UM ESTUDO DAS VULNERABILIDADES NAS REDES IEEE 802.11

ALUNO: ANTONIO NÓBREGA

ORIENTADOR: PAULO GONÇALVES

14 DE JULHO DE 2016

Universidade Federal de Pernambuco

Centro de Informática

Graduação em Ciências da Computação

UM ESTUDO DAS VULNERABILIDADES NAS REDES IEEE 802.11

Antonio Marino da Nóbrega Gomes

(amng@cin.ufpe.br)

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 GONÇALVES

AGRADECIMENTOS

Gostaria de agradecer primeiramente à minha mãe, pelo enorme suporte que me foi dado durante todos esses anos, sempre me apoiando durante as minhas escolhas e nunca deixando de acreditar em mim. Ao meu pai, que do seu jeito, fez eu me apaixonar por Ciências da Computação, sempre acreditando e torcendo por mim. Também gostaria de agradecê-los pela ótima base educacional que me proporcionaram, e pelos valores e princípios que me acompanharão pelo resto da vida. Não menos importante à minha irmã, que sempre me apoiou e me ajudou em momentos difíceis.

Agradeço a todos os familiares que sempre me apoiaram nessa caminhada, tios, tias, primos e minha querida avó.

Agradeço à minha namorada pelo apoio em diversos momentos durante todo o curso, pela paciência, companheirismo, compreensão e amor, e, ainda, por dividir comigo de perto as alegrias e aflições desta graduação e dos últimos 9 anos de relacionamento. Sem a motivação me dada por ela, não teria conseguido chegar até aqui e conquistar tudo que consegui.

Não posso esquecer de agradecer aos gladiadores da minha turma, CC-2010.2, por todos os momentos que passamos juntos no decorrer do curso. Sem eles, o curso com certeza seria muito monótono e sem graça. Muito obrigado pela companhia durante as noites em claro no Centro de Informática, pelos adversários no ping-pong e pelas risadas que vocês me proporcionaram durante esse longo curso.

Por último, porém não menos importante, agradeço aos professores do Centro de Informática pelas aulas inspiradores e pelos ensinamentos. Agradeço particularmente ao professor Paulo André da Silva Gonçalves pela orientação nesta monografia. Durante suas excelentes aulas, tive o primeiro contato com redes de computadores e segurança, o que me impulsionou a querer trabalhar e escrever a monografia a respeito deste tema.

RESUMO

As redes sem fio IEEE 802.11, popularmente conhecidas como redes Wi-Fi são amplamente utilizadas em ambientes comerciais, empresariais e residenciais por todo o mundo. Por causa da sua facilidade de uso, rápida configuração e praticidade, as redes sem fio estão cada dia mais presentes no dia a dia das pessoas.

As redes Wi-Fi possuem múltiplas vulnerabilidades desde as suas primeiras versões, a maioria delas causadas pelo fato de que os dados que trafegam em uma rede sem fio são transmitidos através de frequências de rádio, e podem ser facilmente capturados. Para se obter pacotes de uma rede cabeada, um atacante terá que ter acesso físico a uma conexão de rede, o que muitas vezes significa ter acesso ao roteador da rede, tarefa essa que pode ser bastante trabalhosa. Já com redes Wi-Fi, um atacante poderá ter acessos a todas as informações que trafegam nessa rede muito mais facilmente, bastando estar nas proximidades do ponto de acesso da rede sem fio.

Este trabalho apresenta uma análise aprofundada dos mecanismos de segurança de redes Wi-Fi. Os protocolos WEP, WPA, WPA2 e IEE 802.11w serão analisados em relação a critérios básicos de segurança: autenticidade, confidencialidade, integridade. Também são analisadas as vulnerabilidades e ataques publicamente conhecidos aos protocolos mencionados, assim como os mecanismos de defesa, quando existentes, contra esses ataques. Por fim uma breve análise é feita de mecanismos presentes na literatura para a segurança dos quadros de controle das redes IEEE 802.11.

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

ABSTRACT

Wireless IEEE 802.11 networks, popularly known as Wi-Fi networks are widely used in commercial, residential and business environments around the world. Because of their quick setup and convenience, wireless networks are becoming more present in their day to day life.

Wi-Fi networks always had multiple vulnerabilities since their early versions, most of them caused by the fact that data traveling over a wireless network are transmitted over radio frequencies, and can be easily captured by anyone in possess of a radio receiver. In order to obtain packets on a a wired network, an attacker would have to have physical acess to a network connection, which often means having access to a network router, a task that can be quite tricky to achieve. On wireless networks, none of that is needed, an attacker can have access to all the information being exchanged on said network by simply being near the wireless access point.

This work presents an in-depth analysis of the security mechanisms of IEEE 802.11 networks. The WEP, WPA, WPA2 and IEE 802.11w protocols will be analyzed in regard of basic security concepts: authenticity, confidentiality and integrity. The publicly known vulnerabilities and attacks of the mentioned protocols will also be analyzed, as well as defense mechanisms, if any, against such attacks. Finally a brief analysis is made of proposed mechanisms for encrypting control frames in IEEE 802.11 networks.

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

GLOSSÁRIO

ACK: Acknowledgement, 43

AES: Advanced Encryption Standard, 36

AES-CMAC: Cipher-based Message Authentication Code com AES, 45

AMK: Authenticity Master Key, 45

AP: Access Point, 25

ARP: Adress Resolution Protocol, 22

ATK: Authenticity Temporal Key, 45

BIP: Broadcast/Multicast Integrity Protocol, 41

CBC-MAC: Chaining Message Authentication Code, 36

CCM: Counter with CBC-MAC, 36

CCMP: Counter-Mode Cipher Block Chaining Message Authentication Code Protocol, 36

CRC-32: Cyclic Redudancy Check 32, 17

CTR: AES Counter Mode, 37

CTS: Clear to Send, 43

DoS: Denial of Service, 23

EAP: Extensible Authentication Protocol, 27

EAP-TLS: EAP-Transport Layer Security, 38

EAP-TTLS: EAP-Tunneled Transport Layer Security, 38

FCS: Frame Check Sequence, 42

FMS: Fluhrer, Mantin e Shamir, s˜ao os sobrenomes dos criadores do ataque FMS, 21

GTK: Group Temporal Key, 26

HMAC: Keyed-Hash Message Authentication Code, 29

IAPP: Inter-Access Point Protocol, 43

ICV: Integrity Check Value, 18

IDS: Intrusion Detection System, 32

IEEE: Institute of Electrical and Electronics Engineers, 14

IGTK: Integrity Group Temporal Key, 42

IPN: IGTK Packet Number, 42

IV: Initialization Vector, 19, 29

KSA: Key-scheduling algorithm, 21

LEAP: Lightweight Extensible Authentication Protocol, 38

LLC: Logical Link Control, 22

MAC: Medium Access Control, 25

MIC: Message Integrity Code, 25

MiTM: Man-in-the-Middle, 38

MMIE: Management MIC IE, 42

MSCHAPv2: Microsoft Challenge-Handshake Authentication Protocol 2, 38

NACK: Negative-acknowledgement, 34

NFC: Near field communication, 34

NS: Number Sequence, 45

PBKDF: Password-Based Key Derivation Function, 25

PEAP: Protected EAP, 38

PIN: Personal Identification Number, 34

PMK: Pairwise Master Key, 25

PRF: Pseudo Random Function, 42

PRGA: Pseudo-random generation algorithm, 21

PRNG: Pseudo-Random Number Generator, 19

PSK: Pre-Shared Key, 25

PTK: Pairwise Transient Key, 25

PTW: Pyshkin, Tews e Weinmann, s˜ao os sobrenomes dos criadores do ataque PTW, 23

QoS: Quality of Service, 31

RADIUS: Remote Authentication Dial-In User Service, 27

RC4: Ron's Code 4, 18

RTS: Request to Send, 43

SHA-1: Secure Hash Algorithm 1, 43

SSID: Service Set Identifier, 25; Service Set Identifier ou Identificador de Rede, 16

TA: Transmitter Address, 45

TC: Transmission Counter, 45

TKIP: Temporal Key Integrity Protocol, 28

TSC: TKIP Sequence Counter, 29

VWC: Virtual Wireless Client, 40

WEP: Wired Equivalent Privacy, 6

Wi-Fi: Wireless Fidelity, 14

WPA: Wi-Fi Protected Access, 15

WPA2: Wi-Fi Protected Access 2, 15

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

As redes sem fio IEEE 802.11, popularmente conhecidas como redes Wi-Fi são amplamente utilizadas em ambientes comerciais, empresariais e residenciais por todo o mundo. Por causa da sua facilidade de uso, rápida configuração e praticidade, as redes Wi-Fi estão cada dia mais presentes no dia a dia das pessoas.

As redes Wi-Fi possuem múltiplas vulnerabilidades desde as suas primeiras versões, a maioria delas causadas pelo fato de que os dados que trafegam em uma rede sem fio são transmitidos através de frequências de rádio, e podem ser facilmente capturados. Para se obter pacotes de uma rede cabeada, um atacante terá que ter acesso físico a uma conexão de rede, o que muitas vezes significa ter acesso ao roteador da rede, tarefa essa que pode ser bastante trabalhosa. Já nas redes IEEE 802.11, um atacante poderá ter acessos a todas as informações que trafegam nessa rede muito mais facilmente, bastando estar nas proximidades do ponto de acesso da rede sem fio.

1.1 OBJETIVOS

Este trabalho de graduação tem como objetivo principal, estudar os protocolos de segurança existentes para as redes IEEE 802.11 e analisar alguns esquemas propostos na literatura para aumentar a segurança dos quadros de controle dessas redes. A fim de alcançar esses objetivos, esses protocolos de segurança serão analisados de acordo com atributos básicos de segurança da informação: autenticidade, integridade e confidencialidade. Além disso, as vulnerabilidades e ataques publicamente conhecidos a esses protocolos serão estudados.

1.2 ESTRUTURA DO DOCUMENTO

Visando uma melhor estruturação e entedimento deste trabalho, foram definidos 6 capítulos.

O primeiro capítulo apresenta a introdução e a motivação do trabalho, bem como explicita os objetidos propostos.

No segundo capítulo uma detalhada descrição e análise do protocolo WEP é feita, destacando os mecanismos de autenticidade, integridade e confidencialidade utilizados pelo protocolo, bem como as vulnerabilidades e ataques conhecidos para o mesmo.

O terceiro e quarto capítulos analisam detalhadamente os protocolos WPA e WPA2, respectivamente. Assim como no segundo capítulo, analisaremos os protocolos tendo em vista os princípios básicos de segurança, além de listar as vulnerabilidades e ataques conhecidos contra esse protocolo.

No quinto capítulo, um estudo é feito do IEEE 802.11w, emenda para aumentar a segurança dos quadros de gerenciamento, além de trabalhos propostos na literatura para garantir a integridade dos quadros de controle.

Por fim, o sexto e último capítulo apresenta as considerações finais e discute trabalhos futuros a partir do estudo realizado.

2. Wired Equivalent Privacy (WEP)

A procura por redes sem fio cresceu bastante no fim da década de 90 pois ocorreu uma proliferação de laptops e PDA's além de que a internet também passou a se tornar um importante componente na vida das pessoas. Quando as redes IEEE 802.11 foram introduzidas no mercado, não existia qualquer mecanismo de segurança para proteger os dados que trafegavam na rede, os dados eram transmitidos via ondas de rádio, sem qualquer tipo de criptografia. Por conta disso, qualquer pessoa com um rádio poderia interceptar dados dessa rede. Em 1999, foi desenvolvido o primeiro protocolo de segurança para redes IEEE 802.11, o WEP (Wired Equivalent Privacy) [1]. A proposta do WEP era a de prover a confidencialidade existente nas redes cabeadas, às redes sem fio. O problema é que a falta de conhecimento de segurança dos criadores desse protocolo, fizeram com que o mesmo se tornasse alvo de uma série de ataques [2][3][4][5].

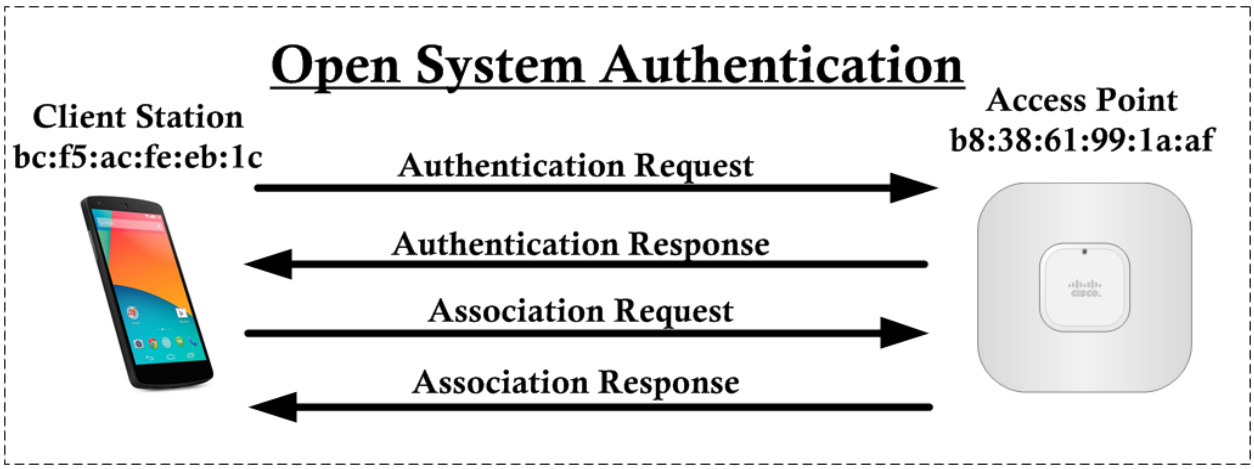
Este capítulo apresenta um estudo da autenticidade, integridade e confidencialidade do WEP, bem como as suas vulnerabilidades, ataques e defesas contra esses respectivos ataques (quando existirem).

2.1 Autenticidade

Para se juntar a uma rede, primeiramente o cliente deve se autenticar ao ponto de acesso. O WEP possui dois tipos de autenticação: a autenticação por Sistema Aberto (*Open System*) e a autenticação por Chave Compartilhada (*Shared Key*).

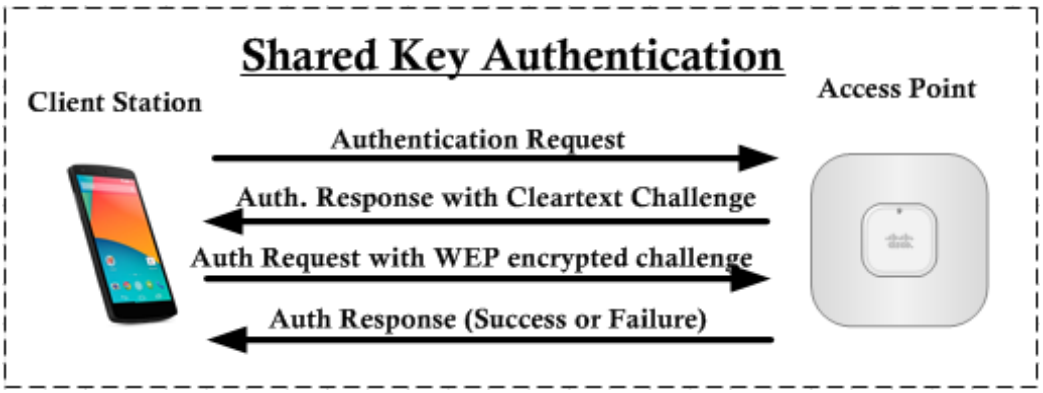
A autenticação por Sistema Aberto ocorre de forma bem simples, o cliente deve enviar um request contendo o SSID (*Service Set Identifier*) da rede ao ponto de acesso. Para obter o SSID, o cliente deve adquirir pequenos pacotes, chamados de *Beacons*, esses são enviados periodicamente pelo ponto de acesso e contêm informações sobre a rede. É importante notar que a rede é aberta, portanto qualquer cliente tem livre acesso a ela. A figura 1 ilustra esse modo de autenticação.

Figura 1 – Autenticação por Sistema Aberto do WEP



A autenticação por Chave Compartilhada se inicia do mesmo modo que a anterior, o cliente envia o *SSID* da rede e recebe um texto-desafio (*challenge text*) sem nenhum tipo de criptografia. O cliente então deve cifrar o texto-desafio com a chave compartilhada previamente entre o cliente e o ponto de acesso e em seguida enviar a cifra de volta ao mesmo. Ao receber a cifra do cliente, o ponto de acesso tentará decifra-la utilizando a mesma chave compartilhada, e caso o resultado seja idêntico ao texto-desafio enviado, o cliente tem permissão de se juntar à rede, o ponto de acesso então envia uma mensagem positiva ao cliente. A figura 2 ilustra essa autenticação.

Figura 2- Autênticação por Chave Compartilhada no WEP

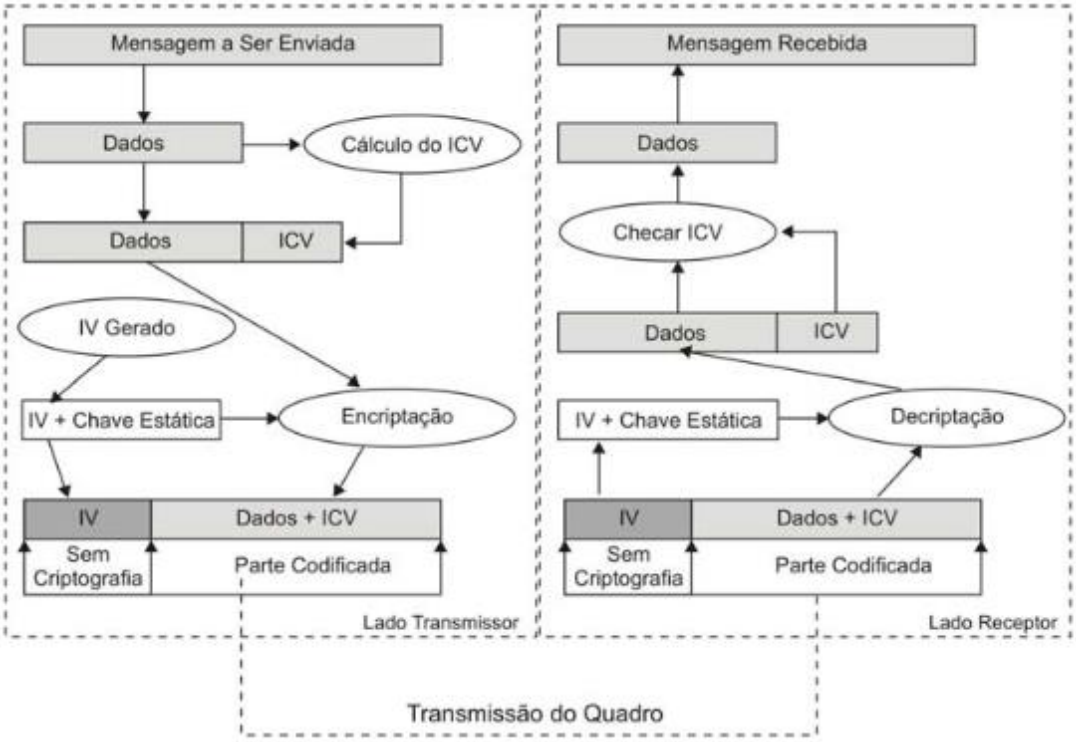


2.2 INTEGRIDADE

Para que os pacotes não sejam modificados enquanto estão sendo transmitidos do cliente ao ponto de acesso, ou vice versa, o WEP utiliza o algoritmo CRC-32 (*Cyclic redundancy*

check 32 bits) para gerar um valor chamado ICV (*Integrity Check Value*), esse valor é enviado criptografado junto à mensagem. Como o CRC-32 é uma função linear da mensagem, quando o destinatário receber o pacote, o mesmo poderá calcular o ICV e compará-lo ao ICV presente no pacote. Caso esses dois valores sejam iguais, a mensagem não foi modificada e pode ser aceita, caso contrário a mensagem foi corrompida ou adulterada, e tem que ser recusada. A figura 3 ilustra o processo descrito nesse item.

Figura 3- Integridade no Protocolo WEP



2.3 Confidencialidade

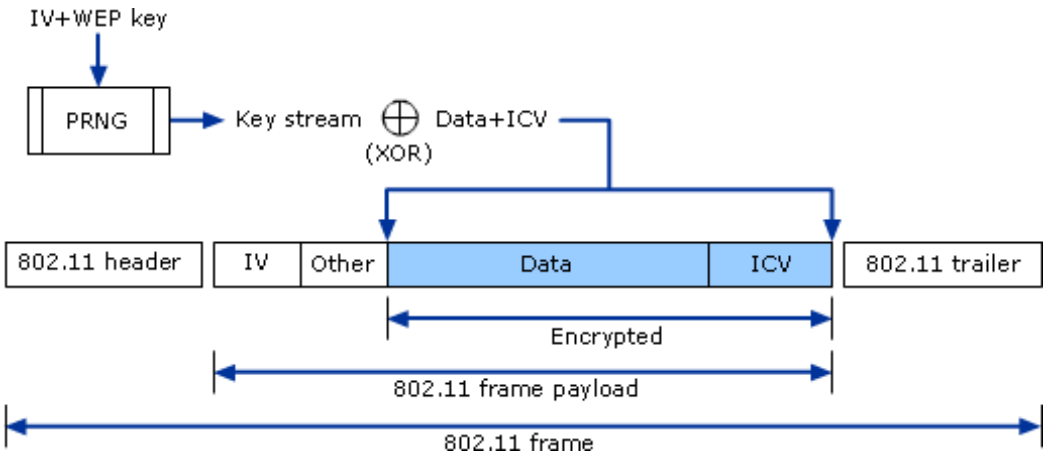
Para garantir que os pacotes que trafegam na rede não sejam interceptados e interpretados por um terceiro, o WEP utiliza um algoritmo de cifra de fluxo chamado RC4 (Ron's Code 4) [6] para cifrar os seus pacotes. É importante notar que o WEP não cifra o pacote inteiro, somente a mensagem e o ICV correspondente a ela, o cabeçalho do quadro de dados é enviado em texto plano.

Para gerar a chave utilizada no RC4, o WEP concatena um IV (*Initilization Vector*) de 24 bits gerado aleatoramente, e uma chave estática de 40 bits (há versões do WEP que utilizam

chaves de 104 e 232 bits) que chamaremos de *K*. A chave resultante vai ser usada como semente (*seed*) para o PRNG (*Pseudo-Random Number Generator*) do RC4. A PRNG terá como resultado um *keystream*, que corresponde a um conjunto de bytes pseudo-randômicos. Para evitar que haja uma repetição de *keystreams*, o IV (parte dinâmica da chave) deve ser único em cada mensagem.

Para cifrar um pacote o WEP o ponto de acesso concatena a mensagem e o ICV relativo à mesma, e realiza uma operação de OU Exclusivo (*XOR*) entre cada byte do pacote e o byte correspondente do *keystream*. Já para decifrar um pacote, o destinatário, que tem prévio conhecimento de *K*, precisa conhecer o IV, motivo esse pelo qual o IV é transmitido em texto plano junto com a mensagem. De posse do IV e de K, o destinatário poderá realizar o mesmo processo de geração do *keystream* e operação de XOR entre o cifrotexto e o *keystream* para decifrar a mensagem. As figuras 4 e 5 ilustram o processo de cifragem e decifragem de uma mensagem, respectivamente.

Figura 4- Encriptação de um pacote WEP



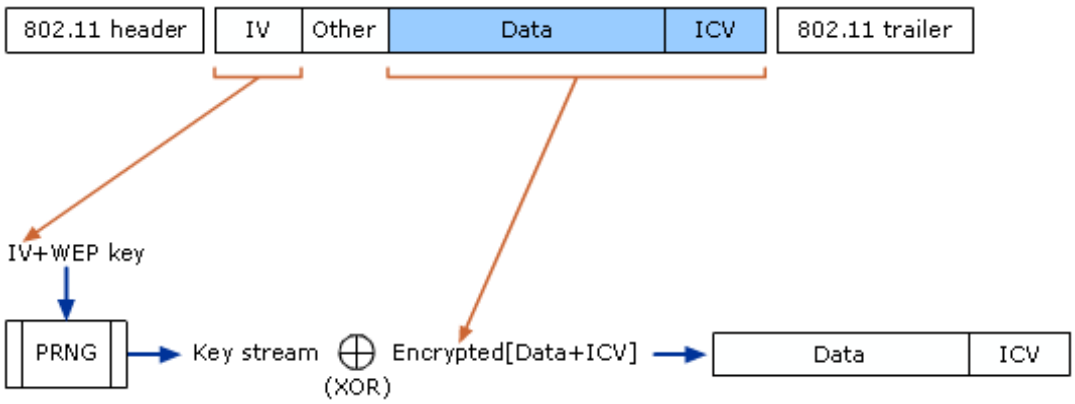
2.4 Vulnerabilidades

Nesta seção serão apresentadas as principais vulnerabilidades do protocolo WEP.

2.4.1 Vulnerabilidades relacionadas à Chave compartilhada

Primeiramente, o tamanho da chave estática é muito pequena. A primeira versão do WEP utilizava chaves de 40bits, tamanho esse que, apesar de suficiente para inibir ataques de força bruta com o poder computacional da época, rapidamente se tornou muito pequena e de fácil quebra. Mais tarde, os fabricantes de dispositivos IEEE 802.11 criaram o WEP com chave estática de 104 e 232 bits, inviabilizando novamente ataques de força bruta. Outro problema é que a chave estática deveria ser trocada frequentemente para garantir que a rede permaneça minimamente segura, mas já que a troca de chaves deve ser feita manualmente em cada um dos dispositivos de rede, essa prática torna-se inviável.

Figura 5- Decriptação de um pacote WEP



Outro problema relacionado à chave compartilhada, é em relação à parte dinâmica da chave, o IV (*Initialization Vector*). O IV possui somente 24 bits, fazendo com que existam apenas 16,777,216 (2^{24}) diferentes vetores, e logo, 2^{24} diferentes *keystreams.* O IV também é enviado em texto plano junto à mensagem, como mencionado previamente. O WEP não especifica como o IV deve ser escolhido, somente que ele deve ser diferente em cada pacote. Alguns vendedores optam por começar o IV com 0 e incrementá-lo a cada novo pacote. Outras implementações optam por escolher o IV aleatoriamente. Apesar dessa última implementação parecer uma boa idéia, com um IV escolhido aleatoriamente, há 50% de chance de ocorrer um reuso do IV após 5000 pacotes [7]. Caso duas mensagens sejam criptografadas com o mesmo *keystream*, o XOR das duas cifras produzem o XOR das duas mensagens originais, fazendo com que o atacante possa inferir informações sobre o conteúdo das duas mensagens, e em alguns casos, obter o

conteúdo exato da mensagem. É importante notar que quantos mais colisões de IV ocorrerem, mais fácil será para um atacante analisar estatisticamente o conteúdo das mensagens originais.

2.4.2 Vulnerabilidades relacionadas à autenticidade, integridade e confidencialidade

A autenticação por Chave Compartilhada é ineficaz em evitar que terceiros que não possuam a chave compartilhada entrem na rede. Por o RC4 utilizar uma cifra de fluxo e ser linear, caso um atacante consiga interceptar o texto-desafio e a cifra enviada pelo cliente durante o processo de autenticação, o mesmo poderá fazer um XOR entre essas duas informações e obter um *keystream* válido. Esse *keystream* pode então ser utilizado para gerar uma resposta válida para qualquer texto-desafio gerado pelo ponto de acesso, autenticando qualquer atacante sem conhecimento da chave WEP.

O WEP utiliza o CRC-32 para garantir a integridade de seus pacotes. Mas devido ao fato de que CRC é uma função linear, um atacante pode modificar arbitrariamente uma mensagem criptografada, modificando o ICV de tal forma que a mensagem parecerá autêntica aos olhos do remetente e do destinatário [2].

O RC4 é composto de duas funções, o PRGA (*Pseudo-random generation algorithm*) e o KSAx (*Key-scheduling algorithm*). O KSA possui duas vulnerabilidades bastante notáveis [4], que são utilizadas em ataques estatísticos para recuperação da chave WEP estática.

2.5 Ataques ao WEP

Nesta seção serão apresentados os principais ataques ao protocolo WEP. Todos os ataques descritos nessa seção são possíveis devido à vulnerabilidades inerentes ao protocolo, portanto não existe mecanismos pera mitigar esses ataques, esse protocolo está obsoleto e não deve mais ser utilizado.

2.5.1 O ataque FMS

Em 2001, Fluhrer, Mantin e Shamir publicaram o primeiro ataque de recuperação de chaves contra o WEP [8], explorando uma vulnerabilidade no KSA do RC4. Um atacante que escute passivamente ao tráfego WEP pode armazenar vários pacotes crioptografados e seus respectivos IVs. O problema é que, como vimos anteriormente, a chave usada para gerar o

keystream é formada pelo IV e pela chave WEP estática. Como o IV é transmitido em texto plano, para que o destinatário possa decifrar a mensagem, o atacante possui os 3 primeiros bytes (24 bits do IV) de toda a chave RC4 usada como *seed* para gerar o *keystream*. Para casos onde os quadros capturados foram cifrados com IVs que possuem o padrão (B+3, 255, N) para $0 \leq B < 13 \forall N$ [4]. Após uma quantidade suficiente de quadros com IVs respeitando o padrão seja capturado, o byte $\mathrm{K}[\mathrm{B}+3]$ da chave utilizada no KSA pode ser encontrada. para se recuperar a chave secreta são necessários cerca de 4 milhões de pacotes caso o contador de IVs seja do tipo *little endian*, e aproximadamente 1 milhão de pacotes caso o contador seja do tipo *big endian*.

2.5.2 Os ataques de KoreK

Já em 2004, KoreK publicou o que muitos consideram como uma generalização do ataque FMS. KoreK publicou a implementação de uma ferramenta, com 17 ataques, para quebra do WEP em um fórum na internet [9]. KoreK utilizou 16 novas correlações entre os primeiro *n* bytes de uma chave RC4, os primeiros 2 bytes to *keystream* resultante, e o próximo byte da chave $K[n]$. Os ataques KoreK necessitam de aproximadamente 700 mil quadros para recuperar a chave secreta com uma probabilidade de sucesso de 50% [10]. O número exato de pacotes muda de acordo com vários fatores, um dos fatores mais importantes é como ocorre a geração do IV (pseudo-aleatoriamente ou incremental).

2.5.3 O ataque PTW

Em 2007, uma nova geração de ataques ao protocolo WEP foram publicados [3][10]. O PTW utiliza uma função descoberta para estimar os bytes da chave secreta, caso o atacante conheça previamente alguns bytes iniciais de uma quantidade “suficiente” de *keystreams* e o respectivo IV.

Para se obter os bytes necessários do *keystream,* o atacante precisa capturar requisições e respostas ARP criptografadas pelo WEP. Os pacotes ARP têm tamanho fixo, e são facilmente distinguíveis de outros tráfegos já que o WEP não esconde o tamanho dos pacotes. Os primeiros 16 bytes de umma requisição ARP são sempre os mesmos. Os primeiros 8 bytes correspondem ao cabeçalho LLC (*Logical Link Control*), enquanto os outros 8 bytes são os primeiros bytes do pacote ARP em si. O cabeçalho LLC é fixo para todo pacote ARP (AA AA 03 00 00 00 08 06) e os 8 primeiros bytes iniciais do pacote ARP também têm um valor fixo, “00

01 08 00 06 04 00 01”. A única diferença em um pacote de resposta ARP é que o último byte tem o seu valor mudado para “02”. Também é fácil distinguir entre os dois tipos de pacote ARP, as requisições ARP são sempre enviadas para broadcast, enquanto as resposta são sempre enviadas para um endereço específico, e o protocolo WEP não criptografa esses endereços. Um atacante então basta fazer um XOR entre o pacote ARP capturado e esses 16 primeiros bytes, o atacante então obtém os primeiros 16 bytes do *keystream*. O PTW possui 50% de chance de recuperar uma chave WEP de 104 bits usando menos de 40.000 pacotes. Para recuperar a chave em 95% dos casos, são necessários 85.000 pacotes. Uma otimização do PTW [4] consegue obter o *keystream* com 50% de chance necessitando apenas de uma média de 24.200 pacotes.

É importante notar que o PTW difere dos ataques anteriores, já que o mesmo não restringe o IV que tem que ser utilizado para se recuperar a chave.

2.5.4 Ataques de Negação de Serviço

Para realizar um ataque de negação de serviço (*Denial of Service - DoS*), o atacante pode forjar pacotes de Desautenticação (*Deauthentication*), usados originalmente pelo ponto de acesso para invalidar a autenticação de um cliente na rede. Em seguida, o atacante pode enviar esses pacotes para um, ou mais, clientes na rede. Um atacante também pode enviar pacotes de *deauthentication* em broadcast para toda a rede. Isso só é possível por que o WEP não criptografa nenhum pacote de gerenciamento.

2.5.5 Ataque ChopChop

Diferentemente dos outros ataques, o ataque ChopChop tem o objetivo de decifrar o conteúdo de uma mensagem sem nenhum conhecimento do *keystream* usado para criptografar a mensagem.

Para realizar o ataque, um atacante tem que primeiramente interceptar o pacote que ele deseja decifrar. Em seguida, o último byte de dados do pacote (último byte antes dos 4 bytes do ICV), deve ser truncado e substituído por um byte com valor entre 0 e 255 (todos os possíveis valores para 1 byte). Devido ao fato que o CRC-32 é linear, o atacante então deverá modificar o ICV com o intuito de tornar a mensagem novamente válida. Por fim, o atacante deve enviar o pacote modificado ao ponto de acesso. Caso o ponto de acesso receba um pacote de um cliente não autenticado (neste caso, o atacante), o mesmo deve retornar uma mensagem de

erro, mas caso nenhuma mensagem de erro seja retornada, isso indicará que o byte escolhido não está correto, já que a maioria dos pontos de acesso rejeitam silenciosamente pacotes que estejam com o ICV errado, o atacante deve escolher um novo valor para o byte modificado e tentar novamente. Caso o ponto de acesso considere o pacote válido, nenhuma mensagem de erro será retornada, e o pacote será introduzido na rede, e o atacante terá decifrado o último byte da mensagem. O mesmo processo pode ser feito para o restante dos bytes. Em média, são necessários 128 pacotes para decifrar um byte da mensagem, e no máximo 256 pacotes.

2.6 Resumo

O WEP foi criado de maneira emergencial com o objetivo de prover a segurança das redes cabeadas à redes Wi-Fi. Mas a falta de conhecimento de segurança dos criadores desse protocolo o tornaram alvo de vários ataques. Em 2001, FMS mostrou que eram necessários de 1 a 4 milhões de pacotes para recuperar a chave compartilhada. Já em 2004, Korek reduziu o número necessário de pacotes para apenas 700.000. Também nesse ano, o ataque de ChopChop foi publicado, ataque esse que tornava possível a decifragem de mensagens sem o conhecimento da chave compartilhada. Em 2007, PTW mostra que eram necessários em média 24.000 pacotes para decifrar a chave compartilhada, tornando o WEP obsoleto.

Este capítulo apresentou um estudo aprofundado do WEP, analisando as suas vulnerabilidades e ataques desenvolvidos contra esse protocolo.

3. WPA

Com o fracasso do WEP, um grupo de trabalho do IEEE 802.11 iniciou pesquisas para o desenvolvimento de um novo padrão seguro que substituiria o WEP, o 802.11i. Enquanto o padrão 802.11i não era concluído, a associação internacional Wi-Fi Alliance desenvolveu, em 2003, um protocolo chamado WPA (Wi-Fi Protected Access) [11]. O intuito do WPA era prover mais segurança do que o WEP, porém sem que grandes alterações nos hardwares (pontos de acesso e placas de rede) precisassem ser feitas. O WPA foi desenvolvido baseado no RC4 e em uma versão preliminar do IEEE 802.11i.

Este capítulo apresenta um estudo da autenticidade, integridade e confidencialidade do WPA, bem como as suas vulnerabilidades, ataques e defesas contra esses respectivos ataques (quando existirem).

3.1 Autenticidade

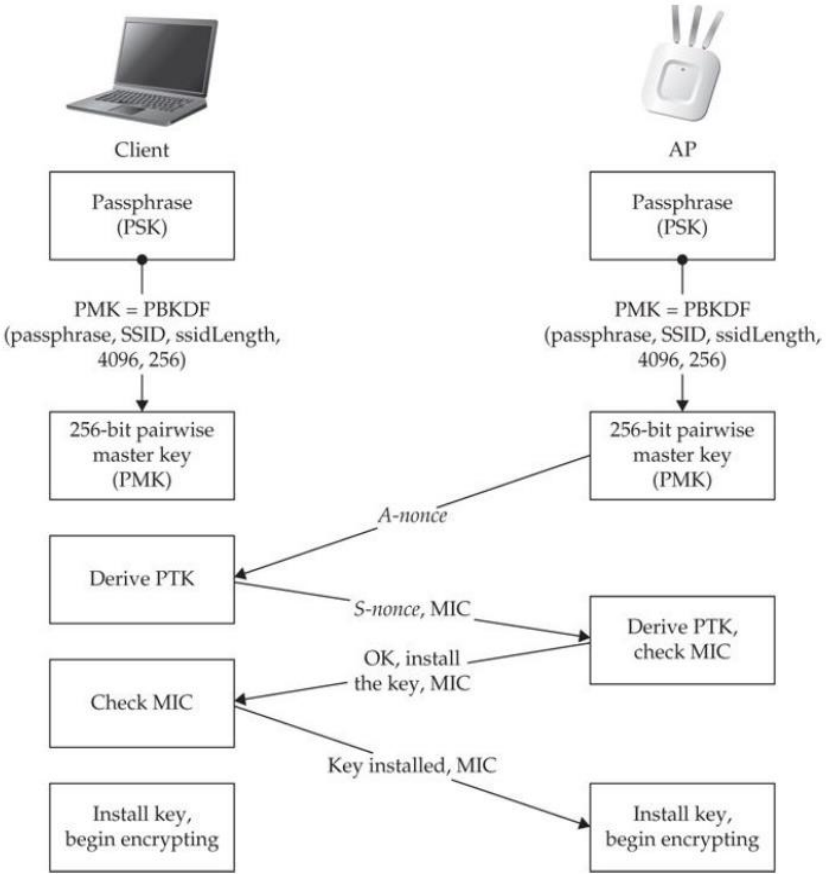
Há dois tipos de autenticação no WPA, o WPA Pessoal (*Personal*) e o WPA Corporativo (*Enterprise*). O primeiro é projetado para redes domésticas ou pequenas empresas, enquanto o segundo foi desenvolvido para empresas de maior porte.

O WPA *Personal* utiliza uma chave conhecida como PSK (*Pre-Shared Key*), possui de 8 a 63 caracteres e é previamente compartilhada entre o AP e os usuários para que ocorra a autenticação. O WPA *Personal* também é conhecido como WPA-PSK devido ao uso da chave para autenticação.

O processo de autenticação, também conhecido como *4-way-handshake*, começa com o ponto de acesso (AP) e o cliente derivando a PMK (*pairwise master key*). A PMK é derivada utilizando o *passphrase*, SSID (*service set identifier*) e o tamanho do SSID como entradas para a função PBKDF. Após a PMK ser derivada no cliente e no AP, os dois irão negociar uma nova chave temporária, chamada PTK (*pairwise transient key*). Essas chaves temporárias são criadas dinamicamente toda vez que um cliente se conecta, e são mudadas periodicamente. A PTK depende da PMK, de um número aleatório enviado pelo AP (chamado de *A-nonce*), de outro número aleatório, dessa vez enviado pelo cliente (chamado *S-nonce*) e dos endereços MAC do

cliente e do AP. Essas chaves temporárias utilizam muitas variáveis como entrada para garantir que as chaves sejam únicas e nunca se repitam. Para verificar que o cliente realmente possui a PMK correta, o AP checa o MIC (*Message Integrity Code*) enviado pelo cliente. O MIC é um hash criptográfico do pacote (junto com a PTK/PMK) que é usado para prevenir que o pacote seja adulterado. Se o MIC estiver incorreto, significa que o PTK e o PMK estão incorretos, já que a PTK é derivada da PMK. O cliente repete o processo de checagem do MIC enviado pelo AP para garantir que o mesmo também possui a PMK. É importante notar que após a PTK ser gerada, o AP também envia ao cliente uma GTK (*Group Temporal Key*), que será utilizada para criptografar mensagens enviadas para *broadcast* e *multicast*. A GTK é trocada toda vez que um cliente sai da rede, ou quando a mesma expira. A figura 6 ilustra o processo de autenticação de um cliente com um ponto de acesso que utiliza WPA-PSK.

Figura 6 - Processo de autenticação no WPA-PSK



Já no WPA *Enterprise*, a PMK é criada dinamicamente para cada cliente que se conecta. Caso um atacante consiga recuperar uma PMK, o mesmo só conseguirá se passar por um dos usuários da rede, e durante aquela conexão específica. No WPA *Enterprise* a PMK é criada em um servidor de autenticação, e repassada para o cliente. Esse servidor de autenticação utiliza o protocolo de autenticação 802.1X, protocolo originalmente desenvolvido para autenticação em redes cabeadas, em conjunto com algum tipo de EAP (*Extensible Authentication Protocol*).

O EAP é um protocolo de rede desenvolvido para "carregar" protocolos de autenticação. Esse protocolo permite que dispositivos, como o AP, sejam ignorantes em relação a detalhes da autenticação que está ocorrendo entre o servidor e o cliente.

O AP e o servidor de autenticação (normalmente um servidor RADIUS) se comunicam através de mensagens EAP e nesse cenário, o servidor de autenticação é quem autentica o cliente, e não o AP, com isso, o ponto de acesso se comporta apenas como um intermediário entre o cliente e o servidor de autenticação.

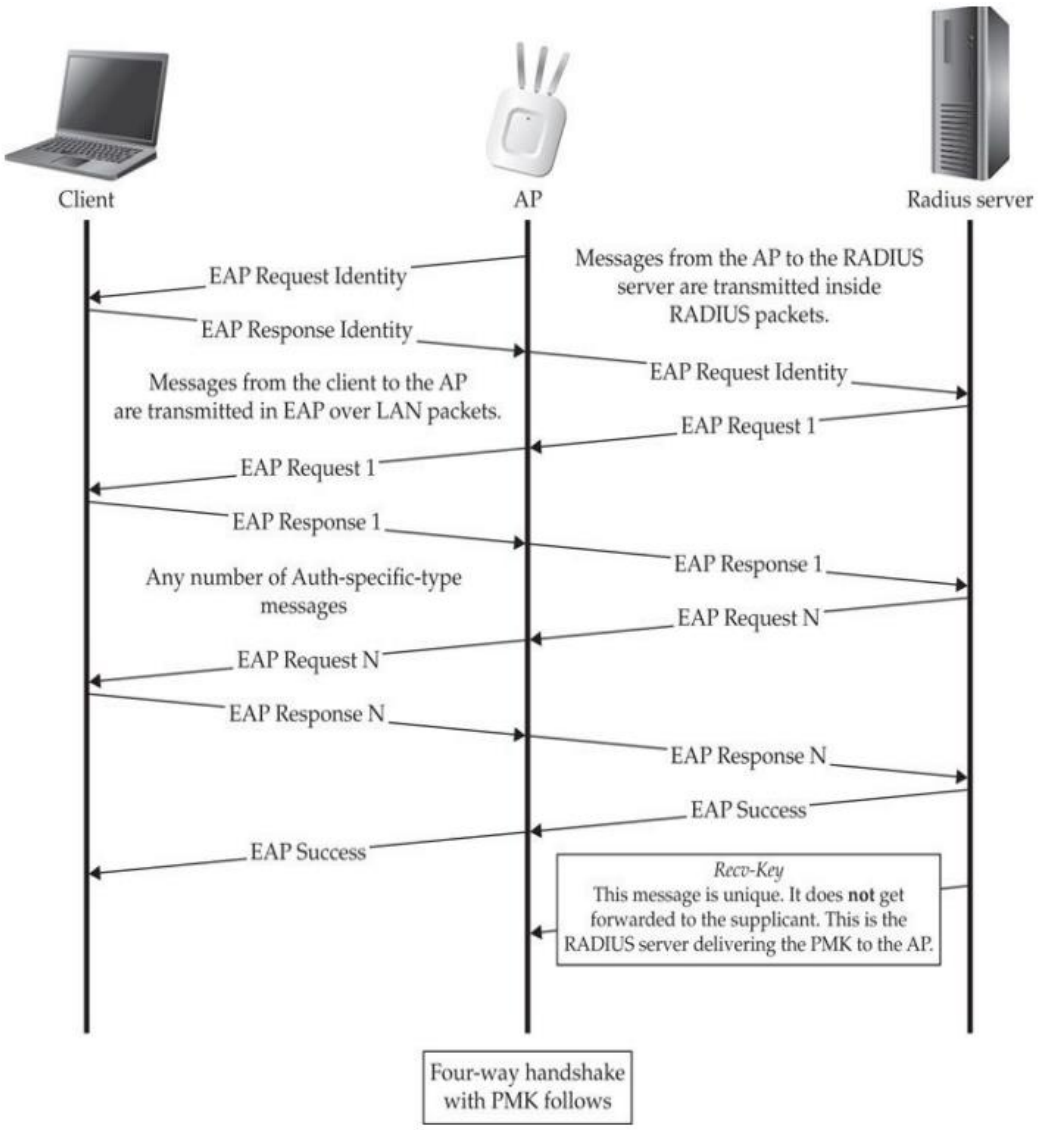
Caso a autenticação seja confirmada, o cliente e o servidor de autenticação derivarão a mesma chave PMK. O servidor então deverá enviar a PMK ao AP, para que o mesmo possa fazer o *4-way-handshake* (igual ao ilustrado na figura 3.1) com o cliente. Esse processo confirma que o AP e o cliente possuem a mesma PMK, e poderão trocar mensagens sem nenhum problema. Como as chaves PMK são criadas dinamicamente, o AP terá que guardar a correspondência entre o usuário e a PMK. Os detalhes de como uma PMK é gerada varia de acordo com o servidor de autenticação utilizado, mas é importante que os dois lados consigam gerar uma PMK que seja um número aleatório e criptograficamente seguro. A figura 7 ilustra o processo de autenticação de um cliente com um ponto de acesso (e servidor de autenticação) que utiliza WPA *Enterprise*.

3.2 Integridade

O WPA utiliza dois mecanismos para garantir a integridade de suas mensagens. O primeiro é o ICV, previamente utilizado pelo WEP. O segundo é o MIC (*Message Integrity Check*), gerado a partir da função hash conhecida como *Michael* passando como entrada a chave *TMK*, os endereços MAC (*Medium Access Control*) do remetente e do destinatário da mensagem, e os dados da mensagem propriamente ditos. Os 4 bytes gerados pelo CRC-32 e os 8 bytes do

MIC compõem os mecanismos de integridade do WPA. A figura 8 ilustra os mecanismos de integridade do WPA.

Figura 7- Processo de autenticação no WPA Enterprise



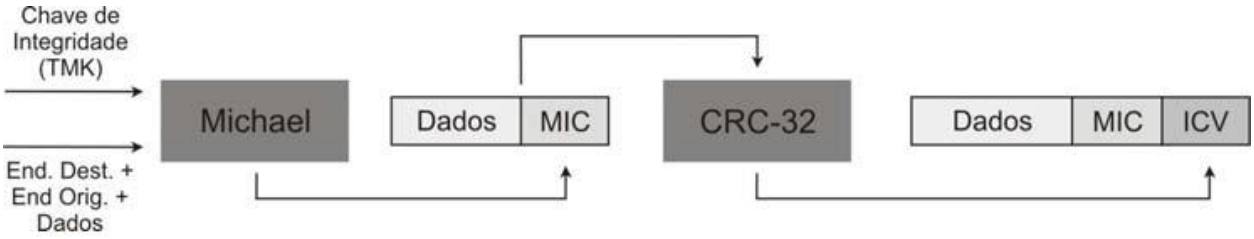
3.3 Confidencialidade

Para fornecer confidencialidade, o WPA utiliza um protocolo conhecido como TKIP (*Temporal Key Integrity Protocol*). O TKIP é um conjunto de algoritmos criado para solucionar

boa parte das vulnerabilidades do WEP. O protocolo foi criado para encapsular o WEP, fazendo com que dispositivos de rede que sejam compatíveis com WEP, também sejam compatíveis com o TKIP. Esse protocolo utiliza chaves temporais que são utilizadas por um período de tempo, e depois substituídas dinamicamente.

Para mitigar o risco de alteração de pacotes e ataques de *man-in-the-middle* , o TKIP introduziu um novo IV (*initialization vector*). Esse novo IV possui 48 bits, é dinâmico, e atua como um contador de quadros conhecido como TSC (*TKIP Sequence Counter*), incrementado a cada quadro criptografado, e zerado quando uma nova chave é gerada. Caso o destinatário receba um quadro com o TSC fora de ordem, esse é descartado imediatamente.

Figura 8 - Integridade no WPA



Apesar de ainda usar o RC4, a principal diferença entre a codificação no WEP e no WPA é como a chave utilizada para produzir o *keystream* do RC4 é gerada. Essa chave é o resultado de um algoritmo de combinação cuja entrada é uma chave temporal de 128 bits, o TSC (IV) de 48 bits e o endereço MAC do transmissor de 48 bits [12]. A chave resultante é então passada, junto ao IV, para o RC4, e o processo de codificação ocorre conforme visto no WEP. A figura 9 ilustra os mecanismos de confidência do WPA.

3.4 Vulnerabilidades

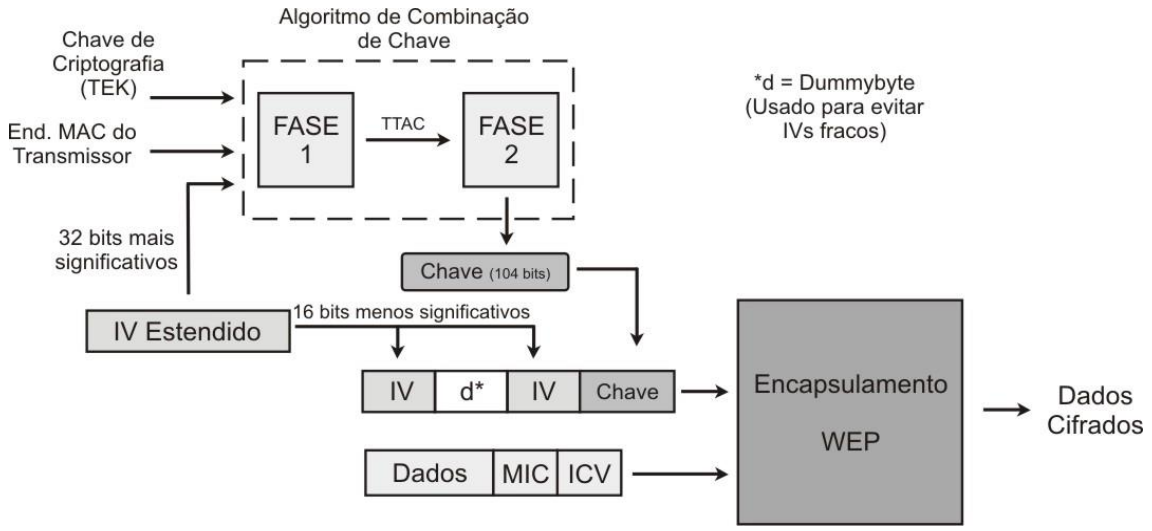
Nesta seção serão apresentadas as principais vulnerabilidades do protocolo WPA.

3.4.1 WPA-PSK vulnerável a ataques de dicionário

No modo de autenticação WPA *Personal*, a PSK (*pre-shared key*) é compartilhada por todos os usuários da rede e pelo AP. Como visto anteriormente, a PMK é derivada da combinação da PSK, do SSID, do tamanho do SSID e dos *nonces* enviados pelo AP e pelo cliente. Essa combinação é submetida a uma função de HMAC 4096 vezes para gerar uma chave de 256 bits. O problema é que todas as informações necessárias para gerar essa chave,

nonces e MAC de origem e destino, são enviadas em texto plano durante o *4-way handshake*, com a exceção da PSK. Então, para que um atacante consiga realizar um ataque de dicionário off-line, basta que o mesmo capture os pacotes do *4-way-handshake.* Caso a PSK seja menor que 20 caracteres, é bastante provável que um atacante consiga recuperar a chave da rede [13].

Figura 9- Mecanismos de confidência do WPA



3.4.2 WPA Vulnerável a Negação de Serviço

Assim como o WEP, os pacotes de gerenciamento do WPA ainda são passados em texto plano na rede. Portanto, ainda é possível utilizá-los para realizar ataques de negação de serviço como visto na seção 2.4.3.

Outro ataque de negação de serviço pode ser realizado utilizando o mecanismo de proteção para evitar ataques de força bruta do MIC. O mesmo faz com que o protocolo seja vulnerável a ataques de negação de serviço direcionadas, já que quando dois erros de MIC são detectados em menos de um minuto, o AP altera a chave de integridade e cancela a conexão desse cliente por 60 segundos [4].

3.4.3 WPA Vulnerável a Recuperação de Chave

Em 2004, um ataque teórico de recuperação de chave é proposto contra o WPA [14]. Caso o atacante tenha conhecimento de pelo menos 2 chaves RC4 geradas por IVs, cujos 32 bits mais significativos são iguais, o mesmo poderá recuperar a chave usada para criptografar os dados e a chave de integridade. Esse ataque não é prático pois é extremamente improvável que um atacante consiga interceptar duas chaves RC4 com as condições necessárias para que o ataque ocorra. A complexidade de tempo do ataque também é $O(2^{105})$ tornando-o ainda mais improvável.

3.5 Ataques

Nesta seção serão apresentadas os principais ataques ao protocolo WPA, e mitigações contra esses ataques, quando houver.

3.5.1 O ataque de Beck-Tews

O ataque de Beck-Tews foi o primeiro ataque desenvolvido contra o WPA, o objetivo desse ataque é decifrar o tráfego da rede, semelhante ao ataque ChopChop (seção 2.4.4) [4]. Para que esse ataque tenha sucesso, algumas condições devem ser respeitadas: 1) A rede atacada tem que estar usando o TKIP para comunicação com o AP; 2) O protocolo IPV4 deve estar sendo utilizado, e o range de IP utilizado na rede é, em sua maioria, conhecido pelo atacante (172.21.20.X); 3) Um longo intervalo de reposição de chaves deve estar sendo utilizado pelo TKIP (por exemplo, 3600 segundos); 4) A rede suporta a qualidade de serviço (IEEE 802.11e – QoS) [15].

Primeiramente, o atacante deve capturar o tráfego da rede que o mesmo deseja atacar, até que uma requisição ou resposta ARP criptografada seja capturado. Lembrando que esses pacotes são facilmente distinguíveis dos outros pacotes da rede, por causa do seu tamanho característico. Os endereços IP do remetente e do destinatário também não são protegidos pelo WEP ou pelo TKIP. A maior parte desse pacote é conhecido pelo atacante, exceto os últimos 8 bits do endereço IP do remetente e do destinatário, os 64 bits do MIC e os 32 bits do ICV.

Para descobrir esses bits não conhecidos, o atacante pode realizar um ataque de *ChopChop* modificado [9]. Para isso, um atacante deve executar esse ataque em um canal QoS

diferente do canal em que o pacote foi originalmente enviado. Normalmente haverá um canal com pouco tráfego, onde o contador TSC é relativamente baixo. Quando um byte for descoberto corretamente através do *chopchop*, o TSC não será incrementado e o AP enviará uma mensagem de erro de MIC ao atacante. Caso ele não descubra o pacote na primeira tentativa, o pacote será descartado silenciosamente, e o atacante deve esperar 60 segundos para tentar advinhar novamente (por conta do mecanismo de proteção contra força bruta do MIC). Com pouco mais de 12 minutos, o atacante consegue decifrar os últimos 96 bits (MIC e ICV) do pacote. Para determinar os outros bits desconhecidos (endereços IP), o atacante pode tentar advinhar os valores e compará-los ao ICV que já foi decifrado.

Com o MIC e o conteúdo do pacote decifrados, o atacante pode reverter o algoritmo *Michael* e recuperar a chave MIC (chave de integridade) usada para proteger os pacotes. Isso só é possível pois o *Michael* não é uma *one-way function* e revertê-lo tem o mesmo custo computacional de usar o algoritmo normalmente.

Com a chave de integridade, o atacante poderá gerar um *keystream* de tamanho igual ou menor ao pacote ARP. Esse *keystream* pode ser utilizado para gerar um pacote válido com conteúdo arbitrário. O pacote do atacante poderá ser enviado para todos os canais QoS que possuírem o TSC menor do que o do pacote capturado. Vale salientar que a maioria das redes usa apenas o canal 0 para enviar dados, o que significa que o atacante poderá enviar 7 pacotes para o cliente.

Para causar danos na rede, o atacante poderia, por exemplo, enviar pacotes que alertem um IDS (*intrusion detection system*) que esteja ativo na rede.

Para evitar ataques desse tipo, um administrador de rede pode simplesmente desabilitar o QoS na sua rede, inviabilizando assim o ataque.

3.5.2 O ataque de Ohigashi-Morii

O ataque de Ohigashi-Morii é uma melhoria ao ataque de Beck-Tews em redes WPA-TKIP [16]. Nesse ataque, não é necessário que a rede tenha suporte a qualidade de serviço (IEEE 802.11e – QoS). O ataque consiste em uma junção do ataque de Beck-Tews com um ataque de *man-in-the-middle*. Para isso, o atacante deve ser posicionar fisicamente em um local onde ele possa interceptar os dados entre o cliente e o ponto de acesso. No melhor caso, esse ataque tem a duração de 1 minuto, e tempo médio de 4 minutos.

3.5.3 O ataque de reset no Michael

Em 2010, Beck descobriu que se o estado interno do algoritmo *Michael* chegar a um certo ponto, o algoritmo reseta [17]. A inicialização do Michael define duas palavras que serão usadas como chaves. Todas as palavras de 32 bits geradas pelo Michael serão derivadas dessas chaves (o MIC consiste em 2 palavras geradas pelo algoritmo). Então, caso um atacante consiga injetar um texto arbitrário em um pacote, e adicionar um texto específico que fará com que o algoritmo retorne ao estado original, o pacote será modificado mas o resultado do *Michael* continuará correto [17]. Com isso, esse ataque torna-se ainda mais restritivo que o atacque de Beck-Tews.

Assim como o ataque de Beck-Tews, o ataque se torna inviável caso o QoS não esteja habilitado na rede.

3.5.4 Ataques de dicionário contra o handshake do WPA-Personal

Como foi mencionado na seção 3.4.1, um atacante pode interceptar o *4-way-handshake* do WPA e aplicar um ataque de força bruta contra a PSK.

Um fator que pode contribuir para o sucesso desse ataque, é caso a rede a ser atacada utilize um SSID comumente utilizado (SSID padrão do modem, por exemplo). Já que a parte mais custosa de um ataque de força bruta contra o WPA, são as 4096 vezes que as entradas são submetidas ao HMAC, um atacante pode pré-computar todos os possíveis resultados contra um SSID comumente utilizado, e usar essa tabela para reduzir o tempo necessário para encontrar a PSK. Essas tabelas são conhecidas como rainbow tables e estão disponíveis gratuitamente na internet.

Também é possível utilizar a criptoanálise para construir um dicionário mais específico e eficiente [34]. O autor desse artigo utiliza engenharia social para construir um dicionário baseado em telefones, datas de nascimento, nomes, conseguindo uma taxa de sucesso de 68% em seus ataques.

Para mitigar esse ataque, recomenda-se o que o SSID da rede seja modificado, a fim de que o mesmo não possua uma *rainbow table* disponível. Já o uso de um *passphrase* maior que 20 caracteres elimina a possibilidade, em tempo hábil, de sucesso de um ataque de força bruta contra a PSK.

3.5.5 Ataque ao WPS

Criado em 2006 pela Wi-Fi Alliance, o WPS (*Wi-Fi Protected Setup*) é um padrão de segurança cujo principal objetivo era fazer com que pessoas que entendem pouco de segurança possam utilizar o WPA. Com o WPS, os usuários também poderiam usar longos *passphrases* na sua rede WPA, sem ter que se preocupar em digitar tal *passphrase* quando um novo dispositivo tentar se conectar à rede. Para se conectar a um AP utilizando o WPS, o usuário possuía duas opções: 1) Um botão no AP, que deveria ser acionado quando um novo dispositivo tentasse se conectar à rede; 2) Outra opção de conexão, essa sem precisar de acesso físico ao AP, necessita que os usuários entrem um PIN (*Personal Identification Number*) de 8 dígitos, previamente atribuído ao AP, para se conectarem à rede.

Em 2011, pesquisadores publicaram um ataque de força bruta online no WPS, explorando uma falha na implementação desse padrão. Inicialmente, acreditava-se que por conter 8 dígitos, eram necessários, no pior caso, 10^8 (100.000.000) tentativas para se descobrir esse PIN, número esse que ainda é vulnerável a ataques de força bruta, mas que faria com que ataques de força bruta online demorassem um tempo considerável. Os pesquisadores descobriram que o oitavo dígito do PIN é usado como um *checksum* para os outros 7 dígitos, fazendo com que a complexidade de um ataque de força bruta caia para 10^7 (10.000.000). Outro problema é como o WPS responde a tentativas de conexão. Caso o PIN submetido esteja errado, o WPS responde com dois pacotes NACK (*Negative-acknowledgement*), o primeiro deles para indicar que a primeira metade (os 4 primeiros bytes) está errada, e o segundo NACK referente à segunda metade (3 outros bytes). O problema é que, com isso, um atacante tem conhecimento de quando ele acertou a primeira ou segunda metade do PIN, mudando a complexidade do ataque de 10^7 para $10^4 + 10^3$, ou seja, 11.000 possíveis valores. Nos dias de hoje, é possível descobrir o PIN de um AP que utiliza o WPS em questão de minutos.

É recomendável que o WPS não seja mais utilizado, caso seja necessário o uso de alguma tecnologia do tipo, tecnologias que utilizam NFC *(Near field communication)* para se conectar ao AP já estão disponíveis em alguns APs.

3.6 Resumo

O protocolo WPA foi desenvolvido pela Wi-Fi alliance para proteger as redes IEEE 802.11 enquanto a versão definitiva do IEEE 802.11i não era concluída. O WPA foi desenvolvido com o objetivo de solucionar as vulnerabilidades presentes no WEP e de ser implementado como um update de firmware, para minimizar os custos de implementação do mesmo. Apesar da preocupação com a segurança do protocolo, algumas vulnerabilidades ainda foram descobertas por pesquisadores, tornando o WPA vulnerável a alguns ataques.

Em 2009, os ataques de Beck-Tews e Ohigashi-Morii foram publicados. Esses ataques têm como objetivo decifrar pacotes em redes WPA-PSK sem o conhecimento da chave PSK, semelhante ao ataque ChopChop do WEP. Já em 2010, Beck descobriu que caso um atacante consiga interceptar um pacote e adicionar um texto específico ao mesmo, esse texto poderá fazer com que o algoritmo Michael, responsável pela geração do MIC, retorne ao seu estado inicial, prejudicando a segurança do mesmo. Em 2011, pesquisados publicaram um ataque de força bruta ao PIN do WPS, com no máximo 11.000 tentativas, era possível recuperar o PIN usado pelo WPS para autênticação dos seus usuários.

Este capítulo apresentou um estudo aprofundado do WPA, analisando as suas vulnerabilidades e ataques desenvolvidos contra esse protocolo.

4. WPA2

Em junho de 2004, o padrão IEEE 802.11i, também conhecido como WPA2, foi ratificado pelo IEEE. Como mencionado anteriormente, o objetivo do 802.11i era oferecer mais segurança para redes sem fio, visto que o WEP apresentava diversas falhas na sua segurança.

Muitos dos seus mecanismos de segurança são idênticos ao WPA, já que o mesmo é baseado em uma versão preliminar do 802.11i. Mas diferente do WPA, o WPA2 não pode ser implementado apenas com uma atualização de *firmware*, já que os novos mecanismos de criptografia usados no protocolo, exigem um maior poder computacional da placa de rede.

Este capítulo apresenta um estudo da autenticidade, integridade e confidencialidade do WPA2, bem como as suas vulnerabilidades, ataques e defesas contra esses respectivos ataques (quando existirem). É importante salientar que alguns dos ataques aqui descritos, podem ser aplicados também ao WPA.

4.1 Autenticação

Os dois modos de autenticação no WPA2 são idênticos aos modos de autenticação do WPA descritos na Seção 3.1. A única melhoria do WPA2 em relação ao WPA, na autenticação, é o suporte a *fast roaming* [18].

No WPA, quando um cliente desloca-se de um AP para outro, a troca de mensagens que ocorrerá entre o cliente e o novo AP, para fins de autenticação, pode durar até 1 segundo, o que causaria interrupção em serviços que requerem uma conexão constante (tráfego de voz e vídeo, por exemplo). O WPA2 adicionou dois mecanismos para evitar essa interrupção, o PMK *Caching* e o *Pre-authentication*.

No PMK *Caching*, o AP guarda as informações de autenticação dos clientes autenticados recentemente, para que caso o cliente tente voltar a se associar ao AP, não haja motivo para uma nova autenticação. No *Pre-authentication*, caso a rede possua um AP central que se comunique com diversos APs periféricos, não será necessária uma nova autenticação caso o

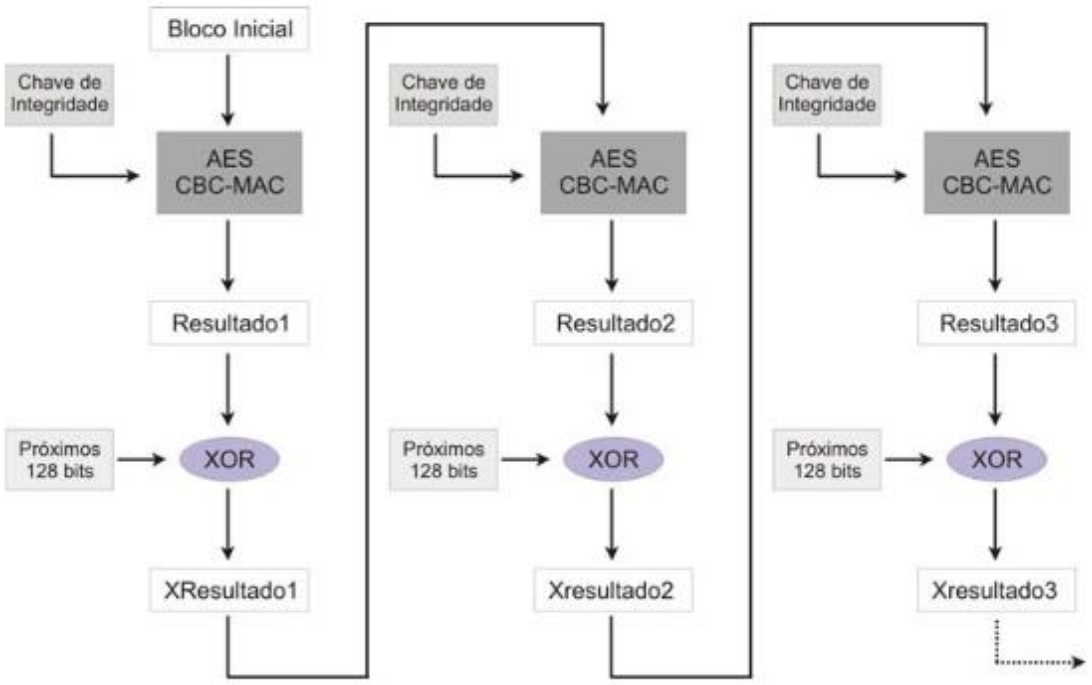
cliente se mova entre dois APs dessa rede. Esses dois mecanismos fazem com que o tempo para se autenticar em outro AP seja 1/10 do tempo no WPA.

4.2 INTEGRIDADE

O WPA2 utiliza o CCMP (*Counter-Mode Cipher Block Chaining Message Authentication Code Protocol*) para proporcionar a integridade e a confidencialidade aos seus quadros. A parte do CCMP que garante integridade é o CBC-MAC (*Chaining Message Authentication Code*) [19].

O CBC-MAC é um algoritmo utilizado para gerar um código de autenticação de mensagem de uma cifra de bloco, ao contrário da cifragem bit a bit utilizada nos protocolos anteriores. Nesse caso, a cifra de bloco utilizada é baseada no AES *(Advanced Encryption Standard*) e o modo de operação utilizado é o CCM (*Counter with CBC-MAC)* [19] cujas chaves e blocos são de 128 bits. O funcionamento do CBC-MAC é ilustrado na figura 10.

Figura 10 - Funcionamento do CBC-MAC



O processo do CBC-MAC pode ser dividido em duas etapas que serão repetidas até que todos os blocos do quadro sejam utilizados. Inicialmente, um bloco inicial de 128 bits e a chave de integridade são passados ao CBC-MAC, gerando uma saída de 128 bits. Na segunda etapa,

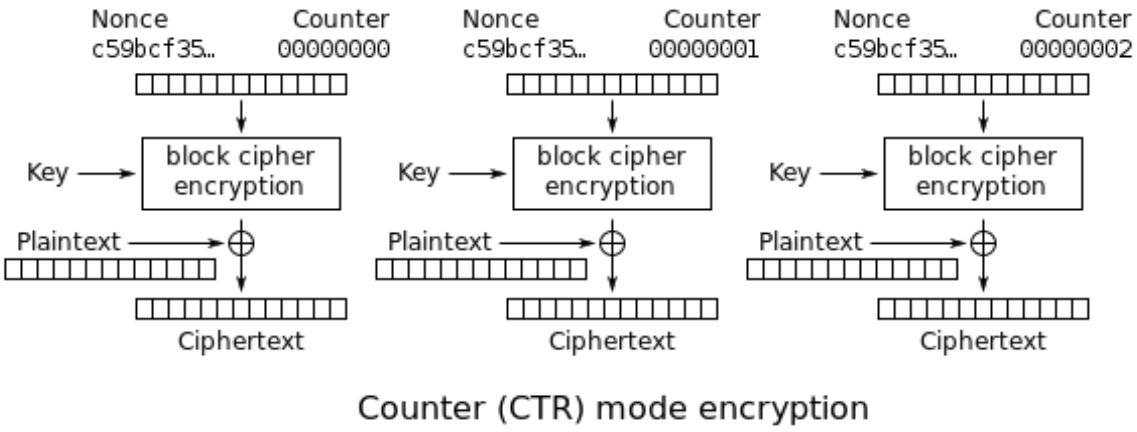
um XOR será realizado entre os 128 bits gerados na etapa anterior e os próximos 128 bits do quadro. Esse bloco resultante será submetido ao CBC-MAC, e as duas etapas anteriores se repetem até o último bloco de 128 bits do campo de dados do pacote. No final do processo, os 64 bits mais significativos do resultado são colocados no campo MIC.

4.3 Confidencialidade

Assim como no WPA, o WPA2 também é baseado no conceito de chaves temporais. Para prover confidencialidade, o WPA2 utiliza um algoritmo chamado AES *Counter Mode* (*CTR*). A chave de criptografia de dados, assim como a de integridade, também possui 128 bits. O IV usado também tem 48 bits, assim como no WPA.

A figura 11 ilustra o modo de operação do CTR. Primeiramente, um contador aleatório é cifrado utilizando a chave de criptografia. Em seguida, um XOR é realizado entre o resultado dessa operação e 128 bits de texto plano a ser criptografado. O resultado desse XOR é o bloco criptografado. Esse processo é repetido até que todos os blocos de 128 bits teham sido criptografados. Uma das vantagens desse método, além de prover mais confidência que o TKIP, é que o mesmo pode ser paralelizado.

Figura 11- AES Counter Mode



4.4 Vulnerabilidades

O WPA2 corrigiu a grande maioria das vulnerabilidades presentes no WEP e no WPA. O ataque de Beck-Tews, por exemplo, se tornou inviável, já que a integridade e a confidência providos pelo CCMP são muito maiores do que no TKIP.

Uma característica que o WPA2 não corrigiu foi o fato de que os quadros de gerência e de controle ainda são passados em texto plano, permitindo que o WPA2 seja vulnerável aos mesmos ataques de DoS que o WPA. A vulnerabilidade do WPA, descrito na Seção 3.4.2 ainda é aplicável ao WPA2.

O WPA2-PSK também se encontra vulnerável a ataques de dicionário, pois a PSK ainda pode possuir menos de 20 caracteres. Como descrito na Seção 3.4.1, uma chave de menos de 20 caracteres está vulnerável a ataques de dicionário.

4.5 Ataques

Assim como o WEP o WPA2 ainda é passível a ataques de negação de serviço, como descrito na Seção 2.5.4. O WPA2-PSK que utiliza uma chave menor de 20 caracteres também está suscetível a ataques de dicionário, como descrito na Seção 3.5.4. Caso a rede esteja utilizando o mecanismo de WPS, a mesma também é vulnerável ao ataque contra o WPS descrito na Seção 3.5.5.

4.5.1 Ataque de dicionário contra o WPA2 Enterprise PEAP

Como visto anteriormente, o WPA2 Enterprise baseia-se no padrão 802.1x e na utilização do EAP (Extensible Authentication Protocol), viabilizando um conjunto de modalidades de autenticação. Dentre as modalidades disponíveis, pode-se citar: PEAP, LEAP, EAP-TLS, EAP-TTLS. PEAP (Protected EAP) é um método de autenticação bastante utilizado em implementações WPA2 Enterprise. Sua larga lista de dispositivos compatíveis, além das facilidades técnicas de implementação e manutenção, colaboraram para a sua popularização. Tal método permite que usuários ignorem o certificado do servidor RADIUS em tempo de autenticação.

Uma abordagem de ataque bastante conhecida é a captura do Challenge e Response do protocolo MSCHAPv2 (utilizado no PEAP), por meio de um ataque MiTM (Man-in-the-Middle), objetivando a submissão de tais insumos para ferramentas de ataques de força bruta offline. Pra piorar, o MSCHAPv2 não é mais considerado seguro desde 2012, quando um pesquisador

demonstrou que a segurança do MSCHAPv2 se resumia a uma cifra do algoritmo DES [21], algoritmo esse considerado inseguro há muitos anos.

Como solução, empresas que utilizam o WPA2 Enterprise PEAP devem mudar imediamente para o WPA2 Enterprise EAP-TLS, considerado atualmente o mais seguro dos protocolos EAP.

4.5.2 Hole 196

Como detalhado anteriormente, durante a autenticação do WPA e do WPA2, o ponto de acesso gera uma GTK (*Group Temporal Key*) e envia para o cliente. A GTK será usada para criptografar pacotes enviados para *broadcast* e *multicast*.

O Hole 196 [22] não é um ataque de recuperação de chaves, em vez disso, esse ataque tem como objetivo envenenar a tabela ARP (*Address Resolution Protocol*) de um cliente, ou causar uma negação de serviço direcionada. Nesse ataque, o atacante cria um pacote ARP malicioso com o endereço IP do ponto de acesso, e o MAC dele próprio, fazendo com que a vítima associe o endereço IP do ponto de acesso ao MAC do atacante. O atacante então, criptografa esse pacote ARP utilizando a GTK, chave essa que é comum a todos os clientes da rede, e envia diretamente à vítima. Isso ignoraria quaisquer restrições de tráfego configuradas no AP para restringir a comunicação entre clientes da rede, ou a detecção de ataques de *ARP Spoofing* na rede. Ao receber o pacote, a vítima o decifra utilizando a GTK e extrai o pacote ARP malicioso do atacante. Isso fará com que a tabela ARP da vítima relacione o endereço IP do ponto de acesso, com o MAC do atacante. A partir de agora, a vítima enviará todo o tráfego para o AP com o atacante como *gateway* de destino. Quando o AP receber esses pacotes, o mesmo irá decifrar o pacote com a PTK da vítima, criptografar com a PTK do atacante, e enviar o pacote para o mesmo. Esse processo define um ataque de *Man-in-the-middle*. Todo o tráfego da vítima será recebido pelo atacante, e todo o tráfego não criptografado da vítima estará exposto ao atacante.

Não há mitigação contra o Hole 196, o mesmo é possível devido a uma vulnerabilidade inerente ao protocolo.

4.5.3 Ataque de dicionário online paralelo contra o WPA2-PSK

Como visto na seção 3.5.4, uma rede IEEE 802.11 que utiliza o protoclo WPA2-PSK, está suscetível a ataques de dicionário offline, para isso um atacante deve capturar o *4-way-handshake* e submetê-lo a uma ferramenta de força bruta. O problema é que caso uma rede não possua clientes conectados, esse ataque torna-se inviável, já que o atacante não terá como capturar um *4-way-handshake* válido.

Ataques de dicionário online são a solução para esse problema. Nesses ataques, o atacante deve submeter a mensagem dois do *4-way-handshake* para o AP, para tentar descobrir a *passphrase* correta. A questão é que submeter várias *passphrases* para o AP afim de descobrir a senha verdadeira é um ataque bastante inviável, já que o AP leva um tempo relativamente alto para responder a essas requisições.

Nesse ataque [33], os autores criam um grande número de VWC (*Virtual Wireless Client*), clientes virtuais que se comportarão como clientes reais tentando se conectar ao AP. É importante notar que todos os VWCs são criados a partir de uma placa de rede, não havendo a necessidade do uso de múltliplas placas, os VWCs também utilizam endereços MAC diferentes para fazer com que o AP acredite que a autenticação está partindo de um cliente real. Cada VWC tentará se autenticar ao AP enviando a mensagem dois do *4-way-handshake* com uma *passphrase* de um dicionário de senhas. Caso o AP responda com a mensagem três do *handshake*, isso significa que a autenticação foi feita com sucesso, e todos os VWCs são finalizados. Caso isso não ocorra, o VWC é destruído, e um novo VWC é criado. Os autores também mostram que a velocidade do ataque é proporcional ao número de VWCs até um certo *threshold*. Isso ocorre por que a partir de um certo número de clientes virtuais, número esse que varia entre cada AP, o aumento de tráfego na rede diminui a velocidade com que o AP responde aos clientes.

Esse ataque pode melhorar em até cem vezes a velocidade de um ataque de dicionário online comum [33]. No caso de uma rede com múltiplos APs compartilhando um único SSID, esse ataque se torna ainda mais rápido. Esse ataque não possui mecanismos de defesa, já que o mesmo não depende de nenhuma vulnerabilidade. É importante notar que quanto mais *bandwidth* a rede possuir, maior o número de VWCs que poderão ser criados. Caso esse ataque seja realizado em uma rede IEEE 802.11ac por exemplo, muito mais clientes virtuais poderão ser criados, já que a *bandwidth* no IEEE 802.11ac é muito maior do que no WPA2.

4.6 Resumo

O IEEE 802.11i, também conhecido como WPA2, foi ratificado pelo IEEE em 2004. O objetivo desse protocolo era solucionar as vulnerabilidades presentes no WEP e prover uma maior segurança as redes Wi-Fi. Assim como no WPA, ataques de dicionário e de negação de serviço ainda são possíveis no WPA2.

Em 2012, dois ataques práticos bastante impactantes foram publicados contra o WPA2. O primeiro ataque explora uma vulnerabilidade no MS-CHAPv2, algoritmo esse utilizado pelo protocolo WPA2 Enterprise PEAP. Nesse ataque, o *challenge* e o *response* do PEAP são capturados e submetidos a um ataque de força bruta, cujo objetivo é descobrir a chave de 56 bits utilizada pelo algoritmo DES do MS-CHAPv2. Com o *hardware* apropriado, o *hash* do *password* utilizado no WPA2 Enterprise PEAP pode ser descoberto em apenas 23 horas.

Já em 2015, uma melhoria aos tradicionais ataques de dicionário foi publicada. Nesse ataque, os autores utilizam clientes virtuais para simular tentativas de conexão a uma rede WPA Personal. Os autores conseguiram melhorar a velocidade de um ataque de dicionário em até 100 vezes.

Este capítulo apresentou um estudo aprofundado do IEEE 802.11, analisando as suas vulnerabilidades e ataques desenvolvidos contra esse protocolo.

5. Quadros de Controle e de gerenciamento

Esse capítulo apresenta um estudo do IEEE 802.11w, emenda do padrão IEEE 802.11 que aumenta a segurança dos quadros de gerenciamento, e dos mecanismos propostos na literatura para a segurança dos quadros de controle para redes Wi-Fi.

O IEEE 802.11w [23] é uma emenda para o padrão IEEE 802.11 cujo objetivo é melhorar a segurança dos quadros de gerenciamento dessas redes. Quadros de gerenciamento nas redes IEEE 802.11, podem ser utilizados para gerar ataques de negação de serviço contra usuários autenticados na rede.

Apesar dos quadros de controle serem tão importantes quanto os quadros de gerenciamento, já que os mesmos também podem ser utilizados para gerar ataques de DoS (*Denial of Service*), não há nenhum planejamento público por parte do IEEE de adicionar um mecanismo de segurança para proteger esses quadros.

Nesta seção analisaremos o mecanismo desenvolvido na emenda IEEE 802.11w para prover melhor segurança aos quadros de gerenciamento e as propostas existentes na literatura para segurança dos quadros de controle.

5.1 Segurança dos quadros de Gerenciamento : 802.11W

Como visto anteriormente, os quadros de gerenciamento do padrão IEEE 802.11 são passados em texto plano na rede, viabilizando ataques de negação de serviço (DoS). Além disso, as emendas 802.11v, 802.11r, 802.11k usam os quadros de gerenciamento para outras funções além dos utilizados no WPA2 (IEEE 802.11i), aumentando ainda mais a importância no desenvolvimento de algum tipo de proteção para os quadros de gerenciamento.

O IEEE 802.11w é uma emenda aprovada para o padrão iEEE 802.11 para “aumentar” a segurança dos quadros de gerenciamento. O mecanismo desenvolvido nessa emenda foi o BIP (*Broadcast/Multicast Integrity Protocol*).

O BIP tem como objetivo prover integridade e proteção contra a reinjeção de quadros de gerenciamento nas redes IEEE 802.11. O BIP utiliza o algoritmo AES-128-CMAC com uma nova chave de 128 bits chamada de IGTK (*Integrity Group Temporal Key*), chave essa criada durante o *4-way-handshake*, e um bloco de dados de 128 bits. Apesar da saída desse algoritmo ser um MIC (*Message Integrity Check*) de 128 bits, somente os 64 bits mais relevantes são colocados em um campo chamado MMIE, que será utilizado para prover a integridade dos quadros de gerenciamento. Quando o cliente receber esse quadro de gerenciamento, o mesmo deve gerar o mesmo MIC e comparar ao contido no campo MMIE, caso os dois sejam iguais, o pacote não foi modificado, caso contrário o pacote deve ser descartado imediatamente.

Já para garantir que quadros de gerenciamento não sejam reinjetados na rede, o BIP utiliza um contador chamado de IPN (*IGTK Packet Number*). Esse contador é mantido pelo ponto de acesso e pelo cliente. Quando um quadro é enviado, o cliente deve checar o IPN, que se encontra no campo MMIE, e comparar com o valor que ele possui localmente, caso o IPN recebido seja maior do que o cliente possui, o cliente pode aceitar o quadro, caso contrário, o mesmo deve ser descartado.

5.2 Propostas para prover segurança dos quadros de Controle

Khan e Hasan

Khan e Hasan [24] são os primeiros a publicarem uma solução para proteger os quadros de controle e gerenciamento contra ataques de DoS. Em 2008, ano da publicação dessa pesquisa, o IEEE 802.1 ainda não havia publicado a emenda 802.11w para proteger os quadros de gerenciamento.

O mecanismo proposto usa uma PRF (*Pseudo Random Function*) para gerar um número pseudoaleatório. Esse número é então colocado no campo FCS (*Frame Check Sequence*), campo esse presente em todos os quadros de controle. Originalmente, o campo FCS contém os 32 bits do CRC-32 (*Cyclic Redudancy Code 32 bits*) e é somente utilizado para verificação de integridade. Khan e Hasan propõem que apenas 16 bits sejam usados para prover integridade e os outros 16 bits seriam destinados ao número pseudoaleatório gerado pela PRF. A troca do CRC-32 para o CRC-16 só acarretaria em uma mudança de 0,0015% de diferença na taxa de detecção e isso faria com que o tamanho dos quadros de controle não fosse alterado.

E já que PRF utilizada é baseada na PTK, chave essa usada para autenticação nas redes IEEE 802.11i, um atacante nunca conseguiria forjar uma mensagem válida, sem o conhecimento prévio da PTK. Para quadros *broadcast* ou *multicast*, a GTK seria usada em vez da PTK.

Esse mecanismo fornece proteção para todos os quadros de controle, sem causar uma sobrecarga na rede, já que o mesmo não altera o tamanho dos pacotes. O problema é que a PRF gera um número de apenas 16 bits, tornando essa autenticação consideravelmente fraca. Outro problema que não é tratado por esse mecanismo são os ataques de *replay*, que continuam sendo possíveis.

5.2.1 MYNENI E HUANG

O mecanismo proposto por Myheni e Huang [25] para proteção dos quadros de controle utiliza um MAC (*Message Authentication Code*) em todos os quadros de controle. Primeiramente os autores utilizam o framework IAPP (*Inter-Access Point Protocol*) para criar e distribuir a chave usada para gerar o MAC. Com essa chave, um código de autenticação de mensagem (MAC) é gerado para os quadros de controle. Esse código é gerado utilizando o HMAC e a função criptográfica SHA-1. O motivo pelo qual os autores utilizam o SHA-1 para gerar o MAC foi por que, de acordo com os mesmos, as estações normalmente já têm o SHA-1 implementado nos seus hardwares e softwares.

O MAC de 160 bits gerado por esse mecanismo é então anexado a todos os quadros de controle, junto com um valor sequencial de 32 bits chamado de *"S",* utilizado para evitar ataques de *replay*. Vale salientar que, para reduzar o *overhead* na rede, o campo FCS (*Frame Check Sequence*) é removido dos quadros de controle RTS e CTS, já que o *"S"* também pode ser usado para garantir a integridade dos quadros.

A proposta pode ser considerada um avanço porém em termos de segurança quando comparada à proposta de Khan e Hasan, a mesma apresenta alguns problemas significativos. Primeiramente, a adição de 160 bits a todos os quadros de controle representa um *overhead* considerável, já que alguns quadros de controle possuem apenas 112 bits (ACK e CTS). Outro problema é relacionado ao HMAC SHA-1. Apesar da praticidade em se escolher o HMAC SHA-1 para gerar o MAC, já que o mesmo já está implementado em vários hardwares e softwares, alguns ataques de colisão nesse *hash* podem enfraquecer a segurança do HMAC [26] [27] [28].

5.2.2 JR. E GONÇALVES

O esquema proposto por JR. E Gonçalves, assim como o mecanismo proposto por Myneni e Huang, busca proteger os quadros de controle das redes IEEE 802.11 através de um Código de Autenticação de Mensagem (MAC) e um número sequencial chamado de “NS” [29].

O MAC é gerado através de um CBC-MAC (*Cipher Block Chaining-Message Authentication Code*) e possui 64 bits. A chave utilizada para esse processo de autenticação é a GTK (*Group Temporal Key*), chave essa que, como visto anteriormente, é usada na encriptação de quadros de dados *multicast* e *broadcast*. Já o “NS” é um valor de 32 bits usado para prevenir ataques de *replay*. O campo FCS também é removido da proposta, já que o “NS” também pode ser usado para prover integridade.

Apesar de apresentar um *overhead* pequeno às redes IEEE 802.11 (acréscimo de apenas 64 bits nos pacotes de controle), esse mecanismo apresenta um problema em relação à sua segurança. Caso o CBC-MAC seja usado para autenticar mensagens de tamanho variável, o mesmo se torna suscetível a ataques de extensão [30]. Como os pacotes de controle possuem tamanhos diferentes, a escolha do CBC-MAC não é a mais recomendada.

5.2.3 MALEKZADEH, GHANI E SUBRAMANIAM

Em [31], os autores propõem dois mecanismos para autenticar os quadros de controle. O primeiro deles, chamado de PCF-O2, é baseado no algoritmo original HMAC-SHA-256, gerando um MAC de 256 bits. Já o PCF-M2, que utiliza uma versão modificada do algoritmo HMAC-SHA-256, gera um MAC de 128 bits. Diferentemente dos outros esquemas propostos, o campo FCS não é removido da proposta. Para prevenir ataques de *replay*, o campo *timestamp* de 32 bits é adicionado aos quadros de controle.

Apesar de garantir a segurança dos quadros de controle, o *overhead* de 288 bits, no caso do PCF-O2, ou de 160 bits, no mecanismo PCF-M2, é extremamente expressivo, tornando esses dois mecanismos inviáveis de serem utilizados nesse momento.

5.2.4 FRANÇA NETO

No esquema proposto em [32] o autor utiliza um MAC de 64 bits para prover segurança aos quadros de controle das redes IEEE 802.11. Esse MAC é gerado a partir de uma função pseudoaleatória (PRF), já presente no IEEE 802.11i. Para gerar a chave que será usada para derivar o MAC, uma chave chamada AMK (Authenticity Master Key) é criada, essa chave auxiliar deve ser configurada previamente no AP, e será usada para gerar a ATK (Authenticity Temporal Key), chave temporária de 128 bits que será usada para criptografar os quadros de controle. A PRF que gera a PTK tem como insumos, a AMK, um string fixo com valor "Authenticity key expansion", o endereço MAC do AP e um nonce, ou seja, um número gerado aleatoriamente pelo AP.

A chave ATK é então distribuída para todos os clientes da rede durante uma versão modificada do 4-way-handshake. Para garantir o sigilo dessa chave, a mesma será encriptada com a PTK antes de ser enviada para os todos os clientes.

Para proteger os quadros de controle de ataques de reinjeção, cada nó transmissor possui um contador de 32 bits chamado de TC (Transmission Counter), incrementado a cada quadro enviado. O valor do TC é colocado no campo NS (Number Sequence), campo esse criado para servir de contador para os quadros de controle, evitando assim ataques de replay. Devido à criação do NS, o campo FCS pode ser removido dos quadros de controle, sem prejudicar a segurança dos quadros. Para garantir que um nó não utilize um determinado TC duas vezes com a mesma ATK, e para mitigar ataques capazes de detectar colisões no MAC, essa chave deve ser trocada a cada 24800 mensagens. A renovação da chave ocorre através de um Group Key Handshake alterado.

Para gerar o MAC, o autor utiliza o algoritmo AES-CMAC, usando como insumos o campo MAC do quadro de controle, a ATK e o NS. Para os quadros de controle que não possuem um campo MAC (ACK e CTS), um novo campo TA (Transmitter Address) de 6 bytes é adicionado a esses quadros.

O overhead causado na rede é de 112 bits, para os quadros Ack e CTS, e 64 bits para os demais. Esse esquema é um aprimoramento em relação ao esquema proposto por JR e GONÇALVES, já que o mesmo utiliza o AES-CMAC, algoritmo esse mais seguro do que o CBC-MAC.

5.3 Resumo

Este capítulo apresentou um estudo de mecanismos de segurança para os quadros de gerenciamento e de controle. O IEEE 802.11w, emenda para o padrão IEEE 802.11 tem como objetivo, prover a integridade dos quadros de gerenciamento das redes Wi-Fi. Com essa proteção, ataques de DoS que utilizam os quadros de gerenciamento para tal fim, não serão mais possíveis. Os padrões IEEE 802.11k, IEEE 802.11v e IEEE 802.11k também utilizam os protocolos de gerenciamento para outros fins, aumentando a importância da proteção desses quadros.

Assim como os quadros de gerenciamento, os quadros de controle também podem ser usados para ataques de DoS. Apesar disso, não há nenhum planejamento público por parte do IEEE de adicionar um mecanismo de segurança para proteger esses quadros. Neste capítulo, apresentamos propostas presentes na literatura para criptografar esses quadros. A maioria dessas propostas adicionam um MIC (*Message Integrity Check*) e um contador aos quadros de controle, provendo assim integridade e proteção contra ataques de replay.

6. Conclusões e trabalhos futuros

Este trabalho apresentou um estudo aprofundado dos mecanismos de segurança dos protocolos WEP, WPA e WPA2, além das vulnerabilidades e ataques publicamente conhecidos contra esses protocolos. A emenda IEEE 802.11w, emenda essa responsável por prover mais segurança aos quadros de gerenciamento, também foi analisada. Já em relação aos quadros de controle, como não há nenhuma emenda proposta pelo IEEE para garantir a integridade desses quadros, mecanismos propostos na literatura foram estudados.

O estudo demonstrou que o protocolo WEP se encontra obsoleto e é extremamente inseguro. O mesmo é vulnerável a uma série de ataques proveniente de vulnerabilidades inerentes ao protocolo, ou seja, incapazes de serem mitigados. Esse protocolo não deve mais ser usado para proteger redes IEEE 802.11, já que alguns ataques conseguem recuperar a chave de segurança em questão de minutos.

Devido ao fato do WPA ter sido desenvolvido com o intuito de prover mais segurança a redes Wi-Fi, mas sem que grandes alterações nos hardwares (pontos de acesso e placas de rede) sejam necessários, o mesmo ainda possui vulnerabilidades provenientes do WEP. Além disso, o algoritmo Michael, utilizado para prover integridade aos quadros de dados, contém vulnerabilidades que podem ser exploradas para comprometer a segurança da rede. É recomendável que as redes IEEE 802.11 utilizam o WPA2 (ou IEEE 802.11i) como protocolo de segurança.

O protocolo WPA2 é mais seguro que os anteriores, e é o protocolo recomendável para proteger as redes Wi-Fi atualmente. Uma das grandes melhorias desse protocolo em relação ao WPA, é o fato de que o mesmo é baseado na cifra AES. Apesar disso, o WPA2 ainda possui vulnerabilidades relativas aos seus quadros de controle e de gerenciamento, quadros esses que ainda não são criptografados no IEEE 802.11i.

O estudo do IEEE 802.11w mostra que essa emenda soluciona as vulnerabilidades relacionadas aos quadros de gerenciamento no WPA2. Quando essa emenda for finalmente difundida comercialmente, alguns ataques de DoS que utilizam os quadros de gerenciamento para tal fim, serão inviabilizados. Alguns mecanismos propostos na literatura para prover segurança aos quadros de controle também foram analisados. Aliado ao IEEE 802.11w, esses mecanismos poderiam ser utilizados para inviabilizar todos os ataques de DoS que ainda são possíveis no WPA2.

Em trabalhos futuros poderíamos propor e implementar um esquema para garantir a integridade dos quadros de controle. Também poderíamos analisar o impacto que a emenda IEEE 802.11w pode causar nas redes, assim como analisar as novas emendas IEEE 802.11k, IEEE 802.11r e IEEE 802.11v em relação a possíveis ataques que podem se tornar viáveis, já que essas emendas utilizam quadros de gerenciamento para novos propósitos.

7. REFERÊNCIAS

[1] L. M. S. C. of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Standard 802.11, 1999 Edition, 1999

[2] Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting mobile communications: the insecurity of 802.11." *Proceedings of the 7th annual international conference on Mobile computing and networking*. ACM, 2001.

[3] Tews, Erik, Ralf-Philipp Weinmann, and Andrei Pyshkin. "Breaking 104 bit WEP in less than 60 seconds." *International Workshop on Information Security Applications*. Springer Berlin Heidelberg, 2007.

[4] Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA."*Proceedings of the second ACM conference on Wireless network security*. ACM, 2009.

[5] Vaudenay, Serge, and Martin Vuagnoux. "Passive–only key recovery attacks on RC4." *International Workshop on Selected Areas in Cryptography*. Springer Berlin Heidelberg, 2007.

[6] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[7] Borsc, M., and H. Shinde. "Wireless security & privacy." 2005 IEEE International Conference on Personal Wireless Communications, 2005. ICPWC 2005.. IEEE, 2005.

[8] Fluhrer, Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4." International Workshop on Selected Areas in Cryptography. Springer Berlin Heidelberg, 2001.

[9] Kore, K. "Next Generation of WEP Attacks?." 2004-10-25). http://www. netstumbler. org/showpost. php.

[10] Tews, Erik. "Attacks on the WEP protocol." IACR Cryptology ePrint Archive 2007 (2007): 471.

[11] Alliance, Wi-Fi. "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks." White paper, University of Cape Town (2003): 492-495.
[12] Han, Wei, Dong Zheng, and Ke-fei Chen. "Some remarks on the TKIP key mixing function of IEEE 802.11 i." Journal of Shanghai Jiaotong University (Science) 14 (2009): 81-85.

[13] Moskowitz, Robert. "Weakness in passphrase choice in WPA interface." ICSA Labs (2003).

[14] Moen, Vebjørn, Håvard Raddum, and Kjell J. Hole. "Weaknesses in the temporal key hash of WPA." ACM SIGMOBILE Mobile Computing and Communications Review 8.2 (2004): 76-83.

[15] IEEE-SA Standards Board. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Communications Magazine, IEEE, 2007.

[16] Ohigashi, Toshihiro, and Masakatu Morii. "A practical message falsification attack on WPA." Procedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System. 2009.

[17] Beck, Martin. "Enhanced TKIP michael attacks." arXiv preprint arXiv:1410.6295 (2014).

[18] Arana, Paul. "Benefits and vulnerabilities of Wi-Fi protected access 2 (WPA2)." INFS 612 (2006): 1-6.

[19] Whiting, Doug, Niels Ferguson, and Russell Housley. "Counter with cbc-mac (ccm)." (2003).

[20] Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." (1999).

[21] "DEFCON 20: Defeating PPTP VPNs And WPA2 Enterprise With MS-Chapv2". YouTube. N.p., 2016. Web. 5 June 2016 . <https://www.youtube.com/watch?v=qjBHTS6BKX4>.

[22] Ahmad, S. "WPA too. Hole 196." Presentation from Def Con 18 (2010).

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

[24] Khan, Mansoor Ahmed, and Aamir Hasan. "Pseudo random number based authentication to counter denial of service attacks on 802.11." 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN'08). IEEE, 2008.

[25] Myneni, Sushma, and Dijiang Huang. "IEEE 802.11 Wireless LAN control frame protection." 2010 7th IEEE Consumer Communications and Networking Conference. IEEE, 2010.

[26] Contini, Scott, and Yiqun Lisa Yin. "Forgery and partial key-recovery attacks on HMAC and NMAC using hash collisions." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer Berlin Heidelberg, 2006.

[27] Rechberger, Christian, and Vincent Rijmen. "New Results on NMAC/HMAC when Instantiated with Popular Hash Functions." *J. UCS* 14.3 (2008): 347-376.

[28] Kim, Jongsung, et al. "On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1." *International Conference on Security and Cryptography for Networks*. Springer Berlin Heidelberg, 2006.

[29] Corrêa Jr., Marcos, and Gonçalves, P. A. S., "Um Mecanismo de Proteção de Quadros de Controle para Redes IEEE 802.11", In Proceedings of Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), Brasília, November 2011.

[30] Bellare, Mihir, Joe Kilian, and Phillip Rogaway. "The security of the cipher block chaining message authentication code." Journal of Computer and System Sciences 61.3 (2000): 362-399.

[31] Malekzadeh, Mina, Abdul Azim Abdul Ghani, and Shamala Subramaniam. "A new security model to prevent denial-of-service attacks and violation of availability in wireless networks." International Journal of Communication Systems 25.7 (2012): 903-925.

[32] FRANÇA NETO, Ivan Luiz de. "Um esquema de segurança para quadros de controle em Redes IEEE 802.11." (2015).

[33] Nakhila, Omar, et al. "Parallel active dictionary attack on WPA2-PSK Wi-Fi networks." Military Communications Conference, MILCOM 2015-2015 IEEE. IEEE, 2015.

[34] Chen, Chia-Mei, and Tien-Ho Chang. "The Cryptanalysis of WPA; WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method." Information Security (AsiaJCIS), 2015 10th Asia Joint Conference on. IEEE, 2015.

[35] Ghanem, Mohamed Chahine, and Deepthi N. Ratnayake. "Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack a novel re-authentication protocol." 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). IEEE, 2016.