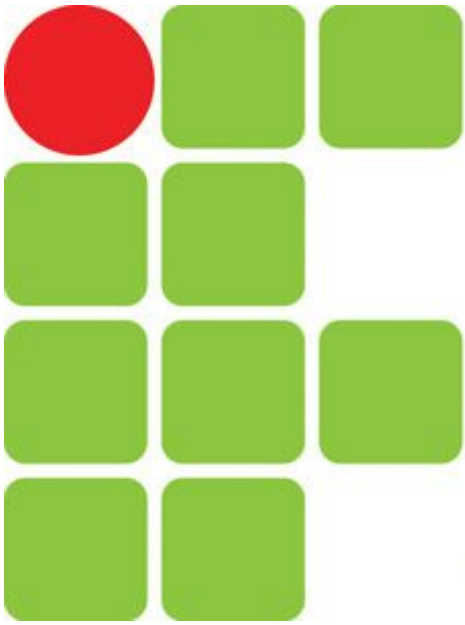


INSTITUTO FEDERAL
SANTA CATARINA

Redes de computadores 2
IEEE 802.11i

Fabiano Kraemer
Gabriel Gonçalves
Iago Soares
Marcos Pinho

São José, 15 de Março de 2016

Com o advento das redes sem fio, vieram as necessidades de se garantir segurança nas transmissões, visto que os sinais se propagam de maneira livre pelo ar, em que qualquer aparelho próximo consegue captar tais sinais. Em 1987 o IEEE aprovou o padrão IEEE 802.11, que garantia padrões de protocolos de transmissão e de segurança. Em 1999 foi introduzido um protocolo de segurança chamado wired Equivalent Privacy (WEP), porém o RC4, algoritmo de criptografia usado no WEP, não é robusto o suficiente para garantir a segurança das informações que circulam pelas redes de comunicação sem fio. Em 2001, o grupo IEEE 802.11 percebeu o grande número de vulnerabilidades que apresentava e formou um grupo com o objetivo de desenvolver um padrão com fortes estratégias de segurança. Tal padrão foi chamado de 802.11i.

Inicialmente foi lançado de maneira provisória o WPA, porém a especificação final se tornou a WPA2, ou 802.11i.

	Protocolo	Algoritmo Criptografia
802.11	WPE	RC4
802.11	WPA	RC4/TKIP
802.11i	WPA2	AES/CCMP

Como a demanda do mercado por redes mais seguras estava crescendo muito rápido foi lançado o WPA(Wi-Fi Protect Acess) pela Aliança Wi-Fi em 2003, que funcionou como um predecessor do WPA2, que é o IEEE 802.11i. Após 3 anos e meio de trabalho o grupo adicionou uma criptografia mais forte, autenticação e estratégia de gerenciamento de chaves para garantir o sistema de segurança.

Como resultado o IEEE 802.11i foi finalmente lançado em 24 de Junho de 2004, e adicionou novos esquemas de criptografia.

	WEP	WPA/TKIP	WPA2/CCMP
Criptografia	RC4	RC4	AES
Tamanho Chave	40 ou 104 bits	128 bits encriptação, 64 bit autenticação	128 bits
Vida da chave	24-bit IV	48-bit IV	48-bit IV
Chave compactada	Concat.	Mixagem FNC	Não precisa
Cabeçalho de integridade de dados	CRC-32	Michael	CCM
Replay	Não	Usa IV	Usa IV
Gerenciamento de Chave	Não	baseado EAP	baseado EAP

O principal benefício do projeto do padrão 802.11i é sua extensibilidade permitida, porque se uma falha é descoberta numa técnica de criptografia usada, o padrão permite facilmente a adição de uma nova técnica sem a substituição do hardware. Outra grande mudança foi a utilização do algoritmo de criptografia, AES.

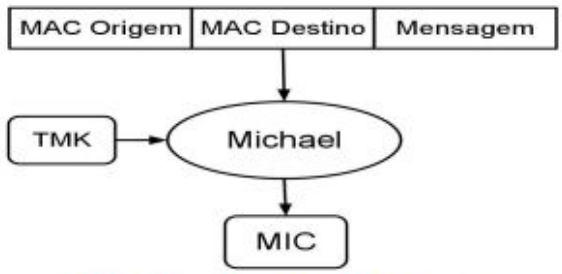
WPA-Tkip:

Protocolo de Integridade de Chave Temporal *(*Tkip), foi desenvolvido com o objetivo de compatibilidade com as versões anteriores. A maioria das falhas de segurança no WEP são por ele não apresentar um código de integridade para a mensagem e confidencialidade dos dados. A integridade do Tkip é obtida através do MIC (Message Integrity Code), para evitar ataques do tipo bit-flipping, que são ataques a uma cifra de criptografia, O MIC é um campo do frame 802.11i, calculado

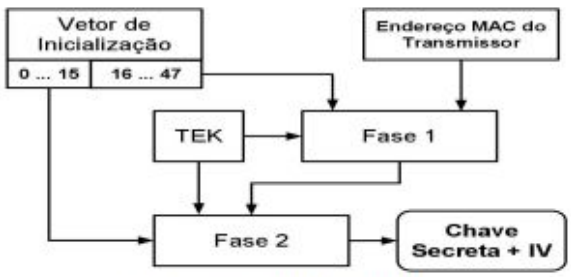
a partir de informações contidas no próprio frame e por uma chave secreta denominada como TMK, pela função hashing conhecida como Michael.

A chave TMK é criada a partir da PTK, ou Chave Transiente de Dupla, a PTK é gerada a partir de algumas informações obtidas durante a conexão. A PTK possui 512 bits, esses 512 bits são divididos em 4 chaves de 128 bits, para diferentes usos neste protocolo, essas chaves são: KCK, KEK, TEK e o TMK.

Para evitar ataques de “força bruta”, é utilizado um vetor de inicialização de 48 bits como identificador do pacote, quando uma comunicação é iniciada, a estação e o ponto de acesso zeram o vetor, após isto, a estação e o ponto de acesso incrementam a cada novo envio, caso um pacote chegue com um valor de vetor menor que o ultimo recebido significa que é um ataque de “força bruta” e então é ignorado. Alem do vetor de inicialização existe uma mistura em duas fases da TEK, com o vetor de inicialização, de modo a aumentar a complexidade de obter a primeira apresentadas na figura abaixo (b).



(a) Código de Integridade de Mensagem



(b) Algoritmo de Mistura de Chaves

WPA2 - RSNA:

Uma RSN, robust security network, que só aceita se comunicar com uma RSNA(robust security network associations). O RSNA é uma conexão lógica entre comunicações IEEE 802.11 estabelecidas através da IEEE 802.11i. O WPA2 para estabelecer uma RSN implementa 2 protocolo: chaves de gerenciamento chamadas de 4-way handshake e o Group Key Handshake. Ele usa os serviços de autenticação e o controle das portas de acesso descritas no IEEE 802.1x para mudar as chaves de criptografia. É um protocolo que valida ambas as entradas com

a PMK (Chave Mestre de Combinação Dupla), sincronizando a instalação de chaves temporais, confirmando a seleção e configuração de dados confidenciais e protocolos de integridade.

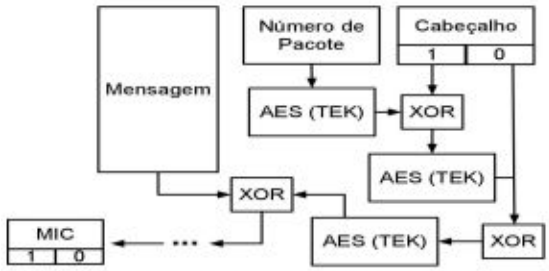
WPA2 - CCMP:

O CCMP é um protocolo de confidencialidade de dados, que controla a autenticação de pacotes e também a criptografia. Para confidencialidade o CCMP usa o AES (Advanced Encryption Standards), no modo contador, já para a autenticação e integridade, ele usa o CBC-MAC (Cipher Block Chaining). O CCMP é totalmente independente do WEP, não faz o uso do algoritmo RC4, foi desenvolvido pois era necessário uma alternativa mais forte para os hardwares mais recentes.

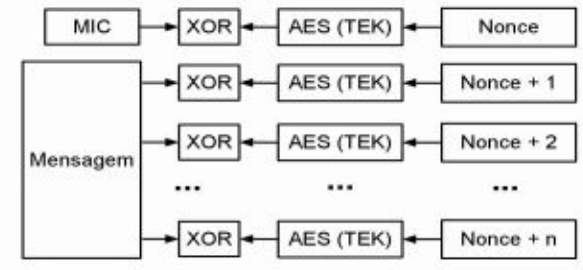
O CCMP utiliza alguns conceitos do TKIP, como a autenticação, que é semelhante a do WAP, como o de chaves temporárias e código de integridade de mensagem, que foi modificado. Uma grande diferença entre o WAP e o WAP2 é no PTK. Enquanto a autenticação do WPA possui 512 bits, a do WPA2 utiliza apenas 384 bits, pelo fato de usar o TEK tanto para encriptação quanto para calculo de MIC, o que retira o uso do TMK. Além disso o vetor inicialização recebe a nomenclatura de número de pacote, e foi criado um vetor com alguns parâmetros, chamado de Nonce, que é incrementado quando passa pelo bloco AES.

AES:

O AES é um algoritmo de criptografia simétrica de cifra de bloco (a entrada deve possuir um tamanho fixo), o AES 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.



(a) Código de Integridade de Mensagem



(b) Encriptação

A autenticação em WPA2 se dá em 4 vias (4-way handshake), realizando diversas tarefas:

- Confirma o PMK (Pairwise Master Key) entre o suplicante e o autenticador;
- Estabelece as chaves temporais para serem utilizadas pelo protocolo de confidencialidade de dados;
- Autentica os parâmetros de segurança que foram negociados;
- Executa o handshake;
- Fornece grupos de chaves para implementar o handshake de grupo;

Não surpreendentemente, a razão pela qual ele é chamado de 4-way handshake é porque quatro pacotes são trocados entre o suplicante e o autenticador:

4-way Handshake mensagem 1:

Na primeira mensagem, o autenticador envia ao suplicante um nonce. Isto é referido como o ANonce.

4-way handshake mensagem 2:

O suplicante cria sua nonce. Isto é referido como o SNonce. O suplicante pode agora calcular o PTK (Pairwise Transient Key). Na segunda mensagem, o suplicante envia o SNonce ao autenticador. O suplicante também envia os parâmetros de segurança que ele utilizou durante a associação. Toda a mensagem recebe uma verificação de autenticação usando o KCK (*EAPOL-key confirmation key)* da chave de pareamento hierárquica. O autenticador pode, então, verificar se as informações, incluindo os parâmetros de segurança enviados em associação, são válidos.

4-way handshake mensagem 3:

Na terceira mensagem, o autenticador envia ao suplicante os parâmetros de segurança que está enviando em seus avisos e respostas de sondagem. O autenticador também envia o GTK (Group Temporal Key) criptografado utilizando a KEK (Key Encryption Key). Mais uma vez, toda a mensagem recebe uma verificação de autenticação, que permite que o suplicante possa verificar se as informações, tais como os parâmetros de segurança autenticadores, são válidas.

4-way handshake mensagem 4:

A quarta mensagem indica que as chaves temporais estão agora no lugar para serem usadas pelos protocolos de confidencialidade de dados.

Alguns tipos de ataques que o IEEE802.11i deve prevenir:

Ataque de dicionário ao EAP: O frame 802.11 é facilmente capturado, possibilitando que um intruso descubra uma senha usando o mecanismo de força bruta baseado em dicionário.

Ataque a chave default: Como 802.11 não implementa um mecanismo de troca de chaves aleatório, como isso descobrir a chave é questão de tempo.

Ataque de DOS baseado no frame EAPOL-Logoff: Como esse tipo de frame não é autenticado, alguém pode enviar um frame EAPOL logoff e desconectar um usuário. Pode-se filtrar esse tipo de solicitação no ponto de acesso (AP).

Ataque de DOS baseado no frame EAPOL-Styart: O atacante pode fazer um envio maciço de frames EAPOL start para sobrecarregar o ponto de acesso (AP) e tira-lo de serviço. Isso pode ser evitado fazendo com que o AP não gaste muito recurso com o atendimento desse tipo de frame.

Ataque de DOS baseado no espaço de identificação do EAP: O atacante pode consumir o espaço de identificação do EAP, que vai de 0 a 255, e tirar o ponto de acesso fora de serviço.

Ataque de DOS baseado no envio antecipado do pacote de sucesso do EAP: O atacante pode enviar um pacote de sucesso do EAP antecipado para permitir que uma estação possa ser vista na rede antes que o ponto de acesso complete o processo de autenticação.

Ataque de DOS baseado no pacote de falha do EAP: O atacante pode enviar um pacote de falha do EAP antecipado para não permitir que uma estação seja vista na rede antes que o ponto de acesso complete o processo de autenticação.

Ataque de DOS baseado na alteração do pacote EAP: O atacante pode modificar o conteúdo do pacote EAP. Para evitar esse tipo de ataque deve-se utilizar protocolos de criptografia como TLS, PEAP ou TTLS.

Referências:

http://www.eetimes.com/author.asp?section_id=36&doc_id=1287503

http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/downloads/trabalho.pdf

http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2013_2/80211i/IEEEi.html

http://br.ccm.net/contents/789-802-11i-wpa2

https://en.wikipedia.org/wiki/IEEE_802.11i-2004

http://www.teleco.com.br/tutoriais/tutorialsrwireless/pagina_4.asp

http://csrc.nist.gov/archive/wireless/S10_802.11i%20Overview-jw1.pdf