UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

CURSO CIÊNCIA DA COMPUTAÇÃO
TURMA 2008.1

Evolução da Segurança em Redes Sem Fio

Autor

Marcos Antonio Costa Corrêa Júnior (maccj@cin.ufpe.br)

Orientador

Prof.º Ruy José Guerra B. de Queiroz

Recife, Junho de 2008

UNIVERSIDADE FEDERAL PERNAMBUCO - UFPE

CENTRO DE INFORMÁTICA- CIN

Graduação em Ciência da Computação

2008.1

Evolução da Segurança em Redes Sem Fio

por

Marcos Antonio Costa Corrêa Júnior

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 – Ph. D. Ruy José Guerra B. de Queiroz

Recife, Junho de 2008

RESUMO

O crescimento do uso de redes sem fio trouxe um inegável aumento de produtividade para as empresas, mas, ao mesmo tempo, desafios aos administradores da infra-estrutura de rede. Como seria possível fornecer acesso só aos recursos necessários e só para os usuários que realmente deveriam obter este acesso?

A padronização através do padrão IEEE 802.11 veio permitir interoperabilidade entre dispositivos de diversos fabricantes além disso definiu um protocolo de segurança - o WEP- que pouco tempo depois foi alvo de duras críticas por conta de suas vulnerabilidades.

A indústria, então, não podendo aguardar a completa conclusão e ratificação dos trabalhos desenvolvidos pelo grupo que conduzia os estudos do padrão IEEE 802.11i, antecipou-se à conclusão destes e aproveitou-se de um subconjunto do estudo, para desenvolver o WPA, que foi concebido para ser um protocolo transitório enquanto o IEEE ainda realizava pesquisas e fazia melhorias. Concluído o trabalho do IEEE, foi lançado o WPA2 baseado no AES-CCMP.

Diante desse quadro histórico da evolução da segurança das redes sem fio, firma-se o objetivo deste Trabalho de Graduação, o qual consiste em analisar toda esta evolução da segurança WLAN, demonstrando algumas de suas fragilidades e ressaltando, quando possível, as melhorias que foram surgindo.

Palavras-chave: IEEE 802.11, WLAN, Redes sem Fio, Segurança, IEEE 802.11i, WEP, WPA

ABSTRACT

The wide use of wireless networks has brought an undeniable increase in productivity for companies, but at the same time, challenges to the network administrators. How can we restrict access to resources of WLAN?

The IEEE 802.11 standard came, and brought interoperability between devices from different manufacturers also established a security protocol - the WEP - that was not strong enough and many vulnerabilities were found. The WEP not achieved the objectives for which it was created.

The industry then, could not wait until the full ratification and completion of the work developed by the task group i (IEEE 802.11i), so, took up a subset of the study, to develop the WPA, which was designed to be a transition protocol while the IEEE is still conducting searches and making improvements. Upon completing the work of the IEEE, was launched the WPA2.

In this historical context of security wireless networks, this work's objective is examine the whole WLAN's security evolution , demonstrating some of their weaknesses and emphasizing, when possible, the improvements that were arise.

Keywords: IEEE 802.11, WLAN, Security, IEEE 802.11i, WEP, WPA

DEDICATÓRIA

Dedico este trabalho à minha esposa e aos meus filhos.

AGRADECIMENTOS

Ao Professor Ruy, meu orientador, pelo apoio e paciência neste Trabalho de Graduação.

A todos que formam o Centro de Informática pelo excelente ambiente e infra-estrutura diferenciada.

A minha família por toda a paciência nas inúmeras noites que passei distante ao longo deste curso realizando projetos.

LISTA DE ILUSTRAÇÕES

FIGURAS

TABELAS

LISTA DE ABREVIAÇÕES E SIGLAS

AAD – Additional Authentication Data

AES – Advanced Encryption Standard

AP – Acess Point ou Ponto de Acesso

CBC – Cipher Block Chaining

CCMP – Counter Mode with CBC-MAC Protocol

CRC – Cyclic Redundancy Check

CRC-32 – Cyclic Redundancy Check 32

DoS – Denial of Service

EAP – Extensible Authentication Protocol

FCC – Federal Communications Commission

FMS – Fluhrer, Mantin e Shamir

GTC – Generic Token Card

HMAC – keyed-Hash MAC

ICV – Integrity Check Value

IEEE – Institute of Electrical and Electronics Engineers

IV – Initialization Vector

IP – Internet Protocol

ISM – Industrial, Scientific, and Medical

LAN – Local Area Network

MAC – Media Access Control

MIC – Código de Integridade da Mensagem

MPDU – MAC Protocol Data Unit

MSCHAP – Microsoft´s Challenge Handshake Authentication Protocol

MSDU – MAC Service Data Unit

NIST – National Institute of Standards and Technology

NWID – Network ID

PBKDF – Password-Based Key Derivation Function

PEAP – Protected EAP

PKCS – Public-Key Cryptography Standard

PMK – Pairwise Master Key

PN – Packet Number

PPK – Per-Packet Key

PSK – Pre-Shared Key

RADIUS – Remote Authentication Dial-In User Service

RC4 – Ron´s Code 4[1]

RSN – Robust Security Network

RSNA – Robust Security Network Association

SHA – Secure Hash Algorithm

SIM – Subscriber Identity Module

SNMP – Simple Network Management Protocol

SSID – Service Set Identifier

SSL – Secure Socket Layer

STA – Station

TACACS – Terminal Access Controller Access-Control System

TKIP – Temporal Key Integrity Protocol

TLS – Transport Layer Security

TSC – TKIP Sequence Counter

TSN – Transition Security Network

TTLS – Tunneled Transport Layer

WEP – Wired Equivalent Privacy

WI-FI – Wireless Fidelity

WLAN – Redes Locais Sem Fio

WPA – Wi-Fi Protected Access

[1] Muitos crêem que trata-se de Rivest Cipher, mas o próprio Ron Rivest diz que o significado original é de Ron´s Code (RIVEST, 2007)

SUMÁRIO

1. INTRODUÇÃO

A preocupação com a segurança da informação transmitida, remonta a milhares de anos e os romanos segundo relatos históricos já usavam métodos, ainda que primitivos, para resguardar as mensagens transmitidas. As redes sem fio não são tão antigas, têm apenas algumas décadas, mas muitos que as usam querem ter a certeza de que seus dados não estarão acessíveis para nenhuma pessoa indesejada.

A criptografia desempenha um papel importantíssimo tanto nos ambientes LAN quantos nos ambientes WLAN. Para utilizadores sem fios, a criptografia é particularmente importante porque a plataforma wireless é muitas vezes a mais fácil porta de entrada em uma rede. Um invasor pode muitas vezes atacar um dispositivo sem fio e ganhar acesso a LAN sem as vítimas sequer ficarem cientes de que suas informações estão sendo acessadas por este invasor. Criptografia faz com que o trabalho de um atacante seja muito mais difícil e ajuda a proteger os usuários de tais falhas, para vermos a evolução da criptografia e de outros mecanismos igualmente importantes para a segurança, integridade e autenticidade, em uma rede sem fio realizamos esta pesquisa.

O uso inicial de soluções de LAN sem fio se deu com um projeto de pesquisa na Universidade do Hawaii nos anos 70, era a ALOHAnet desenvolvida por Normam Abramson, um professor de engenharia apaixonado por surfe, que lecionava anteriormente em Stanford.

Os primeiros passos para a comercialização em larga escala de redes sem fio, no entanto, só começaram mais de dez anos depois da pesquisa do professor Abramson no Hawaii e ocorreram em 1985, com a liberação de uso de uma faixa de freqüência livre de pagamentos de licença pela FCC. A banda que ficou conhecida como ISM, foi permitida pela primeira vez nos Estados Unidos para dispositivos de redes sem fio e foi, em seguida, copiada por diversos outros países do mundo, permitindo a eles o uso desta tecnologia (FEDERAL COMMUNICATIONS COMMISSION, 1985).

Alguns fabricantes começaram a desenvolver produtos de comunicação de redes locais sem fio. O primeiro dispositivo Wi-Fi foi inventado em 1991 pela NCR Corporation/AT&T na Holanda e foi trazido ao mercado com o nome de WaveLAN (Wi-Fi, 2008).

Outros dispositivos de WLAN começam a aparecer e a marca de mais de 100mil unidades de dispositivos de WLAN comercializados é ultrapassada em 1994 pela Aironet, empresa fundada logo após a liberação da banda ISM (COMPTEK, 2001).

Começam a surgir problemas, os equipamentos de diferentes fabricantes não se comunicam e são muito caros, muitas vezes os custos são proibitivos para determinados clientes. Os dispositivos são desenvolvidos pelo fabricante e seu funcionamento interno, desde as mais simples operações até o funcionamento da segurança, é desconhecido por outras empresas, estamos na era da segurança proprietária, na verdade de todo funcionamento proprietário. A falta de padronização começa a prender o cliente a um só fabricante, e lhe trazer outras dificuldades. O comitê para padronização formado no IEEE, que deveria trabalhar para criar um padrão que viesse a facilitar a interoperabilidade, esta praticamente inativo até que Vic Hayes, que ficou conhecido como “o pai do Wi-Fi”, assumiu a presidência em 1990 (KHARIF, 2003).

A liderança de Hayes conseguiu unir cerca de 130 empresas para juntas desenvolverem um padrão aberto. Como resultado, o 802.11 foi publicado em 1997 e hoje temos redes sem fio a um baixo custo, um padrão amplamente adotado que recebeu inúmeros aperfeiçoamentos de 1997 até hoje. Por toda a sua dedicação, Hayes foi reconhecido pela revista PC Advisor como um dos 50 maiores heróis da história da tecnologia (NULL, 2008).

Junto com a padronização das WLAN feita pelo IEEE 802.11, após sete anos de pesquisa e desenvolvimento (1990-1997), criou-se uma versão inicial capaz de atingir taxas de transmissão nominal de 1 e 2 Mbps. Dois anos mais tarde foram aprovados os padrões IEEE 802.11b (2,4 GHz) e 802.11a (5 GHz) cujas taxas de transmissão são de 11 e 54 Mbps, respectivamente, junto com essas definições é também aprovado o WEP, este com a missão de garantir o sigilo da comunicação.

Com o surgimento e rápido crescimento das redes sem fio, a segurança dessas redes começou a ser alvo de questionamentos quanto à sua real capacidade de resistir a ataques e manter o sigilo das informações. A lista de vulnerabilidades do protocolo WEP - que veremos em profundidade em uma seção específica - começou a crescer vertiginosamente criando descrédito na segurança de redes sem fio. Diversos aprimoramentos foram propostos na tentativa de sanar os problemas encontrados no WEP, um a um os aprimoramentos foram demonstrando também suas fraquezas. Chegou-se à conclusão que os problemas do WEP eram muito profundos e a melhor solução seria seu abandono e a concepção de um novo protocolo, criou-se, então, o grupo IEEE 802.11i.

Como frutos do trabalho do grupo IEEE 802.11i, surgiram o WPA e o WPA2, os quais veremos detalhadamente ao longo do nosso trabalho.

Traremos ainda protocolos que, apesar de não terem sido concebidos para redes sem fio especificamente, podem contribuir no projeto de uma rede sem fio e atender aos anseios de seus mais exigentes clientes, são eles o IEEE 802.1x e o RADIUS.

Por fim, trataremos de alguns outros possíveis problemas de redes IEEE 802.11, para então, concluirmos o nosso trabalho.

2. DESENVOLVIMENTO

2.1 - SEGURANÇA PROPRIETÁRIA

Na década de 90, antes da aprovação de um padrão para conectividade sem fio, já havia alguns fabricantes que dispunham de soluções comerciais de comunicação LAN sem fio. Estas soluções se aproveitaram de uma faixa de freqüência disponibilizada pela *Federal Communications Commission* (FCC) em 1985, que permitia o uso público da faixa de freqüência ISM (sigla do inglês *Industrial, Scientific and Medical*) para produtos de LAN sem fio.

A banda ISM era atraente para vendedores de produtos de LAN sem fio pois eles não precisariam obter uma licença da FCC para operar nesta banda.

O WaveLAN foi o primeiro dispositivo criado após a liberação da faixa pela FCC, por questões de segurança, utilizava um NWID (Network ID) de 16-bits, que dá 65.536 possíveis combinações; o dispositivo poderia receber o tráfego de rádio codificado com outro NWID, mas o controlador iria descartar este tráfego. Essa poderia ser uma estratégia segura, mas o mesmo código está em todos os cartões WaveLAN. Isto quer dizer que, embora seja difícil uma pessoa mal intencionada encontrar aleatoriamente o código, para um usuário WaveLAN é simples. Mesmo que pudéssemos mudar o Network ID este ainda não teria segurança suficiente pois seria relativamente fácil escrever um programa que tentasse todos os códigos em seqüência até encontrar o ID correto (WaveLan, 2005)(WaveLAN, 2008).

Os primeiros dispositivos desenvolvidos tinham baixo desempenho em termos de taxa de transmissão de dados e cobertura. Essas penalidades somadas à preocupação com a segurança, ausência de padronização, e alto custo (a primeira *access point* sem fio para LAN custava 1400 dólares, muito, se comparados a um cartão Ethernet de algumas centenas de dólares), resultaram em vendas baixíssimas (GOLDSMITH, 2005).

2.1.1 Vantagens

A segurança proprietária por si só não apresenta vantagens em relação às tecnologias atuais, a menos que levássemos em conta o fato de pouca adoção da tecnologia LAN sem fio não estimular a exploração de possíveis vulnerabilidades, nem estimular a busca por estas, ou ainda, se, cegamente, acreditássemos que por haver um segredo do algoritmo isso nos forneceria mais segurança.

2.1.2 Fragilidades e Desvantagens

Além do custo que em si já é uma desvantagem, pois torna difícil o acesso à tecnologia de LAN sem fio, se é que não o torna proibitivo, tecnologias proprietárias forçam a compra de dispositivos para expansão da rede sempre de um mesmo fabricante, o que é outro forte ponto negativo.

Temos que, nesse período, não havia padronização e o uso comercial de LAN sem fio era muito restrito, as tecnologias eram proprietárias e eram fornecidas apenas características mínimas de segurança. As ameaças eram baixas e muito da segurança devia-se ao que podemos denominar de segurança pela obscuridade (a idéia da segurança pela obscuridade é que a segurança é melhor se o algoritmo criptográfico é mantido em segredo). Algoritmos proprietários têm essa característica de prover segurança pela obscuridade (invocando a lei de patentes e o direito à propriedade intelectual sobre o algoritmo, ele é mantido como segredo industrial) isto pode trazer resultados desastrosos e é recomendável sempre se usar algoritmos publicamente disponíveis e amplamente testados.

A segurança pela obscuridade se opõe aos princípios de Kerckhoffs, que recomenda não só que a segurança não deve ser baseada no segredo do algoritmo, mas diz que para fortalecer esse algoritmo ele deve ser tornado público (KATZ e LINDELL, 2008).

2.2 - WEP

O ar não fornece barreiras bem definidas e permite que os sinais de comunicação se estendam até depois das paredes de uma instituição possibilitando a captura de informação sensível que trafegue pelo ar. Durante o desenvolvimento do padrão para redes sem fio IEEE 802.11 sentiu-se a necessidade de criar algum artifício que permitisse o tráfego de informações sigilosas através do ar sem que um usuário malicioso externo pudesse ter acesso a essa informação de forma inteligível.

Introduzido em 1999, o WEP (*Wired Equivalent Privacy*) seria o artifício capaz de fornecer proteção suficiente para o transporte de informação sensível pelo ar, se não fossem as fragilidades encontradas.

Com o intuito de fornecer aos usuários de redes sem fio um nível de segurança comparável a da redes cabeadas, o WEP define três objetivos principais a serem atingidos.

1. Fornecer confidencialidade - significa simplesmente que o WEP deve ser capaz de evitar que uma pessoa não autorizada, não possa sequer compreender as mensagens que estão trafegando pela rede;

2. Garantir autenticidade – de forma simples garantir autenticidade é garantir que um usuário é quem ele afirma ser. O WEP, então, deve implementar um controle de acesso à infra-estrutura da rede sem fio, de forma que haja garantias de que o usuário que está se comunicando é um usuário legítimo da rede e não um invasor tentando se passar por usuário legítimo.

3. Garantir a integridade dos dados – a integridade dos dados transmitidos é conseguida se uma mensagem enviada pelo emissor chega ao destinatário de forma correta. Pode haver problemas de integridade por um erro comum devido a ruídos do canal ou por adulteração maliciosa dos dados. O WEP implementa uma função chamada de "*checksum*" para que o conteúdo da mensagem transmitida seja verificado ao chegar ao destinatário, se o valor calculado no destinatário for igual ao valor do "*checksum*" então os dados foram mantidos inalterados ao longo da transmissão.

2.2.1 Funcionamento

De maneira abstrata, o algoritmo WEP funciona com uma chave secreta (de 40 bits segurança muito fraca e de 104 bits um pouco menos fraca, porém bem mais cara e rara) a qual é concatenada a um vetor de inicialização (*Initialization Vector* – IV de 24 bits). Apesar de ser relativamente rápido, podendo até mesmo ser processado via software, esse mecanismo apresenta falhas de segurança.

O WEP usa a cifra de fluxo RC4 como algoritmo de encriptação para prover confidencialidade e o *checksum* CRC-32 para prover integridade.

2.2.2 Algoritmo

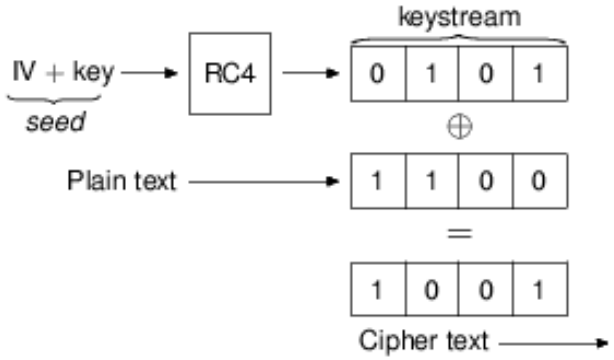

Figura 1 – Cifragem WEP: XOR entre o *keystream* do RC4 e texto xto (*Wired Equivalent Privacy*, 2008).

O processo de cifragem ocorre conforme está sendo mostrado na figura 1 o vetor de inicialização de 24 bits (IV) é concatenado a chave escolhida (que pode ter 40 bits no caso do WEP-40, 104 bits para o WEP-104 ou ainda 232 bits disponível para alguns fabricantes, que fornecem respectivamente chaves WEP de 64, 128 e 256 após concatenação com o IV).

O RC4 irá receber a chave WEP concatenada com o vetor de inicialização que juntos formam o *seed*. O sistema que gerará um fluxo de bits pseudo-aleatório a partir do *seed*, esse fluxo de bits pseudo-aleatório é chamado *keystream*. Para a

cifragem do texto é feito uma XOR do *keystream* (fluxo de bits da saída do RC4) com o texto puro.

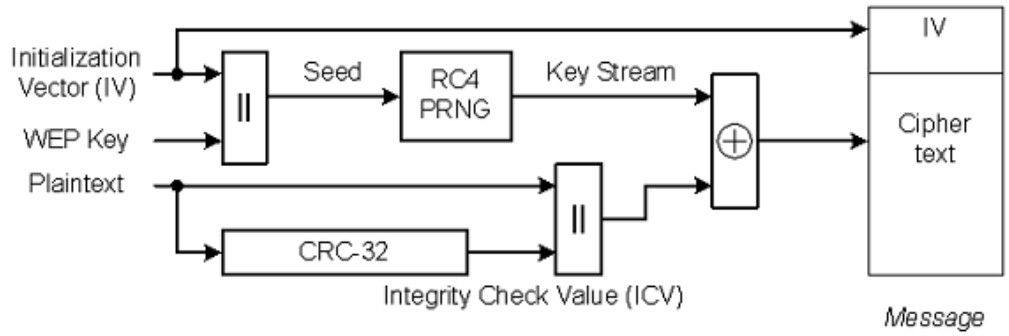

Figura 2 – Diagrama em blocos do encapsulamento WEP (IEEE, 2004)

Na figura 1 temos a cifragem WEP de forma mais simplificada, onde está implícito tanto dentro do purotexto quanto dentro do cifrotexto que há a mensagem mais o seu hash para que seja realizada posteriormente a verificação de integridade. Na figura 2 mostramos com maior riqueza de detalhes como se dá todo esse processo de encapsulamento WEP, temos como entrada o vetor de inicialização (IV), a chave WEP e o purotexto e obtemos como saída a mensagem que é o cifrotexto precedido do vetor de inicialização.

2.2.3 Fragilidade

Durante os quatro primeiros anos de vida do padrão 802.11, pesquisadores construíram uma longa lista de vulnerabilidades encontradas no WEP.

O IEEE conhece os problemas da WEP, mas, como a maioria dos outros padrões de hardware, é muito tarde para corrigir os problemas de milhões de dispositivos 802.11b já implantados.

O WEP é vulnerável a hackers, que podem usando ferramentas distribuídas gratuitamente pela internet, como Airsnort, WEPCrack, Aircrack dentre outras, para decodificar quadros codificados com WEP. Estas ferramentas exploram o pequeno tamanho do vetor de inicialização (IV) que é enviada em texto claro dentro do frame.

Como o vetor de inicialização só tem 24 bits, isso quer dizer que uma rede que envia pacotes de 1500 bytes em uma rede IEEE 802.11b a 11Mbps repete o mesmo vetor de inicialização (IV) a cada $(1500*8*2^{24})/11*10^{6}$ = 18000 seg aproximadamente 5 horas. Esta fraqueza do WEP faz com que ele seja inadequado para redes sem fio de empresas a menos que elas queiram ver seus dados sigilosos facilmente expostos à atividade maliciosa. Como se não bastasse a repetição do vetor de inicialização em 5 horas, alguns detalhes de implementação podem fazer com que a repetição aconteça com uma maior freqüência.

Além de críticas a cifragem dos dados, o *checksum* CRC é também considerado insuficiente para assegurar que um atacante não fez nenhuma alteração na mensagem, o CRC não é um código de autenticação criptograficamente seguro. O CRC foi projetado para detectar erros aleatórios na mensagem; contudo, ele não é suficiente contra ataques maliciosos. Para proteger a integridade de dados de uma transmissão e identificar a adulteração maliciosa de mensagens o uso de um código de autenticação de mensagens (MAC) criptograficamente seguro, tal como HMAC-SHA1 é a atitude mais indicada (BORISOV et al, 2001a).

Tabela 1 – Fraquezas do WEP (EDNEY e ARBAUGH, 2003

1	O vetor de inicialização (IV) é pequeno demais e não oferece proteção alguma contra reuso
2	A forma como são construídas as chaves, por meio dos vetores de inicialização, faz o WEP susceptível a ataques de chaves fracas (ataque FMS)
3	Não há detecção eficiente de adulteração de mensagem (integridade de mensagem)
4	Usa diretamente a chave master e não há possibilidade no WEP de atualizar as chaves
5	Não há proteção contra replay de mensagem

Na tabela 1 extraída de EDNEY e ARBAUGH (2003), temos o resumo de algumas das fragilidades do WEP que se procurou corrigir ou pelo menos minimizar com a concepção e utilização do TKIP:

Outros ataques ao WEP, mais eficientes, podem ser encontrado na seção IEEE 802.11i.

2.2.4 Vantagens

A principal vantagem do WEP é o fato de ser relativamente rápido, em um período que o hardware era mais caro, este podia ser processado até mesmo via software, apesar de suas falhas de segurança.

Até o período em que começaram a ser divulgadas inúmeras vulnerabilidades o WEP era amplamente utilizado por administradores de rede que realmente se preocupavam com a segurança dos seus dados. Hoje, este deve ser encarado como a segurança mínima a ser implementada se você possui uma pequena rede, ou uma rede em casa. O WEP é eficiente para manter afastadas as pessoas que podem acidentalmente se conectar a sua rede WLAN, mas é uma tecnologia que já demonstrou ser ineficaz para impedir a ação de um *cracker* hábil e dedicado (GEIER, 2002).

Por contar com uma quantidade muito grande de dispositivos comercializados, sistemas legados, que não oferecem suporte a criptografia mais forte, ainda é possível encontrar muitas redes, até mesmo de grande porte, fazendo uso do WEP. Há ainda a utilização de dispositivos portáteis (handhelds e *smartphones*) usados por redes varejistas (grandes lojas de departamento, de eletrônicos, de vestuário e supermercados) no controle de seus estoques, pontos de venda sem fio e telefones VoIP que só são capazes de suportar o WEP. Por mais que pareça infrutífero o melhoramento do WEP ainda há quem faça investimento no intuito de permitir uma segurança mais sólida com o uso do WEP, tanto que a AirDefense patenteou em abril de 2007 o módulo WEP Cloaking para proteger dispositivos handheld em uso. Segundo o fabricante, o WEP Cloaking permite que os usuários de dispositivos só capazes de usar o WEP continuem a fazê-lo, sem no entanto, serem pontos vulneráveis da infra-estrutura. Ainda segundo este fabricante,

dispositivos sem o WEP Cloaking seriam facilmente quebrados com ferramentas populares. (AIRDEFENSE ENTERPRISE, 2007).

2.2.5 Desvantagens

Um *cracker* dedicado é capaz de se aproveitar das inúmeras fraquezas do WEP e acessar redes com este habilitado, ainda que bem configurado, especialmente aquelas com alta utilização (GEIER, 2002).

Os problemas encontrados no protocolo WEP são resultado de interpretações equivocadas de algumas premissas criptográficas e de combinações delas de forma insegura. Estes ataques ao WEP apontam para a importância da revisão de algoritmos criptográficos convidando pessoas com experiência no projeto de protocolos criptográficos; se isso já fosse uma prática nos tempos da adoção do WEP, alguns dos problemas encontrados certamente teriam sido evitados (BORISOV et al, 2001b).

2.2.6 Melhorias WEP

Inúmeras melhorias foram sugeridas desde que começaram a surgir ataques ao WEP.

Reparos feitos:

WEP2 – implementado em hardware não hábil a lidar com WPA ou WPA2; estendeu o valor da chave e do vetor de inicialização a valores de 128 bits, com intuito de eliminar a deficiência da duplicação do vetor de inicialização e parar com ataques de força bruta.

WEPplus – um aperfeiçoamento por uma subsidiária da Lucent Technologies que evitava o uso de vetores de inicialização fracos;

Dynamic WEP – mudanças dinâmicas da chave WEP.

Todas essas melhorias listadas foram insuficientes para devolver a confiabilidade no protocolo WEP.

A melhoria sugerida mais recentemente e que parecia promissora não tardou em cair por terra. Conhecida como WEP Cloaking a solução da AirDefense foi

refutada por uma equipe da AirTight Networks no Defcon 15 (última edição da maior convenção hacker anual do mundo).

De acordo com o trabalho divulgado pela AirTight Networks (GUPTA et al, 2007b):

> Veredicto Final sobre o WEP Cloaking
>
> WEP está morto e qualquer tentativa de ressuscitá-lo está fadado a ter um final semelhante. Nossa metodologia provou que o WEP Cloaking pode seguramente ser aniquilado independente da complexidade da Chaffing Engine[2].[3]

Como foi demonstrado pela equipe AirTight Networks soluções como a da AirDefense podem ser quebradas, e técnicas como esta classificadas como técnicas de "Chaffing" são apenas mais uma tentativa de prover segurança pela obscuridade.

2.2.7 Uso atual

As várias vulnerabilidades encontradas no WEP fazem com que ele falhe em atingir os seus objetivos de prover segurança.(BORISOV et al, 2001a)

Hoje o WEP não é considerado um protocolo que oferece uma segurança forte, apesar de suas fraquezas largamente divulgadas, WEP ainda é amplamente utilizado (RSA, 2007).

Com softwares disponíveis gratuitamente na web o WEP poder ser quebrado dentro de minutos quiçá segundos.

AirTight Networks DEFCON 15:

"WEP foi quebrado ... está quebrado ... permanecerá quebrado. PONTO FINAL.[4]"(GUPTA et al, 2007a).

A solução para os problemas de segurança do WEP é mudar, de fato, para o WPA2 ou WPA, ainda que alguns dispositivos tenham que ser substituídos.

---

2 Chaffing Engine – Nome genérico dado pela AirTight Networks para técnicas como a do WEP Cloaking.

3 Final Verdict on WEP Cloaking

WEP is dead and any attempt to revive it, will meet a similar fate. Our techniques prove beyond doubt that WEP cloaking can be reliably and consistently beaten no matter what the complexity of the Chaffing Engine.

4 WEP was broken …. it is broken ….it will remain broken. PERIOD .

2.3 - IEEE 802.11i

Para entender a importância do padrão 802.11i de 2004 - que foi na verdade uma das alterações sofridas ao longo dos anos pelo padrão 802.11 publicado inicialmente em 1997, com novas versões publicadas em 1999 e em 2007 – é muito importante que regressemos à época.

Com o crescimento da popularidade das redes WLAN, e conseqüente crescimento do uso do WEP por parte de empresas preocupadas com o risco da interceptação de dados pelo ar, a curiosidade da comunidade de segurança foi despertada para saber de fato o quão seguro o WEP era.

Já vimos, quando falamos do WEP, as vulnerabilidades que, a partir de 2001, foram sendo publicadas sobre as fraquezas dos mecanismos de segurança do padrão IEEE 802.11. Segundo a literatura, em 2001 uma equipe de Berkley publicou o *paper "Intercepting Mobile Communications: The Insecurity of* 802.11" (BORISOV et al, 2001a) onde são descritas as fraquezas do WEP, protocolo de segurança definido no padrão original; logo em seguida, publicado o *paper "Weaknesses in the Key Scheduling Algorithm of* RC4" (Fluhrer et al, 2001) por Fluhrer, Mantin e Shamir. Pouco depois, Adam Stubblefield e AT&T (STUBBLEFIELD et al, 2001) fizeram uma publicação anunciando a primeira verificação do ataque. Neste ataque, eles conseguiram interceptar a transmissão e obter acesso não autorizado a rede sem fio.

As redes sem fio já não gozavam de credibilidade perante grandes corporações, empresas que usam redes sem fio IEEE 802.11 sentiam-se vulneráveis e temiam pela possibilidade real de terem seus dados sigilosos interceptados.

O comitê do IEEE após conhecer e ver amplamente divulgadas as deficiências da segurança em redes sem fio criou um *task group* para gerar uma solução de segurança capaz de substituir a solução original. Este *task group* denominou-se 802.11i e sua implementação completa seria a *Robust Security Network* (RSN).

Passado algum tempo de trabalho o grupo de trabalho 802.11i ainda não havia publicado nada que pudesse ser usado para atender a demanda do mercado

consumidor de redes sem fio. Os principais fabricantes de dispositivos de redes sem fio perceberam que segurança era tão importante para o usuário final que decidiram que seria necessário urgentemente encontrar uma solução alternativa a fim de substituir o WEP e resgatar a credibilidade da segurança de redes sem fio. Além do mais, com o enorme número de dispositivos capazes de rodar apenas o WEP, a simples criação de um padrão que viesse a substituí-lo não seria suficiente, pois os clientes não estavam preparados para simplesmente se desfazer de todos os seus equipamentos de redes sem fio em funcionamento e mudar para uma solução mais segura; eles enxergaram a necessidade de criar uma forma de poder melhorar a segurança por meio de atualizações de software.

Para atender a necessidade de atualização, o grupo de trabalho 802.11i começou a desenvolver uma solução baseada na necessidade de aperfeiçoar a segurança respeitando as limitações dos dispositivos em uso. O resultado deste trabalho foi a definição do *Temporal Key Integrity Protocol* (TKIP) como um modo alternativo dentro da RSN. O desenvolvimento do TKIP foi uma grande ajuda para a atualização dos sistemas existentes, mas a indústria não poderia esperar mais até chegar ao fim do lento processo de ratificação do padrão. Então, a *Wi-Fi Alliance* resolveu adotar uma nova abordagem baseada em um subconjunto do projeto que vinha sendo desenvolvido pelo *task group* IEEE 802.11i só contemplando o TKIP. Este subconjunto foi chamado *Wi-Fi Protected Access* (WPA) e foi lançado para ser uma especificação provisória.

O WPA começou a surgir implementado nos equipamentos em meados de 2003 e muitas empresas produziram atualizações de softwares para seus produtos. Então, os seus produtos puderam suportar o WPA ao mesmo tempo em que os novos produtos já saíam com o WPA implementado de fábrica. A *Wi-Fi Alliance* fez todo um planejamento para garantir a interoperabilidade entre os diversos fabricantes.

Casos como esse em que a indústria se antecipou à criação dos padrões não são incomuns e muitas vezes ocorrem quando se trata de tecnologia, o que normalmente origina duas linhas distintas de desenvolvimento (uma que leva ao padrão de fato desenvolvido e adotado pela indústria e um padrão de direito desenvolvido e recomendado por um órgão normatizador) que geram

incompatibilidade, como a *Wi-Fi Alliance* arquitetou todo este desenvolvimento isso foi evitado e a maior parte dos fabricantes suporta a especificação do WPA (EDNEY e ARBAUGH, 2003).

O projeto de norma IEEE 802.11i foi ratificado em 24 de Junho de 2004, e substituiu a especificação de segurança anterior. Nessa época *Wi-Fi Protected Access* (WPA) já tinha sido introduzido pela *Wi-Fi Alliance* como uma solução intermédia para inseguranças WEP, a essa as redes foram chamadas por alguns de *Transition Security Network* (TSN).

A norma IEEE 802.11i consistia de três partes principais TKIP, CCMP, 802.1X e gerenciamento das chaves, sua implementação completa também conhecida como RSN faz uso da cifra de bloco *Advanced Encryption Standard* (AES) em oposição a cifra de fluxo RC4 usada no WEP e no WPA (IEEE 802.11i-2004, 2008).

Ninguém pode com legitimidade afirmar que um sistema de segurança é inquebrável, contudo as redes sem fio RSN/WPA foram desenvolvidas com profundo envolvimento de especialistas e receberam muito mais análise e testes da comunidade que trabalha com criptografia do que o WEP recebeu quando foi desenvolvido. O WEP só foi testado e analisado com profundidade depois de completamente desenvolvido o que resultou em um número enorme de vulnerabilidades que poderiam ser evitadas se descobertas durante o ciclo de desenvolvimento. O fato de haver a participação de diversos especialistas em segurança durante o desenvolvimento da RSN/WPA não garante que ela não vai ser quebrada na semana que vem, mas certamente nos dá a confiança de que os métodos de ataque conhecidos atualmente a rede está pronta para enfrentar (GARG, 2007).

2.4 - WPA, TKIP

O IEEE, já sabendo das fragilidades de segurança existentes no WEP, estava trabalhando em um novo padrão que pudesse garantir, dentre outras coisas, o sigilo das informações que trafegavam pelas ondas eletromagnéticas através do ar.

Com uma boa parte do trabalho do grupo IEEE 802.11i rumo à padronização de um novo protocolo concluído e com respaldo dos principais fabricantes de equipamentos para redes sem fio a *Wi-Fi Alliance* lançou o WPA, que pretendia ser uma especificação provisória que viesse atender aos anseios do mercado consumidor e que, ao mesmo tempo, seguisse o padrão que estava por surgir. A *Wi-Fi Alliance* criou o WPA que vinha a ser, portanto, esse subconjunto do trabalho que estava sendo desenvolvido pelo IEEE, nesse subconjunto apenas o TKIP era especificado. A *Wi-Fi Alliance* preocupou-se não só com o planejamento para que todas as empresas associadas a ela seguissem um padrão, fez muito além disso, houve todo um planejamento para garantir a interoperabilidade entre os diversos fabricantes, e que esse novo padrão fosse adotado em dispositivos capazes de suportar o padrão de segurança anterior, portanto, os dispositivos deveriam estar preparados para trabalhar com o WEP, bem como suportar inovações que ainda estavam por surgir fruto do trabalho do IEEE, reforçando assim o caráter transitório do WPA quando foi concebido.

O WPA foi projetado para aperfeiçoar a segurança das redes sem fio. Ele foi desenvolvido de duas formas, podemos dizer: WPA para uso pessoal e o WPA para uso empresarial. Na sua forma empresarial, o WPA seria capaz de operar com servidores de autenticação e IEEE 802.1x (veremos um pouco mais do funcionamento do 802.1x à frente), haveria distribuição de diferentes chaves para cada usuário. Em sua forma pessoal, conhecida como WPA-PSK o WPA utilizaria uma chave previamente combinada (*pre-shared key*), solução bem menos escalável, onde toda AP receberia a mesma chave, no modo WPA-PSK a segurança é extremamente dependente da força e sigilo da chave.

O WPA tem suporte a WEP, TKIP e 802.1x, e possui vetor de inicialização da chave criptográfica de 48 bits. O WPA, conforme requerido na recomendação

802.1x, contém os avanços e melhorias para segurança no que diz respeito às Integridade, Autenticação e Privacidade.

2.4.1 Funcionamento

De forma sucinta, o WPA sendo apenas parte do padrão 802.11i, funciona basicamente através de uma chave temporal (*Temporal Key Integrity Protocol* – TKIP), a qual fornece encriptação de dados através de melhoramento na concatenação de chaves, verificação da integridade das mensagens (*Message Integrity Check* – MIC), melhoramentos no vetor de inicialização (IV), e um mecanismo de atualização de chaves a cada sessão.

Para reforçar a autenticação de usuários, o WPA implementa também o suporte a 802.1x e o *Extensible Authentication Protocol* (EAP). Juntos, estes mecanismos proporcionam um ambiente de forte segurança que permite distribuição de chave dinâmica e autenticação mútua.

Além da criptografia em si, envolvida no processo com intuito de garantir o sigilo da informação que trafega na rede e impedir que pessoas de fora da rede saibam o que estamos transmitindo, há algo que falamos com freqüência, mas que talvez permaneça um tanto obscuro: a Autenticação da Rede.

WPA – AUTENTICAÇÃO DE REDE

Referimo-nos bastante a *Autenticação da Rede*, sem, no entanto, nos preocuparmos em mostrar em que fase do processo de comunicação entre a AP e seus clientes ela se insere.

A autenticação da rede está no início da comunicação entre a AP e seus clientes, quando a AP começa a perceber o sinal de seus potenciais clientes estes entram no processo de autenticação, para só então, obtendo sucesso na autenticação eles se associarem e considerarem um ao outro, componentes legítimos da rede.

A autenticação pode ocorrer de diversas formas, algumas (de nosso interesse e que julgamos relevantes) são, autenticação *Open, Shared*, WPA e WPA com *pre-shared key*, cada uma com suas nuances:

Open - existe apenas uma avaliação da AP por parte do cliente, em seguida envia-se a solicitação que é prontamente aceita, podendo haver criptografia dos dados com o WEP outro protocolo de criptografia ou mesmo inexistir criptografia dos dados;

Shared - a AP, para permitir que o cliente se associe, lança um desafio e a associação só é bem sucedida caso a resposta ao desafio esteja correta;

WPA e WPA com *pre-shared key* - divergem por se tratar de uma versão para empresas e outra para uso pessoal, como vimos, sendo esta última, muitas vezes referenciada na literatura apenas como WPA-PSK (como trazemos). Nesta há um compartilhamento prévio de chave, colocada manualmente presente no WPA-PSK, em seguida, um dos tipos de EAP existentes entra em cena, isso se repete no WPA2. Em outras palavras, a chave pré-compartilhada é colocada manualmente mas depois disso há sucessivas atualizações dinâmicas do EAP (método que suporta autenticação mútua, gerenciamento de chaves e resistência a ataques de dicionário).

No 802.11 original, a autenticação por porta 802.1x é opcional. Já quando se utiliza o WPA, a autenticação 802.1x é exigida. A autenticação WPA é uma combinação de sistemas abertos com o 802.1x e utiliza as seguintes fases, segundo CABIANCA e BULHMAN (2006):

A primeira fase usa uma autenticação de sistema aberto para indicar a um cliente sem fio que pode enviar quadro para o ponto de acesso;

A segunda fase usa o 802.1x para executar a autenticação do usuário.

Para ambientes sem infra-estrutura RADIUS, o WPA suporta o uso de chave pré–compartilhada. Já para ambientes com infra–estrutura de RADIUS, o WPA suporta EAP e RADIUS(CABIANCA E BULHMAN, 2006).

WPA – CRIPTOGRAFIA

Os novos protocolos para confidencialidade dos dados, frutos do trabalho do grupo IEEE 802.11i, são TKIP (*Temporal Key Integrity Protocol*) e o CCMP (*counter-mode/block chaining message authentication code protocol*). No momento, estamos

falando do WPA, por isso nos aprofundaremos na discussão sobre o TKIP, deixando para um momento posterior as explicações relativas ao CCMP.

Com o 802.1x, a troca de chaves de criptografia *unicast* é opcional. Adicionalmente, o 802.11 e o 802.1x não provêem o mecanismo para troca de chave de criptografia que é usada para o tráfego *multicast* e *broadcast*. Com o WPA, a troca destas chaves de criptografia para ambos é necessária. O TKIP altera a chave de criptografia única para todo o quadro, e é sincronizada a cada alteração entre o cliente e o ponto de acesso (CABIANCA E BULHMAN, 2006).

Para a chave de criptografia *multicast*/global, o WPA inclui uma facilidade para o ponto de acesso, para avisar mudanças dos clientes sem fio conectados. Para o 802.11, a criptografia WEP é opcional. Para o WPA, a criptografia usando o TKIP é necessária. O TKIP substitui o WEP com um novo algoritmo de criptografia que é mais forte que o algoritmo WEP e ainda pode ser executado usando as facilidades de cálculo presentes no hardware existente do equipamento wireless (CABIANCA E BULHMAN, 2006).

O TKIP provê também a verificação da configuração de segurança depois de determinar a chave de criptografia e a alteração de sincronização da chave de criptografia para cada quadro e determinação do start (CABIANCA E BULHMAN, 2006).

O TKIP vem a ser um aperfeiçoamento da segurança WEP através da adição de medidas como PPK (*per-packet key* – que seria uma chave diferente para cada pacote), MIC (*message integrity code*) e mudanças na chave de broadcast (CISCO SYSTEMS, 2004).

No TKIP cada pacote transmitido tem um número serial de 48 bits que é incrementado toda vez que um novo pacote é transmitido e usado tanto como vetor de inicialização quanto como parte da chave. Colocando um número de seqüência na chave assegura-se que a chave é diferente para cada pacote, o que resolve outro problema do WEP chamado ataque de colisão, que pode ocorrer quando a mesma chave é usada por dois pacotes diferentes. Com chaves diferentes não há colisões. Usando o número serial também como vetor de inicialização ajuda a reduzir o problema de ataques de replay pois os pacotes demorarão muito tempo para se

repetir e, se for feito um replay de pacotes antigos, eles serão reconhecidos como fora de ordem por causa do número de seqüência que não estará correto.

TKIP, assim como o WEP, usa como cifra de fluxo o RC4 (por conta do suporte dado pelo hardware), com chaves de 128 bits para cifragem e chaves de 64 bits para autenticação. Cifrando as mensagens com uma chave que possa ser usada só pelo destinatário desejado, TKIP ajuda a assegurar que só os destinatários entenderão os dados transmitidos.

O TKIP começa com uma chave temporal de 128 bits que é combinada com um vetor de inicialização (IV) de 48 bits que juntamente com os endereços MAC da origem e do destino passou por um complexo processo conhecido como mistura da chave por pacote[5] que consiste justamente na utilização de uma chave diferente para cada pacote.

Esse processo de mistura da chave é capaz de mitigar os problemas já conhecidos com o vetor de inicialização e ataques a chaves usados contra o WEP.

Por conta de algumas das vantagens apresentadas pelo TKIP aliados ao fato do TKIP usar o algoritmo RC4 e simplicidade de se atualizar o firmware de equipamentos que suportavam apenas o WEP vários fabricantes disponibilizaram versões para atualização do firmware que tornavam seus dispositivos capazes de usar cifragem TKIP.

Mais um importante problema que é resolvido com o TKIP é o freqüente reuso de uma chave bem conhecida de todos da LAN sem fio. Na tabela 2 extraída de EDNEY e ARBAUGH (2003) temos uma coluna com os principais problemas do WEP, relacionando-a aos objetivos a serem atingidos e as mudanças trazidas pelo TKIP.

[5] Per-packet key mixing

Tabela 2 – Mudanças do WEP para o TKIP (EDNEY e ARBAUGH, 2003)

Propósito	Mudança	Fraqueza (relacionar com tabela no WEP)
Integridade	Adiciona um protocolo de integridade à mensagem para evitar adulteração do conteúdo	(3)
Seleção e uso de Vetor de inicialização	Mudar a regra como valores do Vetor de Inicialização (IV) são selecionados e reusar o (IV) como um contador	(1)(3)
Per-Packet Key Mixing	Mudar a chave de encriptação para cada frame	(1)(2)(4)
Tamanho do Vetor de Inicialização	Aumentar o tamanho do IV para evitar o reuso do mesmo IV	(1)(4)
Gerenciamento da Chave	Adicionar um mecanismo para distribuir e mudar o broadcast das chaves	(4)

WPA – INTEGRIDADE DOS DADOS

Integridade de dados é também um ponto fundamental na discussão sobre a segurança de um sistema. Se um atacante é capaz de modificar mensagens e enviar essas mensagens adulteradas ao seu sistema, há diversas formas de comprometer o seu sistema.

No IEEE 802.11 e WEP, o processo usado para proteger dados contra modificação não autorizada usa um algoritmo que opera sobre o purotexto para gerar um *Cyclic Redundancy Check* (CRC). Este algoritmo gera um valor de 4 bytes, *Integrity Check Value* (ICV), que é concatenado ao fim do purotexto, conforme

mostrado na figura 3. O ICV também conhecido como ICV 32–bit é quem assegura a integridade de dados, ele é incorporado ao payload (corpo) do quadro 802.11 e criptografado com WEP. Embora o ICV seja criptografado, é possível através de analisador de criptografia alterar bits no payload criptografado e atualizar o ICV criptografado sem ser detectado pelo receptor.

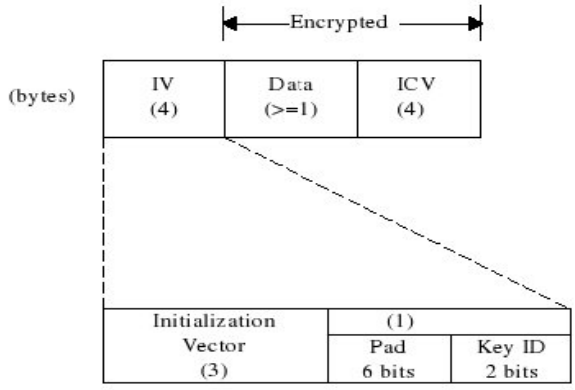

Figura 3 – Uso do ICV-32

Para o problema da integridade de dados, que não encontrou no WEP ferramenta eficiente para detectar adulteração na mensagem, o TKIP usa um meio mais poderoso para checar a integridade dos dados. Há diversos métodos muito seguros de se calcular o MIC, esses métodos já foram testados em outros protocolos e outras aplicações de segurança, contudo, para o TKIP temos um problema. Todos os métodos necessitam de um novo algoritmo criptográfico ou precisam realizar cálculos usando operações de multiplicação com grande velocidade. Os microprocessadores dentro dos chips MAC da maioria dos cartões para redes sem-fio não é muito poderosa; tipicamente não possui qualquer hardware para multiplicação. Um método sem o uso de multiplicações foi proposto pelo criptógrafo Niels Ferguson, esse método que ele resolveu chamar de Michael, só usa deslocamentos e operações de adição, e é limitado a uma pequena palavra de checagem. Michael foi um boa solução na época não só pelos benefícios que trouxe mas também por não trazer consigo o efeito colateral de arruinar o desempenho dos pontos de acesso. Como tudo tem seu preço, Michael é vulnerável a ataques de força bruta.

2.4.2 Algoritmos

Para o entendimento do funcionamento do algoritmo tanto do AES-CCMP quanto do TKIP precisamos entender a diferença de um MSDU e de um MPDU, é bom que sempre seja clara a distinção de quando nos referimos a um ou a outro.

Ambos referem-se a pacotes de dados com endereço de origem e de destino. MSDUs são enviados pelo sistema operacional para a camada MAC e são convertidos em MPDUs para serem enviados por ondas de rádio. Na recepção os MPDUs são captados pela antena e em seguida convertidos em MSDUs para serem enviados para o sistema operacional.

Durante a explicação dos passos para encapsulamento de pacotes TKIP estamos assumindo que o par de chaves master (PMK) é conhecido dos dois lados da comunicação,bem como as chaves de sessão.

Os processos principais na transmissão TKIP são:

- Michael
- Geração do IV/TSC
- RC4
- Derivação das chaves a partir da PMK

Já havíamos assumido que as chaves foram derivadas, portanto TK é nossa chave de criptografia gerada a partir da PMK e MIC *Key* é nossa chave de integridade também obtida através do processo de derivação de chaves, agora vamos assumir também que o TSC já foi corretamente gerado e é ele que provê proteção contra ataques de replay.

Feitas as considerações iniciais vamos a figura 4 que mostra o diagrama de blocos do encapsulamento TKIP.

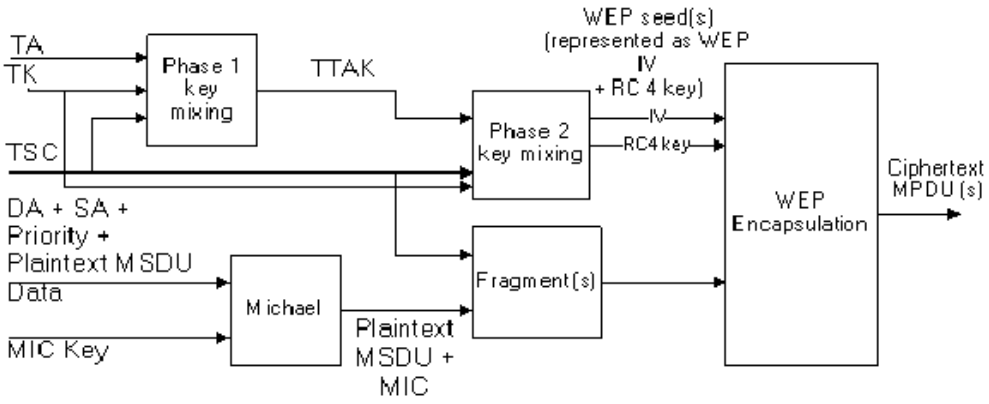

Figura 4 – Diagrama de Blocos do Encapsulamento TKIP (IEEE, 2004)

O TKIP trouxe melhorias a segurança colocando diversas funções adicionais ao encapsulamento WEP como vimos.

1. O cálculo do MIC protege o campo de dados do MSDU, o de endereço de origem (SA), o de endereço de destino (DA) e o de Prioridade. O cálculo do MIC é feito com a entrada da concatenação dos campos SA, DA, Prioridade e dados do MSDU e a entrada da chave de integridade (MIC *Key*). O MIC calculado é então anexado ao campo de dados do MSDU (Plaintext MSDU+MIC). Se necessário o MSDU com MIC podem ser fragmentados em um ou mais MPDUs, para isso valores incrementais do TSC seriam usados.

2. Para cada MPDU, TKIP usa as funções de mistura da chave para calcular o WEP *seed*.

3. O TKIP representa o WEP *seed* como um vetor de inicialização WEP e uma chave RC4 e passa os com cada MPDU para o WEP para que possa ser feita a geração do ICV e para a cifragem do purotexto do MPDU, incluindo o MIC. O WEP usa o WEP *seed* como uma chave default WEP, identificada por um identificador de chave associado com a chave temporal (IEEE, 2004).

Para a geração do WEP *seed*, é importante ressaltar que, fazemos uso da função de mistura do TKIP em duas fases. A entrada da fase 1 temos o endereço do transmissor (TA – 48 bits), a chave temporal (TK – 128 bits) e o TKIP *sequence counter* (TSC – 48 bits, mas só são usados os 32 bits mais significativos na fase 1), computados, temos como saída TTAK (80 bits de comprimento). Na fase 2 o TTAK servirá de entrada juntamente com a chave temporal (TK – 128 bits) e o TKIP

sequence counter (TSC – 48 bits, mas só são usados os 16 bits menos significativos restantes na fase 2), a saída é ó próprio WEP *seed*.

2.4.3 Fragilidades

Ataques a Michael e retaliação

Michael é vulnerável a força bruta e trata esta vulnerabilidade, introduzindo o conceito de represália. O conceito de represália é simples: Tenha um método confiável para detectar quando um ataque está sendo feito e tomar medidas para fechar a porta na cara do atacante, ou seja negar a possibilidade deste atacante continuar tomando aquela ação considerada danosa ao sistema. O mais simples é, tomar a atitude de apenas fechar toda a rede quando é detectado um ataque, impedindo assim que o atacante faça repetidas tentativas (*Wi-Fi Protected Access,* 2008).

Vulnerabilidades de ataques de dicionário no modo PSK

WPA inclui o padrão para a criação de chaves mestras previamente compartilhadas[6] baseadas em caracteres ASCII. O fato de permitir que as chaves sejam baseadas em caracteres ASCII abre a possibilidade de um ataque de dicionário, se um atacante for capaz de descobrir qual password foi usada para gerar a chave (PSK), ele também estará apto a se comunicar perfeitamente com a rede protegida. Se um administrador escolher fazer uso de chaves baseadas em ASCII, ele deve assegurar-se de que a chave usada é longa e inclui também caracteres não alfanuméricos. Pelo fato da chave (PSK) não ser uma password de usuário e ser configurada apenas uma vez, é possível gerá-la pela própria máquina no intuito de torná-la mais robusta (HURLEY et al, 2004).

Quem descobriu que o WPA é vulnerável a ataques de dicionário (ataque de força bruta que tenta senhas e/ou chaves de uma lista de valores pré-escolhidas) foi

[6] *Preshared Master Keys*

Robert Moskowitz do ICSA, em Novembro de 2003 (FLEISHMAN e MOSKOWITZ, 2003).

WPA pode utilizar chaves de 256 ou *passphrase* que podem variar de oito até 63 bytes. Considera-se que frases com menos de 20 bytes de comprimento (consideradas chaves pequenas) são vulneráveis a ataques de dicionário.

2.4.4 Vantagens

O WPA tem diversas vantagens em relação ao seu antecessor o WEP e surgiu justamente devido as inúmeras fraquezas encontradas no WEP. Considera-se hoje que o WEP falhou na missão que lhe foi confiada, ele foi o protocolo concebido pelo IEEE como o encarregado de garantir a mesma segurança, ou melhor, a mesma resistência à escuta indesejada que teriam os dados que trafegassem em uma rede cabeada. Para atingir requisitos de sigilo/confidencialidade, controle de acesso e integridade de dados que era o que inicialmente se esperava do WEP, e que ele não foi capaz de fornecer, pelo menos não por muito tempo, foi desenvolvido o WPA que evolui posteriormente para o WPA2.

O WPA trás consigo não só a melhoria no sigilo, completamente comprometido e susceptível a quebra em pouquíssimo tempo (segundos ou minutos) - que foi um dos principais motivos do WEP ter se tornado ineficaz contra indivíduos dispostos a quebra o sigilo da informação - mas também outros benefícios a segurança como por exemplo a melhoria da integridade da comunicação com o uso do Michael.

A escolha de um novo algoritmo para autenticação de mensagem, ou integridade de mensagem (conhecido como MAC – *Message Authentication Code* ou como MIC - *Message Integrity Code*) foi duplamente vantajosa, com o Michael sendo usado para checar a integridade das mensagens em substituição ao CRC (*Cyclic Redundant Check*) usado no WEP atingiu-se o objetivo de melhoramento de segurança de forma otimizada. Há diversos algoritmos excelentes e testados em diversas aplicações capazes de realizar a checagem de integridade com altíssimos níveis de segurança, mas em sua imensa maioria esses sistemas necessitam de muito processamento, recurso escasso em dispositivos mais antigos presentes no mercado. Com o Michael, conseguiu-se melhorar significativamente a verificação da

integridade dos dados sem no entanto penalizar demasiadamente o desempenho dos dispositivos sem fio, visto que o hardware utilizado nesses dispositivos são muitas vezes muito limitados em capacidade de processamento.

O WPA por utilizar o RC4 como cifra de fluxo podia ser utilizado em várias das placas de rede sem fio que suportavam apenas o WEP apenas por meio da atualização do firmware, o que trouxe economia e estendeu a utilização do hardware já adquirido em uso por diversos clientes no mundo todo.

Outra vantagem do WPA é ser um protocolo que apesar de ter sido desenvolvido com certa urgência preserva compatibilidade entre os fabricantes até mesmo pelo fato de ter sido desenvolvido pela *Wi-Fi Alliance* baseado no padrão que estava em desenvolvimento pelo IEEE.

2.4.5 Desvantagens

O WPA não é fruto de um estudo concluído, apesar de ter sido desenvolvido de forma criteriosa e utilizado parte do padrão que estava em estudo pelo IEEE, não fornece muitas das funcionalidades consideradas indispensáveis para prover segurança a grandes empresas (grandes empresas não aceitam correr o risco de sofrerem com a quebra de sigilo de sua comunicação, por exemplo).

Por não serem uma solução definitiva, podemos afirmar de forma grosseira - mas que não deixa de ser verdade - que o WPA foi uma “gambiarra” em que se buscou realizar melhorias em relação ao WEP sem que se fosse necessário abandonar todo o hardware já comercializado. É como se o WPA já nascesse com data para acabar.

Por conta de diversas pequenas melhorias, como no uso do Michael surgiram vulnerabilidades, neste a vulnerabilidade era a sua a susceptibilidade a ataques de força bruta. Outro fator importante na própria adoção do Michael é que ele é um algoritmo novo, o que é sempre olhado com desconfiança por especialistas em criptografia pois estes algoritmos podem muitas vezes fornecer uma falsa sensação de segurança baseando-se na obscuridade e na falta de testes destes algoritmos.

Embora esquemas de criptografia bem melhores já existissem na época em que foi criado o WPA eles não poderiam ser utilizados pois os projetistas do WPA precisavam encontrar uma forma de não condenar todos os milhões de dispositivos

(interfaces de redes e pontos de acesso sem fio) legados que foram comercializados e ainda estavam em produção.

2.4.6 Uso atual

Apesar de ser um protocolo concebido para ser uma transição entre o WEP e o WPA2 que usa o AES. O WPA, talvez por não possuir nenhuma vulnerabilidade capaz de abalar a confiança que se tem nele hoje, continua a ser bastante utilizado. Tomando como base os estudos realizados pelo Kaspersky Lab (estudos esses que são prova cabal da falta de preocupação com a segurança na maioria das redes sem fio implementadas), em São Paulo 22% da redes usam ainda criptografia WPA (BESTÚZHEV, 2007). Na China em estudos desenvolvidos pelo mesmo laboratório nas cidades Tianjin e Pequim, no final de 2005, não foi encontrada rede com implementação do WPA e nem do WPA2 (GOSTEV, 2005), apenas com criptografias mais antigas, como o WEP .

2.4.7 Tamanho das Chaves

TKIP usa para cifragem uma chave de criptografia de 128 bits. Para o cálculo do MIC, a chave é de 64 bits (IEEE, 2004).

2.5 - WPA2

Se o WPA foi um protocolo que já nasceu com os dias contados, criado já com o rótulo de protocolo provisório, já que implementava apenas um subconjunto do padrão IEEE 802.11i, o WPA2 veio com a idéia de ser o protocolo de segurança de rede sem fio. O WPA2 implementa todos os elementos obrigatórios do padrão IEEE 802.11i.

É importante ressaltar, que apesar de haver vulnerabilidade no modo de operação PSK do WPA sujeitando-o a ataques de dicionário sob certas circunstâncias, o TKIP foi muito bem sucedido como solução provisória. O TKIP foi projetado para ser uma solução transitória e atingiu o objetivo de fornecer segurança suficiente por 5 anos enquanto as organizações realizariam gradativamente a transição para o mecanismo de segurança baseado no padrão IEEE 802.11i completo. Durante este período não foi encontrada nenhuma falha catastrófica no protocolo TKIP, tais como as que foram encontradas no WEP (as falhas do WEP serviram de motivação para que a indústria deixasse a inércia e buscasse melhores formas de fornecer segurança para as redes sem fio) (WRIGHT, 2006).

Em particular, o WPA2 introduz um novo algoritmo criptográfico baseado no AES, o CCMP, que é considerado completamente seguro, mas traz o inconveniente de não poder se comunicar com algumas interfaces de rede mais antigas.

Tanto o WPA quanto o WPA2 são padrões que foram criados pela *Wi-Fi Alliance* e por isso gozam da interoperabilidade e segurança padronizada para a indústria de dispositivos para redes locais sem fios. O padrão WPA2 implementa todos os elementos obrigatórios do padrão IEEE 802.11i e foi lançado logo após a conclusão dos trabalhos do grupo de trabalho i (TGi responsável pelo desenvolvimento do IEEE 802.11i) finalizado em julho de 2004.

O WPA2 implementa todo o padrão, mas não será capaz de trabalhar com algumas placas de rede mais antigas. A *Wi-Fi Alliance* refere-se a sua implementação de todo o 802.11i como WPA2, também conhecido como RSN.

2.5.1 Funcionamento

O WPA2 é baseado nos mecanismos da *Robust Security Network* (RSN) e oferece suporte a todos os mecanismos disponíveis no WPA tais como:

- Suporte para cifragem e autenticação fortes para redes Ad-hoc e redes Infra-estruturadas (WPA limita-se a redes Infra-estruturadas);
- Custo reduzido na derivação da chave durante a troca de informação para autenticação em uma LAN sem fio;
- Suporte para armazenamento da chave para reduzir o atraso no processo de *roaming* entre *access points*;
- Suporte a pré-autenticação, onde uma estação completa o processo de troca de informação para autenticação IEEE 802.1x antes de realizar o *roaming*;
- Suporte ao CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) mecanismo de encriptação baseado no AES (*Advanced Encryption Standard*), esse mecanismo é uma alternativa ao protocolo TKIP existente no WPA (WRIGHT, 2006).

Assim como o WPA o WPA2 tem um modo de operação pessoal e um modo de operação empresarial que visam atender necessidades distintas destes dois diferentes segmentos do mercado. O WPA2 empresarial tem como alvo clientes que irão realizar autenticação fazendo uso de IEEE 802.1x e o EAP, enquanto que no modo de operação do WPA2 pessoal, também conhecido como WPA2-PSK, uma chave pré-compartilhada (por isso o PSK, de *pre-shared key*) é usada para a autenticação. Tipicamente, no modo Enterprise há a necessidade de um servidor de autenticação tal qual um servidor RADIUS presente na rede e no *personal* apenas uma *access point* e um dispositivo cliente são necessários.

O WPA2 apresenta componentes que são cruciais para a segurança da rede sem fio, Autenticação, Cifragem e Integridade.

WPA2 – AUTENTICAÇÃO DE REDE

A parte relacionada a autenticação usada tanto pelo WPA quanto pelo WPA2 antes de ser atualizada se restringia ao uso da PSK para o modo de operação

pessoal e ao EAP-TLS para o método empresarial. Após a atualização quatro novos métodos de autenticação foram adicionadas e a lista de WPA/WPA2 EAP certificados pelo padrão passou a ser:

- EAP-TLS;
- EAP-TTLS/MSCHAPv2;
- PEAPv0/EAP-MSCHAPv2;
- PEAPv1/EAP-GTC;
- EAP-SIM.

Abaixo falaremos um pouco de cada um dos métodos WPA/WPA2 EAP certificados pelo padrão e também da autenticação para o modo de operação pessoal (PSK).

✓ EAP-TLS

É considerado um dos padrões de autenticação (EAP) mais seguros disponíveis, é universalmente suportado por todos os fabricantes de hardware e software para redes sem fio. O que o torna um padrão tão seguro é a necessidade de um certificado do lado do cliente, isso também o torna impopular e raramente implementado. EAP-TLS é baseado no protocolo SSL (*Secure Socket Layer*) usado para dar segurança ao tráfego Web. O uso de certificado tanto do lado do cliente quanto do lado do servidor requer uma infra-estrutura que pode estar além do que uma determinada empresa tem condições de investir e por conta disso torna proibitivo o seu uso.

Certificados são usados para autenticar o servidor de autenticação para o *supplicant* no EAP-TLS com uma opção para autenticar o *supplicant* para o servidor de autenticação. O processo é iniciado quando o servidor de autenticação envia seu certificado digital para o *supplicant*. Na autenticação *one-way* um servidor envia seu certificado para um browser para provar sua identidade. É preferível para proteção contra ataques de homem no meio o uso da autenticação mútua. O EAP-TLS permite a autenticação mútua entre *supplicant* e servidor de autenticação, negociação do método de cifragem, e troca de chaves privadas com segurança (RITTINGHOUSE e RANSOME, 2004).

- ✓ EAP-TTLS/MSCHAPv2

EAP-*Tunneled Transport Layer Security* ou simplesmente EAP-TTLS é um protocolo que foi desenvolvido pela Funk Software e pela Certicom. Embora seja um bom protocolo até mesmo melhor que PEAP em alguns aspectos, pesa contra ele o fato de não ser suportado nativamente por clientes como Windows 2000, XP, *Mobile* 2003 ou CE da Microsoft, para funcionar em SO da Microsoft é necessária a instalação de pequenos programas extra. Dentre os servidores sua ausência é sentida no MS Windows 2003 e Cisco ACS. O EAP-TTLS simplifica o processo pois o cliente não precisa se autenticar para o servidor através de uma Autoridade Certificadora, mas o servidor precisa se autenticar para o cliente. Depois de certificado o servidor estabelece uma conexão segura (túnel) para autenticar o cliente. Depois de estabelecido o túnel pode-se usar mecanismos obsoletos de lidar com senhas e base de dados de autenticação, pois o túnel já fornece proteção contra escuta indesejada do canal e ataque de homem-no-meio. Uma das vantagens deste método é o fato do nome do usuário jamais trafegar em texto plano.

O ponto principal onde o EAP-TTLS se destaca em relação a autenticação PEAP é que o nome do usuário não é revelada em texto puro, o que pode evitar alguns ataques de negação de serviço (DoS) onde alguém pode com má intenção tentar se autenticar com um nome de usuário correto e com uma senha errada para bloquear o acesso daquele usuário. PEAP por sua vez só protege a senha com um túnel TLS, mas envia o nome do usuário em texto plano (VACCA, 2006).

- ✓ PEAPv0/EAP-MSCHAPv2

Sempre que se ouvir falar em PEAP quase sempre estará sendo feita referência a esta forma de PEAP, a maioria das pessoas não fazem idéia dos vários tipos de PEAP. Depois de EAP-TLS, esta é a versão mais disponível dentre os padrões de EAP no mundo. Há implementações cliente e servidores deste na Microsoft, Cisco, Apple, Linux e código aberto. O PEAPv0/EAP-MSCHAPv2 goza de suporte universal e é conhecido como o padrão PEAP (VACCA, 2006).

- ✓ PEAPv1/EAP-GTC

O PEAPv1/EAP-GTC foi criado pela Cisco como uma alternativa ao PEAPv0. A Microsoft nunca adicionou suporte para o PEAPv1/EAP-GTC, logo os SO Windows não oferecem suporte nativo. Somado-se a falta de suporte nos sistemas operacionais da Microsoft está a falta de incentivo da própria Cisco para disseminar o uso deste protocolo o que faz do PEAPv1 um protocolo que é raramente usado e que não é suportado nativamente por nenhum SO (VACCA, 2006).

- ✓ EAP-SIM

EAP-SIM é um padrão da IETF que foi desenvolvido pelo 3GPP (3rd *Generation Partnership Project*) e uma RFC a de número 4186 (RFC 4186 – *Extensible Authentication Protocol Method for Global System for Mobile Communications "GSM" Subscriber Identity Modules* "EAP-SIM") foi divulgada em 2006 para servir de informação para a comunidade. Este método de autenticação e geração de chaves de encriptação baseia-se na utilização de um SIM-card (*reader*) no cliente e apoia-se em elementos de rede já existentes nas redes GSM/GPRS (HLR/AuC, etc) e como tal será à partida apenas utilizado pelos operadores móveis que já têm uma rede GSM/GPRS. Especifica um mecanismo de autenticação mútua e acordo de chave de sessão usando o GSM-SIM e usado em redes de telefonia móvel baseadas em GSM (CISCO SYSTEMS, 2003).

- ✓ Autenticação *Pre-Shared Key* (PSK)

Algumas redes, principalmente de pequenas empresas e de uso pessoal, apesar de implementarem criptografia e outros recursos para resguardar a sua segurança podem não ter sido planejadas para usar um servidor de autenticação, seja por seu pequeno número de clientes, seja por um custo que a administração da rede não queira arcar. Para tal nicho existe o modo de segurança com chave pré-compartilhada que oferece segurança sem a complexidade de ter um servidor de autenticação. Nesse modo (também conhecido como modo pessoal) cada usuário deve digitar uma frase secreta para obter acesso a rede. A frase secreta pode ter entre 8 e 63 caracteres ASCII ou 64 dígitos hexadecimais (256 bits).

Se a escolha for por usar caracteres ASCII, uma função de hash reduzirá a frase de 504 bits (63 caracteres*8 bits/caractere) para 256 bits (usando também o SSID). A frase de acesso deve permanecer gravada na *access point* e no computador do usuário para evitar a necessidade de freqüentemente ter que se digitar novamente. No caso do uso de chaves pré-compartilhadas a segurança é reforçada pelo emprego de uma função de derivação de chave PBKDF2. Esta função de derivação de chaves é parte do *Public-Key Cryptography Standards* number 5 (PKCS5 v2.0), também publicado como RFC 2898 da IETF. O PBKDF2 aplica uma função pseudo-aleatória, tal como um hash criptográfico, uma cifragem ou um HMAC a uma senha ou uma frase de acesso juntamente com um valor de sal e repete o processo muitas vezes para produzir a chave derivada, que poderá ser usada como uma chave criptográfica nas operações subseqüentes.

A segurança é reforçada com o emprego dessa função de derivação de chave PBKDF2 pois o sal adicionado a senha reduz a susceptibilidade a ataques de dicionário e as iterações aumentam o trabalho que o atacante deve ter para construir um ataque de força bruta. Contudo, assim como no caso do WPA-PSK também WPA2-PSK o uso de frases de acesso fracas são vulneráveis a ataques que podem conseguir burlar o sistema de acesso, por meio de força bruta, por exemplo. Para proteger contra ataques de força bruta uma frase de acesso aleatória de pelo menos 20 caracteres deve ser usada, e 33 ou mais caracteres é o que é recomendado. Na tentativa de evitar a escolha de frases de acesso fracas que facilitariam o acesso indevido a rede, alguns fabricantes adicionaram um método de automaticamente gerar e distribuir chaves fortes através de uma interface de software ou hardware que usa um método externo de adicionar um novo adaptador *Wi-Fi* ou *appliance* a rede. A *Wi-Fi Alliance* padronizou este método em um programa chamado *Wi-Fi Protected Setup* (*Simple Config*).

WPA2 – CIFRAGEM e INTEGRIDADE

Terminado o desenvolvimento do padrão IEEE 802.11i veio com ele a definição de um novo método de cifragem baseado no *Advanced Encryption Standard* (AES). Fazendo uso de cifragem baseada no AES poder-se-ia usar um grande número de diferentes algoritmos e modos de operação. O modo que foi

escolhido no padrão definido pelo IEEE foi o modo contador (*Counter Mode - CTR*) com CBC-MAC (*Cipher Block Chaining – Message Authentication Code*). O modo contador fornece a privacidade dos dados enquanto o CBC-MAC é responsável pela integridade e autenticidade. AES é um cifrador de bloco simétrico em que múltiplos passos (ciclos) são dados sobre os dados para cifragem, e o texto puro é cifrado em blocos de comprimento fixo. O AES padrão usa blocos de 128 bits para cifragem, e para o 802.11 a chave de cifragem também tem comprimento fixo de 128 bits.

Formato MPDU CCMP

Para ajudar a solidificar o conhecimento acerca do CCMP é interessante conheçamos o formato do MPDU CCMP. Na figura 5 temos a representação gráfica deste formato.

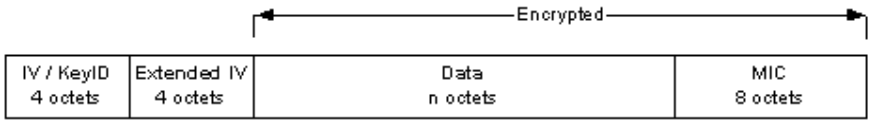

Figura 5 – Formato MPDU do CCMP (EATON, 2002)

O processamento CCMP expande o tamanho original do MPDU em dezesseis octetos, oito octetos para o campo de cabeçalho CCMP e oito octetos para o campo do MIC. Perceba que o CCMP não usa o *Integrity Cheack Value* do WEP.

O CCMP usa o chamado *packet number* (PN). O *packet number* é usado com outras informações para inicializar o cifrador AES tanto para o cálculo do MIC (*Message Integrity Code*) quanto para a cifragem do quadro.

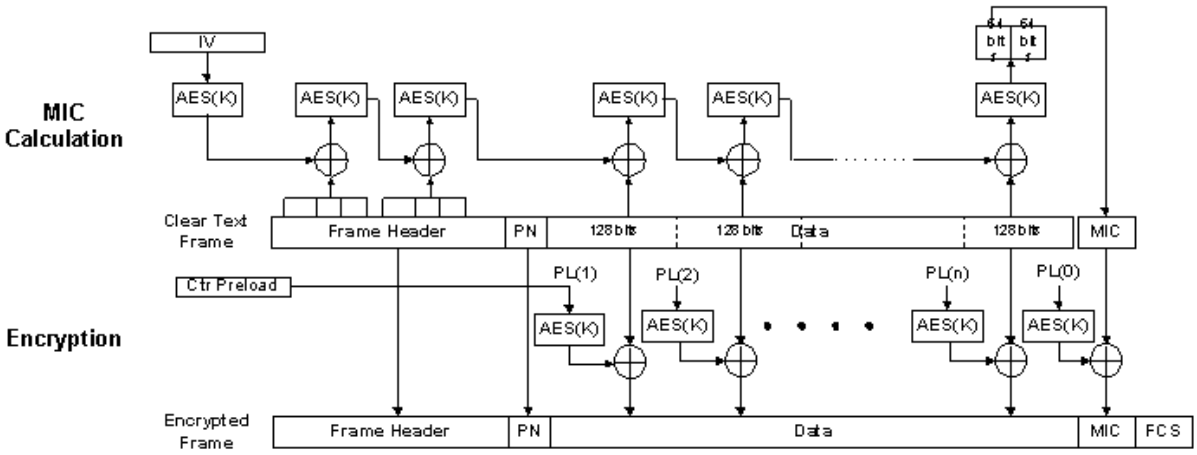

Figura 6 – Processo de encapsulamento CCMP (EATON, 2002)

Os blocos de cifragem AES no cálculo do MIC e a cifragem do pacote usa a mesma chave temporal de cifragem. O cálculo do MIC e o processo de cifragem seguem por caminhos paralelos como mostrado na figura 6. O cálculo do MIC recebe um Vetor de Inicialização formado por um flag, o PN, e outros dados retirados do cabeçalho do quadro. Este Vetor de Inicialização é alimentado em um bloco AES e com sua saída é feita um XOR com os elementos selecionados do cabeçalho do frame, que depois são alimentados no próximo bloco AES. Este processo continua sobre o resto do cabeçalho do quadro e ao longo de todo o comprimento do pacote de dados para computar um valor CBC-MAC final de 128 bits. Os 64 bits superiores deste MAC são extraídos e usados no MIC anexado ao final do quadro cifrado.

O processo de cifragem tem o acréscimo de um Ctr preload formado pelo PN, um valor de flag, dados do cabeçalho do quadro, e um valor contador que é inicializado com 1. Este valor de Ctr preload alimenta o bloco AES e com sua saída é feito um XOR com texto puro de 128 bits do quadro não cifrado. O valor do contador é incrementado de um e o processo é repetido para o bloco seguinte de 128 bits de texto puro. Este processo continua ao longo do comprimento do quadro até o quadro inteiro ter sido cifrado. O valor final do contador é colado para 0 e a entrada para um bloco AES do qual com a sua saída é feito um XOR com o valor do MIC calculado previamente antes de anexar ao fim do quadro cifrado para a transmissão.

O processo de desencapsular o CCMP não vai ser mostrado mas é essencialmente o inverso do processo de encapsulamento da figura 6. Um passo final é adicionado para comparar o valor do MIC calculado ao MIC recebido antes do quadro decifrado ser passado pelo MAC.

2.5.2 Algoritmo

O processo de encapsulamento de CCMP já foi mencionado anteriormente, agora, vamos ver com maior riqueza de detalhes como o CCMP cifra o payload de um purotexto MPDU, quais os passos que são dados para isso e qual o cifrotexto resultante, para nos auxiliar nesta tarefa, e tornar de mais fácil assimilação o funcionamento temos abaixo a figura 7 que representa o diagramas de bloco do encapsulamento CCMP:

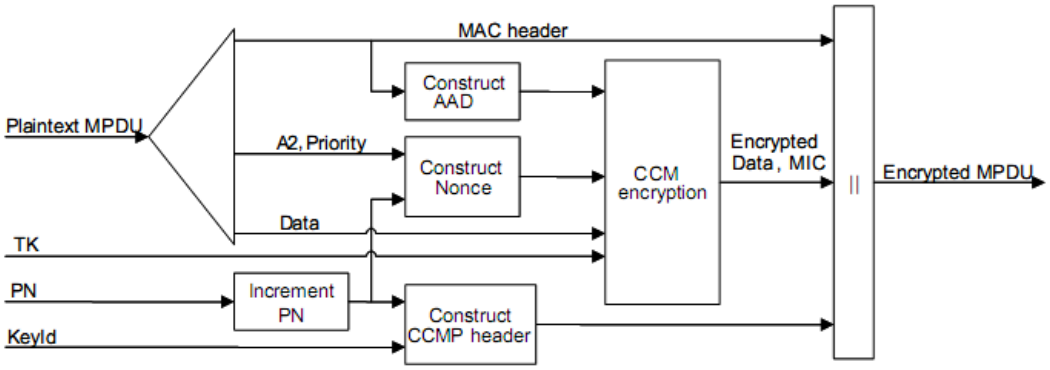

Figura 7 – Diagrama em blocos do encapsulamento CCMP (IEEE, 2004)

1. Incrementa o PN, para obter um PN novo para cada MPDU, então o PN nunca se repete para a mesma chave temporal.
2. Use os campos do cabeçalho do MPDU para construir um *additional authentication data* (AAD) para o CCM. O algoritmo CCM provê integridade para os campos incluídos no AAD.
3. Construa o bloco CCM Nonce que recebe como entradas o campo PN, o A2 e o *Priority* do MPDU onde A2 é o *Address* 2 do MPDU. O campo *Priority* tem um valor setado para 0.

4. Coloque o novo PN e o identificador da chave (KeyId) no cabeçalho CCMP de oito octetos.
5. No processo originador do CCM, como é conhecido o CCM *encryption*, usamos a temporal key, AAD, nonce e os dados do MPDU para formar o cifrotexto e o MIC.
6. Forma-se o MPDU cifrado pela combinação cabeçalho do MPDU original, o cabeçalho CCMP e os dados cifrados e o MIC.

2.5.3 Fragilidade

Assim como ocorreu com o WPA que no modo PSK pode ser alvo de ataques de dicionário ocorre também sob as mesma circunstâncias com o WPA2 funcionando no modo PSK.

Já em relação a integridade, que tínhamos problema com ataques de força bruta ao Michael, o WPA2 trás melhorias e não encontramos na literatura consultada menção a vulnerabilidades.

2.5.4 Vantagens

A segurança baseada no AES é considerada mais forte do que a segurança baseada no TKIP. Isso não quer dizer que o TKIP seja ruim ou apresente falhas.

O CCMP foi projetado desde o início usando as melhores técnicas conhecidas para oferecer segurança para o padrão IEEE 802.11, por isso é considerado mais forte do que o TKIP.

Para simplicidade da implementação e para aliviar o usuário de fazer mais essa escolha durante a instalação foi estabelecido pelo grupo de trabalho IEEE 802.11i que o tamanho da chave e o tamanho do bloco seriam de 128 bits.

O modo de operação define como provê encriptação e autenticidade.

2.5.5 Desvantagens

Falta interoperabilidade com dispositivos legados IEEE 802.11b, forçando uma atualização de todo o hardware de rede sem fio legado que só operava com WEP e cujo hardware foi concebido para trabalhar com o RC4 e não com o AES.

2.5.6 Uso atual

A tendência é que ganhe cada vez mais adeptos por oferecer uma segurança mais robusta já que o WPA usa o TKIP e foi concebido com o intuito de ser provisório, servir como transição entre o WEP e o novo padrão do IEEE. A medida que o hardware legado venha sendo substituído as novas redes devem passar a usá-lo com maior freqüência.

Seu uso ainda é muito pequeno, em termos percentuais, a sua adoção fica atrás do WEP e do WPA segundo estudos desenvolvidos pelo Kaspersky Labs nas cidade de São Paulo (BESTÚZHEV, 2007), na China em estudos desenvolvidos pelo mesmo laboratório nas cidades Tianjin e Pequim não foi encontrada rede com implementação do WPA e nem do WPA2 (GOSTEV, 2005).

2.5.7 Tamanho das chaves

Para a implementação do AES no WPA2/802.11i, uma chave de comprimento de 128 bits é usada (*Wi-Fi Alliance*, 2005)(IEEE, 2004).

2.6 - USO DE RADIUS, IEEE 802.1x

Vimos que apesar do enorme reforço advindo com o surgimento e padronização do WPA e do WPA2 as suas versões pessoais (PSK) apresentam vulnerabilidades para chaves de comprimento menor que 20 caracteres. (MARTIN, 2005)

Por isso a necessidade de se implementar mecanismos mais robustos de autenticação é fundamental para grandes empresas, principalmente, para tanto, as versões enterprise tanto do WPA quanto do WPA2 permitem o uso de servidores de autenticação (RADIUS), IEEE 802.1x e EAP.

Com o uso de EAP há a geração dinâmica de chaves durante a autenticação, eliminando problemas relativos ao uso de chaves estáticas. Embora o RADIUS (IETF RFC 2865) não seja parte do padrão IEEE 802.11i, muitas implementações práticas usam-no para realizar a comunicação entre a AP e o servidor de autenticação. 802.1x oferece suporte a padrões EAP e RADIUS que além de flexibilidade fornecem interoperabilidade na realização da autenticação em um ambiente que se deseje gerenciamento de chave e identificação do usuário centralizados.

A padronização do EAP deu-se com o intuito de amenizar a disseminação de soluções de autenticação proprietárias, acreditava-se que as soluções criadas pelos diferentes fabricantes traziam como efeito colateral a falta de compatibilidade e interoperabilidade entre sistemas. Cada implementação EAP oferece diferentes características e funcionalidades, é importante analisar como veremos a frente diversos fatores antes de decidir a solução EAP mais apropriada para nosso ambiente (RITTINGHOUSE e RANSOME, 2004).

Quando o interesse pelo nível de segurança da infra-estrutura cresce, a necessidade de afastar a possibilidade de ataques de dicionário e facilitar a expansão da rede passa a se tornar relevante e com boa relação custo/benefício a implementação de um servidor de autenticação.

O padrão IEEE 802.1X é um padrão IEEE para controle de acesso a rede baseado em portas. Ele é também usado em redes sem fio e é baseado na EAP, *Extensible Authentication Protocol* (RFC 2284/RFC 3748) (IEEE 802.1X, 2008).

O próprio padrão 802.11i que define uma correção na segurança do 802.11 já traz em seu interior informações da autenticação fazendo uso do IEEE 802.1X.

> 8.4.5 Gerenciamento da porta controlada do IEEE 802.1x
>
> Quando a política de seleção escolhe a autenticação IEEE 802.1X, esta alteração do IEEE 802.11 assume que Supplicants e Authenticators IEEE 802.1X Supplicants e Authenticators trocam informações do protocolo através da porta não-controlada do IEEE 802.1X. A porta controlada do IEEE 802.1X é bloqueada para passar o tráfego de dados em geral entre as STAs até que o processo de autenticação termine com sucesso na porta não-controlada. A garantia de um RSNA depende desta hipótese ser verdadeira.[7](IEEE, 2004)

Lembre-se o padrão IEEE 802.1X não é especificamente um padrão voltado para redes sem fio, essa má compreensão leva a muitos referenciarem incorretamente o padrão 802.1X como 802.11X.

O 802.1X pode ser implementado tanto em redes cabeadas ou em redes sem fio. O 802.1X tem em sua estrutura três componentes principais:

Supplicant WN – um nó da rede que está solicitando autenticação e acesso aos recursos da rede;

Authenticator AP - um dispositivo que bloqueia ou permite que o tráfego passe através de sua porta; quando o *authenticator* detecta um novo cliente sua porta fica habilitada mas em um estado "não-autorizado", neste estado apenas o tráfego de autenticação 802.1X será permitido enquanto todo o tráfego restante é bloqueado até que a identidade do cliente (*supplicant* WN) seja verificado.

O autenticador para isso mantém duas portas virtuais: uma porta não-controlada e uma porta controlada. A porta não-controlada permite que o tráfego de autenticação EAP passe, enquanto a porta controlada bloqueia todo o outro tráfego até o WN ter sido autenticado.

---

[7] "8.4.5 RSN management of the IEEE 802.1X Controlled Port

When the policy selection process chooses IEEE 802.1X authentication, this amendment assumes that IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled port. The IEEE 802.1X Controlled Port is blocked from passing general data traffic between the STAs until an IEEE 802.1X authentication procedure completes successfully over the IEEE 802.1X Uncontrolled Port. The security of an RSNA depends on this assumption being true."

Authentication server (AS) – um servidor que irá validar as credenciais passadas pelo *supplicant* que está solicitando acesso e notifica o autenticador que o *supplicant* foi autorizado. O servidor de autenticação manterá uma base de dados ou pode buscar em uma base de dados externa para autenticar as credenciais do usuário.

Em nosso ambiente sem fios, o *supplicant* pode ser uma estação cliente que requisita acesso à rede. Uma *access point* ou um switch sem fio poderiam fazer o papel de *authenticator*, bloqueando o acesso através de portas virtuais. O servidor de acesso em geral é um servidor RADIUS, outras opções como Kerberos e TACACS+ também podem ser utilizadas. Na figura 8 temos um cliente WN tentando obter acesso aos recursos da rede, e os passos até que ele tenha permissão para acessar esses recursos.

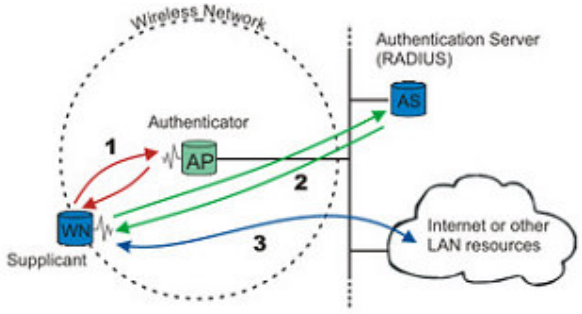

Figura 8 – Autenticação IEEE 802.1X (IEEE 802.1X, 2008)

Embora já tenhamos mostrado os principais elementos de uma estrutura de controle de acesso 802.1X, ainda nos falta uma forma para que a comunicação entre os elementos se processe, falta um protocolo de autenticação para realizar o processo de autenticação. *Extensible Authentication Protocol* (EAP) é usado para fornecer a autenticação do usuário.

No 802.1X o *authenticator* serve como um caminho de passagem para os dados, permitindo o tráfego de dados EAP através de sua porta virtual não-controlada, enquanto o cliente (*supplicant*) e o servidor de autenticação (AS) que possuem mais recursos de processamento fazem os cálculos criptográficos e comunicam-se usando este protocolo EAP. Uma vez que o AS verificar as credenciais do *supplicant*, o servidor envia uma mensagem para o *authenticator* que

o *supplicant* foi autenticado e o *authenticator* pode liberar a porta virtual controlada, permitindo todo o tráfego passar através dela. A figura 9 mostra de forma genérica a troca de dados 802.1X/EAP.

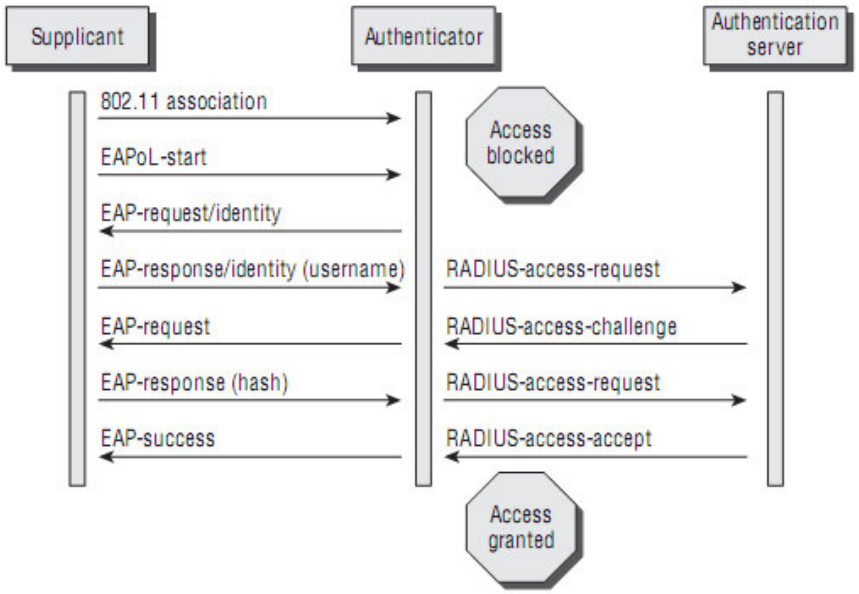

Figura 9 - 802.1X/EAP authentication

O protocolo EAP então é usado nas implementações de rede sem fio como um método para conduzir informações de autenticação através de uma AP entre um usuário (*supplicant*) e um servidor de autenticação (em geral RADIUS). O EAP fornece a metodologia de autenticação enquanto o 802.1x provê o controle de acesso baseado na porta. Dessa forma EAP e 802.1x estão intimamente ligados para fornecer uma solução de autenticação.

A autenticação através do IEEE 802.1x/EAP pode ainda usar as diferentes implementações do EAP. Dentre os métodos de autenticação EAP disponíveis, há a possibilidade de variação dentre outras coisas em decorrência do sistema operacional do cliente e do servidor de acesso, além da base de dados. A escolha do tipo de EAP está condicionada não só as características de cliente e servidor de autenticação (mas eles são fundamentais visto que determinados tipos de EAP podem não ter implementação para um sistema operacional específico, por isso a enaltecemos), mas também não podemos negligenciar que além do sistema

operacional existem outros custos envolvidos que podem tornar esta ou aquela solução proibitiva ou inadequada são elas:

- aceitação da indústria;
- padronização;
- custo de gerenciamento e suporte;
- requisitos de implementação;
- geração, distribuição e rotação de chave dinâmica;
- dificuldades relativas a implementação em determinados ambientes.

Como exemplo de solução muito segura, mas raramente implementada segundo VACCA (2006) temos o EAP-TLS, que é suportado por diversos hardwares e sistemas operacionais, mas é raramente implementado por exigir um certificado do lado do cliente.

Por conta dos vários custos associados é extremamente recomendada uma ampla análise (levantamento e validação dos custos de manutenção, gerenciamento, treinamento e implantação) antes de dar início a implementação de um EAP. Outros custos devem ser igualmente analisados com cuidado, advindos da necessidade de hardware e software adicionais, como licenças de software para servidores e licenças para as máquinas clientes que podem ser necessárias, já que alguns pacotes de software podem ser gratuitos e rodar em máquinas comuns, enquanto outros precisam de muitos recursos do hardware e licenças de software pagas. Uma má análise pode acarretar comprometimento da própria segurança, ou mesmo gastos além dos planejados, o que dizer de uma empresa que tem uma rede toda baseada em sistema operacional Microsoft uma equipe preparada para dar suporte a esta rede e resolve mudar a solução para Linux, o custo total da solução, apesar da economia com as licenças, pode ser proibitivo dada a necessidade de contratar pessoal novo, ou mesmo dar treinamento ao pessoal para ambientá-los a nova plataforma.

A escolha de um método de autenticação é um processo crítico para o sucesso da segurança de sua rede sem fio, a escolha deve ser pensada sempre se levando em conta no mínimo as características do servidor de autenticação e do cliente. A escolha da melhor opção dada a quantidade de métodos disponíveis pode ser uma tarefa difícil, pois todos os métodos têm vantagens, desvantagens e

características que os tornam mais adequados a esse ou àquele ambiente. Para ambientes sem fio uma característica extremamente importante em um EAP, para combater possíveis ataques, é a autenticação mútua (o cliente autentica o servidor e o servidor autentica o cliente) recomendada, pois assegura que o cliente se conectou a rede correta e evita ataques por meio de dispositivos e servidores impostores (rogue). Usando autenticação só do cliente deixa-se a possibilidade de ocorrência de ataque de homem no meio (RITTINGHOUSE e RANSOME, 2004).

Para certificar um produto como um produto WPA-Enterprise e WPA2-Enterprise há certo tempo atrás apenas era testado o método EAP-TLS. Para permitir maior interoperabilidade entre os múltiplos vendedores e fornecer uma maior diversidade de protocolos, a *Wi-Fi Alliance* aumentou o número de protocolos que devem ser implementados pelos fabricantes que queiram certificar seus produtos como WPA- e WPA2- Enterprise após esse acréscimo os tipos de EAP suportados, como visto anteriormente, são:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

(Wi-Fi Alliance, 2007).

Esses vários tipos de EAP servem para diferentes tipos de *supplicant* e de *login*. Cada um com uma proposta de resolver diferentes problemas, com diferentes vantagens e desvantagens, com diferentes custos de execução.

Para ambientes sem fio são mais adequados e devem ser adotados métodos de EAP que suportem autenticação mútua.

2.7 - Problemas: Rogue APs e Sinal Atingindo Áreas Além das Desejadas

2.7.1 APs Impostores

Especialistas e analistas concordam que com a disseminação de redes WLAN, há uma alta probabilidade de dispositivos sem autorização passarem a fazer parte da rede de grandes empresas. A esses dispositivos de rede sem fio não autorizados, mas que se conectam a uma rede ou dispositivo desta rede damos o nome de Rogue APs. Esses APs instaladas em um rede sem o consentimento das instituições ou corporações e que podem funcionar como uma porta para visitantes indesejáveis e por isso são considerados um dos maiores riscos para a segurança da rede de um empresa (AIRDEFENSE, 2007).

Rogue APs podem ser instalados por:

- Usuários internos sem fins maliciosos;
- Usuários internos maliciosos;
- Atacantes.

Negligenciar a segurança de redes sem fio é negligenciar a segurança de toda uma infra-estrutura de rede, pois mesmo sem nenhum dispositivo sem fio planejado, podemos ter uma rede sem fio abrindo as portas de nossa infra-estrutura para o mundo.

De acordo com o Gartner, empresas que não tem uma infra-estrutura de rede sem fio têm um maior risco de exposição a rogue APs e até mesmo empresas que tenham uma infra-estrutura de rede sem fio podem sofrer do problema de rogue APs através de empregados que não têm acesso sem fio e que poderiam trazer seus próprios equipamentos sem fio e colocá-los em operação por comodidade e mobilidade dentro do ambiente de trabalho (AIRDEFENSE, 2007).

Ainda segundo o Gartner, pelo menos 20% das empresas já têm rogue WLANs ligadas as suas redes corporativas instaladas por usuários em busca da conveniência e que não tem paciência de esperar pela implantação da rede WLAN da organização. A instalação dessas APs com as configurações padrão de fábrica sem a ativação de mecanismos de segurança podem aparentemente aumentar a

produtividade dos empregados, mas a instalação inocente, sem a preocupação com a segurança traz muito mais riscos para a segurança da corporação do que benesses para a sua operação (AIRDEFENSE, 2007).

As rogue APs, ou APs impostoras, podem ser essa porta aberta deixada na rede mesmo que o ambiente não tenha uma WLAN implementada.

Alguns Riscos Trazidos pelas Rogue APs

Uma vez acessada uma rede WLAN insegura pode haver comprometimento de:

- dados financeiros, levando a perdas financeiras;
- reputação, prejudicando a imagem de uma instituição;
- informação proprietária, perdendo segredos industriais ou patentes;
- informação de terceiros, ferindo os direitos de privacidade de clientes;
- infra-estrutura cabeada.

Cenários de Ataque explorando Rogue AP

✓ Ataques Ativos Usando Rogue AP

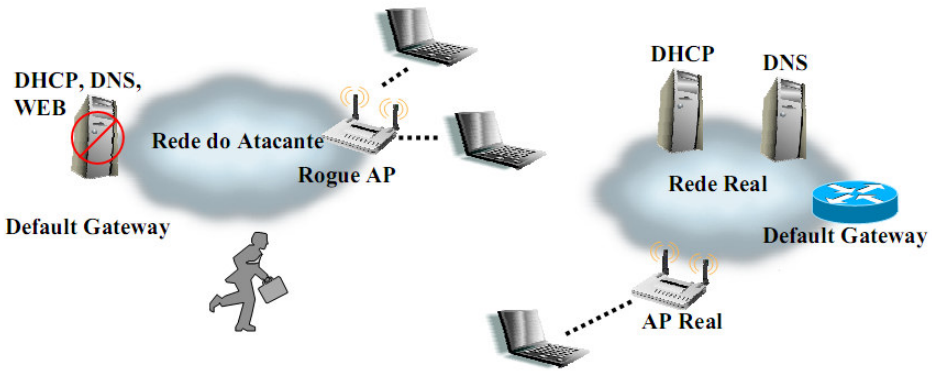

Figura 10 – Ataque com Rogue AP (LIMA e NAKAMURA, 2003)

Atacante precisa recuperar algumas informações antes de implementar o ataque:

- SSID (Service Set IDentifier);
- Criptografia habilitada ou não, se usada criptografia a chave utilizada;

Todos estes parâmetros devem ser configurados no rogue AP. Para finalizar, deve ser construída uma rede falsa, deve-se criar a ilusão de uma rede normal para máquinas móveis com servidor DHCP, servidor DNS, etc. Apenas estações mais próximas da Rogue AP e ainda não associadas podem ser atacadas.

- ✓ AP instalado por um usuário sem ciência das questões de segurança

Por comodidade, um usuário de nossa infra-estrutura pode simplesmente conectar uma AP sem configuração de segurança alguma a nossa rede cabeada e utilizar o seu notebook para acessar a intranet como se este estivesse ligado a rede cabeada, o que ele não levou em consideração é que este ponto de acesso que ele criou para si, está disponível para qualquer pessoa bem intencionada ou não, dentro da área de alcance da AP, fazer o uso que quiser da infra-estrutura da empresa;

Precauções Importantes

Uma rede bem configurada com SSID, filtro por endereço MAC, autenticação com WPA (TKIP) ou WPA2 (AES) e autenticação por porta 802.1x podem mitigar essa fragilidade.

Alguns softwares de monitoração podem enxergar Rogue APs.

Identificando e Eliminando Rogue APs

Há diversas abordagens para identificar e tentar expurgar as Rogue APs de uma rede em produção. Se a AP instalada na rede indevidamente lá foi colocada inocentemente por um funcionário apenas com o intuito de trazer comodidade em geral será facilmente localizada e o funcionário pode ser punido por sua ação ou pelo menos conscientizado do problema que ele pode estar trazendo conforme seja a política da empresa. Se a AP for instalada com o intuito de permanecer oculta na infra-estrutura da empresa para servir de ponto de acesso a invasores com propósitos de trazer algum prejuízo a busca por essa AP é bem mais desafiador. Há exemplos de AP que podem permanecer em silêncio completo até que escute uma seqüência especial de bits através do ar que a trará a operação e após a comunicação ser encerrada a levará de volta ao modo silencioso.

A AirDefense™ em seu documento *Tired of Rogues – Solutions for Detecting and Eliminating Rogue Wireless Networks* (AIRDEFENSE, 2007) traz as principais técnicas para detectar Rogue WLANs, estas técnicas são enumeradas abaixo:

- Sistemas de Detecção de Intrusão do lado cabeado;
- SNMP *Polling* do lado cabeado;
- Scanners de rede do lado cabeado;
- Scanners e Sniffers sem fio;
- Injeção de Tráfego do lado cabeado;
- Injeção de Tráfego do lado sem fio;
- Monitoramento Cabeado e Sem Fio Centralizado 24x7 da AirDefense.

A eficácia dos métodos de detecção é ainda alvo de contestações e estudos e a busca por novos métodos parece ainda estar aberta, apesar de soluções proprietárias se autodeclararem a solução. Além da solução da AirDefense, AirMagnet, encontramos soluções da Cisco Systems e da Proxim que se propõem a realizar esta detecção.

"WIDS deve continuamente realizar uma varredura e detectar atividades autorizadas ou não. Varredura continua é 24 horas/dia e 7 dias/semana.[8]"

(Department of Defense Policy, 2006, apud AIRDEFENSE, 2007).

2.7.2 Alcance da Rede Sem Fio Maior do que o Desejável

Muitas vezes grandes corporações implementam redes sem fio onde os sinais de rádio freqüência ultrapassam os limites físicos da corporação e chegam a locais públicos como ruas, avenidas e praças ou mesmo particulares apartamentos vizinhos, casas e outras corporações facilitando o trabalho do invasor que não precisa fisicamente entrar na corporação.

Poderíamos ter uma redução significativa das nossas preocupações a cerca da segurança de uma rede sem fio se conseguíssemos limitar o alcance desta rede.

[8] WIDS must continuously scan for and detect authorized and unauthorized activities. Continuous scanning is 24 hours/day, 7 days/week.

Notadamente existem barreiras físicas que impedem ou atenuam demasiadamente a passagem do sinal deixando-o imperceptível ou altamente instável para impedir que o sinal transponha os limites da corporação barreiras físicas poderiam ser construídas, a utilização de equipamentos que sobrecarreguem a faixa de freqüência com ruído destrutivo também pode ser uma alternativa.

2.8 - PASSOS PARA A SEGURANÇA DE UMA WLAN

Durante todo o desenrolar dos tópicos anteriores, procuramos deixar claro, atitudes, tecnologias, boas práticas em projetos de redes sem fio que permitissem uma rede com um número de vulnerabilidades aceitável.

Consideramos de extrema importância a ênfase na divulgação de novas ações que possam ser tomadas, para dar mais segurança à rede, estamos, por isso, divulgando este *checklist,* que traz ações simples, mas que podem ser a diferença entre manter a sua rede segura ou ser invadido.

O que você pode fazer para deixar segura sua rede sem fio?

1. Mudar a senha padrão de sua AP;
2. Cheque se o *firmware* e *drivers* estão atualizados, atualize se necessário, mantenha-se atento às evoluções;
3. Use o mais alto nível de WEP/WPA (WPA2/802.11i preferível)—Use chaves seguras.
4. Autentique os usuários com protocolos como 802.1X, RADIUS, EAP (incluindo EAP-PAX, EAP-PSK, EAP-TLS, EAP-FAST, EAP-POTP, EAP-TTLS, PEAP, e EAP-SIM). Estes protocolos suportam autenticação que incluem certificados digitais, usuários e senhas, *tokens* seguros, etc.
5. Use criptografia forte para todas as aplicações que você usa sobre a rede sem fio ex. SSH e TLS/HTTPS.
6. Criptografe o tráfego sem fio usando uma VPN (Virtual Private Network), ex. Usando IPSEC ou outra solução VPN.
7. Use ferramentas de segurança de WLAN. Este software é especialmente projetado para dar segurança em redes sem fio 802.11.
8. Crie um segmento dedicado para a WLAN e crie barreiras adicionais para ter acesso a esse segmento.
9. Use um proxy com controle para requisições externas (web proxy e outros).

Teste regularmente a segurança de sua rede sem fio, usando as mais recentes ferramentas de *Wardriving* (as mesmas que os invasores usam).

Não use para outras redes e sempre saiba das leis locais e outros regulamentos antes de usar essas ferramentas.

Habilite filtragem por MAC *address* em sua AP.

3. CONCLUSÃO

Pela diversidade de mecanismos, pelo escrutínio público que esses mecanismos já sofreram e, por conseguinte, a evolução que sofreram, há motivos suficientes para acreditarmos que as redes locais sem fio dispõem, hoje, de uma segurança bastante confiável.

A dificuldade principal na segurança de redes sem fio IEEE 802.11 está muito ligada a um estudo feito em São Paulo pelo Kaspersky Lab (BESTÚZHEV, 2007), trata-se da conscientização da importância de proteger os seus dados.

A menos que um indivíduo, ou mesmo uma empresa, queira divulgar os dados que trafegam em sua rede, e talvez pior, sujeitar-se a receber dados de qualquer computador malicioso externo como se fosse dados de um computador de sua própria rede interna, ele deve implementar alguns mecanismos para impedir ou pelo menos dificultar o acesso a sua WLAN, implementando formas de cifragem e autenticação para acessar a rede.

No estudo da Kaspersky Lab na cidade de São Paulo verificou-se que:

- Métodos de criptografia mais modernos e, até o momento, fortes o suficiente para proteger as redes sem fio do ataque de pessoas mal-intencionadas mais habilidosas, como o WPA e o WPA2 estão implementados em 22% e 4% de todas as redes, respectivamente;
- 50% das redes encontradas na cidade durante o estudo usavam o WEP que pode ser facilmente quebrado com ferramentas distribuídas gratuitamente pela internet, por mais tentativas que tenham sido feitas para reforçar o WEP como a mais recente WEP Cloaking, solução da AirDefense, viu-se que nenhuma delas era eficaz em consertar as inúmeras fragilidades do mecanismo;
- 24% de todas as redes não utilizam qualquer tipo de criptografia, são redes abertas para todo o público ou talvez algumas delas utilizem

mecanismos de segurança mais simples, como a filtragem de acesso por endereço MAC, facilmente forjável.

Apenas este fragmento do estudo da Kaspersky já seria suficiente para demonstrar o descaso com a segurança das redes sem fio e serve para demonstrar que a insegurança no mundo Wi-Fi se deve, no momento, muito mais a falta de cuidado na implantação de uma infra-estrutura de rede WLAN do que propriamente da carência de mecanismos para resguardá-la. A grande maioria dos dispositivos encontrados em São Paulo no estudo funciona em 802.11g que já oferecem suporte a mecanismos de criptografia WPA ou WPA2, que apresentam segurança mais robusta que a do WEP.

São Paulo não é um caso isolado, no mundo todo, estima-se através das varreduras feitas por praticantes de *WarDriving* que as cidades têm aproximadamente 70% de suas redes wireless sem qualquer cifragem de dados. Pesquisas feitas pela Kaspersky Lab encontram valores altos, embora, sejam nas principais cidades, menores do que os 70% estimados. Em Moscou em 2005 atingiu-se a marca de 69% das redes WLAN sem cifragem. O resultado na China em 2005 (GOSTEV, 2005) foi diferente do resto do mundo lá, “apenas” 58,8% das redes sem fio não usavam nenhuma criptografia, em compensação, nenhuma das redes com criptografia implementada encontradas usavam padrões de criptografia mais modernos como WPA ou 802.11i. Pesquisa semelhante for realizada em Hannover durante a CeBIT-2006 (GOSTEV e SCHOUWENBERG, 2006) lá verificou-se que 55,67% das redes não apresentavam nenhum tipo de criptografia. Em Varsóvia 58% das redes apresentavam algum tipo de criptografia, dados de fevereiro de 2007. As condições de redes sem fio na Varsóvia está em sintonia com os dados de outras cidades da União Européia (Paris têm 70% de suas redes WLAN com cifragem, Londres 50% e Hannover, como visto, pouco mais de 44%)(KAMLUK, 2007).

ANEXO - Fragmento de entrevista

Fragmento de entrevista

Este fragmento foi retirado da entrevista do engenheiro de sistemas da Cisco, Stephen Orr, para o jornal Washington Post, em maio de 2007, na coluna Viewpoint (plataforma de publicidade). O engenheiro falou sobre segurança e os dispositivos que a Cisco oferece para redes sem fio.

Arlington, Va.: How does Cisco WIDS deal with Rogue AP's and Clients?

Stephen Orr, Cisco: The Unified Wireless Architecture's WIDS will perform multiple actions on Rogue devices. First, the Wireless Control Software will detect the Rogue device and then produce an alert/alarm on the management console (an email/page can also be sent). Once the rogue is confirmed by the administrator, you can take action by having the Wireless System send de-authentication and disassociation message to the Rogue device. The Location Appliance is critical to any WIDS deployment so that you can track the rogue device and physically remove it from the network.

Washington, D.C.: I have no plans for WLAN deployment over the next 12 - 18 Months, so why do I need a WIDS?

Stephen Orr, Cisco: In order to safeguard your network from Rogue Access Points and Rogue clients even if you have not deployed a Wireless Access Solution, a WIDS should be deployed as part of a defense in depth architecture. In context to the Department of Defense, the DoD 8100.2 supplemental policy mandates WIDS for all networks to prevent Rogues. Cisco's UWL can be deployed as a WIDS only today and when ready, client access may be enabled (WASHINGTON POST, 2007).

REFERÊNCIAS BIBLIOGRÁFICAS

AIRDEFENSE. **TIRED OF ROGUE? Solutions for Detecting and Eliminating Rogue Wireless Networks.** 2007.
Disponível em: http://www.airdefense.net/whitepapers/roguewatch_request2.php
Acessado em: 22/03/2008

AIRDEFENSE ENTERPRISE. **AIRDEFENSE WEP CLOAKING: Protection For Legacy Encryption Protocols.** 2007.
Disponível em: http://www.airdefense.net/products/features/wep.php
Acessado em: 13/04/2008

BESTÚZHEV, Dmitry. **Wardriving em São Paulo.** Kaspersky Lab, 2007.
Disponível em: http://www.kaspersky.com.br/analise_de_rede/
Acessado em: 22/04/2008

BORISOV, Nikita; GOLDBERG, Ian; WAGNER, David. **Intercepting Mobile Communications: The Insecurity of 802.11.** In: International Conference on Mobile Computing and Networking,VII; Rome: Italy, 2001a, pág. 180-189.
Disponível em: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
Acessado em: 19/03/2008

BORISOV, Nikita; GOLDBERG, Ian; WAGNER, David. **(In)Security of The WEP algorithm.** 2001b.
Disponível em: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
Acessado em: 13/04/2008

CABIANCA, Luís Antonio; BULHMAN, Haroldo José. **Redes LAN / MAN Wireless III: Aplicação do Padrão 802.11.** 2006.
Disponível em: http://www.teleco.com.br/tutoriais/tutorialrwlanman3/default.asp
Acessado em: 12/04/2008

CISCO SYSTEMS. **Cisco Systems Recomendações de Implementação WLAN na E-U.** 2003
Disponível em: http://www.fccn.pt/files/documents/Cisco-CookBook_WLAN_E-U_v1_0.pdf?947cda2253a1dc58fe23dc95ac31cbed=7e45d603b47cfffdab606bf07a1ba7eb
Acessado em: 12/04/2008

CISCO SYSTEMS. **Cisco Wi-Fi Protected Access, WPA2 AND IEEE 802.11i.** 2004.
Disponível em:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_qas0900aecd801e3e59.pdf
Acessado em: 12/04/2008

COMPTEK. **AIRONET´S BUSINESS HISTORY**, 2001.
Disponível em:
http://web.archive.org/web/20010723081809/http://www.comptek.ru/learning/wireless/beseda96/aironet1.html
Acessado em: 21/06/2008

EATON, Dennis. **Diving into the 802.11i Spec: A Tutorial.** 2002.
Disponível em: http://www.commsdesign.com/showArticle.jhtml?articleID=16506047
Acessado em: 11/04/2008

EDNEY, John; ARBAUGH, William A. **Real 802.11 Security: Wi-Fi Protected Access and 802.11i.** Boston-MA: Addison-Wesley, 2003. 480 p.

FEDERAL COMMUNICATIONS COMMISSION (FCC). **Authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations.** 1985.
Disponível em: http://www.marcus-spectrum.com/documents/81413RO.txt
Acessado em: 22/06/2008

FLEISHMAN, Glenn; MOSKOWITZ, Robert. **Weakness in Passphrase Choice in WPA Interface.** 2003
Disponível em: http://wifinetnews.com/archives/002452.html
Acessado em: 19/03/2008

FLUHRER, Scott R.; MANTIN, Itsik; SHAMIR, Adi. **Weaknesses in the Key Scheduling Algorithm of RC4.** 2001.
Disponível em: http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps
Acessado em: 19/03/2008

GARG, Vijay Kumar. **Wireless Communications and Networking.** San Francisco-CA: Morgan Kaufman, 2007. 931 p.

GEIER, Jim. **802.11 WEP: Concepts and Vulnerability.** 2002.
Disponível em: http://www.wi-fiplanet.com/tutorials/article.php/1368661
Acessado em: 13/04/2008

GOLDSMITH, Andrea. **Wireless Communications.** Stanford-CA: Cambridge University Press, 2005. 672 p.

GOSTEV, Alexander. **Wardriving in China**. Kaspersky Lab, 2005.
Disponível em: http://www.viruslist.com/en/analysis?pubid=175676429
Acessado em: 22/04/2008

GOSTEV, Alexander; SCHOUWENBERG. **Wardriving in Germany - CeBIT 2006**, 2006.
Disponível em: http://www.viruslist.com/analysis?pubid=182068392
Acessado em: 22/04/2008

GUPTA, Deepak; RAMACHANDRAM, Vivek; AMIT; GOPI; PRAVIN. **T140 – The Emperor Has No Cloak, WEP Cloaking Exposed.** In: DefCon 15; Las Vegas: USA, 2007a.
Disponível em: http://video.google.com/videoplay?docid=-4931602590970144801
Acessado em: 13/04/2008

GUPTA, Deepak; RAMACHANDRAM, Vivek; AMIT; GOPI; PRAVIN. **T140 – The Emperor Has No Cloak, WEP Cloaking Exposed.** In: DefCon 15; Las Vegas: USA, 2007b.
Disponível em:
http://www.airtightnetworks.com/fileadmin/pdf/resources/WEP_Cloaking_Analyzed.pdf
Acessado em: 13/04/2008

HURLEY, Chris; PUCHOL, Michael; ROGERS, Russ; THORNTON, Frank. **WarDriving: Drive, Detect, Defend: A Guide to Wireless Security.** Syngress Publishing, Inc. Rockland-MA, 2004. 524 pag.

IEEE 802.11i-2004. 2008.
Disponível em: http://en.wikipedia.org/wiki/IEEE_802.11i
Acessado em: 21/04/2008

IEEE 802.1X. 2008.
Disponível em: http://en.wikipedia.org/wiki/802.1x
Acessado em:12/04/2008

IEEE. **IEEE Std 802.11i-2004.** 2004.
Disponível em: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
Acessado em: 19/03/2008

KATZ, Jonathan; LINDELL, Yehuda. **Introduction to Modern Cryptography.** Boca Raton-FL: Chapman & Hall/CRC, 2008. 534 p.

KAMLUK, Vitaly. **Wardriving in Warsaw.** 2007.
Disponível em: http://www.viruslist.com/en/analysis?pubid=204791934
Acessado em: 22/04/2008

KHARIF, Olga. **Paving the Airwaves for Wi-Fi**. In: Special Reports: Gurus of Technology, BusinessWeek, 2003.
Disponível em: http://www.businessweek.com/technology/content/apr2003/tc2003041_5423_tc107.htm
Acessado em: 19/03/2008

LIMA, Marcelo B.; NAKAMURA, Emilio T. **Rogue Access Point um Grande Risco para WLAN.** CPqD, 2003.
Disponível em: http://www.kcmelo.com.br/Files/RogueAP.pdf
Acessado em: 12/04/2008

MARTIN, Flynn. **WiFi Security Setup Guide.** DataPro, 2005.
Disponível em: http://www.datapro.net/techinfo/wifi_security.html
Acessado em: 19/03/2008

NULL, Christopher. **The 50 biggest heroes in technology history: Innovators, legends and geeks who shaped our world.** 2008.
Disponível em: http://www.pcadvisor.co.uk/news/index.cfm?newsid=13124&pn=7
Acessado em: 22/06/2008

RITTINGHOUSE, John; RANSOME, James. **Wireless Operational Security.** Burlington-MA: Digital Press/Elsevier, 2004 468 p

RIVEST, Ron. **Frequently Asked Questions.** 2007.
Disponível em: http://people.csail.mit.edu/rivest/faq.html
Acessado em: 24/06/2008

RSA. **Wireless Adoption Leaps Ahead, Advanced Encryption Gains Ground in the Post-WEP Era.** 2007.
Disponível em: http://www.rsa.com/press_release.aspx?id=8451
Acessado em: 19/03/2008

STUBBLEFIELD, Adam; IOANNIDIS, John; RUBIN, Aviel D.
Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.
AT&T Labs Technical Report TD-4ZCPZZ, 2001, 8pp.
Disponível em: http://ftp.die.net/mirror/papers/802.11/wep_attack.pdf
Acessado em: 19/04/2008

VACCA, John R. **Guide to Wireless Network Security.** Pomeroy-Ohio: Springer Science+Business Media/LLC, 2006. 880 p.

WASHINGTON POST. **Viewpoint Discussion: CISCO.** 2007.
Disponível em:
http://www.washingtonpost.com/wp-adv/advertisers/cisco/chat_archives/cisco_conversations_070503_wireless.html
Acessado em: 13/06/2008

WaveLAN. 2008.
Disponível em: http://en.wikipedia.org/wiki/WaveLAN
Acessado em: 17/06/2008

WaveLAN. 2005.
Disponível em: http://sinister.com/radio/wavelan.html
Acessado em: 17/06/2008

Wi-Fi Alliance. **Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise.** 2005.
Disponível em:
http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf
Acessado em:13/06/2008

Wi-Fi. 2008.
Disponível em: http://en.wikipedia.org/wiki/Wi-Fi
Acessado em: 19/03/2008

Wi-Fi Alliance. **Knowledgwe Center – FAQ.** 2007
Disponível em: http://www.wi-fi.org/knowledge_center_overview.php?type=2
Acessado em: 13/06/2008

Wired Equivalent Privacy. 2008.
Disponível em: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
Acessado em: 19/03/2008

Wi-Fi Protected Access. 2008
Disponível em: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
Acessado em: 19/03/2008

WRIGHT, Joshua. **Explaining WPA2.** In: Network World. 2006.
Disponível em:
http://www.networkworld.com/columnists/2006/091106-wireless-security.html
Acessado em: 12/04/2008

GLOSSÁRIO

AP ou access point - é um dispositivo que conecta dispositivos de comunicação sem fio para criar uma rede sem fio. Em uma rede sem fio infra-estruturada é através do AP que os dispositivos *wireless* se comunicam.

Ataque FMS – O ataque que se aproveita da fraqueza do algoritmo de key scheduling do RC4 para reconstruir a chave após haver coletado um número de mensagens cifradas.

Camada MAC (Multiple Access Control) - em uma Rede Sem Fio, como o padrão 802.11, tem como função controlar o acesso dos terminais móveis aos canais, gerenciar a qualidade de serviço e fornecer segurança.

Chaffing Engine – é uma técnica criptográfica para se obter confidencialidade sem usar cifragem mesmo enviando os dados por um canal inseguro.

IEEE 802.11 - é um conjunto de padrões de mercado para tecnologias de rede local sem fio (*WLAN*) compartilhadas, dentre os quais o que predomina é o *IEEE* 802.11b, também conhecido como *Wi-Fi*.

Kerberos – é o nome de um protocolo de autenticação, que permite que indivíduos se comuniquem de forma segura, através de um canal inseguro, com a finalidade de que se autentiquem.

Protocolos - Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. Um conjunto de regras padronizado que especifica o formato, a sincronização, o seqüenciamento e a verificação de erros em comunicação de dados. O protocolo básico utilizado na Internet é o *TCP/IP*.

Rede ad-hoc - é uma rede sem um ponto de controle central. Nesse caso a rede é formada pela proximidade dos dispositivos que tem a necessidade de se comunicar e que não dispõem de uma *AP*.

Rede infra-estruturada - é uma rede com um dispositivo concentrador (*Access Point*). Em uma rede infra-estruturada os dispositivos wireless se comunicam por meio do AP.

Redes Sem Fio ou WLANs – referem-se a redes de computadores que são conectadas aos seus ambientes de trabalho via enlaces sem fio, tais como radio freqüência (RF) e raios infravermelhos (IR). Surgiram com a finalidade de superar as limitações de mobilidade e instalação das redes tradicionais.

Roaming – refere-se a possibilidade de uma estação estender seu serviço de conectividade para uma rede diferente da qual ela se registrou...

SSID – é um código que vem junto a todos os pacotes em uma rede *wireless* para identificar cada pacote como parte daquela rede. Consiste no máximo de 32 caracteres alfanuméricos.

TACACS+ - é um protocolo que provê acesso controlado para roteadores, servidores de acesso de rede e outros dispositivos de rede, via um ou mais servidores centralizados.

WEP Cloaking™ - é um modulo, dentro de uma solução proprietária da AirDefense Enterprise, para prover proteção para a infra-estrutura de rede sem fio tornando seguro protocolos de criptografia legados.

ASSINATURAS

_____

Marcos Antonio Costa Corrêa Júnior
Graduando

_____

Prof. Dr. Ruy José Guerra Barretto de Queiroz
Orientador

Recife, 25 de Junho de 2008