acesso o SSID (*Service Set IDentifier*) da rede, o qual pode ser adquirido através de *BEACONs*, que são pequenos pacotes

enviados periodicamente[1] em *broadcast* pelo próprio ponto de acesso.

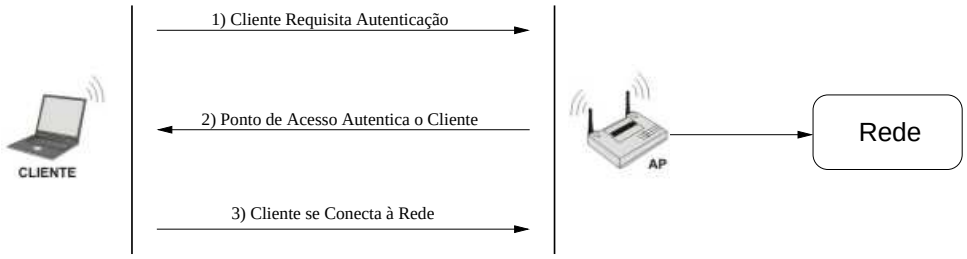

Figura 2.1 Autenticação por Sistema Aberto *(Open System)*

A Figura 2.2 ilustra o modo de autenticação por Chave Compartilhada.Esse modo de autenticação utiliza a chave de segurança do WEP que deve ser configurada previamente tanto no ponto de acesso como nos clientes. Para realizar a autenticação o cliente deve inicialmente enviar um pedido ao ponto de acesso, o qual envia um texto sem criptografia ao cliente conhecido como texto-desafio (*challenge text*). O cliente utiliza a chave de segurança para cifrar o texto-desafio e envia o resultado de volta para o ponto de acesso, que decifra o que foi recebido com sua própria chave de segurança. Caso o texto resultante e o texto-desafio sejam iguais, o cliente é associado à rede.

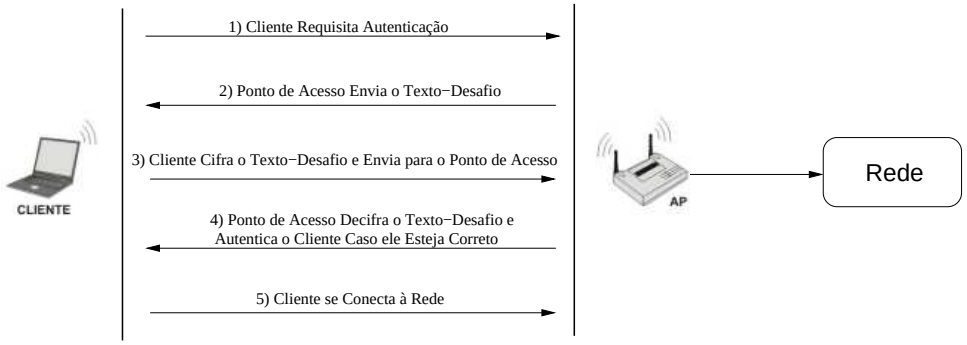

Figura 2.2 Autenticação por Chave Compartilhada *(Shared Key)*

[1]O envio periódico de *BEACONs* pode ser desabilitado pelo administrador da rede

2.2 INTEGRIDADE

A Figura 2.3 ilustra o procedimento de checagem de integridade do protocolo WEP. Para a realização desse procedimento o WEP utiliza o algoritmo CRC-32 (*Cyclic Redundancy Check 32*). Esse algoritmo utiliza um gerador padronizado de 32 bits para calcular o valor do ICV (*Integrity Check Value*) que é enviado juntamente com a mensagem. Quando a mensagem chega ao seu destino o ICV é novamente calculado e comparado ao ICV original. Caso os dois valores sejam iguais, a mensagem é aceita, caso contrário ela está corrompida ou foi adulterada, sendo então recusada.

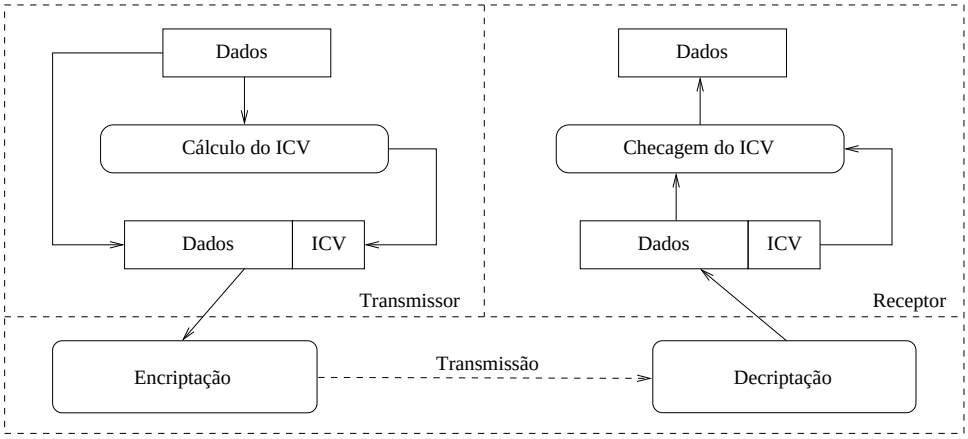

Figura 2.3 Checagem de Integridade no Protocolo WEP

2.3 CONFIDÊNCIA

Para garantir a confidencialidade das mensagens que trafegam nas redes IEEE 802.11, o WEP utiliza o algoritmo de criptografia RC4 (*Ron's Code 4*) [13]. O RC4 criptografa apenas a mensagem e o ICV correspondente, deixando o cabeçalho do quadro de dados do 802.11 sem nenhum tipo de proteção.

A chave utilizada pelo algoritmo é dividida em duas partes, sendo que a primeira é, a princípio, dinâmica e a segunda estática. A primeira parte é um vetor de inicialização (*Initialization Vector* - IV) de 24 bits, o qual deveria ser modificado para cada

mensagem enviada. Já a segunda parte é uma chave estática tipicamente de 104 bits[2] utilizada no procedimento de autenticação, a qual deve ser pré-configurada em cada um dos dispositivos pertencentes à rede.

O algoritmo RC4 é dividido em dois algoritmos menores, o KSA (*Key-Scheduling Algorithm*) e o PRGA (*Pseudo-Random Generation Algorithm*). No KSA, um *array* de 256 posições conhecido como *S-box* é inicializado e em cada uma das posições é armazenado um número entre 0 e 255 correspondente a mesma na ordem crescente. Em seguida, o KSA executa 256 permutações entre as posições do *S-box*, as quais são feitas de acordo com a chave de segurança, que se encontra armazenada em um segundo *array* conhecido como *K-box*. O *S-box* resultante é utilizado pelo PRGA, que realiza novas permutações no *array* e gera um *byte* pseudo-randômico por iteração. O conjunto de *bytes* pseudo-randômicos gerados pelo RC4 é conhecido como *keystream*.

Para cifrar cada mensagem com seu respectivo ICV, o WEP realiza uma operação de *OU Exclusivo (XOR)* entre cada *byte* do pacote e o *byte* do *Keystream* correspondente. Para evitar que haja repetição de *Keystream*, o IV, que é a parte dinâmica da chave, deve ser modificado a cada quadro de dados a ser criptografado. No entanto, a maneira como esse IV deve ser gerado ou incrementado foi delegada para cada fabricante de dispositivos. Alguns deles optaram por iniciar o IV com o valor 0 e o incrementar em uma unidade a cada quadro criptografado, enquanto outros optaram por gerar o IV randomicamente. O IV é transmitido em claro, concatenado ao pacote criptografado, para que o destinatário possa decifrar o quadro de dados recebido. A Figura 2.4 mostra o esquema de criptografia do WEP.

2.4 VULNERABILIDADES

Os mecanismos presentes no WEP possuem uma série de vulnerabilidades, visto que o protocolo foi desenvolvido de forma emergencial por uma equipe que não era especializada na área de segurança. Nas seções seguintes serão analisadas as principais vulnerabilidades de cada mecanismo utilizado pelo protocolo WEP.

[2]Existem versões do WEP com chaves de 40, 104 e 232 bits

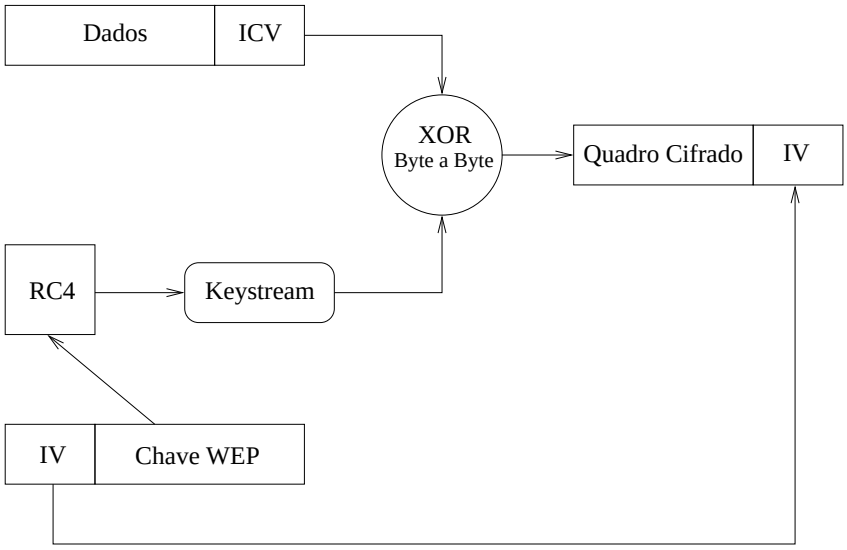

Figura 2.4 Esquema de criptografia do WEP

2.4.1 Problemas Relacionados a Chave de Segurança

O principal problema relacionado à chave de segurança WEP é que grande parte dos mecanismos do protocolo a utilizam diretamente, o que implica que ela deve ser mantida em segredo para que os mesmos se mantenham eficazes. Para garantir que a rede continue minimamente segura a chave deveria ser trocada em um curto espaço de tempo, o que é inviável em redes de grande porte, já que a troca da chave deve ser feita manualmente em cada um dos dispositivos da rede.

Um segundo problema deve-se ao fato de que a primeira versão do protocolo WEP utilizava uma chave estática de apenas 40 bits, o que para os padrões de segurança atuais é um número muito pequeno, pois basta um simples ataque de força bruta para recuperar uma chave com esse tamanho. Posteriormente, foi lançada uma segunda versão do WEP conhecida como WEP2, na qual a chave estática foi estendida para 104 e 232 bits, inviabilizando os ataques de força bruta.

Outro ponto bastante problemático da chave WEP é a sua parte dinâmica, o IV. Os 24 bits de tamanho que esse campo possui, fazem com que existam pouco mais de 16,7 milhões de vetores diferentes. Esse número de combinações é considerado pequeno e dependendo da quantidade de tráfego na rede, pode implicar na repetição da chave

utilizada pelo algoritmo RC4, o que fere a confidência de dados, pois dois pacotes poderão ser criptografados com o mesmo *keystream*. Além disso, esse campo é transmitido em claro no cabeçalho do quadro enviado, o que implicou no desenvolvimento de ataques estatísticos poderosos que serão analisados posteriormente neste trabalho.

2.4.2 Problemas nos Mecanismos de Autenticação, Integridade e Confidência

O modo de autenticação por chave compartilhada é totalmente ineficiente em evitar a entrada de intrusos na rede. Isso ocorre porque basta que o atacante capture o texto-desafio e o respectivo texto de resposta para que o mesmo consiga descobrir os *keystreams* que foram usados para cifrar o texto-desafio. Os *keystreams* podem ser usados para gerar uma resposta válida para qualquer novo texto-desafio gerado pelo ponto de acesso, o que implica na autenticação do atacante sem a necessidade da utilização da chave WEP.

O algoritmo CRC-32, que é utilizado para gerar o ICV no WEP, consegue detectar grande parte dos erros de transmissão que possam ocorrer em uma rede IEEE 802.11 devido a ruídos inerentes ao meio de comunicação. No entanto, esse algoritmo foi desenvolvido como uma função linear, que não é criptograficamente segura. Isso implica que é bastante simples modificar o conteúdo de qualquer pacote e modificar o ICV de forma que pareça que o mesmo continue íntegro. Essa vulnerabilidade permitiu a criação de um ataque capaz de revelar o conteúdo de um quadro de dados sem a utilização da chave de segurança.Tal ataque será analisado na Seção 2.5.

O algoritmo KSA utilizado pelo RC4 possui uma série de vulnerabilidades [4] que permitiram o desenvolvimento de diversos ataques estatísticos de recuperação da chave WEP.Tais ataques também serão analisados na Seção 2.5.

2.5 ATAQUES

Existem três tipos de ataques desenvolvidos contra o protocolo WEP: Ataques estatísticos de recuperação de chaves, ataque para obtenção do conteúdo dos quadros e ataques de negação de serviço. Nas seções seguintes, serão descritos cada um desses tipos de ataque.

2.5.1 Ataques Estatísticos de Recuperação de Chaves

Os ataques estatísticos de recuperação da chave WEP surgiram após a descoberta de diversos problemas do RC4. Primeiramente, as chaves utilizadas como entrada para o algoritmo KSA que respeitam determinados padrões permitem a ocorrência de padrões fixos no prefixo do *keystream* do PRGA. Essas chaves são geralmente denominadas chaves "fracas". Segundo, o conhecimento de uma pequena fração dos bytes dessas chaves é suficiente para se determinar uma grande parte do estado interno do RC4. E por fim, o conhecimento de alguns bytes da chave de entrada do KSA traz bastante informação sobre os bytes restantes da chave. Em particular, essa foi a maior fraqueza do WEP.

Analisando-se uma certa quantidade de informações criptografadas com diversas chaves fracas, é possível então, recuperar com certa probabilidade a chave secreta. Os principais ataques estatísticos para a recuperação de chaves WEP são os seguintes: o FMS [4] e suas otimizações [14], a família de 17 ataques KoreK [9] e o PTW [12].

O ataque FMS explora comportamentos conhecidos do KSA e do PRGA para casos onde os quadros capturados foram cifrados com base em IVs que possuem o padrão $[B+3|255|X]$ para $0 \leq B < 13$ e X qualquer. Caso uma quantidade suficiente de quadros com IVs respeitando tal padrão seja capturada, o byte $K[B+3]$ da chave utilizada como entrada para o KSA pode ser encontrado. Aproximadamente 4 milhões de quadros são necessários para se recuperar a chave secreta quando o contador de IVs é do tipo *little endian* e aproximadamente 1 milhão de quadros são requeridos quando contadores de IVs do tipo *big endian* são utilizados [4]. Diversas otimizações do FMS são apresentadas em [14]. Essas otimizações reduzem, para entre 1 milhão e 2 milhões, o número de quadros necessários para a recuperação da chave.

A família de 17 ataques KoreK [9] é uma generalização do ataque FMS onde o que importa é como os IVs produzidos fazem o KSA e o PRGA se comportarem e não mais como alguns IVs que seguem determinados padrões fazem isso. Os ataques KoreK requerem aproximadamente 500 mil quadros para recuperar a chave que protege a rede.

O PTW [12] é um ataque especializado contra o WEP e baseado no ataque FMS otimizado proposto em [15]. O PTW utiliza uma função descoberta para estimar os

bytes da chave secreta à condição de que se conheça previamente vários bytes iniciais de uma quantidade "suficiente" de *keystreams* e o IV usado para a geração de cada um deles. A descoberta dos bytes iniciais dos *keystreams* é feita através da captura de requisições e respostas ARP criptografadas pelo WEP. Os resultados teóricos sugerem que o PTW possui 50 % de chance de recuperar uma chave WEP de 104 bits com a captura de 40 mil quadros. Para ter sucesso em 95 % dos casos, são necessários 85 mil quadros. Ao contrário de todos os ataques anteriormente citados, cada byte da chave no PTW é computado de forma independente dos outros e ,por isso, o ataque pode ser executado mais rápido. Em [12] é demonstrada a efetividade do PTW ao se recuperar a chave de uma rede em menos de 60 segundos.

Os ataques apresentados exigem a captura vários quadros (ou IVs) para encontrar cada byte da chave. Vários bytes candidatos vão surgir e votos serão acumulados. Para cada byte candidato, aquele que receber mais votos é, provavelmente, o byte procurado da chave secreta. Na prática, os ataques mais eficientes existentes são o PTW e uma versão combinada dos ataques ou técnicas FMS, KoreK e de força-bruta. A força-bruta consiste em se testar valores para um ou mais bytes da chave.

2.5.2 Ataque para Obtenção do Conteúdo do Pacote (Chopchop)

O ataque *chopchop* [11, 7] se baseia na linearidade do CRC-32 para decifrar qualquer pacote que trafegue pela rede sem que a chave de segurança precise ser utilizada. Para revelar os $\mathbf{x}$ últimos bytes de determinado pacote basta que o atacante envie em média $\mathbf{x} \cdot 128$ pacotes para a rede.

Para realizar o *chopchop* deve-se primeiramente truncar o último byte do pacote que será decifrado, o que provavelmente tornará errado o ICV do restante do pacote. Em segundo lugar, o atacante deve tentar adivinhar o valor do byte que foi truncado e corrigir o ICV de acordo com o valor escolhido. Por fim, ele deve enviar o pacote para o ponto de acesso, que responderá com uma mensagem de erro caso o ICV esteja incorreto. Se nenhuma mensagem de erro for recebida, indicará que o byte escolhido está correto e o atacante poderá repetir o processo para decifrar o próximo byte, caso contrário, o

atacante deve escolher um novo valor para o byte atual e repetir o processo. Em média são necessários 128 tentativas para cada byte do pacote cifrado.

2.5.3 Ataques de Negação de Serviço

Os ataques de negação de serviço (*Denial of Service* - DoS) fazem com que a conexão ou associação do cliente com o ponto de acesso seja encerrada sem o conhecimento do mesmo. Isso pode ser feito em qualquer rede sem fio através de um aparelho de bloqueio de freqüência (*jammer*), o qual gera grandes quantidades de ruído que inviabilizam qualquer tipo de recepção correta na região de funcionamento do mesmo.

No caso do WEP, existe ainda uma segunda forma de realizar ataques de negação de serviço. Para realizá-los, o atacante deve inicialmente forjar pacotes do tipo *De-Authentication*, que servem para invalidar a autenticação do cliente na rede. Em seguida, o atacante deve enviar os pacotes forjados para um determinado endereço MAC, se o objetivo for negar serviço a um cliente especifico. Se o objetivo for negar serviço para todos os clientes em determinado raio de alcance basta enviar os pacotes em *broadcast*. Os pacotes do tipo *De-Authentication* podem ser facilmente forjados, pois são transmitidos em claro como qualquer pacote de gerenciamento do WEP.

2.6 RESUMO

O protocolo WEP foi criado de forma emergencial com o intuito de fornecer a segurança das redes cabeadas às redes IEEE 802.11. No entanto, os mecanismos de autenticação, integridade e confidência utilizados pelo protocolo possuem uma série de vulnerabilidades, o que fez com que o protocolo fosse alvo de diversos tipos de ataques. Esse capítulo apresentou um estudo completo do WEP, incluindo as vulnerabilidades e os ataques desenvolvidos contra o protocolo.

CAPÍTULO 3

WPA, IEEE 802.11I (WPA2) E IEEE 802.11W

Os protocolos WPA, IEEE 802.11i (WPA2) e IEEE 802.11w foram desenvolvidos para resolver as diversas vulnerabilidades presentes nos protocolos de segurança anteriores. Este capítulo realiza um estudo detalhado dos três protocolos, mostrando as melhorias, mecanismos e vulnerabilidades presentes em cada um deles.

3.1 WI-FI PROTECTED ACCESS (WPA)

Pressionada devido a grande quantidade de vulnerabilidades encontradas no protocolo WEP, o IEEE começou a desenvolver um novo mecanismo de segurança conhecido como IEEE 802.11i, o qual será analisado posteriormente. No decorrer desse desenvolvimento, a *Wi-Fi Alliance*, visando amenizar as críticas recebidas pelas grandes empresas que adotaram o protocolo WEP, utilizou uma versão preliminar (*draft*) do IEEE 802.11i para desenvolver o WPA (*Wi-Fi Protected Access*)[5]. O principal objetivo do WPA foi eliminar as vulnerabilidades apresentadas pelo WEP sem que grandes alterações de *hardware* precisassem ser feitas.

Esta seção apresenta as melhorias do WPA em relação à chave de segurança e ao gerenciamento da mesma, aos mecanismos de autenticação, integridade e confidência do protocolo, bem como aos ataques recentemente desenvolvidos para burlar o mecanismo de verificação de integridade do protocolo.

3.1.1 Melhorias da Chave de Segurança do WPA

Uma das melhorias feitas em relação à chave de segurança do WEP foi a extensão do campo IV de 24 para 48 bits, o que reduz a praticamente zero a probabilidade de repetição

dessa parte da chave num curto espaço de tempo. Além disso, o WPA especifica regras para a escolha e a verificação dos IVs, o que torna os ataques de reinjeção de pacotes do WEP ineficazes.

Outra melhoria foi a substituição da chave estática do WEP por um conjunto de chaves temporais hierárquicas. Nesse novo conceito, existe uma chave principal conhecida como PMK (*Pairwise Master Key*), a qual é utilizada para derivar periodicamente o conjunto de chaves temporárias que será utilizado pelos mecanismos do protocolo. Essa melhoria evita que a chave principal seja utilizada diretamente, mantendo-a em segurança caso uma das chaves temporárias seja descoberta.

3.1.2 Autenticação

A autenticação no WPA possui dois modos de funcionamento: WPA pessoal e WPA corporativo. No primeiro, direcionado para pequenas empresas e usuários domésticos, a autenticação é feita pelo AP através de uma chave previamente compartilhada entre o AP e os usuários da rede. Essa chave é conhecida como PSK (*Pre-Shared Key*)e possui de 8 a 63 caracteres ASCII. O primeiro modo também é conhecido como WPA-PSK. No segundo, direcionado para empresas de maior porte, um servidor 802.1X/EAP (*Extensible Authentication Protocol*) dedicado é o responsável pela autenticação dos usuários da rede e pela distribuição da MSK (*Master Session Key*). No final do processo de autenticação, uma chave PMK (*Pairwise Master Key*) é derivada. Se o modo de autenticação for baseado no WPA-PSK, a PMK é a própria PSK. Caso contrário, a PMK é obtida a partir da derivação da MSK que foi compartilhada durante o processo de autenticação 802.1X/EAP.

O servidor utilizado no modo WPA corporativo é responsável tanto pela autenticação do usuário quanto do ponto de acesso. Esse servidor utiliza o protocolo de autenticação 802.1X combinado com algum tipo de EAP. O 802.1X é um protocolo utilizado em redes cabeadas que se mostrou adequado para realizar a comunicação entre o ponto de acesso e o servidor de autenticação nas redes IEEE 802.11. Já o EAP é responsável por criar uma canal lógico seguro entre o cliente e o servidor de autenticação, por onde serão

transferidas as credenciais utilizadas na autenticação. Na realidade, por baixo do EAP existem dois protocolos realizando a comunicação: o EAPOL (*Extensible Authentication Protocolo over LAN*), que realiza a comunicação entre o cliente e o AP, e o 802.1X, que realiza a comunicação entre o AP e o servidor de autenticação. A Figura **??** apresenta o esquema de protocolos do WPA corporativo.

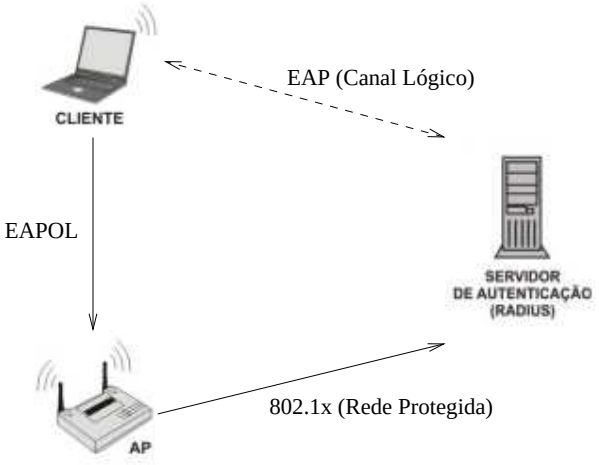

Figura 3.1 Esquema de protocolos do WPA corporativo

A Figura 3.2 ilustra o processo de autenticação do WPA corporativo. Nesse processo quando o cliente deseja se autenticar em uma rede que utiliza o WPA coorporativo ele deve enviar suas credenciais (binômio usuário/senha, *smart cards*, certificados digitais, entre outros) através do canal lógico criado pelo EAP diretamente para o servidor de autenticação (em geral um servidor RADIUS). O servidor verifica as credenciais e autentica o cliente caso elas estejam corretas.

Após a autenticação é iniciado o processo de derivação das chaves que ocorre durante o *4-way-handshake*. Nesse processo a PMK é derivada no conjunto de chaves temporárias conhecido como PTK (*Pairwise Transient Key*). O PTK é composto por diversas chaves, entre elas a chave que será utilizada na confidência dos dados conhecida como TEK ou TK (*Temporal Encription Key*), a chave utilizada na integridade dos dados conhecida como TMK (*Temporal MIC Key*) e outras chaves de menor uso.

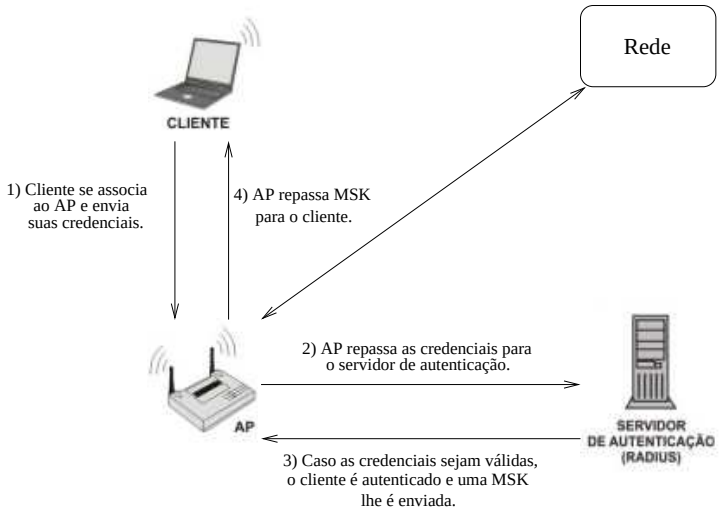

Figura 3.2 Autenticação WPA corporativo

3.1.3 Integridade

A Figura 3.3 ilustra o processo de integridade do WPA. Nesse processo o WPA utiliza o ICV, que já era utilizado no WEP, em conjunto com um novo campo denominado MIC (*Message Integrity Check*) para a verificação da integridade de dados. O MIC é calculado utilizando-se uma função *hash* não-linear conhecida por *Michael* que recebe como entradas a chave TMK, os endereços MAC (*Medium Access Control*) de origem e de destino do quadro e os dados propriamente ditos. No total, o WPA utiliza 12 bytes para verificação de integridade, sendo 8 bytes do MIC e 4 bytes do ICV.

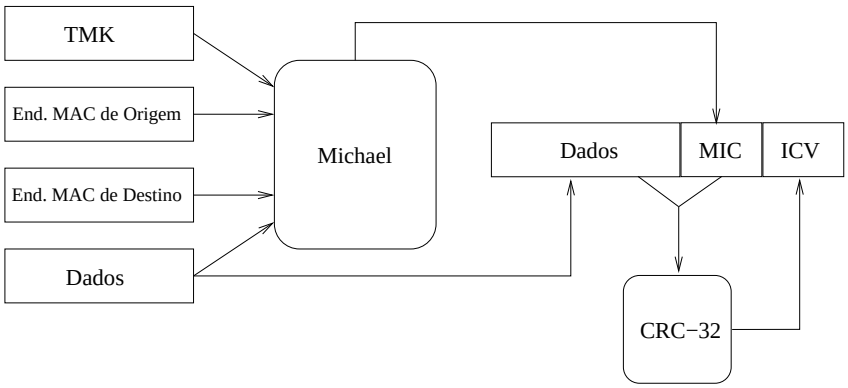

Figura 3.3 Integridade WPA

É importante ressaltar que a escolha do *Michael* para o processo de integridade do WPA foi feita por ele ser um algoritmo leve e não por sua segurança. A segurança fornecida por ele é de apenas 20 bits, o que implica que um valor aleatório do MIC tem uma chance em um milhão de ser aceito como válido. Essa probabilidade torna o mecanismo fraco do ponto de vista criptográfico, o que fez com que os desenvolvedores do WPA utilizassem uma medida extra para garantir a segurança do MIC. Essa medida faz com que a autenticação de um determinado cliente seja invalidada pelo AP caso ocorram 2 erros de MIC em pacotes provenientes do mesmo num intervalo de um minuto. Isso força uma nova derivação de chaves e evita que um atacante descubra o valor do MIC por força-bruta.

3.1.4 Confidência

A Figura 3.4 ilustra o mecanismo de confidência do WPA. Essa confidência é fornecida por um protocolo conhecido como TKIP (*Temporal Key Integrity Protocol*). Esse protocolo utiliza o conceito de chaves temporais, no qual as chaves são utilizadas por um período limitado de tempo e depois substituídas de maneira dinâmica.

No TKIP, o vetor de inicialização (IV) continua existindo, mas agora é representado por uma cadeia de 48 bits e conhecido como IV estendido. Além de ser utilizado durante a cifragem dos dados, o IV estendido também atua como um contador de quadros conhecido como TSC (*TKIP Sequence Counter*). Esse contador é zerado quando uma nova chave TK é gerada. O TSC é incrementado a cada quadro criptografado e se um deles for recebido com TSC fora de ordem é imediatamente descartado.

No TKIP, o algoritmo RC4 ainda é utilizado devido as limitações de processamento dos equipamentos que utilizavam WEP. No entanto, a cada quadro enviado, a chave TK passa por um algoritmo de combinação. Esse algoritmo usa como entradas a chave, o IV estendido e o endereço MAC do transmissor e gera a chave que será utilizada para gerar o *keystream*.

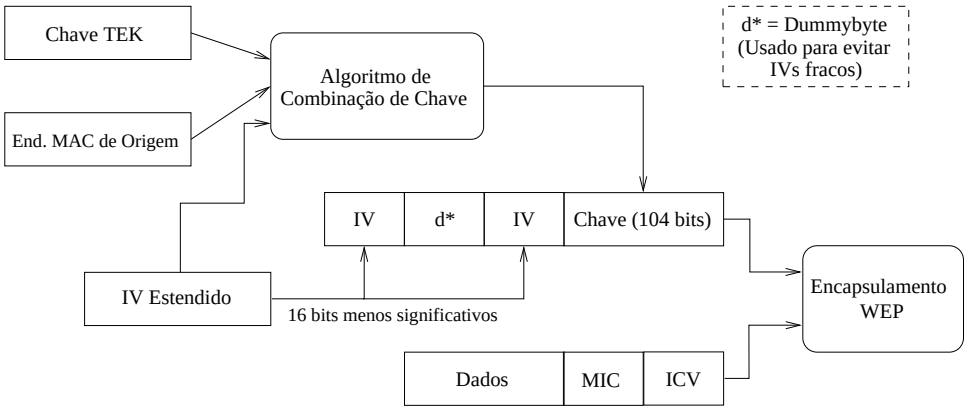

Figura 3.4 Confidência WPA

3.1.5 Vulnerabilidades e Ataques

Apesar de corrigir grande parte das falhas de segurança presentes no protocolo WEP, o WPA possui quatro vulnerabilidades conhecidas até o presente momento. A primeira foi encontrada no algoritmo de combinação de chaves utilizado pelo TKIP, a segunda no modo de autenticação WPA-PSK, a terceira é sua susceptibilidade a ataques de negação de serviço e a última no processo de integridade dos dados. Tais fraquezas são detalhadas a seguir.

Uma falha no algoritmo de combinação de chaves faz com que o atacante possa recuperar a chave TK. Para que ela possa ser explorada, o atacante deve ter acesso à no mínimo duas chaves RC4 geradas com IVs que possuam os 32 bits mais significativos iguais [16]. No entanto, esse ataque ainda não é factível na prática já que o atacante não tem como ter acesso às chaves RC4 necessárias. Vale ressaltar que esse ataque possui complexidade O($2^{(}105$)) o que representa uma boa redução quando comparado ao ataque de força bruta que tem complexidade O($2^{(}128$)), ainda assim, não poderia ser realizado em tempo hábil pelos computadores atuais.

No modo de autenticação WPA-PSK, a chave é pré-compartilhada por todos usuários da rede e pelo AP. Se a chave utilizada tiver menos de 20 caracteres, esse modo de autenticação é susceptível a ataques de dicionário off-line [17]. Para que esses ataques possam ser realizados, basta que o atacante capture os endereços MAC de origem e de

destino e os *nonces*, os quais estão disponíveis nos 2 primeiros pacotes do *4-way-handshake* de qualquer usuário que se conecte a rede. Com essas informações o atacante pode utilizar um dicionário previamente construído para tentar recuperar a chave.

Os pacotes de gerência do WPA continuam sendo passados em claro como era feito no WEP. Portanto, ainda é possível utilizá-los para fazer ataques de negação de serviço. Além disso, o mecanismo de proteção do MIC contra ataques de força-bruta cancela a associação do cliente com o AP por 60 segundos quando dois erros de checagem de MIC são detectados em menos de um minuto. Isso significa que um atacante pode forjar dois quadros com erros e utilizá-los para realizar um ataque de negação de serviço.

A vulnerabilidade do algoritmo *Michael* e a previsibilidade de conteúdo de pacotes do tipo ARP foram utilizadas para a criação do primeiro ataque prático contra o protocolo WPA, conhecido como ataque *Beck-Tews* [7]. Para o sucesso do ataque, as seguintes condições devem ser respeitadas: 1) a rede deve utilizar o protocolo IPv4 e o range de endereços IP deve estar configurado de forma que o atacante conheça a maioria dos bits do endereço (*i.e.* 192.165.8.X); 2) o protocolo TKIP deve estar utilizando um intervalo para reposição das chaves bastante longo; 3) o quadro que avisa sobre erros de checagem do MIC deve estar habilitado e; 4) o AP deve dar suporte a qualidade de serviço (IEEE 802.11e - QoS) [3].

O ataque *Beck-Tews* inicialmente realiza a captura de pacotes com tamanhos curtos e bem definidos, como os do tipo ARP. Adicionalmente, como os endereços da camada de enlace não são cifrados, boa parte do conteúdo dos pacotes ARP torna-se previamente conhecido pelo atacante. Para descobrir os bytes do ARP que não são previsíveis, o ICV e o MIC, o atacante realiza um ataque *chopchop*[11] modificado. Nessa modificação do ataque, a cada byte adivinhado corretamente através do procedimento convencional do *chopchop* será recebida uma mensagem de erro de MIC. Essa mensagem indica que caso ocorra outro erro de MIC em menos de 60 segundos ocorrerá a renegociação imediata das chaves. Devido a essa limitação somente um byte pode ser adivinhado por minuto. Após a obtenção dos completo do pacote, o atacante é capaz de inverter o algoritmo de integridade *Michael*, levando-o a obtenção da *MIC key*, que é a chave de integridade. De

posse da *MIC key*, o atacante tem a possibilidade de gerar um *keystream* de tamanho igual ou menor do que o ARP. O *keystream* pode ser utilizado para forjar um pacote personalizado e íntegro. O pacote falso pode ser enviado aos clientes da rede em cada um dos canais fornecidos pelo IEEE 802.11e para a criação de novos ataques. Isso é possível desde que o TSC do canal seja menor que o TSC do pacote enviado.

Se utilizando de uma abordagem semelhante à proposta de *Beck* e *Tews*, *Ohigashi* e *Morii* desenvolveram um ataque para o WPA no qual não se faz necessário que a rede proveja suporte ao IEEE 802.11e [8]. Neste caso o atacante se posiciona fisicamente em um local onde possa alcançar o cliente e o ponto de acesso, mas que essas entidades não consigam se comunicar diretamente. Nesse caso, a entidade maliciosa executa um ataque *Beck-Tews* em conjunto com um ataque de *man-in-the-middle*. Por conseguinte, esse ataque também se utiliza da previsibilidade de tamanho e conteúdo existente em alguns tipos de pacotes.

3.2 IEEE 802.11I (WPA2)

O IEEE 802.11i [3], também conhecido Wi-Fi Protected Access 2 (WPA2), foi aprovado em 2004 pelo IEEE. Alguns mecanismos do WPA também estão presentes no WPA2, visto que o primeiro foi desenvolvido em cima de um rascunho (*draft*) do segundo. Os grandes avanços desse novo protocolo são os novos processos de integridade e confidência dos dados que utilizam cifragem por bloco ao invés da cifragem bit a bit dos seus antecessores. Os novos algoritmos exigem um maior poder computacional, o que impossibilitou que o WPA2 fosse implementado como uma atualização de firmware.

Esta seção apresenta os mecanismos de autenticação, integridade e confidência do protocolo WPA2, bem como as vulnerabilidades presentes no protocolo.

3.2.1 Autenticação

Os dois modos de autenticação utilizados no WPA se mantiveram no WPA2. No entanto o conceito de mobilidade foi incluído nessa nova versão. No WPA caso o usuário quisesse

se mover entre um AP e outro ele teria que realizar todo o procedimento de autenticação novamente, o que causava a interrupção da conexão. Para resolver esse problema, os equipamentos WPA2 podem fornecer suporte a *PMK Caching* e *Preauthentication*. O *PMK Caching* permite que o AP armazene as informações das autenticações feitas pelos clientes da rede e caso um cliente queira se re-autenticar o número de mensagens trocadas é reduzido. Já o *Preauthentication* permite que dentro de uma rede exista um AP central que comunica com diversos APs periféricos e caso o cliente se mova entre dois APs periféricos, não será necessária uma nova autenticação.

3.2.2 Integridade e Confidência

O protocolo responsável pela integridade e confidência do WPA2 é o CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*), que continua utilizando o conceito de chaves temporárias presente no WPA. Ele utiliza o modo de operação CCM (*Counter with CBC-MAC*) [18], o qual é baseado no padrão AES (*Advanced Encryption Standard*) [19] que utiliza cifragem por blocos de tamanho fixo, ao invés da cifragem bit a bit utilizada nos protocolos anteriores. No caso do WPA2, o tamanho dos blocos e das chaves é padronizado em 128 bits.

A parte do CCMP responsável pela integridade dos dados é o CBC-MAC (*Cipher Block Chaining Message Authentication Code*). A Figura 3.5 ilustra o processo de integridade do WPA2. Nesse processo, existem duas etapas que são repetidas até que todos os blocos do quadro a ser enviado sejam utilizados. Na primeira etapa, um "bloco resultado" de 128 bits é gerado a partir da chave de integridade e do bloco de 128 bits atual. O bloco de 128 bits atual é o primeiro bloco do quadro caso seja o primeiro ciclo do algoritmo, ou o bloco de 128 bits gerado pelo ciclo anterior caso o algoritmo esteja do segundo ciclo em diante. Já na segunda, etapa é gerado um "bloco Xresultado" a partir de um XOR entre o "bloco resultado"gerado na primeira etapa e o bloco atual do quadro a ser enviado. No final, os 64 bits mais significativos do "bloco Xresultado" gerado no último ciclo são colocados no campo MIC.

Para a confidência dos dados, o CCMP utiliza o algoritmo de criptografia *AES*

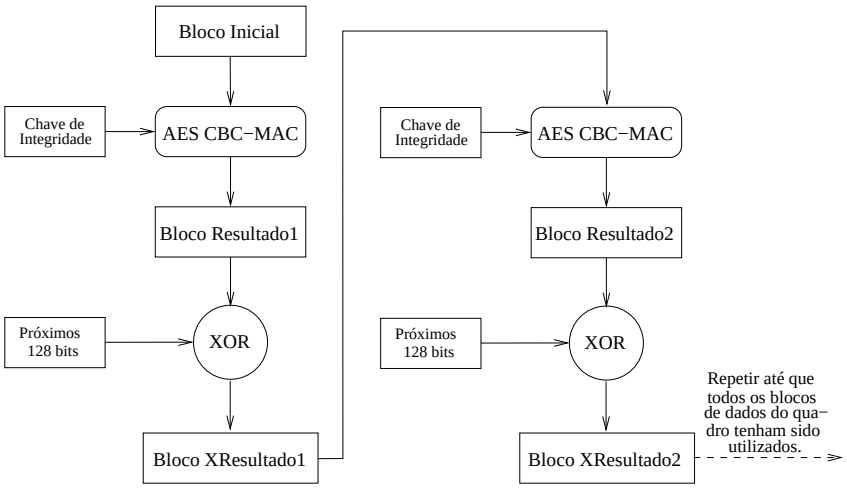

Figura 3.5 Integridade WPA2

Counter-Mode (CTR). A chave utilizada por esse algoritmo também é de 128 bits e o vetor de inicialização mantém os 48 bits do WPA. O algoritmo de combinação de chaves do WPA2 se encontra embutido no CTR e utiliza um esquema baseado em *S-boxes* e operações com matrizes. As *S-boxes* são matrizes de substituição pré-definidas e de conhecimento público. A combinação das *S-boxes* com as demais operações do CTR fornecem um nível de confidência muito maior que o do TKIP do WPA.

3.2.3 Vulnerabilidades

O WPA2 conseguiu corrigir a grande maioria das falhas presentes no WEP e no WPA. No entanto, ainda existem duas vulnerabilidades conhecidas nesse protocolo. A primeira delas é referente ao modo de autenticação com chave PSK que como no WPA é vulnerável aos ataques de dicionário se a chave possuir menos de 20 caracteres. Já a segunda vulnerabilidade é referente aos quadros de gerência que continuam sendo passados em claro, permitindo a utilização dos mesmos ataques de negação de serviço que ocorriam no WEP.

3.3 IEEE 802.11W

Em março de 2005 o grupo de trabalho do IEEE 802.11w [6] foi aprovado para melhorar a segurança das redes IEEE 802.11, principalmente no que diz respeito à proteção dos quadros de gerenciamento. Essa proteção é necessária principalmente devido a utilização desses quadros nos ataques DoS do tipo *De-authentication*. Além disso, os padrões IEEE 802.11v, 802.11k e 802.11r estenderam o funcionamento desses quadros, o que fez com que informações sensíveis sobre a rede fossem transportadas por esse tipo de quadro. A aprovação do protocolo estava prevista para 2008, mas só foi realizada no final de 2009.

É importante salientar que o IEEE 802.11w é um encapsulamento do IEEE 802.11i (WPA2), já que os mecanismos de autenticação, integridade e confidência são os mesmos em ambos os protocolos. A grande novidade introduzida pelo IEEE 802.11w é o BIP (*Broadcast/multicast Integrity Protocol*), que foi o mecanismo desenvolvido para garantir a integridade dos quadros de gerenciamento e evitar a reinjeção dos mesmos.

Esta seção apresenta o funcionamento do BIP, bem como uma análise das possíveis vulnerabilidades ainda existentes no IEEE 802.11w.

3.3.1 Broadcast/multicast Integrity Protocol (BIP)

O BIP é responsável por garantir a integridade e evitar a reinjeção dos quadros de gerenciamento das redes IEEE 802.11. Para isso, ele utiliza o algoritmo *AES-128 CMAC mode* para calcular um valor MIC de 64 bits, que é utilizado para realizar a checagem da integridade dos quadros de gerenciamento transmitidos pela rede. O *AES-128 CMAC mode* recebe como entrada a chave de 128 bits IGTK (*Integrity Group Temporal Key*) e blocos de dados também com 128 bits. A saída do algoritmo é truncada de 128 para 64 bits ao final do processo.

Outra importante adição do BIP é o contador IPN (*IGTK Packet Number*). Esse contador é utilizado para garantir que pacotes antigos capturados não sejam reinjetados na rede. Quando um pacote é recebido o IPN contido no mesmo é verificado e caso ele seja inferior ao IPN do receptor, o pacote é silenciosamente descartado, já que o pacote

estaria sendo reinjetado.

3.3.2 Vulnerabilidades

Apesar de resolver o problema dos ataques DoS do tipo *De-authentication*, o IEEE 802.11w ainda sofre com os ataques DoS do tipo *Radio Frequency Jamming*. Esse tipo de ataque inviabiliza transmissão de dados em determinada região através da introdução de ruídos em excesso na frequência utilizada pela rede. Além disso, o IEEE 802.11w também não prevê a proteção dos quadros de controle desse tipo rede, os quais também poderiam ser utilizados para ataques de negação de serviço.

3.4 RESUMO

Os protocolos WPA, IEEE 802.11i e IEEE 802.11w foram desenvolvidos com o intuito de resolver as vulnerabilidades na segurança das redes IEEE 802.11. O WPA foi desenvolvido a partir de um rascunho do IEEE 802.11i para ser utilizado como uma atualização do WEP na tentativa de minimizar as críticas feitas pelas empresas que adotaram o protocolo. Já o IEEE 802.11i é um protocolo mais complexo, que teve como objetivo aumentar ainda mais a segurança das redes IEEE 802.11 substituindo os mecanismos ultrapassados dos protocolos anteriores por algoritmos baseados no AES. O IEEE 802.11i resolveu grande parte das vulnerabilidades das redes IEEE 802.11, mas somente no IEEE 802.11w os pacotes de gerenciamento receberam a devida proteção contra ataques. Esse capítulo apresentou o estudo completo dos três protocolos.

CAPÍTULO 4

MECANISMO DE DEFESA PROPOSTO PARA O WPA

No capítulo anterior foram citados dois ataques [7, 8], recentemente desenvolvidos contra o protocolo WPA, os quais são baseados na previsibilidade de conteúdo de determinados tipos de pacotes. Esses ataques possuem a capacidade de burlar o mecanismo de integridade do protocolo e inserir pacotes falsos nas redes IEEE 802.11 que o utilizam.

Neste capítulo é feito um estudo dos pacotes do tipo ARP, os quais são utilizados nesse tipo de ataque, e é proposto e avaliado um mecanismo para evitar a realização dos ataques desenvolvidos contra o WPA, sendo esta a maior contribuição deste trabalho.

4.1 PACOTES DO TIPO ARP

Nessa seção serão mostradas tanto a estrutura básica dos pacotes do tipo ARP quanto as características que o tornam previvisíveis.

4.1.1 Estrutura dos Pacotes do tipo ARP (Adress Resolution Protocol)

A Figura 4.1 ilustra a estrutura dos pacotes do tipo ARP. Esses pacotes possuem 28 bytes de tamanho divididos em 9 campos fixos com tamanhos e funções específicas. São eles:

1. Tipo de *hardware* (bytes 1 e 2);
2. Tipo de protocolo (bytes 3 e 4);
3. Tamanho do *hardware* (byte 5);
4. Tamanho do protocolo (byte 6);
5. Opcode (bytes 7 e 8);

6. Endereço MAC de origem (bytes 9 a 14);

7. Endereço IP de origem (bytes 15 a 18);

8. Endereço MAC de destino (bytes 19 a 24);

9. Endereço IP de destino (bytes 25 a 28);

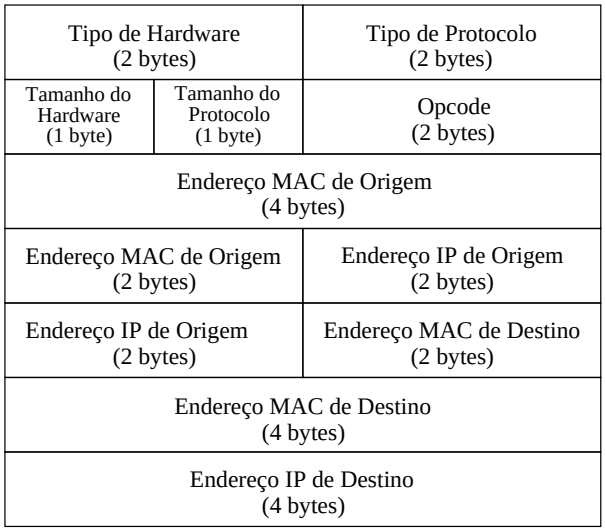

Figura 4.1 Estrutura de um Pacote do Tipo ARP

4.1.2 Padrões e Campos com Conteúdo Previsível

Foi realizada uma análise visando identificar características relevantes em relação a possíveis padrões em determinados tipos de pacotes [20]. Nessa análise foram feitos experimentos sobre o conteúdo de pacotes do tipo ARP, através de *Clustering* com técnicas de *(p,n)-grams* [21, 22]. A princípio, para qualquer entidade que capture pacotes cifrados de uma rede, é possível identificar se o pacote é do tipo ARP a partir do seu tamanho, sendo este 28 bytes mais o tamanho correspondente aos campos da camada de enlace.

Dos 28 bytes utilizados por pacotes do tipo ARP, ao menos 20 bytes possuem um elevado grau de previsibilidade. Isso ocorre principalmente devido à existência de campos com conteúdos fixos ou de pouca variação, como o *tipo de protocolo da camada superior*

ou *tipo de protocolo de enlace*. Além da existência de campos com conteúdos fixos, os *endereços da camada de enlace* de fonte e de destino também se tornam conhecidos a um possível atacante, visto que esses campos também fazem parte do cabeçalho do protocolo de enlace, que trafega em texto-plano.

O conhecimento da faixa de endereços IP que a rede está operando fornece informações relevantes sobre o conteúdo dos pacotes ARP. Em redes locais de pequeno porte, geralmente os endereços IP dos dispositivos diferem apenas no último byte, sendo os outros 3 bytes valores fixos. Considerando um ambiente como esse, o percentual de previsibilidade dos pacotes do tipo ARP é de aproximadamente 93%.

4.2 ARQUITETURA DO MECANISMO PROPOSTO

Visando evitar a categoria de ataques citada anteriormente e reduzir a previsibilidade de determinados tipos de pacote, é proposto um mecanismo que modifica o tamanho dos mesmos, visto que esta é a característica que os torna mais previsíveis. Esse mecanismo insere uma quantidade aleatória de bytes no conteúdo dos pacotes antes da execução dos procedimentos de cifragem realizados pelo WPA. O funcionamento do mecanismo depende da utilização de um algoritmo criptográfico baseado em funções *Hash* da classe HMAC, a qual será brevemente analisada na próxima seção.

4.2.1 Hash-based Message Authentication Code (HMAC)

O HMAC [23] é uma classe algoritmos criptográficos utilizados originalmente para gerar códigos de autenticação de mensagens (MAC), os quais são utilizados verificação de integridade e autenticidade de pacotes. Esse tipo de algoritmo combina uma função *hash* resistente a colisão iterativa com uma chave secreta para gerar os MACs. A segurança desse tipo de algoritmo está diretamente ligada a força da função *hash* utilizada e ao tamanho e qualidade da chave secreta.

As funções *hash* resistentes à colisão mais utilizadas nos algoritmos HMAC são a *SHA-1* e a *MD5*, as quais consideradas como as mais seguras criptograficamente falando.

Esse tipo de função recebe um bloco de tamanho fixo como entrada e quebra esse bloco em partes menores de igual tamanho. As partes menores são comprimidas, gerando uma saída aleatória de tamanho fixo. No caso da *SHA-1* a saída é de 160 *bits*, já no da *MD5* a saída é de 128 *bits*.

O algoritmo *HMAC-SHA-1* é utilizado nos mais diversos protocolos de segurança, como *TLS*, *glsglo:IPsec*, *WPA*, *IEEE 802.11i*, entre outros. No caso especifico dos protocolos de segurança de redes IEEE 802.11 (WPA e IEEE 802.11i), ele é utilizado para realizar derivação das chaves de segurança durante o *4-way-handshake*

4.2.2 Procedimento de Inserção

A Figura 4.2 ilustra a arquitetura do mecanismo de inserção. Esse mecanismo é composto por dois módulos: o módulo gerador e o módulo montador. O módulo gerador define a quantidade de bytes falsos e as posições que os mesmos devem ser inseridos no pacote. O módulo montador insere os bytes falsos nas posições corretas e repassa o pacote modificado para protocolo de segurança.

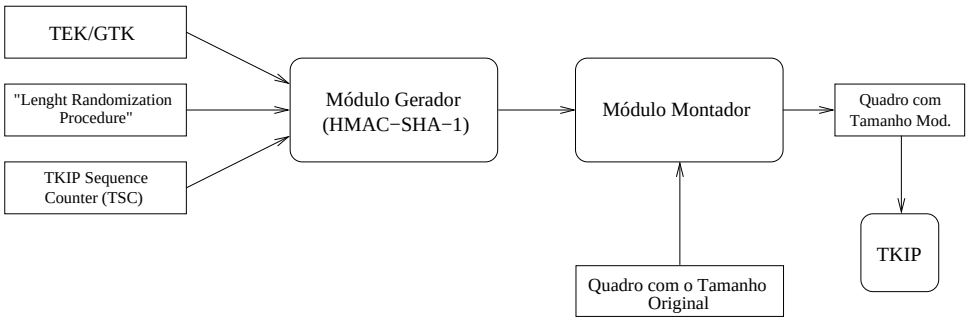

Figura 4.2 Procedimento de Inserção

No primeiro módulo, está presente um algoritmo HMAC que recebe como entradas: a chave TK para transmissões *unicast* ou a GTK para transmissões em *broadcast*; a *string* de diferenciação com o nome do procedimento, no caso "*Length Randomization Procedure*" e; o *TKIP Sequence Counter* (TSC), o qual é o contador de pacotes do WPA e permite que a saída do algoritmo HMAC seja modificado a cada pacote. O algoritmo HMAC utilizado no WPA é o *HMAC-SHA-1*, o qual é responsável pela geração do valor

n, que indica a quantidade de bytes falsos inseridos, e dos blocos **k** bits, que indicam a posição de inserção de cada byte no pacote.

O segundo módulo recebe como entrada o pacote com o tamanho original e as saídas do modulo anterior. Os bytes falsos são inseridos no pacote nas posições indicadas pelos blocos de **k** bits. O pacote com o tamanho alterado é enviado para o TKIP para a realização da cifragem do mesmo.

4.2.3 Procedimento de Remoção

A Figura 4.3 ilustra a arquitetura do mecanismo de remoção. Esse mecanismo também possui uma estrutura com dois módulos: módulo gerador e módulo removedor. O módulo gerador é utilizado novamente mecanismo de recepção, portanto ele gera exatamente qual foi a quantidade de bytes falsos inseridos e a posicionamento no pacote de cada um deles. O módulo removedor recebe o pacote e a saída do módulo gerador e remove os bytes falsos, devolvendo o pacote ao tamanho e conteúdo originais.

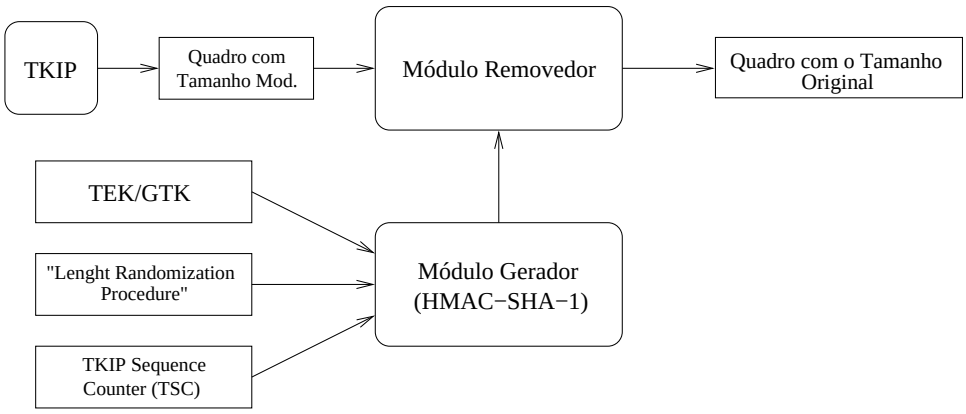

Figura 4.3 Procedimento de Remoção

4.2.4 Modificações na Segurança no WPA

Como apresentado anteriormente, os ataques *Beck-Tews* e *Ohigashi-Morii* utilizam a previsibilidade de pacotes pequenos, como ARPs, para descobrir a chave *MIC key* e forjar pacotes que podem ser injetados como autênticos na rede. A arquitetura do mecanismo

proposta para o WPA inviabiliza a execução dos dois ataques através da redução da previsibilidade do tamanho e do conteúdo dos pacotes.

A inserção de *bytes* falsos faz com que o tamanho dos pacotes varie de forma aleatória, evitando que o atacante consiga identificar pacotes a partir do tamanho de seus textos-cifrados. Isso ocorre porque a variação de tamanho faz com que pacotes de diferentes tipos, que possuem tamanhos próximos, se misturem, confundindo o atacante. Sem a certeza do tipo de pacote capturado, o atacante terá grandes dificuldades para identificar um pacote ARP e, por conseguinte, não conseguirá realizar o ataque.

Outra barreira criada pelo mecanismo proposto é que os bytes falsos são inseridos em posições aleatórias, gerando alterações significativas no conteúdo dos pacotes. Essas modificações fazem com que a descoberta da chave do MIC se torne inviável, pois ela depende da obtenção completa do pacote para poder ser realizada. Sem a chave *MIC key* os dois ataques perdem o sentido, pois não será possível forjar e injetar pacotes na rede.

4.3 AVALIAÇÃO

Nesta seção é realizada uma avaliação tanto do mecanismo em si como da arquitetura apresentada anteriormente. São avaliados os pontos fortes e fracos do mecanismo, o seu custo computacional de funcionamento e a viabilidade de uso na prática.

O ponto mais importante do mecanismo apresentado é que o mesmo impede a realização dos ataques ao WPA baseados na previsibilidade de pacotes fazendo o uso de algoritmos HMAC, os quais são criptograficamente seguros. Outro ponto relevante é que a arquitetura do mecanismo é bastante simples e pode ser adaptada para qualquer protocolo de segurança de redes de computadores.

O número máximo de bytes falsos inseridos **n** deverá ser proporcional ao tamanho do pacote, ou seja, pacotes pequenos receberão uma quantidade menor de bytes extras que os pacotes maiores. Esse percentual poderá ser ajustado pelo administrador da rede, de forma que o *overhead* causado pelo mecanismo e o nível de segurança fornecido pelo mesmo sejam reguláveis. Esse *overhead* pode ser minimizado se o mecanismo for configurado pelo administrador para trabalhar apenas com pacotes menores do que 150

bytes, o que pode ser feito sem perda de segurança já que os pacotes previsíveis são menores do que esse tamanho.

A utilização de um algoritmo HMAC (como o *HMAC-SHA-1* ou o *HMAC-MD5*) para gerar a quantidade e a posição dos bytes falsos inseridos também acarreta em um custo computacional adicional, que é inerente a qualquer mecanismo de segurança. No entanto, esse tipo de algoritmo é amplamente utilizado em protocolos de segurança e não causa problemas de rendimento nos sistemas atuais.

Na arquitetura apresentada, o maior custo computacional é o da utilização do algoritmo *HMAC-SHA-1*, já que o restante dos procedimentos realizados pelo mecanismo possuem custo desprezível. Esse custo não degenera o rendimento do protocolo, visto que os *hardwares* que utilizam o WPA já possuem o algoritmo *HMAC-SHA-1* implementado para a derivação de chaves durante o *4-way-handshake*.

A arquitetura apresentada ainda precisa ser implementada e testada na prática. No entanto a tendência é que ela seja viável já que a maioria dos mecanismos e chaves utilizados fazem parte do próprio WPA. Por conseguinte, os *hardwares* que implementam o WPA só precisam ser adaptados para receber o mecanismo através de uma atualização de *firmware*.

4.4 RESUMO

Os ataques *Beck-Tews* e *Ohigashi-Morii* utilizam a previsibilidade de tamanho e conteúdo dos pacotes do tipo ARP para burlar o mecanismo de integridade do WPA e injetar pacotes falsos nas redes protegidas por esse protocolo. Nesse capítulo foi feito um estudo sobre os ataques baseados em previsibilidade de informações e sobre as características dos pacotes do tipo ARP. Além disso, foi proposto e avaliado um mecanismo que permite a modificação do tamanho e do conteúdo de pacotes previsíveis, inviabilizando a realização dos ataques contra o WPA citados anteriormente.

CAPÍTULO 5

CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou um estudo dos mecanismos e vulnerabilidades dos protocolos WEP, WPA, IEEE 802.11i e IEEE 802.11w, responsáveis pela segurança das redes IEEE 802.11. Os estudos levaram a proposição de um mecanismo de defesa que protege o protocolo WPA contra os ataques *Beck-Tews* e *Ohigashi-Morii*, os quais são baseados na previsibilidade dos dados de determinados tipos de pacotes que trafegam na rede.

O estudo demonstrou que o protocolo WEP já não possui a capacidade de proteger as redes IEEE 802.11, visto que o protocolo possui uma série de vulnerabilidades e não consegue prover os três princípios básicos de segurança: autenticação, integridade e confidência. Os ataques mais recentes desenvolvidos contra o WEP, como o PTW, conseguem recuperar a chave de segurança em poucos minutos, o que faz com que o protocolo seja extremamente inseguro.

O protocolo WPA ainda consegue fornecer segurança para as redes IEEE 802.11, mas a utilização de mecanismos do WEP em seu funcionamento pode resultar na redução dessa segurança daqui a algum tempo. Além disso, o algoritmo *Michael* já demonstrou não fornecer a segurança necessária, visto que os ataques *Beck-Tews* e *Ohigashi-Morii* conseguiram violar a integridade da rede.

O estudo mostra que os protocolos IEEE 802.11i (WPA2) e IEEE 802.11w são mais seguros que os anteriores, por serem baseados no esquema de criptografia por blocos AES. Os dois protocolos resolvem grande parte das vulnerabilidades do WEP e do WPA e são as melhores opções para a segurança de qualquer rede IEEE 802.11.

O mecanismo proposto nesse trabalho consegue proteger o protocolo WPA dos ataques *Beck-Tews* e *Ohigashi-Morii* fazendo o uso de algoritmos e funções já presentes no protocolo, como o *HMAC-SHA-1*. Assim sendo, o mecanismo além de seguro também é

compatível com os equipamentos que utilizam o WPA.

Em trabalhos futuros poderíamos incluir o estudo mais aprofundado do IEEE 802.11w, visto que o mesmo ainda não foi introduzido em nenhum produto comercial. Além disso, a proteção dos quadros de controle deve ser analisada para que solução viável para essa vulnerabilidade do protocolo possa ser proposta. Outro trabalho futuro é a implementação do mecanismo proposto nesse trabalho em um ambiente real para avaliar de forma mais concreta a segurança e o desempenho do mesmo.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] V. Hayes *et al.*, " IEEE Standard 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Computer Society*, 1999.

[2] S. J. Kerry *et al.*, "IEEE Standard 802.11g-2003, Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications - Amendment 4: Further Higher Data Rate Extensionin the 2.4 GHz Band," *IEEE Computer Society*, 2003.

[3] S. J. o. Kerry, " IEEE Standard 802.11i-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*, 2004.

[4] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key Scheduling Algorithm of RC4," *Lecture Notes in Computer Science - Selected Areas in Cryptography*, no. 2259, pp. 1–24, 2001.

[5] "Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for Today's Wi-Fi Networks," Tech. Rep., 2003.

[6] B. P. Kraemer *et al.*, " IEEE Standard 802.11w-2009, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Protected Management Frames," *IEEE Computer Society*, September 2009.

[7] M. Beck and E. Tews, "Practical Attacks Against WEP and WPA," in *Proceedings of the Second ACM Conference on Wireless Network Security - WiSec'09*, 2009, pp. 79–86.

[8] T. Ohigashi and M. Morii, "A Practical Message Falsification Attack on WPA," in *Procedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System*, August 2009.

[9] KoreK, "Next Generation of WEP Attacks?" 2004. [Online]. Available: http://www.netstumbler.org/showpost.php?p=93942&postcount=35

[10] M. Borsc and H. Shinde, "Wireless Security & Privacy," in *Procedings of IEEE International Conference on Wireless Comunications*, 2005, pp. 424–428.

[11] KoreK, "Chopchop (Experimental WEP Attacks)," 2004. [Online]. Available: http://www.netstumbler.org/f50/chopchop-experimental-wep-attacks-12489/

[12] E. Tews, R.-P. Weinmann, and A. Pyshkin, "Breaking 104 Bit WEP in Less Than 60 Seconds," *Lecture Notes in Computer Science - Information Security Applications*, no. 4867, pp. 188–202, 2007.

[13] R. Rivest, "The RC4 Encryption Algorithm," Tech. Rep., March 1992.

[14] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 2, pp. 319–332, 2004.

[15] A. Klein, "Attacks on the RC4 Stream Cipher," *Designs, Codes and Cryptography*, vol. 48, no. 3, pp. 269–286, September 2008.

[16] V. Moen, H. Raddum, and K. J. Hole, "Weakness in the Temporal Key Hash of WPA," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 8, no. 2, pp. 76–83, April 2004.

[17] J. L. MacMichael, "Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode," *Linux Journal*, vol. 2005, no. 137, p. 2, September 2005.

[18] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," RFC 3610, United States, September 2003.

[19] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," Tech. Rep., June 1998. [Online]. Available: http://www.comms.scitech.susx.ac.uk/fft/crypto/rijndael.pdf

[20] B. G. D'Ambrosio and P. A. da Silva Gonçalves, "Previsibilidade de Dados e Impactos na Segurança de Redes IEEE 802.11," in *Proceedings of XVII Congresso de Iniciação Científica da UFPE - XVII Conic*, October 2009.

[21] A. Matrawy *et al.*, "Mitigating Network Denial-of-Service Through Diversity-Based Traffic Management," in *Applied Cryptography and Network Security.* Springer Berlin / Heidelberg, 2005, vol. Volume 3531, pp. 104–121.

[22] A. Hijazi, H. Inoue, A. Matrawy, P. C. van Oorschot, and A. Somayaji, "Discovering Packet Structure through Lightweight Hierarchical Clustering." in *Procedings of IEEE ICC*, March 2008, pp. 33–39.

[23] Krawczyk *et al.*, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104 (Informational), February 1997.