WEP, WPA e EAP

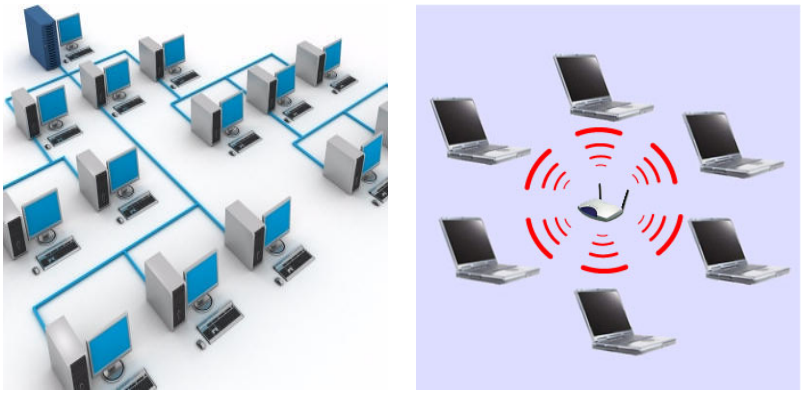
Rodrigo R. Paim

Resumo

O surgimento de redes sem fio foi um marco na área de redes de computadores. Porém, junto com os benefícios que ela proporciona vieram os perigos, tendo em vista que passa a não existir um controle rígido sobre quem terá acesso às mensagens transmitidas. A fim de garantir, entre outros, autenticação e confidencialidade à comunicação sem fio, surgem protocolos para a realização da criptografia dos quadros transmitidos, como o WEP e WPA. Este trabalho objetiva a uma análise destes dois tipos de protocolos citados, com a descrição de funcionamento, além de apontar pontos positivos e negativos de cada um. Por fim, seá abordado brevemente o funcionamento de um mecanismo de autenticação neste tipo de rede que é amplamente utilizado, o EAP.

1 Redes sem fio e segurança

A palavra rede sempre esteve associada a uma abstração de nós conectados através de fios, por meio do qual realizavam a comunicação. Entre os exemplos mais comuns, estão as redes de computadores e de telefonia. Porém, este paradigma, que perdura desde o surgimento do telégrafo, vem sendo substituído gradativamente por uma nova maneira de realizar comunicação sem a necessidade do uso de fios conectando nós, permitindo, portanto, uma maior mobilidade para os usuários.



(a) Redes com Fio (b) Redes sem Fio

Figura 1: Mudança de paradigma das redes comunicação

Esta mudança de paradigma também afetou a maneira como a comunicação é realizada: grande parte das redes com fio realizam unicast (envio para um destino) por padrão, enquanto as redes sem fio transmitem para qualquer ouvinte que estiver perto o suficiente (em broadcast). Assim, teoricamente todos que estão a uma certa distância do aparelho emissor do sinal são capazes de "ouvir" todo o processo de comunicação, algo impraticável quando se deseja confidencialidade. Surge, então, a necessidade de prover segurança aos dados que circulam pela rede sem fio, além de controle de acesso, para que estranhos não usufruam de conexões à Internet privadas.

Existem diversos protocolos implementando algoritmos para segurança em rede; os mais conhecidos e utilizados são o WEP e o WPA, usados, por exemplo, em access points de residências. Estes dois utilizam uma chave que é compartilhada por todos os usuários da rede. Além deles, existe uma

abordagem diferente para tentar solucionar este o problema, sendo implementada pela família de protocolos EAP, onde cada um realiza a autenticação de maneira diferenciada.

2 Wired Equivalent Privacy

O protocolo WEP, sigla de "Privacidade Equivalente à de Redes com Fios", foi o pioneiro no assunto de proteção de redes sem fio, tendo sido lançado como um padrão de segurança neste tipo de rede em 1997. Ele utiliza o algoritmo de criptografia RC4, que é apontado por muitos como seu principal ponto negativo. Mesmo estando obsoleto no quesito segurança, o WEP continua sendo amplamente utilizado em residências de todo o mundo, reflexo da falta de informação dos usuários de redes sem fio e da insistência de fabricantes de pontos de acesso em permitir que ele seja um dos padrões de segurança.

2.1 Algoritmo RC4

O algoritmo de criptografia RC4 foi criado em 1987 por Ronald Rivest, o mesmo criador do RSA e do MD5, e seu funcionamento permaneceu em segredo até o ano de 1994, quando foi vazado em uma página de discussões na Web. Ele possui duas funcionalidades básicas: uma para gerar um "código" que será usado para encriptar e decriptar (KSA) e outra para realizar a criptografia propriamente dita da mensagem com o uso deste código (PRGA).

A função KSA, sigla de Algoritmo Escalonador de Chaves (do inglês "Key Scheduler Algorithm"), é responsável por gerar uma permutação pseudo-aleatória do conteúdo de uma chave secreta. O fato de ela ser pseudo-aleatória se deve à invariância do valor retornado com relação ao tempo, dependendo apenas do valor de entrada. Portanto, é necessária a execução desta função apenas uma vez para a obtenção da permutação que será usada.

A função PRGA, sigla de Algoritmo de Geração Pseudo-Aleatória (do inglês "Pseudo Random Generation Algorithm"), é responsável pela encriptação da mensagem a partir do valor retornado pelo KSA. Ela consiste basicamente de operações de Ou-Exclusivo entre a permutação da chave secreta e a mensagem de entrada, retornando uma mensagem cifrada. Pela lógica de Boole, sabe-se que operações deste tipo são simétricas e, portanto, a aplicação do PRGA na mensagem cifrada gera a mensagem original caso a permutação utilizada seja a mesma do processo de encriptação.

Uma implementação deste algoritmo em C/C++ pode ser encontrada aqui, com chave secreta de 256 bits, correspondendo fielmente ao algoritmo atualmente utilizado para criptografia em redes sem fio domésticas. Repare que o número de operações realizadas é muito pequeno, refletindo a simplicidade do mesmo.

O RC4 é considerado um algoritmo de chave simétrica de cifra de fluxo ("stream cypher") pelo fato de o processo de encriptação e decriptação serem independentes do tamanho da mensagem de entrada. Em contrapartida aos algoritmos de cifra de fluxo, existem os de cifra em bloco, cujo funcionamento requer mensagens de tamanho fixado, geralmente com o comprimento sendo uma potência de 2. A grande vantagem daquele sobre este é a sua simplicidade de implementação, requerendo poucas operações. Contudo, ele peca no quesito segurança, pelo fato de cada bit de saída ser uma função apenas do bit de entrada, enquanto no outro é uma função de todos os bits do bloco original.

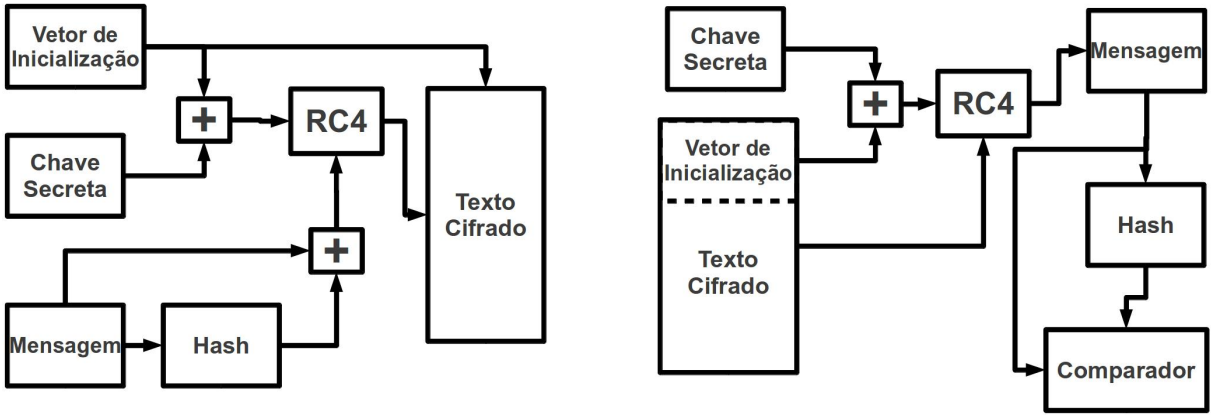
2.2 Funcionamento do WEP

O funcionamento do WEP pode ser dividido em duas partes: autenticação e encriptação/decriptação de mensagens. Ele é todo baseado na troca de quadros encriptados pelo algoritmo RC4. A ordem apresentada seá a inversa da de textos da área: primeiro o processo de troca de mensagens e então, o de autenticação. Esta ordem é mais interessante pelo fato de a autenticação utilizar mecanismos que estão presentes na troca de mensagens.

A compreensão do funcionamento do mecanismo de encriptação/decriptação baseia-se no entendimento do algoritmo RC4. Como detalhe adicional, para garantir maior segurança ao processo, a

permutação oriunda do KSA deve ser diferente a cada mensagem enviada. Para isto, existe um vetor de inicialização pseudo-aleatório que é recalculado a cada iteração do algoritmo e é acrescido à chave secreta. Como quem recebe a mensagem não possui este valor, o mesmo deve ser incluído no texto cifrado que será enviado. Por fim, existe ainda um mecanismo que provê integridade ao conteúdo do texto cifrado que é recebido, tendo em vista que o meio de propagação da mensagem - o ar - é muito suscetível a erros.

A Figura 2(a) demonstra o processo de encriptação da mensagem. Em um primeiro momento, a entidade responsável pelo seu envio calcula o próximo valor da sequência do vetor de inicialização, concatena o mesmo com a chave secreta que ele compartilha com a entidade que receberá a mensagem e calcula o valor da permutação a partir do KSA. Após este processo, ela divide a mensage original de forma que possa caber em um quadro WEP e calcula o valor do hash (a partir da função resumo CRC-32). Em seguida, ocorre a aplicação do algoritmo PRGA sobre o pedaço da mensagem e seu respectivo valor de hash. Por fim, o resultado deste processo é concatenado com o valor atual do vetor de inicialização e finalmente enviado.



(a) Encriptação (b) Decriptação

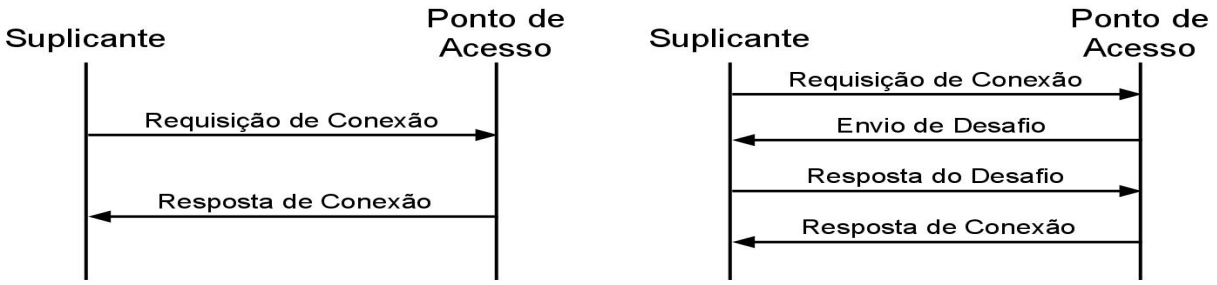
Figura 2: Diagrama de Blocos do Protocolo WEP

A Figura 2(b) apresenta o processo inverso, que é realizado pela entidade que recebe o texto cifrado. Primeiramente, ocorre a separação do vetor de inicialização e da mensagem cifrada. O primeiro é concatenado com a chave secreta que é compartilhada com a entidade que realizou o envio e passa novamente pelo KSA. Com isto, ele calcula a mensagem original acrescida do hash no PRGA, lembrando que esta função é composta de operações de Ou-Exclusivo (sendo, portanto, simétrica). Assim, ele divide o resultado desta função em mensagem original e hash. Por fim, é aplicada a mesma função resumo que fora usada pela entidade que enviou a mensagem e ocorre a comparação com o que recebeu. Caso haja alguma discrepância dos resultados, é solicitado o reenvio do quadro; caso contrário, é enviada uma mensagem de confirmação de recebimento.

Todo o processo enunciado acima supôs que a máquina já possuía algum tipo de mecanismo de comunicação com o ponto de acesso. Para tanto, foi necessária a realização de um processo tipo de autenticação. Existem dois métodos básicos para a realização dele: o modo sistema aberto ("Open System") e o de chave compartilhada ("Shared Key").

O WEP Open System assume que qualquer um que conheça o nome de identificação da rede, ou SSID (do inglês "Service Set Identifier"), é passível de se conectar a ela. Assim, conforme ilustrado na Figura 3(a), a máquina que deseja se conectar deve apenas enviar uma requisição junto com o SSID. Caso ele esteja correto, o access point retorna uma resposta positiva de conexão; caso contrário, uma resposta de negação de conexão é enviada.

Em contrapartida ao WEP Open System, o WEP Shared Key só realiza a conexão de quem possuir



(a) WEP Open System

(b) WEP Shared Key

Figura 3: Métodos de Autenticação do WEP

a chave secreta que o access point possui. Assim, quando for solicitada a conexão na rede por alguma máquina, o ponto de acesso lhe envia uma mensagem com um desafio" composto de um número inteiro aleatório. A máquina deve responder com uma mensagem contendo este número encriptado de acordo com o processo da Figura 2(a). Ao receber a mensagem, o ponto de acesso tenta repetir os passos da Figura 2(b). Em caso de sucesso, isto é, caso o valor decriptado seja idêntico ao original, ele envia uma mensagem confirmando a conexão; caso contrário, há o envio de uma mensagem indicando falha de conexão.

2.3 Falhas

Existem diversas falhas conhecidas há mais de uma década no protocolo WEP. Elas são muitas vezes exploradas por pessoas maliciosas que desejam prejudicar o uso da rede sem fio ou simplesmente obter acesso à Internet. Entre as falhas mais graves, encontram-se a presente no mecanismo de confirmação de recebimento de quadros WEP, a possibilidade de inundação da rede com quadros repetidos e a fragilidade do algoritmo RC4.

2.3.1 Acesso de Estranhos

Dentre os diversos ataques existentes para a obtenção da chave secreta utilizada no WEP, alguns se destacam pela simplicidade e tempo de execução muito baixos, da ordem de minutos:

- *Força Bruta*: A chave secreta do WEP possui 40 bits, valor relativamente alto, mas que, com o uso de ataques de dicionário, isto é, através da utilização de nomes que são comumente utilizados, torna-se plausível sua execução.
- *Conexão*: Durante a conexão de um suplicante ao ponto de acesso, o desafio passa em claro e logo depois encriptado. Assim, é possível ter acesso ao mesmo conteúdo das duas formas, facilitando o processo de obtenção da chave secreta.
- *Escuta*: Existem outros tipos de ataque que conseguem recuperar a chave secreta a partir da escuta do tráfego por alguns minutos, até que o valor do vetor de inicialização se repita.

O maior agravante do processo de encriptação do WEP é a utilização da chave secreta (que não é provisória), em todas as etapas. Assim, a descoberta deste valor significa a utilização da rede até que o mesmo seja trocado pelo administrador da mesma.

2.3.2 Troca de bits

Outro tipo de ataque bastante conhecido no protocolo WEP é a captura de quadros transmitidos e a alteração do conteúdo de alguns deles. A função resumo utilizada como provedora de integridade

(CRC-32) possui um comportamento conhecido para determinados padrões de alteração de bits, o que possibilita alguém mal-intencionado forjar o conteúdo de mensagens.

2.3.3 Inundação

Não existe nenhum tipo de ordem nos quadros transmitidos, isto é, teoricamente não há como saber se um quadro veio fora de ordem. Portanto, um dos ataques mais comuns é o de captura de um e sua retransmissão continuamente, a fim de congestionar o tráfego de alguma máquina especial da rede.

2.4 Evolução

Várias tentativas foram feitas para melhorar o WEP. Porém, elas foram em vão, pois não focaram na essência do principal problema deste protocolo: a maneira como o algoritmo RC4 é utilizado. Todas essas implementações não são nenhum tipo de padrão da indústria, sendo de uso específico de grupos de usuários.

2.4.1 WEP2

Nesta implementação, para tentar diminuir a chance de que algum estranho descubra o valor da chave secreta, seu número de bits foi aumentado e o vetor de inicialização teve seu comprimento dobrado. Porém, isto surtiu pouco efeito, tendo em vista que o problema não se encontra apenas no tamanho da chave, mas na fragilidade do algoritmo como um todo.

2.4.2 WEP+ e WEP Dinâmico

WEP+ e WEP Dinâmico são duas implementações proprietárias do protocolo WEP. A primeira escolhe de maneira mais "inteligente" o valor dos vetores de inicialização, tentando diminuir a chance de um eventual ataque ser bem sucedido. O WEP Dinâmico, porém, muda o valor da chave periodicamente. Contudo, caso o tempo de alteração de valor seja maior que o tempo que leva para a quebra do algoritmo, ele não surte o efeito desejado. Todavia, a ideia por trás desta implementação foi utilizada em parte pelo WPA.

3 Wi-Fi Protected Access

O protocolo WPA, sigla de "Acesso Protegido a Wi-Fi", foi criado em 2002 pela WFA (Wi-Fi Alliance) como postulante a substituto do WEP. Durante a sua concepção, foi dado um enfoque maior na correção das falhas de segurança encontradas neste protocolo. Dentre as melhorias propostas, a mais significativa foi a utilização do algoritmo RC4 de uma forma mais segura, dentro do protocolo TKIP.

Em 2004, a WFA lançou o sucessor do WPA, o WPA2, após a descoberta de algumas falhas de segurança presentes no TKIP. Assim, para tentar contorná-las, ele foi substuído pelo protocolo CCMP, que faz uso de um algoritmo de criptografia simétrica muito robusto e amplamente utilizado, o AES.

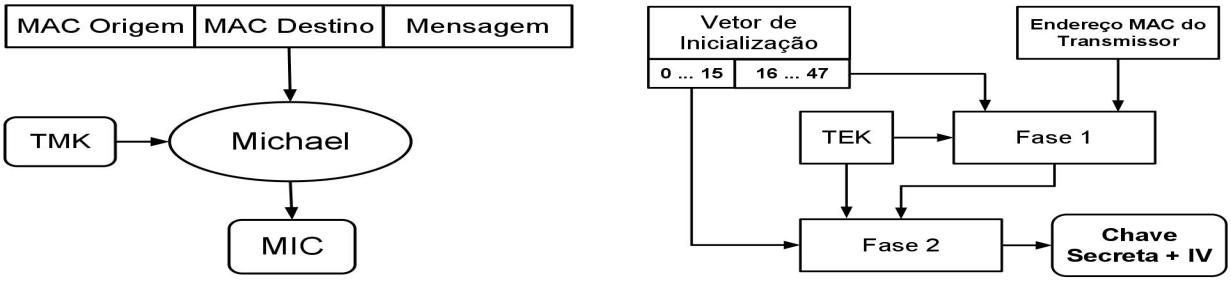
3.1 WPA: Protocolo TKIP

O TKIP, sigla de Protocolo de Integridade de Chave Temporal (do inglês "Temporal Key Integrity Protocol"), é o protocolo usado pelo WPA para encriptação da mensagem transmitida. Ele faz uso do algoritmo RC4, da mesma forma que o WEP, mas toma algumas precauções para evitar ataques, como não enviar a chave secreta "em claro" e trabalhar com uma política de vetores de inicialização mais inteligente.

O WPA funciona a partir de uma chave secreta contendo entre 32 e 512 bits conhecida como PMK, ou Chave Mestra Dupla, que gera uma PTK, ou Chave Transiente de Dupla (do inglês "Pairwise Transient Key"), a partir de alguns parâmetros obtidos durante a conexão, sendo compartilhada entre

o computador e o ponto de acesso. Ela é composta de 512 bits e pode ser dividida em 4 outras chaves de 128 bits - KCK, KEK, TEK, TMK - que são usadas em processos distintos deste protocolo.

No WEP, é possível a alteração do conteúdo de uma mensagem transmitida sem que o receptor perceba alguma mudança. O TKIP impede que isto ocorra através do uso do MIC (também apelidado de Michael), sigla de Código de Integridade de Mensagem (do inglês "Message Integrity Code"). Esta função utiliza metade (em número de bits) do TMK, Chave Temporária do MIC, para o "embaralhamento" do conteúdo da mensagem original, acrescido do endereço MAC de origem e de destino, retornando um valor de 8 bytes após operações de permutação e deslocamento de bits e Ou-Exclusivo. Vale acrescentar, ainda, que na especificação do protocolo, computador local e ponto de acesso usam metades distintas do TMK para cálculo do MIC. Um esquema simplificado do processo pode ser visto na Figura 4(a). A robustez do MIC se encontra no fato de o seu produto final não ter nenhum tipo de correlação com o vetor de inicialização, tornando qualquer tentativa de ataque restrita à força bruta.



(a) Código de Integridade de Mensagem

(b) Algoritmo de Mistura de Chaves

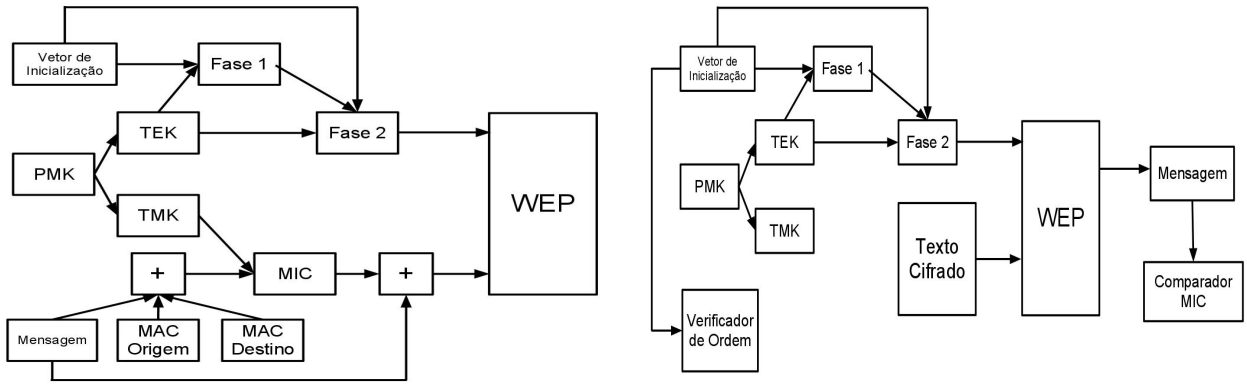
Figura 4: Algoritmos do TKIP

Outra fraqueza do WEP reside no fato de uma terceira pessoa poder capturar um pacote e reenviá-lo por tempo indefinido. A política adotada pelo WPA é muito simples e consiste no uso do vetor de inicialização de 48 bits como um identificador do pacote: o cliente da rede e o ponto de acesso zeram o vetor de inicialização referente à comunicação entre eles quando esta começa e o incrementam a cada novo envio; caso algum pacote chegue com o valor do IV menor do que o último recebido, é sinal de uma tentativa de ataque de repetição e este é ignorado.

Por fim, durante a troca de mensagens, existe uma mistura em duas fases da TEK, ou Chave Temporal de Encriptação, com o vetor de inicialização, de modo a aumentar a complexidade de obter a primeira. Na primeira fase, os 32 bits mais significativos do vetor de inicialização, o TEK e o endereço MAC de quem está transmitindo a mensagem entram como parâmetros de uma função resumo (Fase 1) que retorna um valor de 80 bits. Este valor e os 16 bits menos significativos do vetor de inicialização são enviado para uma nova função resumo (Fase 2), que retorna um valor de 128 bits: os 24 primeiros correspondem ao vetor de inicialização usado pelo RC4, enquanto que os outros 104 correspondem à chave secreta. Um esquema resumido deste algoritmo de mistura de chaves é apresentado na Figura 4(b).

O processo de troca de mensagens no WPA ocorre a partir do uso dos dois mecanismos descritos acima. Ocorre a geração da chave secreta e vetor de inicialização que serão usados no processo do WEP. E, enfim, é feito o cálculo do MIC para a mensagem, sendo também acrescido a ela e enviado para o bloco WEP. Este processo pode ser visto de maneira resumida na Figura 5(a). A parte de decriptação segue o mesmo princípio, com a avaliação do número de sequência da mensagem como um adicional. Após passar pelo decodificador WEP, há o cálculo do MIC, que é comparado com o que foi recebido; caso haja erro, é sinal de que a integridade da mensagem está compreendida. A Figura 5(b) representa este processo de maneira simplificada.

A parte de conexão do WPA-PSK é parecida com a do WEP Shared Key. Porém, ela provê mais segurança ao não passar pelo ar nem a chave compartilhada (PMK), nem a chave de sessão (PTK). Este processo é composto por dois atores, o suplicante e o ponto de acesso. O primeiro passo é o envio



(a) Encriptação (b) Decriptação

Figura 5: Diagrama de Blocos do Protocolo WPA

de uma requisição de conexão por parte do suplicante. O ponto de acesso responde com o envio de uma mensagem com um número aleatório chamado de ANonce. O suplicante, então, gera um novo número aleatório, SNonce, e a partir da combinação destes dois com a chave secreta compartilhada, PMK, ele calcula a chave secreta que será utilizada na sessão. Conforme já visto, a PTK pode ser dividida em quatro partes, dentre as quais duas tem propósito de realizar conexão, a KEK e a KCK (a primeira é usada para encriptar mensagens, enquanto a segunda serve como chave usada pelo MIC). Após o cálculo do PTK, o suplicante envia uma nova mensagem contendo o SNonce em claro e o MIC do ANonce, a partir do uso do KCK. Com isso, o ponto de acesso consegue calcular o valor do PTK e confere se o MIC recebido está correto. Então, ele calcula a GTK, que é a chave utilizada durante a sessão para o envio de mensagens broadcast. Ela é uma combinação do GMK (chave mestra de grupo) com um outro número aleatório, o GNonce. Por fim, ele envia para o suplicante uma mensagem com o GTK encriptado com o uso do KEK, acrescido do MIC desta mensagem (usando o KCK). Ao receber esta última mensagem, o suplicante confere se os valores estão corretos e tem acesso à chave de grupo. Por último, ele valida as duas chaves enviando um ACK para o ponto de acesso, que as valida igualmente. Um diagrama resumido deste processo pode ser visto na Figura 6.

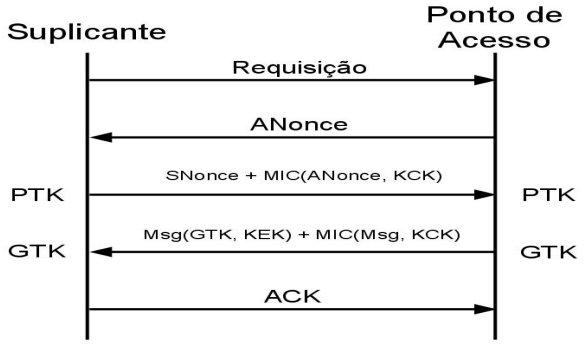


Figura 6: Diagrama de Inicialização de Comunicação do WPA-PSK

3.2 Algoritmo AES

O algoritmo AES, sigla de Padrão de Encriptação Avançado (do inglês "Advanced Encryption Standard"), é um algoritmo de criptografia simétrica de cifra de bloco (a entrada deve possuir um tamanho fixo) criado em 1997 pelo NIST (National Institute of Standards and Technology), órgão do governo dos Estados Unidos. Ele surgiu como uma alternativa ao algoritmo DES, que começava a apresentar

problemas de segurança.

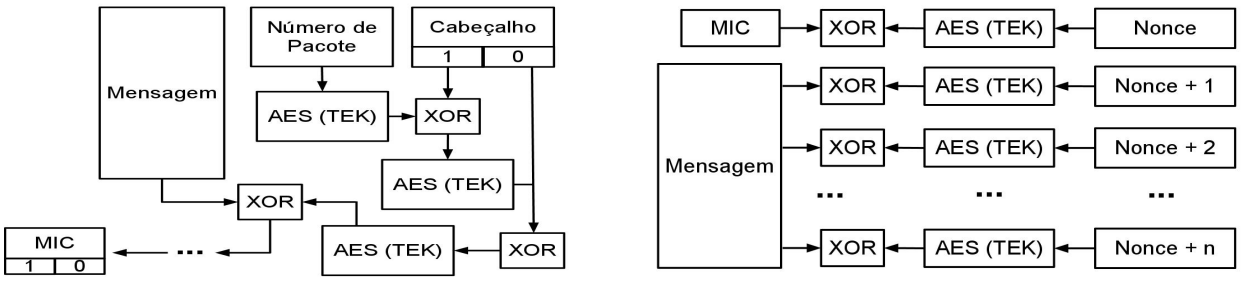
O AES, na verdade, foi originalmente proposto por Vincent Rijmen e Joan Daemen, sendo conhecido como algoritmo Rijndael. Ele sofreu algumas modificações para comportar a encriptação apenas de palavras de 128, 192 e 256 bits. Ele funciona em rodadas, nas quais ocorrem operações de permutações e combinações dos bits. Assim, o algoritmo é eficiente computacionalmente, podendo ser calculado rapidamente.

3.3 WPA2: Protocolo CCMP

O CCMP é o protocolo usado pelo WPA2 para encriptação das mensagens transmitidas. Ele é totalmente independente do funcionamento do WEP, diferentemente do WPA, pelo fato de não usar o algoritmo RC4. Ao invés disto, a mensagem é codificada antes de ser transmitida com o uso do AES. Porém, o conceito de chaves temporárias e código de integridade de mensagem introduzido pelo WPA continuou a ser usado, só que funcionando de maneira diferente. Além disto, a parte de autenticação é bem semelhante à do último e, portanto, será omitida.

A primeira grande diferença se encontra na PTK: enquanto a do WPA possui 512 bits, a do WPA2 dispõe de apenas de 384, pelo fato de usar a TEK tanto para encriptação quanto para cálculo do MIC (ele "alimenta" o algoritmo AES em todos os passos), o que exclui o uso da TMK. Além disto, o vetor de inicialização recebe uma nomenclatura: número de pacote. Outro ponto importante é o uso do cabeçalho do quadro nas duas partes principais do protocolo. Por fim, existe um vetor com determinados parâmetros, chamado de Nonce, que é incrementado cada vez que passa pelo bloco AES.

A parte de cálculo do MIC é bem simples, envolvendo sucessivas operações de Ou-Exclusivo e encriptação com o AES. Primeiramente, o número de pacote passa pelo AES e seu resultado é levado para um bloco de Ou-Exclusivo com a parte mais significativa do cabeçalho. O produto passa novamente por um bloco AES e vai junto com a parte menos significativa do cabeçalho para outro bloco de Ou-Exclusivo. A partir deste ponto, começa a entrar o conteúdo da mensagem, em blocos de 128 bits, seguindo o seguinte padrão: realização da operação de Ou-Exclusivo com o último resultado e envio da saída para o bloco AES. Por fim, quando todos os pedaços da mensagem tiverem passado por este processo, o resultado será uma saída de 128 bits, dos quais os mais significativos são o MIC. Uma simplificação deste processo pode ser visto na Figura 7(a).



(a) Código de Integridade de Mensagem

(b) Encriptação

Figura 7: MIC e Encriptação no WPA2

O processo de encriptação (e, analogamente, de decriptação) utiliza o Nonce para codificar a mensagem, que tem seu conteúdo dividido em pedaços de 128 bits. O primeiro passo é a geração de um novo valor de MIC, ao passar o Nonce pelo bloco AES e realizar um Ou-Exclusivo da parte mais significativa do resultado com o valor atual do MIC. Após este passo, para cada pedaço da mensagem, realiza-se o incremento de Nonce, que passa por um bloco AES e é combinado com o pedaço através de uma operação de Ou-Exclusivo, gerando o pedaço encriptado correspondente. Como este tipo de operação é invertível, fica óbvio que a parte de decriptação corresponde ao mesmo processo, além da verificação do MIC obtido com o recebido. Uma simplificação deste processo de encriptação pode ser

visto na Figura 7(b).

4 Extensible Authentication Protocol

Tanto o WEP quanto o WPA possuem duas versões distintas, uma de uso pessoal, ou PSK (sigla de Chave Previamente Compartilhada, do inglês "Pre-Shared Key"), e outra de uso comercial. A grande diferença entre elas reside no fato de, enquanto a primeira funciona a partir do compartilhamento de uma chave secreta entre o usuário e o servidor, a outra requer um método de autenticação à parte, que é realizado pelo protocolo EAP.

O protocolo EAP, sigla de Protocolo de Autenticação Estendível (do inglês "Extensible Authentication Protocol"), é um arcabouço que permite que um usuário se autentique em um servidor específico a fim de receber mensagens provenientes do ponto de acesso. Este servidor trabalha com o uso do protocolo RADIUS (Serviço de Autenticação Remota de Chamada de Usuário) e tanto pode ser representado pelo ponto de acesso quanto por uma outra máquina dedicada a este fim.

4.1 Funcionamento do EAP

O EAP foi desenvolvido originalmente para trabalhar com o protocolo PPP (Protocolo Ponto-a-Ponto). Assim, seu funcionamento pode ser entendido como uma evolução deste tipo de modelo. Ele possui quatro tipos de mensagem básica que são usadas durante a conexão: Requisição, Resposta, Sucesso e Falha.

O primeiro passo para a conexão em uma rede sem fio que trabalho com o EAP é o envio de uma mensagem de Requisição para o ponto de acesso. Este, por sua vez, retorna um pedido da identidade que o suplicante possui. Ao receber a resposta do suplicante, o ponto de acesso a envia diretamente para o servidor RADIUS. Ele, então, cria um desafio pelo qual o suplicante deve passar com o uso da senha que ele possui. Assim, caso este responda de maneira correta, terá acesso à rede sem fio; caso contrário, receberá uma mensagem de falha de conexão. Por fim, se o protocolo usado para encriptação for o WPA ou WPA2, então ocorre o acordo entre o suplicante e o ponto de acesso a fim de decidir os valores de chaves temporais que serão usadas durante a comunicação. A Figura 8 apresenta uma versão simplificada deste processo.

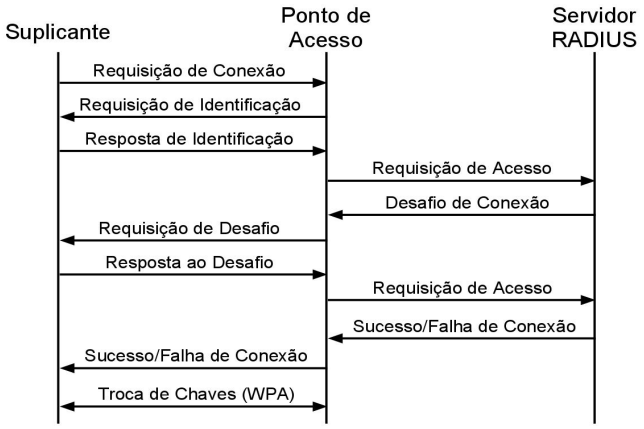


Figura 8: Diagrama de Autenticação EAP com Servidor RADIUS

Este modelo apresenta uma característica muito interessante que é o isolamento do servidor RADIUS: em nenhum momento o suplicante envia uma mensagem diretamente para ele; sempre deve haver o intermédio do ponto de acesso. Isto garante uma maior segurança ao servidor, o que é vital, pois ele contém informações referentes a todos os usuários que são passíveis de acessar a rede. Além disto, o isolamento é importante ao permitir uma maior flexibilidade na hora da manutenção da rede,

pois caso o esquema de segurança seja alterado, deve-se apenas mexer na conexão entre o servidor e o ponto de acesso.

4.2 Protocolos EAP

Existem diversas implementações do EAP, dentre as quais, duas vertentes se destacam: as que usam uma chave secreta para autenticação e as que usam criptografia assimétrica. Uma explicação sucinta de cada um seguida de um exemplo será apresentada a seguir:

- *Chave Secreta*: suplicante e servidor possuem uma chave secreta compartilhada. Esta chave é acrescida ao desafio recebido pelo suplicante e, então, aplica-se uma função resumo e ocorre o envio indireto para o servidor RADIUS. Este método não provê ao suplicante autenticação do servidor e, portanto, é sujeito a ataques do tipo Man-In-The-Middle, além de ataques de dicionário. A implementação mais comum deste tipo é o EAP-MD5, que usa a função hash MD5.

- *Criptografia Assimétrica*: nesta implementação, existe uma autoridade certificadora que possui tanto a chave pública do suplicante quanto a do servidor. Assim, este envia o desafio encriptado com sua chave privada para o suplicante, que o decripta com a chave pública obtida na autoridade certificadora, encripta com a sua privada e reenvia para que o servidor RADIUS repita o mesmo procedimento. Caso o processo seja bem sucedido, a comunicação é garantida de ser imune a ataques de Man-In-The-Middle. Um exemplo deste tipo de implementação é o EAP-TLS (do inglês Transport Layer Security), que utiliza o algoritmo de criptografia assimétrica RSA.

5 Conclusão

As redes sem fio estão longe de serem seguras, mas o avanço dos protocolos de segurança provavelmente perimitirá melhorias muito grande neste aspecto. Atualmente, WPA e, principalmente, o WPA2 suprem bem a demanda nesta área, contando ainda com a ajuda de protocolos EAP para realização de autenticação de forma bastante segura, enquanto que a utilização do WEP pode ser considerada apenas um pouco melhor do que deixar a rede livre para acesso de qualquer pessoa.

O maior problema da área de segurança de redes sem fio reside no fato de os usuários serem leigos no assunto segurança, escolhendo senhas que podem ser facilmente descobertas a partir de ataques de dicionário, por exemplo. Além disto, existe uma resistência por parte dos fabricantes em retirar o protocolo WEP dos pontos de acesso, o que faz com que ele continue sendo usado, causando vulnerabilidade em milhares, senão milhões, de redes espalhadas pelo mundo.

Referências

[1] A. Lashkari, M. Danesh e B. Samadi. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *International Conference on Computer Science and Information Technology*, pages 48–52, 2009.

[2] A. Lashkari, M. Mansoor e A. Danesh. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). *International Conference on Signal Processing Systems*, pages 445–449, 2009.

[3] A. Linhares e P. Gonçalves. Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w.

[4] A. Memon, A. Raza, S. Iqbal. WLAN Security. Master's thesis, 2010.

[5] A. Stubblefield, J. Ioannidis e A. Rubin. A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP). *ACM Transactions on Information and System Security*, pages 319–332, 2004.

[6] B. Aboba, D. Simon e P. Eronen. [RFC 5247] Extensible Authentication Protocol (EAP) Key Management Framework, 2008.

[7] B. Aboba, J. Vollbrecht e J. Carlson. [RFC 3748] Extensible Authentication Protocol (EAP), 2004.

[8] D. Halasz, W. Zorn, S. Norman, D. Smith. [U.S. Patent 6996714] Wireless authentication protocol, 2006.

[9] D. Stanley, J. Walker e B. Aboba. [RFC 4017] Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, 2005.

[10] G. Lehembre. Wi-Fi security – WEP, WPA and WPA.

[11] H. Bulbul, I. Batmaz e M. Ozel. Wireless Network Security : Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.

[12] IEEE Standard for Information technology. IEEE Standards: Part 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancement, 2004.

[13] JANET - The UK's Educational and Research Network. Extensible Authentication Protocol (EAP). Factsheet.

[14] L. Han. A Threat Analysis of The Extensible Authentication Protocol. Technical report, Carleton University, 2006.

[15] L. Silva. Segurança em Redes sem Fio (Wireless).

[16] R. Souza e F. Oliveira. O padrão de criptografiaa simétrica AES.

[17] S. Fluhrer, I. Mantin e A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4.

[18] S. Reddy, K. Ramani, K. Rijutha, S. Ali e C. H. Reddy. Wireless hacking-a WiFi hack by cracking WEP. In *Proceedings of the 2nd International Conference on Education Technology and Computer (ICETC '10)*, pages 1189–1193, 2010.

[19] S. Sotillo. Extensible Authentication Protocol (EAP) Security Issues. 2008.

[20] W. Stallings. *Cryptography and Network Security: Principles and Practice*, chapter 17. Prentice Hall Press, 5th edition, 2010.