Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento – ICPD

Roberto de Oliveira Silva

ESTUDO ANALÍTICO DA EVOLUÇÃO DA SEGURANÇA DE REDES SEM FIO 802.11

Brasília
2006

Roberto de Oliveira Silva

ESTUDO ANALÍTICO DA EVOLUÇÃO DA SEGURANÇA DE REDES SEM FIO 802.11

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área de Rede de Computadores.
Orientador: Prof. Marco Antonio

Brasília
2006

Roberto de Oliveira Silva

ESTUDO ANALÍTICO DA EVOLUÇÃO DA SEGURANÇA DE REDES SEM FIO 802.11

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*, na área de Rede de Computadores.
Orientador: Prof. Marco Antonio

Brasília, 30 de setembro de 2006.

Banca Examinadora

_____

_____

A meus pais,

pela educação e carinho

a mim dedicados.

A minha esposa e filhos

pelo apoio que me permitiu

chegar a esse ponto.

AGRADECIMENTOS

Ao meu orientador Professor Marco Antonio de O. Araújo, pelo tempo, paciência, apoio e incentivo dedicados à orientação para o desenvolvimento deste trabalho.

Aos demais professores do curso de Rede de Computadores, pelas aulas que me mostraram a riqueza do tema segurança em redes, motivando-me ainda mais para seguir este caminho.

Aos colegas do PRODASEN, pelo apoio e compreensão.

Aos colegas da biblioteca do PRODASEN pelo apoio na obtenção de materiais de estudo.

A Deus pelo dom da vida e por me permitir vivê-la com saúde.

RESUMO

Desde o lançamento do padrão 802.11, as redes sem fio têm se difundido fortemente tanto no ambiente empresarial quanto no doméstico. O crescimento tem sido tanto no número de redes sem fio instaladas, quanto no número de estações conectadas por esta tecnologia. Este crescimento traz como conseqüência imediata o aumento do tráfego de informações importantes, restritas, sigilosas e confidenciais. A evolução no uso das redes sem fio tornou necessária a evolução na segurança dessas redes. Este trabalho apresenta as falhas encontradas no mecanismo de segurança proposto no padrão inicial, o WEP, e o caminho trilhado pela indústria juntamente com o IEEE para o estabelecimento de um padrão de segurança robusto, o 802.11i.

Palavras-chave:

Segurança. Redes sem fio.

ABSTRACT

Since the launching of standard 802.11, the wireless networks have spread out strong in the enterprise as much in the domestic environments. The growth has been in the number of wireless networks, as much as in the number of stations connected by this technology. This growth brings as immediate consequence the increase of the traffic of important, restricted, secret and confidential information. The evolution in the use of wireless networks made needed then evolution in the security of these nets. This work presents flaws found in the proposed security mechanism of the initial standard, the WEP, and path taken by the industry with the IEEE for the establishment of a robust standard of security, 802.11i.

Key-words:

Security. Wireless.

SUMÁRIO

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

ABREVIAÇÕES

ABNT	Associação Brasileira de Normas Técnicas
AES	Advanced Encryption Standard
AP	Access Point
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode CBC-MAC Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DOS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
FHSS	Frequency-Hoping Spread Spectrum
GMK	Group Master Key
GTK	Group Transient Key
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISM	Industrial, Scientific and Medical
ISO	International Standards Organization
IV	Initialization Vector
LAN	Local Area Network
LEAP	Lightweight EAP
LLC	Logical Link Control
MAC	Media Access Control
MIC	Message Integrity Check
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency Division Multiplexing
PEAP	Protected EAP

PMK	Pairwise Master Key
PN	Packet Number
PTK	Pairwise Transient Key
PRNG	Pseudo-Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RFC	Request For Comments
RSN	Robust Security Network
RSNA	Robust Security Network Association
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TSN	Transition Security Network
TTLS	Tunneled TLS
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2

Introdução

Motivação

Apesar das redes sem fio terem surgido na década de 1970, com a ALOHA, na Universidade do Havaí, sua disseminação em larga escala só aconteceu a partir do final da década de 1990, após a publicação do padrão IEEE 802.11 em novembro de 1997 (IEEE, 1997).

Seguindo a definição do padrão 802.11, outros sub-padrões (802.11a, 802.11b e 802.11g) foram publicados incorporando novas tecnologias de transmissão, variações na freqüência de transmissão e, sobretudo, aumentos significativos na velocidade de funcionamento da rede em relação ao padrão inicial.

O grande mérito do padrão 802.11 é o de ter-se tornado um padrão na indústria, que o rebatizou como Wi-Fi, o que possibilitou a produção de equipamentos em larga escala e, razoavelmente, interoperáveis. Estes dois fatores – larga escala e interoperabilidade – fizeram com que os preços dos equipamentos para redes sem fio caíssem o suficiente para tornar as redes sem fio financeiramente viáveis tanto em empresas quanto em lares.

Com intuito de alcançar todo tipo de usuário, iniciantes a profissionais, os equipamentos tiveram suas interfaces simplificadas.

Outra facilidade relevante das redes sem fio advém de sua própria denominação, ou seja, não há necessidade de utilização de cabeamento. Isto na verdade é mais significativo do que parece, pois elimina a necessidade de se planejar a infra-estrutura da rede e, o mais importante, o trabalho de se passar os cabos pelas paredes, tetos e pisos.

Todas estas vantagens, somadas à razão de ser das redes sem fio, a mobilidade, fizeram com que este tipo de rede se popularizasse rapidamente. Mas, na medida em que as redes sem fio se tornam comuns, torna-se também comum o tráfego de informações valiosas por meio dessas.

Assim, a necessidade de estabelecer um caminho seguro através de redes sem fio tem se tornado uma preocupação para uma quantidade cada vez maior de profissionais da área de Tecnologia da Informação. Na verdade, esta preocupação não é recente, ela já havia sido demonstrada deste o estabelecimento do padrão em 1997.

A importância da segurança nas redes sem fio é reconhecida desde a publicação do padrão original, IEEE 802.11. Esse padrão dedicou todo um capítulo, intitulado "Segurança e Privacidade", para definir um mecanismo de segurança que provesse as redes sem fio com um nível de privacidade equivalente ao das redes cabeadas. O mecanismo, que por suas pretensões foi batizado de *Wired Equivalent Privacy* (privacidade equivalente ao das redes cabeadas), ou simplesmente WEP, propõe formas de autenticação das estações e criptografia de dados. No entanto, o nível de proteção provida por este mecanismo mostrou-se insuficiente para muitas redes sem fio.

Muitos estudos e propostas foram feitos para tentar suprir as redes sem fio com uma segurança de nível adequado para permitir o tráfego de informações sensíveis. Concluindo um grande esforço do IEEE, o padrão 802.11i, intitulado "Melhorias na Segurança da camada MAC", foi aprovado em junho de 2004 (IEEE, 2004a).

Objetivo

O objetivo deste trabalho é mostrar o caminho traçado pelas propostas de segurança para redes sem fio 802.11, desde o padrão inicial até a aprovação da emenda

802.11i. Serão demonstradas as falhas encontradas, suas conseqüências, modos de explorá-las e alternativas para saná-las.

Organização do Trabalho

O capítulo 1 traz alguns conceitos úteis para a compreensão do trabalho e algumas questões de segurança em redes sem fio não relacionadas diretamente com os mecanismos de segurança dessas redes; o capítulo 2 analisa os mecanismos de segurança, desde o mecanismo original do padrão 802.11: o WEP, explicando seu funcionamento, e suas falhas; a solução intermediária, WPA, definida pela Wi-Fi Alliance para mitigar as falhas de segurança encontradas no WEP; e, por fim, a solução definitiva para segurança de redes sem fio: o padrão 802.11i; o capítulo 3 mostra os ataques contra o WEP, as soluções paliativas para esses ataques apresentadas por diversos fabricantes de dispositivos e a evolução na segurança obtida com os padrões WPA e 802.11i; o capítulo final contém as conclusões finais sobre o trabalho e sugere alguns trabalhos futuros no estudo da segurança de redes sem fio.

1 Aspectos Conceituais

Logo em sua introdução, o padrão 802.11 define alguns aspectos de funcionamento importantes para as redes sem fio:

> **Este padrão define o protocolo e interconexão compatível de equipamentos de comunicação de dados via "ar", rádio, ou infravermelho, em uma rede local (LAN) usando o protocolo *carrier sense multiple access* com o mecanismo de compartilhamento do meio *collision avoidance* (CSMA/CA).**

A primeira definição que se percebe é que a transmissão de dados pode ser feita via rádio ou infravermelho. A implementação via infravermelho, apesar de pouco usada é aceita pelo padrão, que mais adiante define que a velocidade deve ser de 1Mbps ou, opcionalmente de 2 Mbps. Para rádio são definidas as velocidade de 1 Mbps ou opcionalmente 2 Mbps em *Frequency-Hoping Spread Spectrum* (FHSS) ou 1 e 2 Mbps em *Direct Sequence Spread Spectrum* (DSSS).

Outra definição importante é o uso do protocolo CSMA/CA na subcamada MAC no lugar do CSMA/CD, utilizado em redes ethernet. A principal característica de CSMA/CA é que este não escuta o canal durante a transmissão para detectar colisões, como faz o CSMA/CD. Ao invés disso, o CSMA/CA escuta o canal antes de transmitir para tentar evitar a ocorrência de colisões e assim minimizar a necessidade de retransmissões (TANENBAUM, 2003).

A freqüência utilizada nas transmissões via rádio é definida com sendo 2,4 GHz. Esta é uma das faixas públicas reservadas para uso industrial, científico e médico, assim denominada ISM (Industrial, Scientific and Medical). No sub-padrão 802.11a, é utilizada a freqüência de 5GHz que também é ISM fora do Brasil.

As técnicas de modulação utilizadas, FHSS e DSSS, baseiam-se na tecnologia de *spread spectrum* (espectro espalhado). Nesta tecnologia o sinal é distribuído por toda a faixa

de freqüência uniformemente. Desta maneira o sinal sofre menos efeitos de interferências ou ruídos. Além disso, como o sinal está espalhado em várias freqüências, pode ser confundido com ruído quando detectado em apenas algumas freqüências, o que pode melhorar a privacidade da transmissão.

O FHSS divide a largura da banda em 79 canais de 1 MHz e transmite por todos eles segundo uma seqüência pseudo-aleatória conhecida apenas pelas estações que compõem a rede. Sua principal desvantagem é a baixa largura de banda (TANENBAUM, 2003) além de ter velocidade limitada a 2 Mbps.

No DSSS cada bit é transmitido como 11 chips utilizando a seqüência de Baker. Estes chips são transmitidos por vários canais simultaneamente. Também apresenta velocidade limitada a 11 Mbps, no caso do 802.11b.

Uma terceira técnica denominada *Orthogonal Frequency Division Multiplexing* (OFDM) é utilizada nos sub-padrões 802.11g e 802.11a. Esta técnica utiliza 52 freqüências diferentes, sendo 48 para dados e 4 para sincronização. É o método mais utilizado nas redes atuais podendo alcançar a velocidade de 54 Mbps.

A tabela 1.1, abaixo, apresenta um quadro comparativo do padrão original, 802.11, e dos sub-padrões, 802.11a, 802.11b e 802.11g.

Tabela 1.1 – Comparativo dos padrões 802.11

Padrão	Freqüência	Modulação	Velocidade de transmissão
802.11	2,4 GHz	FHSS / DSSS	2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2,4 GHz	DSSS	11 Mbps
802.11g	2,4 GHz	OFDM / DSSS	54 Mbps

O padrão 802.11 (IEEE, 1997) define dois modos de funcionamento de redes sem fio comumente denominados infra-estrutura e *ad-hoc*.

No modo infra-estrutura (figura 1.1) toda comunicação entre as estações é feita através de um ponto de acesso (AP). Este é modo mais comum de redes sem fio, pois através dos pontos de acesso, as estações são conectadas a redes cabeadas obtendo assim acesso a servidores e demais estações da rede local. O escopo deste trabalho se limitará a este modo.

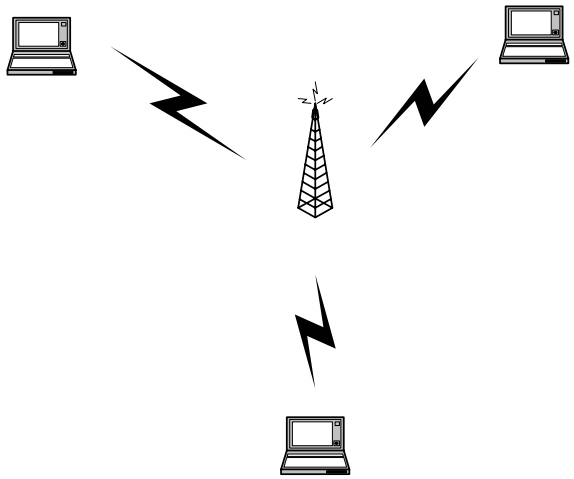

Figura 1.1 – Rede sem fio no modo infra-estrutura

No modo *ad-hoc* (figura 1.2) a comunicação entre as estações é feita diretamente. Este modo tem a vantagem poder ser implementada sem planejamento prévio. Para a criação de uma rede *ad-hoc* basta a presença de duas estações equipadas com placas de rede sem fio. Este modo é utilizado basicamente onde não há pontos de acesso disponíveis. A comunicação entre veículos militares é um exemplo deste modo.

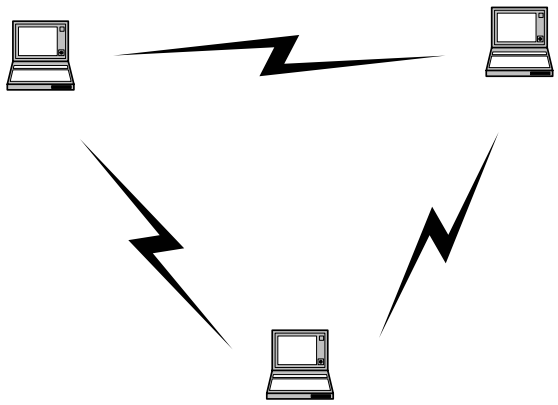

Figura 1.2 – Rede sem fio no modo *ad-hoc*

1.1 Considerações sobre Segurança

Na norma NBR ISO/IEC 17799 (ABNT, 1999) temos:

> **A segurança da informação é aqui caracterizada pela preservação de:**
>
> **a) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;**
>
> **b) integridade: salvaguarda da exatidão e completeza da informação e métodos de processamento;**
>
> **c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.**

Contudo, segundo o padrão IEEE 802.11 (IEEE, 2004a), os serviços de segurança fornecidos pelo WEP e suas definições são:

a) confidencialidade: propriedade da informação de não ser tornada disponível ou revelada a indivíduos, entidades ou processos não autorizados.

b) autenticação: serviço usado para estabelecer a identidade de uma estação como um membro do conjunto de estações autorizadas a associar com outra estação.

c) controle de acesso: a prevenção de uso não autorizado de recursos.

Mesmo não mencionados explicitamente como serviços fornecidos pelo WEP, a preocupação com a integridade e a disponibilidade das informações pode ser observada ao longo do padrão.

Na medida em que as redes sem fio se tornaram comuns, surgiram ferramentas capazes de analisá-las. Algumas destas ferramentas além de auxiliar no trabalho de auditoria feita por administradores de redes, serviram de instrumentos para os novos ataques. Assim a próxima seção cita essas ferramentas, e na seção seguinte são relacionados os ataques.

1.2 Ferramentas de Auditoria

1.2.1 Kismet

Ferramenta muito utilizada para mapeamento de redes e captura de pacotes. Identifica redes sem fio por meio de coleta passiva de pacotes, detectando inclusive redes que não se anunciam com *beacons*. Opera em Linux. Está disponível para *download* gratuito em http://www.kismetwireless.net.

1.2.2 NetStumbler

Ferramenta muito simples de mapeamento de redes sem fio 802.11 nos padrões **a**, **b** e **g**. Opera em sistema operacionais Windows. Permite integração com equipamentos GPS (*Global Positioning System*). Apresenta várias informações importantes sobre as redes detectadas, conforme ilustrado na figura 2.1. Está disponível para *download* em http://www.netstumbler.com/downloads.

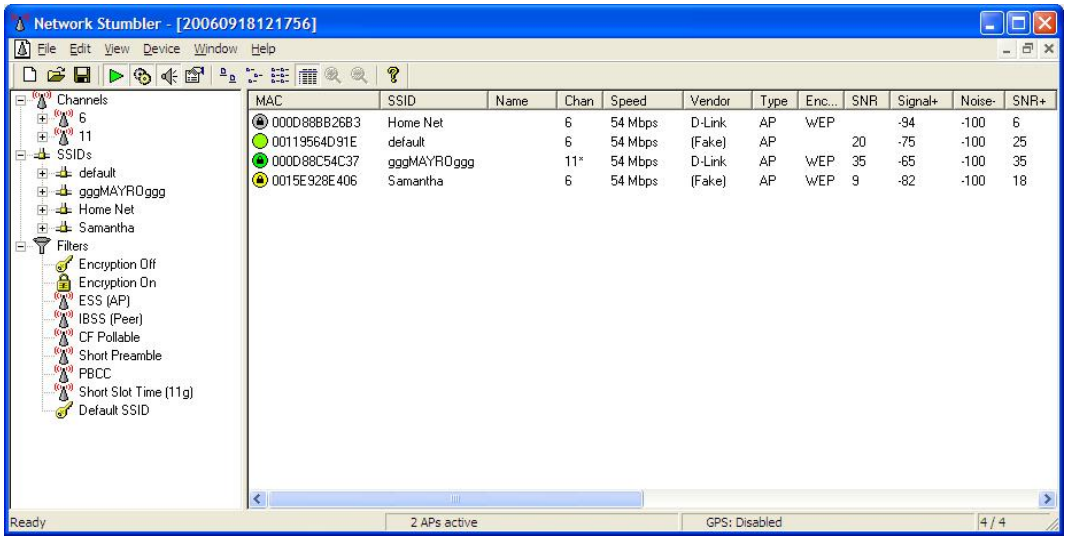

Figura 1.3 – Redes detectadas no NetStumbler

1.2.3 Ethereal

Analisador de protocoles de redes, muito útil como ferramenta de captura de pacotes (figura 2.2) e com muitas opções para visualização e filtragem de pacotes. Opera em sistemas operacionais Windows, Red Hat/Fedora e Solaris. Constantemente atualizado, sua versão mais recente, 0.99 foi lançada em 24/4/2006. Está disponível para *download* em http://www.ethereal.com/download.html.

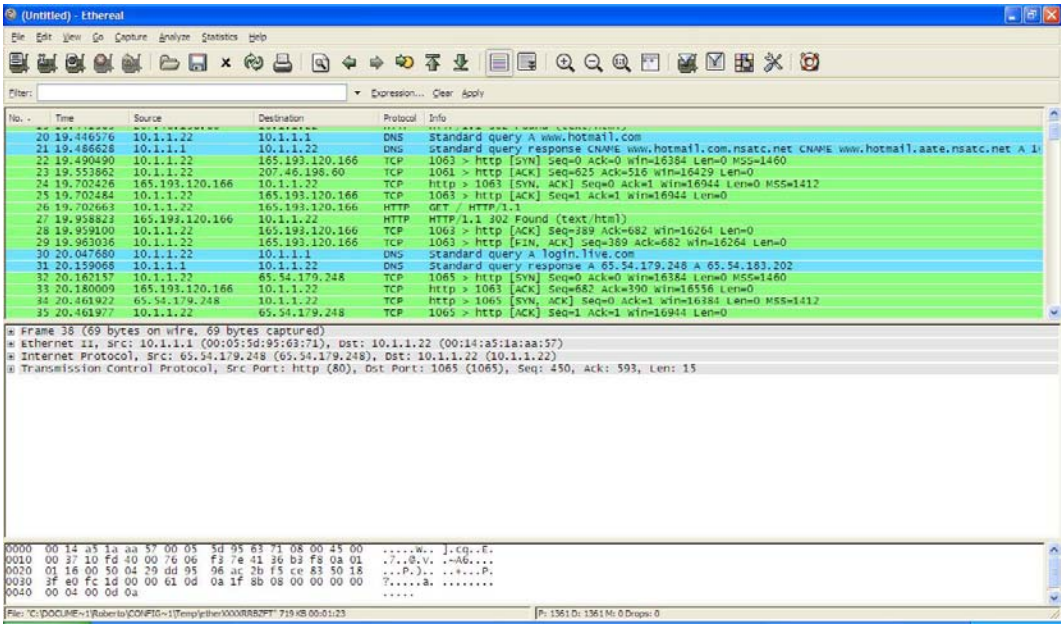

Figura 1.4 – Pacotes capturados com o Ethereal

1.3 Ataques

As redes sem fio podem ser vítimas de alguns ataques comuns em redes cabeadas, além disso alguns ataques novos surgiram especificamente para as redes sem fio. Os ataques mais comuns são citados a seguir (PEIKARI; FOGIE, 2002).

1.3.1 Vigilância

Consiste em realizar o reconhecimento do local da rede a ser atacada a procura de indícios da existência de redes sem fio. Alguns dos indícios a serem observados estão listado na tabela 2.1.

Tabela 1.2 – Indícios de rede sem fio

Coisas para procurar	Potenciais localizações
Antenas	Paredes, tetos, corredores, telhados e janelas
Pontos de Acesso (AP)	Tetos, paredes, suportes e prateleiras
Cabos de rede	Correndo por paredes ou calhas ou teto
Plataformas recém instaladas	Paredes, corredores e suportes
Dispositivos – scanners/PDA's	Funcionários, áreas de recepção ou saídas

Fonte: PEIKARI; FOGIE, 2002

Apesar de parecer algo muito básico, em alguns caso pode-se conseguir obter até mesmo o modelo do ponto de acesso. A dificuldade neste ataque está apenas na possibilidade do local da rede – corporação ou domicílio – ter acesso restrito a estranhos.

1.3.2 War-driving

Este ataque tanto pode ser feito após a vigilância, para complementar as informações, como antes da vigilância para localizar-se um local que possa ter rede sem fio. O termo *war-driving* derivou do termo *war-dialing*, comum nos anos 1980, que consiste em discar para uma série de números de telefone a procura de modem. O *war-driving*, por sua vez, consiste em mover-se, usualmente de carro ou ônibus, na tentativa de localizar-se redes sem fio nas redondezas com o uso de ferramentas de mapeamento de redes.

O *war-driving* se tornou popular a partir de 2001, com o lançamento de ferramentas de mapeamento de redes sem fio como o NetStumbler. O próprio Windows XP apresenta a lista de redes sem fio ao alcance para conexão (figura 2.3).

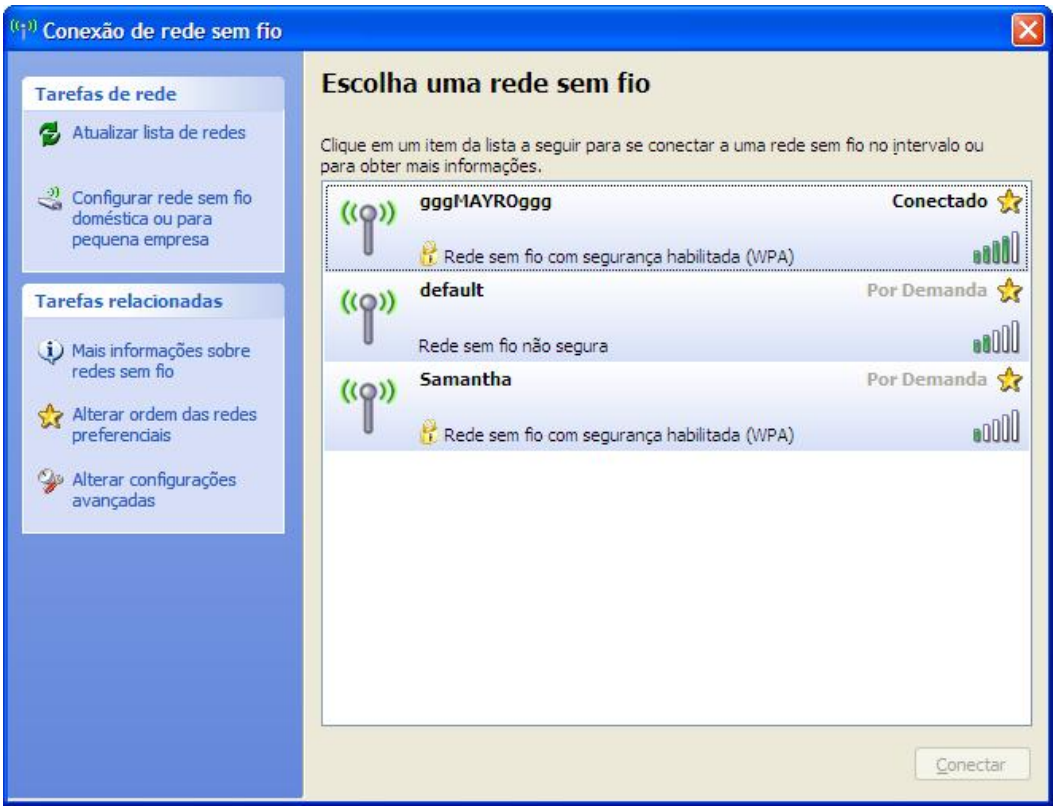

Figura 1.5 – Redes detectadas pelo Windows XP

1.3.3 War-chalking

Uma variante do *war-driving*, conhecida como *war-chalking*, consiste em detectar a existência de sinal de redes sem fio, conectar-se a tais redes e então marcar as paredes externas dos edifícios em giz com sinais predeterminados que indicam a presença de redes capazes de serem penetradas. Esta informação pode então ser utilizada por alguém com a simples intenção de conseguir um acesso à Internet gratuito bem como por pessoas mais mal-intencionadas que podem "escutar" livremente o tráfego da rede e/ou ter acesso aos seus equipamentos.

1.3.4 Hacking cliente-a-cliente

Um atacante pode atacar um *notebook* que esteja conectado a uma rede cabeada e esteja com a interface de rede sem fio ativa e configurada para o modo ponto a ponto. Com este ataque é possível ganhar acesso ao *notebook* e, com algum trabalho, à rede cabeada.

Este ataque é especialmente perigoso, pois em muitas das vezes o usuário do *notebook* não possui conhecimentos suficientes para detectar ou prever o ataque, pondo em risco a segurança da rede com o um todo.

1.3.5 Negação de Serviço (DOS)

Ataques de negação de serviço visam impedir que as estações tenham acesso aos serviços da rede. Considerando que as redes sem fio operam através de transmissões de rádio, é possível gerar-se ondas em freqüências que correspondam às usadas pela rede sem fio de modo a interferir nas transmissões de dados.

2 Análise dos mecanismos de seguraça

2.1 Definições do WEP

A especificação IEEE 802.11 no seu capítulo 8, intitulado “Autenticação e privacidade”, define os modelos de autenticação e o mecanismo de privacidade denominado *Wired Equivalent Privacy* (WEP), que pode ser traduzido como “privacidade equivalente à de rede cabeada”.

Os detalhes sobre a autenticação e a privacidade são dados nas seções a seguir.

2.1.1 Autenticação

Um detalhe interessante da especificação é que esta diz que a de autenticação **deve** ser usada em redes de infra-estrutura e que **pode** se usada em redes *ad-hoc*. São definidos dois subtipos de serviços de autenticação: *Open System* (Sistema aberto) e *Shared Key* (Chave Compartilhada).

A autenticação *Open System* é a autenticação padrão. Basicamente, consiste em não efetuar qualquer autenticação, mas apenas responder à solicitação de autenticação. Assim, é composta de apenas duas mensagens *Request* e *Result* (figura 3.1). Contudo, não necessariamente a resposta à solicitação deve ser positiva, ou seja, é permitido recusar a solicitação de autenticação.

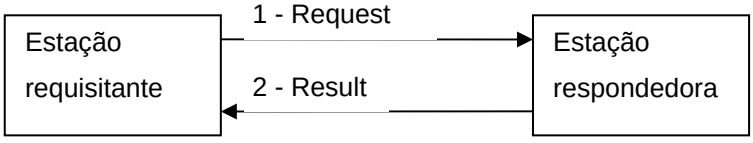

Figura 2.1 – Autenticação *Open System*

A autenticação *Shared Key* só está disponível se a opção de WEP estiver implementada. Utiliza uma chave secreta que não deve trafegar na rede em claro. Contudo, esta chave é “presumivelmente” compartilhada por canal seguro que não é definido no padrão. A autenticação é feita em quatro passos (figura 3.2):

1. estação requisitante envia solicitação de autenticação;
2. estação respondedora envia desafio (tamanho fixo de 128 octetos);
3. estação requisitante envia desafio criptografado;
4. estação respondedora informa sucesso ou insucesso.

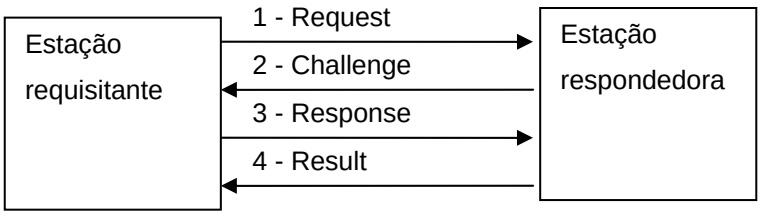

Figura 2.2 – Autenticação *Shared Key*

2.1.2 Privacidade (WEP)

O mecanismo WEP foi definido para proteger de escutas casuais. Isto é, a privacidade equivalente a de redes cabeadas não significa uma proteção intransponível. Na verdade a rede cabeada também não é intransponível. Sua segurança reside na necessidade de ter-se acesso ao cabo para obter-se acesso às mensagens que trafegam pela rede. Mas, uma vez conectado ao cabo, grande parte da informação trafegada pode ser capturada por não ser utilizada criptografia em boa parte do tráfego.

O padrão 802.11 define as seguintes propriedades para o algoritmo WEP:

- Razoavelmente forte: baseado no comprimento da chave secreta e na sua freqüência de troca.
- Auto-sincronizavel: a cada mensagem; importante para algoritmo de cifragem da camada de enlace, pois são assumidas altas taxas de perda de pacote.
- Eficiente: implementável em hardware ou software.
- Possivelmente exportável: feito esforço neste sentido, mas sem garantia.
- Opcional.

2.2 Algoritmo do WEP

O núcleo do mecanismo de privacidade do WEP é o gerador de números pseudo-aleatórios RC4 da RSA. Este é um algoritmo de cifragem de fluxo que utiliza uma seqüência aleatória de números para cifrar a mensagem.

O funcionamento da cifragem, ilustrado na figura 3.3 (IEEE, 1997), inicia com a concatenação da chave secreta com o vetor de inicialização (*Initialization Vector* – IV) para criar a semente que será utilizada no gerador de números pseudo-aleatórios do WEP (WEP *Pseudo-Random Number Generator* – WEP PRNG). O WEP PRNG então gera uma seqüência de bits, denominada seqüência-chave, que deverá ter o comprimento do texto a ser cifrado (texto em claro) mais o comprimento do valor de verificação de integridade (*Integrity Check Value* – ICV), calculado pelo algoritmo de integridade com base no texto em claro. Isto porque a seqüência-chave será utilizada para cifrar a seqüência formada pela concatenação destes dois elementos efetuando o ou-exclusivo das duas seqüências o que resultará no texto

cifrado. A mensagem transmitida pela estação será composta do texto cifrado e do vetor de inicialização que será necessário para o decifragem.

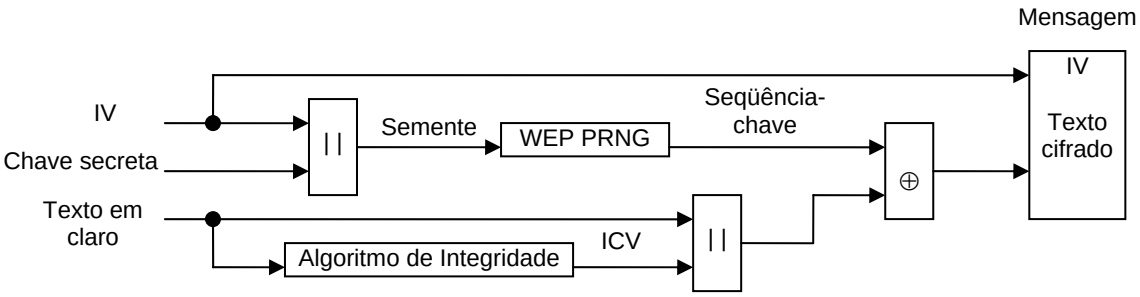

Figura 2.3 – Diagrama de bloco da cifragem WEP

A decifragem do WEP, ilustrada na figura 3.4 (IEEE, 1997), também inicia com concatenação da chave secreta com o vetor de inicialização (IV) para criar a semente que será utilizada no gerador de números pseudo-aleatórios do WEP (WEP PRNG). O WEP PRNG então gera a seqüência-chave, que, neste caso deverá ter o comprimento do texto cifrado. A seqüência-chave será então utilizada para decifrar a o texto cifrado efetuando o ou-exclusivo entre estas duas seqüências. A seqüência obtida contém o texto em claro e o ICV. Para verificar a integridade da mensagem, é utilizado o algoritmo de integridade para calcular o valor de verificação de integridade (ICV') que será comparado ao ICV contido na mensagem recebida.

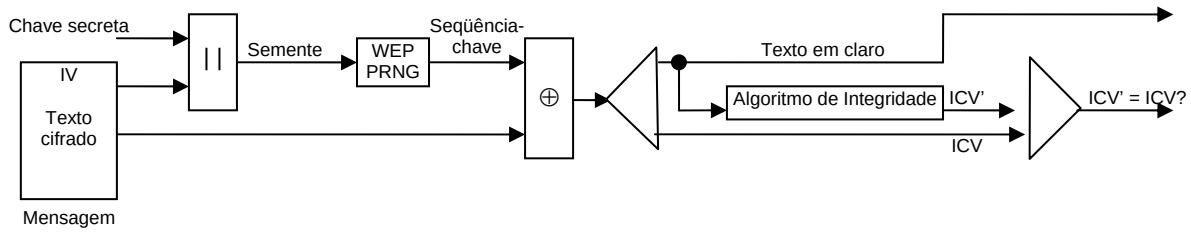

Figura 2.4 – Diagrama de bloco da decifragem WEP

Para compreendermos melhor o funcionamento do algoritmo WEP, veremos em detalhes os seus componentes nas subseções a seguir.

2.2.1 Vetor de Inicialização (IV)

No padrão 802.11, a semente do PRNG é definida com tendo 64 bits, sendo que os bits 0 a 23 correspondem ao vetor de inicialização e os bits 24 a 63 correspondem à chave secreta. Assim, o comprimento do vetor de inicialização é de 24 bits, enquanto o comprimento da chave secreta é de 40 bits.

O propósito do vetor de inicialização é variar a semente do gerador de números pseudo-aleatórios de modo a torná-lo menos previsível, pois se este for alimentado com a mesma semente irá sempre gerar a mesma seqüência de números pseudo-aleatórios. Como a chave secreta supostamente não é trocada freqüentemente, cabe ao vetor de inicialização, que é sempre trocado, fazer com que a semente varie. Contudo, dado o tamanho do vetor de inicialização, 24 bits, seu valor irá variar entre 0 e 16.777.215. Assim para uma mesma chave secreta haverá 16.777.216 valores possíveis de semente a serem utilizadas no gerador de números pseudo-aleatórios.

2.2.2 Chaves WEP

Juntamente com o vetor de inicialização de 24 bits, é também enviado outro octeto composto de seis bits de enchimento e dois bits denominados *keyID*. Este dois bits permitem a seleção de até quatro valores para a chave secreta. Desta forma as estações podem armazenar até quatro chaves secretas para serem selecionadas para a utilização em cada mensagem enviada.

A chave secreta é também referida como *default key* no padrão 802.11, por ser utilizada por todas as estações para se comunicarem com o ponto de acesso.

Em oposição à *default key*, há as chamadas chaves *key mappings*. Estas são individuais, para cada estação. Neste caso, em redes de infra-estrutura, o ponto de acesso tem de ter cadastrado as chaves *key mapping* de cada um das estações. Já em redes *ad-hoc*, as chaves *key mapping* são compartilhas entre pares de estações de modo a tornar privada a comunicação entre essas.

2.2.3 Algoritmo de integridade

O valor de verificação de integridade (ICV) é calculado utilizando-se CRC-32, isto é, *Cyclic Redundancy Check* (verificação cíclica de redundância) de 32 bits. Esse é cifrado juntamente com a mensagem para não permitir que seja recalculado no caso da mensagem ser alterada.

2.2.4 Criptografia RC4

A criptografia RC4 é composta de dois blocos principais: o gerador de números pseudo-randômicos (PRNG), e a operação ou-exclusivo.

O gerador de números pseudo-randômicos utiliza um número inicial, denominado semente, para gerar uma seqüência de bits pseudo-aleatórios. O algoritmo do gerador é projetado de modo que a seqüência de bits gerada seja única para cada semente utilizada e tenha um ciclo de repetição grande o bastante para parecer randômica para o fim que se destina. Assim, a seqüência só é reproduzível se for utilizada a mesma semente.

No caso do WEP a mesma semente, composta pela chave secreta + IV, é utilizada pela estação transmissora ao cifrar a mensagem e pela estação receptora ao decifrar a mensagem.

A cifragem WEP, propriamente dita, consiste em uma cifra de fluxo efetuada entre o texto claro e a seqüência-chave gerada pelo PRNG. A operação efetua pela cifragem é

simples, consistindo apenas em um ou-exclusivo. A simplicidade da cifragem tem como benefício o grande desempenho do algoritmo mesmo se implementado via *software*.

Para explicar a teoria matemática em que se baseia a cifragem, vamos primeiro elucidar o funcionamento do ou-exclusivo. Este operador binário, simbolizado por ⊕, tem como resultado 0 (zero) sempre que os dois operandos forem iguais, e 1 (um) sempre que os dois operando forem distintos, conforme a tabela 3.1.

Tabela 2.1 – Tabela-verdade do ou-exclusivo

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

A propriedade matemática do ou-exclusivo que permite a utilização em cifragem é o fato de que se efetuarmos o ou-exclusivo de um número A por outro número B e efetuarmos o ou-exclusivo do resultado, C novamente pelo número B obtemos o número A inicial. Por exemplo:

(A) 00101000 (C) 00110001
⊕ (B) 00011001 => ⊕ (B) 00011001
(C) 00110001 (D) 00101000

No caso do WEP, a primeira operação ocorre na estação transmissora durante a cifragem. O número A representa o texto em claro, o número B representa a seqüência-chave, o resultado, o número C, representa o texto cifrado.

A segunda operação, é a decifragem que ocorre na estação receptora. O número C representa o texto cifrado recebido, o número B representa a seqüência-chave, e o resultado, número D, representa o texto decifrado, que é idêntico ao texto em claro A.

2.3 Falhas do WEP

Diversos estudos sobre o mecanismo WEP apontaram falhas de segurança em seu comportamento. Dentre estas se destacam (EDNEY; ARBAUGH, 2004) (WALKER, 2000) (IEEE, 1997):

- Canal de compartilhamento da chave secreta.
- Mesma chave para autenticação e cifragem do tráfego.
- Falta de autenticação mútua.
- Verificação de integridade criptograficamente insegura.
- Reuso do vetor de inicialização.
- Chaves fracas.

2.3.1 Canal de compartilhamento da chave secreta

A primeira falha no WEP vem da falta de uma definição no padrão 802.11. O padrão define que a chave secreta deve ser compartilhada entre as estações através de um canal seguro, contudo não informa qual seria este canal seguro (IEEE, 1997).

Na prática, a chave secreta é cadastrada manualmente em cada estação. Geralmente, isso é feito pelo administrador. No entanto, no caso de redes maiores, este trabalho pode ser atribuído a um grupo de pessoas. É senso comum que qualquer segredo compartilhado por muitas pessoas tende a deixar de ser segredo. Assim a chave secreta, nessas condições tem sua confidencialidade bastante fragilizada.

Acontece também da chave secreta ser cadastrada pelo usuário da estação, que neste caso tem de ser informado de seu valor verbalmente ou por escrito. Assim, além de aumentar o problema citado acima, temos também que considerar a segurança do canal. Ou

seja, a chave pode ser informada pessoalmente, por telefone, documento ou, pior ainda, por e-mail.

Outra dificuldade com relação à distribuição da chave secreta acontece no caso de necessidade de trocá-la. Isto porque se a chave anterior tiver sido descoberta a troca deve ser feita quase que imediatamente e em todas as estações simultaneamente. Quando se trata de rede doméstica ou de pequena empresa, isto não chega a ser um problema. Mas, para uma rede corporativa, com dezenas ou centenas de estações, torna-se um bom exercício de logística.

Por tudo isso, o requisito do canal seguro para compartilhar a chave secreta pode, muitas vezes, não ser atendido.

2.3.2 Mesma chave para autenticação e cifragem do tráfego

Outro problema da chave secreta, é o fato de que esta não ser usada apenas na autenticação, mas também na cifragem do tráfego. Deste modo, a descoberta da chave secreta possibilita não só a autenticação junto ao ponto de acesso, mas, o que é ainda pior, a decifragem do tráfego (EDNEY; ARBAUGH, 2004).

2.3.3 Falta de autenticação mútua

Como visto no algoritmo WEP, este apresenta apenas autenticação da estação móvel junto ao ponto de acesso. Este último, por sua vez não é autenticado, sendo, assim, erroneamente dado como confiável. Portanto, não há garantias de que o ponto de acesso seja exatamente aquele que alega ser (EDNEY; ARBAUGH, 2004).

2.3.4 Verificação de integridade criptograficamente insegura

O algoritmo WEP implementa um valor de verificação de integridade utilizando um CRC de 32 bits. Para tornar o verificador mais seguro, este é cifrado juntamente com o texto. Desta forma, qualquer alteração na mensagem torna o CRC inválido e como este também está cifrado, não é possível recalculá-lo.

Contudo, o algoritmo de CRC foi projetado para detectar erros aleatório, comuns em transmissões de dados por meios com qualidade não-confiável. Ou seja, o CRC não é adequado para prover segurança contra ataques. Borisov *et al*. (2002) mostrou que mesmo cifrado é possível ajustar o CRC para que se torne válido após alterar-se uma mensagem cifrada, mesmo sem decifrá-la.

Como o CRC é um algoritmo linear, é possível calcular a alteração do CRC para alterações feitas na mensagem. Isto é, é possível calcular que bits devem ser alterados no CRC para torná-lo válido após uma alteração de determinados bits na mensagem. Para tornar o problema ainda maior, as alterações de bits feitas no texto em claro e no CRC se propagam após a cifragem, por se tratar de um ou-exclusivo. No ou-exclusivo se invertemos um dos operandos o resultado também é invertido, conforme mostrado na tabela 3.2.

Tabela 2.2 – Tabela-verdade do ou-exclusivo com operando invertido

A	A’	B	A ⊕ B	A’ ⊕ B
0	1	0	0	1
0	1	1	1	0
1	0	0	1	0
1	0	1	0	1

Assim, é possível alterar a mensagem, mesmo sem decifrá-la, e ajustar o valor de verificação de integridade adequadamente para que alteração não seja percebida.

2.3.5 Reuso do vetor de inicialização

O algoritmo RC4, por se tratar de um cifrador de fluxo, é vulnerável ao reuso da seqüência-chave. Ou seja, mensagens cifradas com mesma seqüência-chave permitem analises criptográficas que podem revelar o texto em claro (WALKER, 2000).

Na implementação do RC4 no WEP a seqüência-chave é gerada com base em uma semente composta pela chave secreta concatenada com um vetor de inicialização. Como a chave secreta é fixa – ou pelo menos alterada com pouca freqüência, devido aos problemas expostos acima – a variação da semente se torna função do vetor de inicialização. Este, por sua vez, sendo composto de 24 bits, apresenta menos de 17 milhões de valores possíveis. Assim, o reuso do vetor de inicialização não é apenas possível, mas sim garantido, podendo inclusive se dar em questão de horas, dependendo do tamanho do tráfego da rede.

2.3.6 Chaves fracas

“Todas as falhas do WEP são insignificantes se comparadas a esta” (EDNEY; ARBAUGH, 2004). Fluhrer, Mantin e Shamir (2001) demonstraram que explorando determinadas classes de chaves, denominadas chaves fracas é possível obter-se a chave secreta.

A chaves fracas se caracterizam pelo fato de um pequeno número de bits da chave determinar um grande número de bits da seqüência-chave. Assim, é possível correlacionar o texto cifrado com o texto em claro e a chave secreta.

A exploração das chaves fracas é possível devido o conhecimento de alguns bits iniciais de determinadas mensagens, no caso o cabeçalho LLC 802.1 presente no 802.11. Assim a captura de aproximadamente 60 mensagens possibilita supor com razoável grau de

certeza o primeiro byte da chave (EDNEY; ARBAUGH, 2004). Conjuntamente com outras técnicas, esta falha possibilita a identificação de toda a chave secreta.

Em referência a seus autores, este ataque é conhecido por ataque FMS e é reconhecido pela própria RSA (detentora dos direitos do RC4), que destaca o fato de que a falha ser na forma de utilização do algoritmo RC4 e não no algoritmo propriamente (RSA, 2001).

2.3.7 Resumo das Falhas do WEP

As falhas apresentadas no WEP, comprometem os três pilares da segurança, confidencialidade, integridade e disponibilidade. Isto é demonstrado no Tabela 3.3 abaixo.

Tabela 2.3 – Resumo da falhas do WEP

Falha	C	I	D
Canal de compartilhamento da chave secreta	X		
Mesma chave para autenticação e cifragem do tráfego	X		
Falta de autenticação mútua	X		X
Verificação de integridade criptograficamente insegura		X	
Reuso do vetor de inicialização	X		
Chaves fracas	X		

C - Confidencialidade, I - Integridade e D - Disponibilidade

2.4 Definições do WPA

Visando resolver os problemas da segurança em redes sem fio, foi criada uma força tarefa do IEEE, 802.11i, para definir um padrão robusto para a segurança de redes sem fio. Contudo, o padrão 802.11i só foi aprovado em 24 de junho de 2004, causando grande expectativa no mercado de redes sem fio e conseqüente queda na venda dos produtos. Para possibilitar a retomada das vendas, a Wi-Fi Alliance, grupo formado por grandes fornecedores de solução em redes sem fio, publicou, em 29 de abril de 2003, uma especificação

denominada WPA – Wi-Fi *Protected Access*. Contando com a parceria do IEEE, o padrão WPA antecipou grande parte dos padrões que foram adotados pelo 802.11i.

O WPA logo em sua capa se auto-intitulava “segurança forte, baseada em padrões, interoperável, para redes Wi-Fi de hoje” (WI-FI ALLIANCE, 2003). Para endereçar os problemas do WEP, o WPA utilizou três mecanismos principais:

- Autenticação baseada no padrão 802.1X
- *Temporal Key Integrity Protocol* (TKIP)
- *Message Integrity Check* (MIC)

2.5 Autenticação baseada no padrão 802.1X

O padrão 802.1X começou a ser definido antes do padrão 802.11 original ser completado em 1997. Assim, foi projetado originalmente para redes cabeadas conforme se pode observar no primeiro parágrafo do escopo do padrão revisado (IEEE, 2004b) :

> **LAN´s IEEE 802 são freqüentemente dispostas em ambientes que permitem que dispositivos não autorizados sejam fisicamente ligados à infra-estrutura da LAN, ou permitem que usuários não autorizados tentem acessar a LAN através de equipamentos já ligados. Exemplos de tais ambientes incluem LAN´s corporativas que provêem conectividade com LAN em áreas de um prédio que são acessíveis ao público em geral, e LAN´s que são dispostas por uma organização de modo a oferecer serviços de conectividade a outras organizações (por exemplo, como pode ocorrer em um estacionamento comercial ou um prédio de escritórios que preste o serviço). Em tais ambientes, é desejável restringir o acesso aos serviços oferecidos pela LAN a aqueles usuários e dispositivos que são permitidos a fazer uso daqueles serviços.**

No segundo 2º parágrafo do escopo do padrão revisado (IEEE, 2004b), no entanto, já cita redes sem fio:

> **O controle de acesso a redes baseado em portas faz uso das características do acesso físico das infra-estruturas de LAN IEEE 802 de modo a prover um meio de autenticar e autorizar dispositivos ligados a uma porta de LAN que tenha características de conexão ponto-a-ponto, e de impedir o acesso a aquela porta em casos nos quais o processo de autenticação e autorização falhe. Uma porta neste contexto é um ponto simples de conexão com a infra-estrutura da LAN. Exemplos de portas nas quais o uso de autenticação pode ser desejável incluem as portas de MAC *Bridges* (conformo especificado no padrão IEEE 802.1D), as portas usadas para conectar servidores ou roteadores à infra-estrutura da LAN, e associações entre estações e pontos de acesso em redes sem fio IEEE 802.11.**

Como sugere o escopo acima, a idéia do 802.1X é prover controle de acesso nas portas dos dispositivos de conexão – *bridges*, *hubs* e AP´s, por exemplo – de modo a permitir que eventuais conexões clandestinas à rede – via cabo ou “ar” – não ganhem acesso à rede.

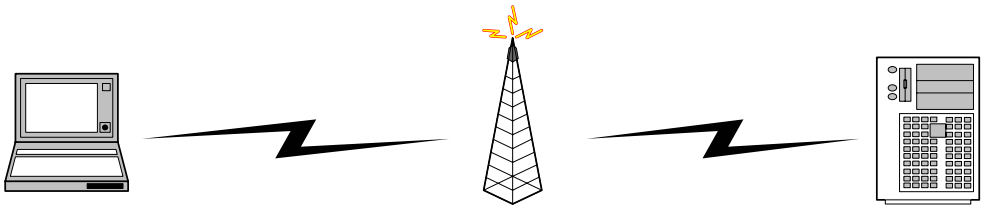

Figura 2.5 – Autenticação 802.1x

O padrão define três atores durante a autenticação, conforme a figura 4.1:

- Suplicante: cliente que deseja ser autenticado, representa o dispositivo dotado de interface de rede sem fio no padrão 802.11, trata-se geralmente de um *notebook*.
- Autenticador: dispositivo intermediário entre o suplicante e o servidor de autenticação, constituído pelo ponto de acesso (AP).
- Servidor de autenticação: dispositivo responsável pelo controle de acesso, geralmente trata-se de um servidor RADIUS.

O controle de acesso é feito mantendo-se as portas em um de dois estados: autorizado ou não-autorizado. A figura 4.2 ilustra o modelo do 802.1X conforme extraído do padrão por Edney (EDNEY; ARBAUGH, 2004). Na figura observa-se que o Sistema Suplicante comunica-se com o Sistema Autenticador através da LAN. Antes de ocorrer a autenticação, toda comunicação entre os dois sistemas se dá através das portas não controladas ligadas às PAE´s (*Port Access Entity* – Entidade de Acesso a Porta). A

Suplicante
(estação)

autenticação será feita através da PAE do Autenticador. Esta se comunicará com o Servidor de Autenticação por meio do protocolo EAP para obter a autenticação do Sistema Suplicante. Uma vez que o Servidor de Autenticação autentique o Sistema Suplicante, o PAE do Autenticador alterará o estado da porta controlada para autorizado, permitindo que o Sistema Suplicante ganhe acesso aos serviços oferecidos pelo Sistema Autenticador, o que geralmente corresponde a ganhar acesso à rede.

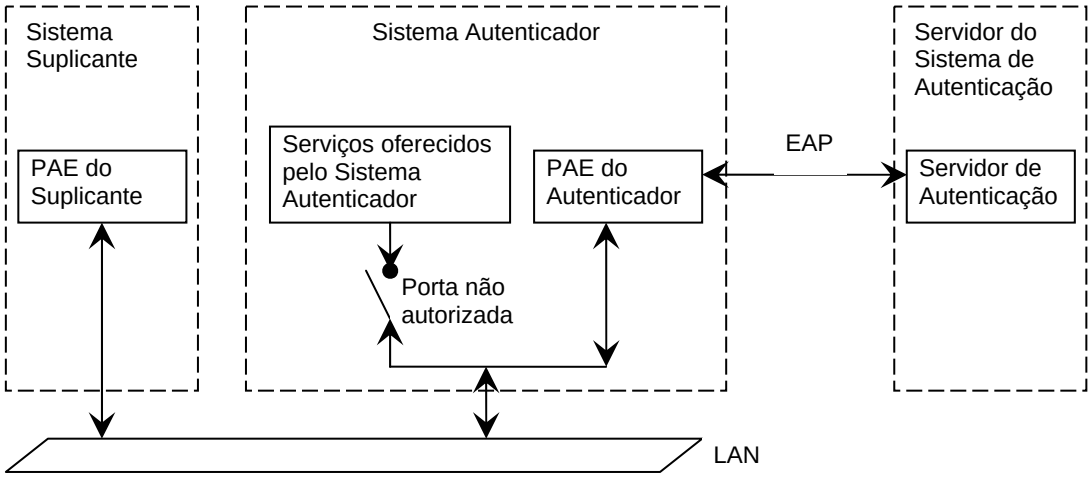

Figura 2.6 – Modelo 802.1x

Os passos necessários para a autenticação no 802.1X são:

- O suplicante inicia a conexão com o autenticador, que habilita apenas as portas 802.1X.
- O autenticador solicita a identidade do suplicante.
- O suplicante responde com sua identidade e o autenticador passa a identidade para o servidor de autenticação.
- O servidor de autenticação autentica o servidor e informa ao autenticador que habilita a comunicação do suplicante nas demais portas.

- O suplicante solicita a identidade do servidor de autenticação.
- O servidor de autenticação informa sua identidade.
- O suplicante autentica o servidor de autenticação.

A autenticação através do EAP, *Extensible Authentication Protocol* (Protocolo de Autenticação Extensível), pode se dar de várias maneiras. A RFC 3748 (ABOBA *et al*, 2004) que descreve o EAP não define de que maneira a autenticação se dá mas apenas as mensagens necessárias para a inicialização e encerramento da negociação.

Dentre os tipos de EAP utilizados temos (WONG, 2003):

- EAP-LEAP: padrão desenvolvido pela Cisco. Usa uma combinação usuário/senha para transmitir a identidade para o servidor RADIUS para autenticação.
- EAP_TLS: usa um certificado X.509 para efetuar a autenticação.
- EAP-TTLS: o autenticador identifica-se para o cliente com um certificado do servidor, o suplicante usa uma identidade do tipo usuário/senha.
- EAP-PEAP: utiliza um certificado de chave pública do lado do servidor para efetuar a autenticação através de um túnel TLS/SSL.

O modo de utilização do 802.1X descrito acima, onde a autenticação é feita em um servidor RADIUS é denominado *Enterprise mode* (modo corporativo). No caso de redes domésticas ou de pequeno porte, o autenticador pode acumular a função de servidor de autenticação, sendo a autenticação feita por um mecanismo de chave pré-compartilhada. Este modo especial é denominado *Pre-Shared Key mode*, comumente conhecido como WPA-PSK.

2.6 Temporal Key Integrity Protocol (TKIP)

Devido ao fato do WPA ter sido desenvolvido com a premissa de ser utilizável em equipamentos legados, todos os esforços foram feitos para que criptografia adotada utilizasse o mesmo algoritmo RC4 utilizado no WEP. A criptografia no WPA é feita pelo TKIP, *Temporal Key Integrity Protocol*. O TKIP de fato utiliza o algoritmo RC4, contudo, foram feitas várias melhorias de modo a suprimir as falhas existentes no WEP.

As principais alterações no TKIP foram:

- Aumento do comprimento do vetor de inicialização.
- Vetor de inicialização utilizado como contador.
- Combinação IV + chave secreta complexa.
- Hierarquia de chaves.

2.6.1 Aumento do comprimento do vetor de inicialização

O vetor de inicialização do WEP tem comprimento de 24 bits, o que possibilita pouco menos de 17 milhões de valores. O vetor de inicialização no TKIP é de 48 bits. Este aumento no comprimento do vetor de inicialização gera aproximadamente 17 milhões de vezes mais valores possíveis. Em termos práticos, em uma rede em que o tráfego fosse grande o bastante para o IV se repetir de hora em hora, passará a levar mais de 1.900 anos para repetir.

2.6.2 Vetor de inicialização utilizado como contador

O padrão WEP sugere que o vetor de inicialização deve ser sempre trocado, contudo, não sugere nenhuma metodologia para esta troca. Assim, alguns fabricantes implementam apenas como um contador.

No caso do TKIP, o padrão determina que o IV seja implementado como um contador, que neste caso é denominado TKIP *sequence counter* (contador de seqüência TKIP), ou simplesmente TSC. Desta forma em toda mensagem é verificado se o valor de TSC foi incrementado.

2.6.3 Combinação IV + chave secreta complexa

No WEP o vetor de inicialização, que transita em claro na mensagem transmitida, é simplesmente concatenado com a chave secreta para gerar a semente do gerador de números pseudo-randômicos do algoritmo RC4. O fato do IV transitar em claro, a quantidade relativamente pequena de valores possíveis de IV, e as chamadas chaves fracas tornaram possível o chamado ataque FMS.

A semente do gerador de números pseudo-randômicos que é utilizada no algoritmo RC4 do TKIP é gerada utilizando-se uma combinação complexa dos valores de IV, chave secreta e ainda o endereço MAC do transmissor, representada na figura 4.3 (EDNEY; ARBAUGH, 2004).

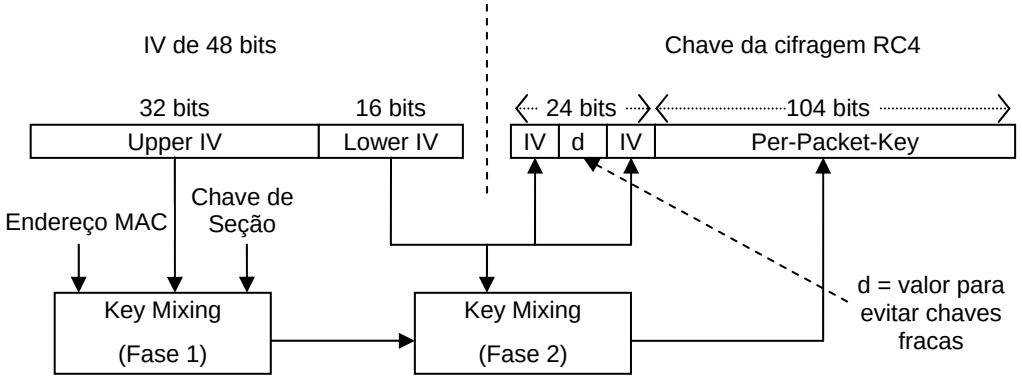

Figura 2.7 – Criação da chave da cifragem RC4 no TKIP

A criação da chave da cifragem RC4 no TKIP é feita em duas fases denominadas *Key Mixing* (mistura de chave) . A fase 1 utiliza o endereço MAC do transmissor, os 32 bits

superiores do vetor de inicialização e a chave de seção (a forma de criação da chave de seção será explicada mais à frente). A fase 2 utiliza apenas os 16 bits inferiores do vetor de inicialização e o resultado da fase 1.

A utilização do IV em partes tem um propósito muito importante: desempenho. Visto que os algoritmos de mistura de chaves envolvem cálculos que exigem muito do processador, estes podem se tornar um problema em AP´s legados, com capacidade de processamento limitado. Assim, a fase 1 utiliza apenas valores quase estáticos, só havendo a necessidade de ser recalculado a cada 2^{16} (65.536) pacotes. A utilização do endereço MAC no cálculo da fase 1 torna a chave única por cliente, isto é, evita que dispositivos distintos venham a gerar a mesma chave.

A fase dois utiliza os 16 bits inferiores do IV que variam a cada pacote, contudo, possui um algoritmo mais leve do que a fase 1, e além disso pode-se calcular previamente valores para pacotes futuros, visto que o IV é um contador. Com estas artimanhas é possível obter-se uma chave de cifragem bem mais segura sem exigir grande esforço computacional por parte dos dispositivos.

Os 24 bits iniciais da chave de cifragem são obtidos através do acréscimo de 8 bits com valor específico pré-determinado aos 16 bits inferiores do IV. A escolha desses bits de preenchimento foi feita de forma a evitar a geração de chaves fracas de classes conhecidas. A chave de cifragem resultante possui comprimento de 128 bits.

2.6.4 Hierarquia de chaves

Um dos problemas do WEP está na utilização da mesma chave secreta para os processos de autenticação e de criptografia de dados (EDNEY; ARBAUGH, 2004). O WPA utiliza chaves distintas para cada processo que necessite de segurança.

As chaves secretas do WPA estão divididas em dois grupos: *Pairwise Key Hierarchy* e *Groupwise Key Hierarchy*.

Pairwise Key Hierarchy diz respeito às chaves utilizadas em transmissões de dados *unicast*, isto é, comunicações que ocorrem entre pares de estações, ou, mais comumente, entre estação e AP. O esquema da *Pairwise Key Hierarchy* está representado na figura 4.4 (EDNEY; ARBAUGH, 2004).

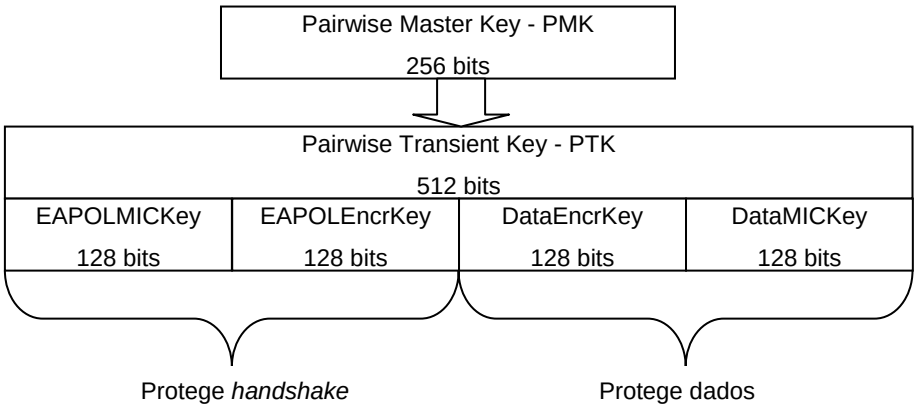

Figura 2.8 – TKIP *Pairwise Key Hierarchy*

A *Pairwise Key Hierarchy* inicia com a *Pairwise Master Key* (PMK). A PMK é criada durante o processo de autenticação EAP, no caso de WPA modo corporativo. Para o WPA no modo chave pré-compartilhada, a PMK é a própria chave pré-compartilhada.

A PMK não é usada diretamente para proteger nenhum processo. Na verdade, a PMK é utilizada para gerar um grupo de quatro chaves temporárias conhecido por *Pairwise Transient Key* (PTK). A PTK é recalculada a cada associação da estação com o AP com base na PMK, nos endereços MAC da estação e do AP e dois valores conhecidos como *nonces*. Os *nonces* são valores de natureza aleatória e que são gerados um pela estação e outro pelo AP e trocados entre estes. O termo vem do inglês N *once*, isto é, um valor N que será usado uma única vez (*once*). São justamente os *nonces* que fazem com que a PTK tenha um valor distinto a cada recalculo.

Os quatro valores que compõem a PTK são:

- EAPOLEncrKey
- EAPOLMICKey
- DataEncrKey
- DataMICKey

A EAPOLEncKey e a EAPOLMICKey são utilizadas durante o *handshake* (autenticação e autorização) EAPOL, respectivamente para proteger a cifragem de dados e a integridade dos dados.

A DataEncKey e a DataMICKey são utilizadas durante a comunicação de dados *unicast*, respectivamente para proteger a cifragem de dados e a integridade dos dados.

A *Group Key Hierarchy* diz respeito às chaves utilizadas em transmissões de dados *multicast*, isto é, comunicações que ocorrem entre múltiplas estações. O esquema da *Group Key Hierarchy* está representado na figura 4.5 (EDNEY; ARBAUGH, 2004).

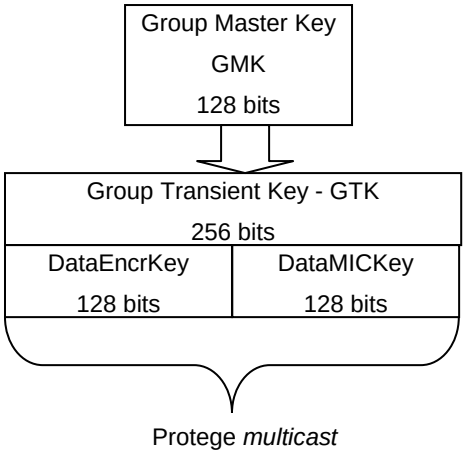

Figura 2.9 – TKIP *Group Key Hierarchy*

De forma análoga à *Pairwise Key Hierarchy*, a *Group Key Hierarchy* inicia com a *Group Master Key* (GMK). A GMK é criada pelo AP e, como a PMK, não é usada diretamente para proteger nenhum processo. A PMK é utilizada para gerar um grupo de apenas duas chaves temporárias conhecido por *Group Transient Key* (GTK). Diferentemente da PTK, a GTK é calculada utilizando-se a GMK e apenas o endereço MAC do AP e um *nonce*, gerado pelo AP. A GTK é enviada às estações pelo AP que aguardará pela confirmação do recebimento de cada estação. Uma vez que a GTK é conhecida por todas as estações, cada vez que uma estação deixa a rede é necessário trocá-la.

Os dois valores que compõem a GTK são:

- DataEncrKey
- DataMICKey

A DataEncrKey e a DataMICKey são utilizadas durante a comunicação de dados *multicast*, respectivamente para proteger a cifragem de dados e a integridade dos dados.

2.7 Message Integrity Check

O MIC, *Message Integrity Check* (Verificador de Integridade de Mensagem) utilizado no TKIP é conhecido como Michael. Sua função é evitar criação ou alteração de pacotes por possíveis atacantes à rede. O Michael é implementado através de uma função matemática usada para gerar uma mensagem de 64 bits adicionada ao pacote TKIP e recalculada no receptor para verificação da autenticidade do pacote.

O algoritmo do Michael foi inventado por Niels Ferguson tendo como fator determinante a necessidade de funcionar em dispositivos WEP legados. Desta forma o algoritmo não poderia exigir grande capacidade de cálculo do dispositivo. O algoritmo desenvolvido utiliza basicamente ou-exclusivos, deslocamentos de bits e módulos.

Justamente por “abrir mão da segurança em favor da implementabilidade em dispositivos pré-RSN” (IEEE, 2004a) o Michael apresenta uma fraqueza quanto a ataques ativos. Para estas fraquezas foram implementadas algumas contramedidas.

2.7.1 Contramedidas do Michael

As contramedidas do Michael são disparadas no caso de ocorrer mais de uma falha na verificação do MIC em um intervalo de menos de 60 segundos. Nesses casos as contramedidas adotadas, basicamente, consistem em desabilitar a rede, desassociando estações, trocar chaves temporárias e aguardar 60 segundos antes de reabilitar a rede. O propósito dessas ações é tornar o ataque tão demorado que se torne inviável.

Os fluxogramas das contramedidas para o autenticador e o suplicante são mostrados nas figuras 4.6 e 4.7, respectivamente (IEEE, 2004a).

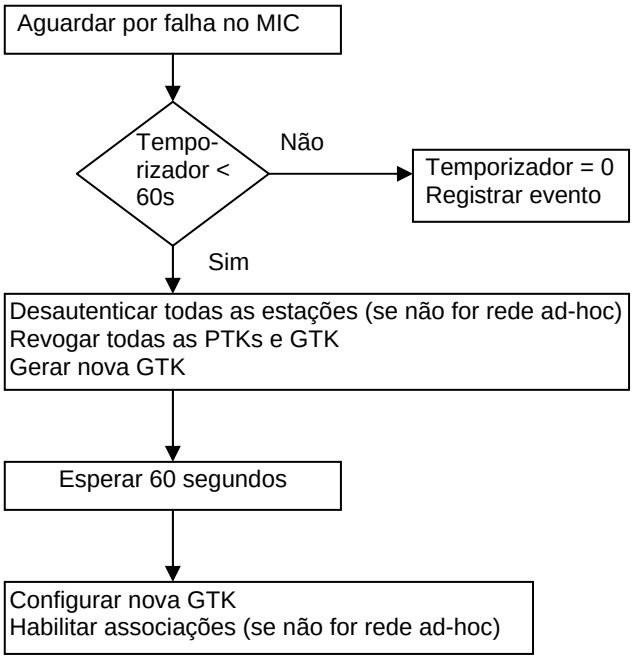

Figura 2.10 – Contramedidas MIC do autenticador

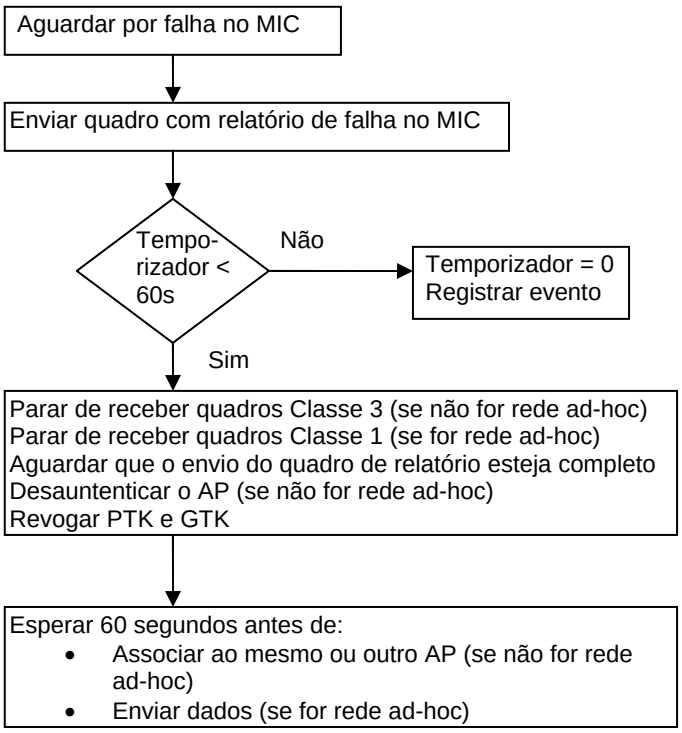

Figura 2.11 – Contramedidas MIC do suplicante

2.8 Encapsulação TKIP

O modo que mecanismo TKIP utiliza para encapsulação está representado na figura 4.8. O MSDU com o texto em claro, o endereço de destino (DA, *destination address*), o endereço do remetente (SA, *sender address*) e o campo prioridade – a ser utilizado futuramente no padrão 802.11e para prover qualidade de serviço – são utilizados para calcular o Michael. O Michael é apendido ao texto em claro. Durante a fragmentação, para cada fragmento gerado, o TSC é incrementado e incluído no cabeçalho. Cada fragmento gerado é então encapsulado no modo WEP utilizando-se a semente WEP gerada a cada fragmento.

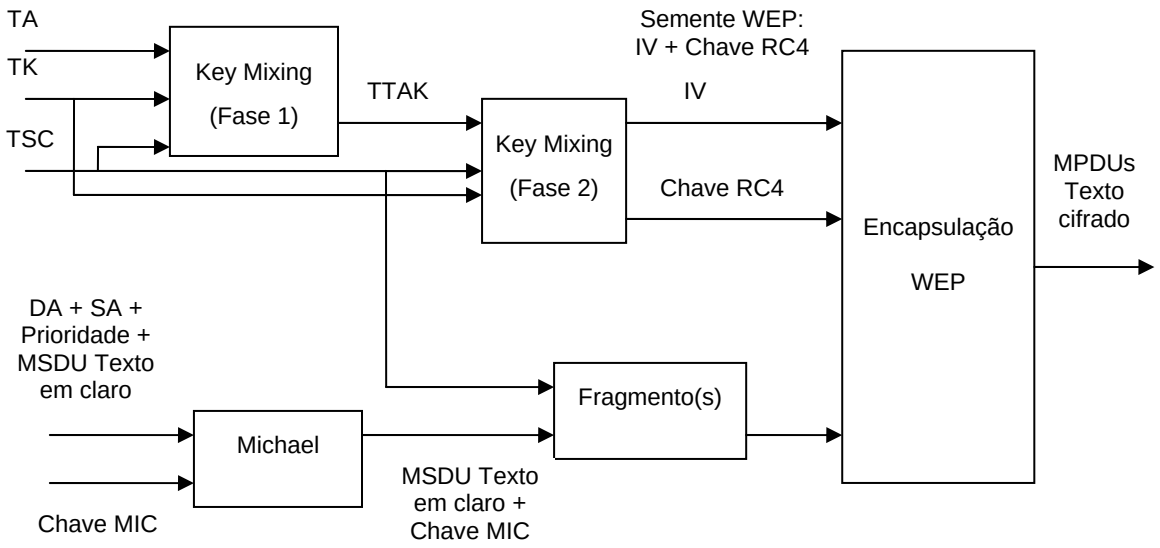

Figura 2.12 – Diagrama de bloco do encapsulação TKIP

A desencapsulação no TKIP está representada na figura 4.9. Antes mesmo de ocorrer a desencapsulação WEP é feito uma verificação de seqüência do MPDU. Após a desencapsulação WEP as MSDU´s são remontadas e então é verificado se o MIC calculado corresponde ao MIC recebido. Uma falha no MIC irá ativar as contramedidas.

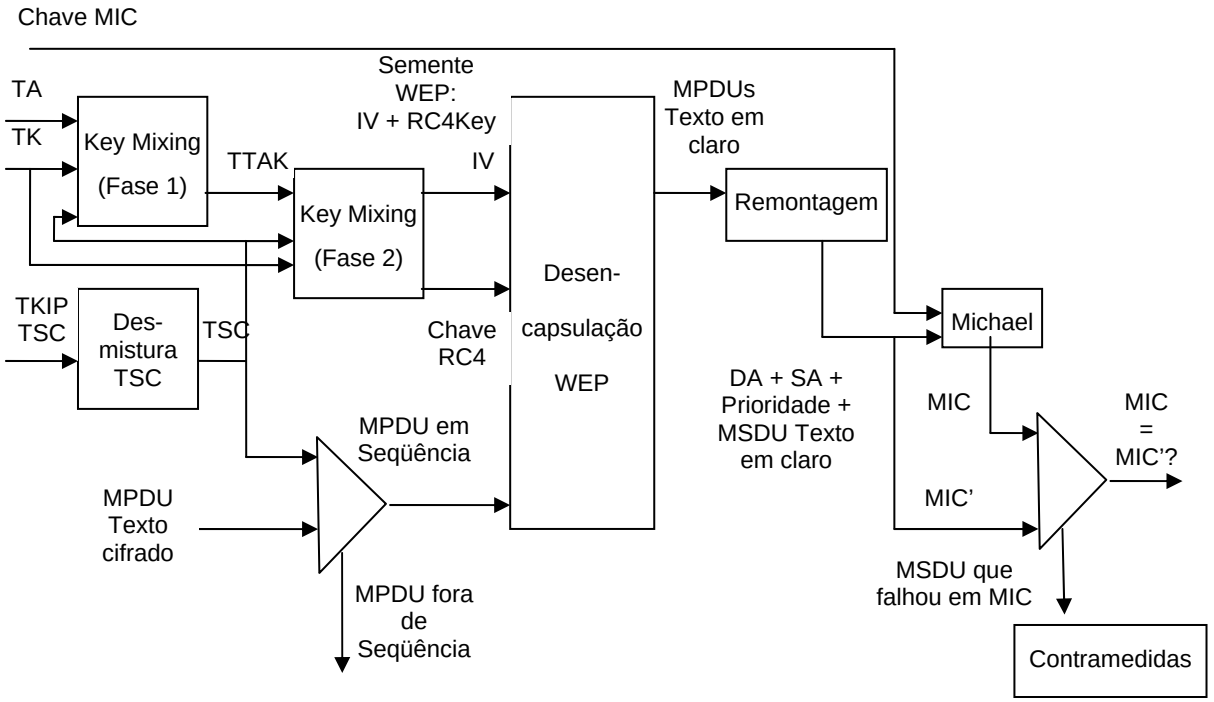

Figura 2.13 – Diagrama de bloco do desencapsulação TKIP

2.9 Comparativo com o WEP

O padrão WPA foi projetado de modo a solucionar todas as falhas encontradas no WEP. Além disso, outra premissa fundamental em sua definição foi a de poder ser implementado nos dispositivos legados – aqueles projetados originalmente para o WEP – com performance aceitável.

Desta forma podemos rever pela tabela 4.1, que enumera as mesmas falhas do WEP citadas na tabela 3.3, de que forma cada falha WEP foi mitigada com a implementação dos três mecanismos principais do WPA: 802.1X, TKIP e o Michael MIC.

Tabela 2.4 – Respostas do WPA às falhas WEP

Falha	A	B	C
Canal de compartilhamento da chave secreta	X		

Mesma chave para autenticação e cifragem do tráfego		X	
Falta de autenticação mútua	X		
Verificação de integridade criptograficamente insegura			X
Reuso do vetor de inicialização		X	
Chaves fracas		X	

A – 802.1X, B – TKIP e C – Michael MIC

2.10 Falhas do WPA

O foco do WPA era solucionar as falhas WEP. Neste sentido seu objetivo foi alcançado plenamente. Contudo nem todas as falhas de segurança que podem ocorrer em uma rede sem fio dizem respeito a falhas no WEP. Duas falhas no WPA foram apontadas e que o tornam sujeito a ataques do tipo negação de serviço ou DOS (*Denial of Service*).

A primeira falha no WPA é devido às contramedidas do Michael. Uma vez que a contramedida para quadros indevidos é interromper a rede por 60 segundos, um possível atacante poderia forjar pacotes constantemente de forma a tornar a rede indisponível. A respeito desta falha, Niel Ferguson, o criador do Michael comenta (FERGUSON, 2002):

> **O ataque DOS baseado nas contramedidas do Michael não é importante pela seguinte razão: há outros ataques DOS, mais sérios, no protocolo 802.11. Se nós "consertarmos" as contramedidas para fazer o ataque DOS mais difícil, o atacante irá simplesmente mudar para outros modos de ataque DOS. O ganho da rede é zero, então não há razão para não usar as contramedidas como especificado.**

A segunda possibilidade de ataque DOS utiliza o *handshake* do protocolo 802.1X. Após as quatro mensagens do *handshake* terem sido feitas entre o autenticador e o suplicante, um atacante envia uma mensagem inicial como se fosse o autenticador. Isso força o suplicante a gerar nova PTK. Assim quando tentar se comunicar novamente com o autenticador, o suplicante terá sua mensagem recusada por falha na PTK (HE; MITCHELL, 2004).

Nos mecanismos WPA especificamente, Wool (WOOL, 2004) mostrou que a segurança do MIC é quebrada completamente se uma simples mensagem for exposta com seu MIC, ou como um ataque à mensagem relacionado pode expor o MIC se uma implementação do TKIP reutilizar o IV.

Um caso mais restrito de falha no WPA acontece no modo PSK (chave pré-compartilhada). *Passphrases* mal escolhidas podem permitir que um potencial atacante as quebre através de ataques de dicionário feitos *offline*. Segundo Moskowitz (MOSKOWITZ, 2003), nesses casos o WPA pode ser menos seguro do que o próprio WEP.

2.11 Definições do 802.11i

O padrão 802.11i diferencia do WPA basicamente pelo uso do algoritmo de criptografia AES (*Advanced Encryption Standard*) no lugar do RC4 usado no WEP e WPA. O algoritmo AES, além de mais robusto, foi definido como padrão pelo NIST (*National Institute of Standards and Technology*). A certificação 802.11i dada pela Wi-Fi Alliance foi denominada WPA2.

2.12 AES

2.12.1 Mecanismo de cifragem

O mecanismo do AES é baseado no algoritmo de Rijndael, inventado por Vincent Rijmen e Joan Daeman. O Rijndael concorreu com 14 outras propostas de algoritmos em um concurso promovido pelo NIST para a escolha do novo padrão de para uso não confidencial (TANENBAUM, 2003).

O AES é uma cifra de bloco, podendo utilizar chaves e blocos de tamanhos 128, 192 ou 256 bits. Contudo, a implementação dada no protocolo de segurança do WPA utiliza

um cifragem de fluxo. Isto é possível através do uso do AES no modo conhecido por CCMP (*Counter Mode CBC-MAC Protocol*).

O CCMP utiliza o modo de contador conforme ilustrado na figura 5.1 (EDNEY; ARBAUGH, 2004). O valor do contador é cifrado com AES e no valor resultante é efetuado um ou-exclusivo com o bloco de mensagem para gerar o bloco de mensagem cifrada. O interessante desta implementação é que a decifragem do bloco de mensagem também utiliza o processo de cifragem AES, pois basta efetuar outro ou-exclusivo entre o bloco de mensagem cifrada e valor resultante da criptografia do contador.

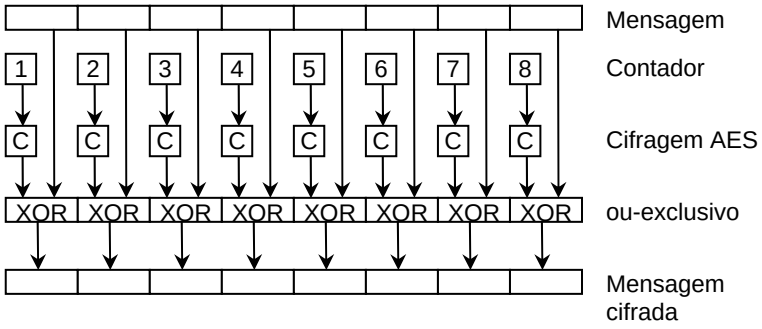

Figura 2.14 – AES no modo contador

O CCMP utiliza ainda um verificador de integridade de mensagem chamado de *Cipher Block Chaining Message Authentication Code* (CBC-MAC). O CBC-MAC funciona da seguinte forma:

1º) Cifra-se o primeiro bloco de mensagem com o AES.

2º) Efetua-se um ou-exclusivo entre o resultado da cifragem e o segundo bloco.

3º) Efetua-se um ou-exclusivo entre o resultado da cifragem e o próximo bloco.

4º) Repete-se o processo até o último bloco da mensagem.

Este processo resulta em um bloco único que combina todos os dados na mensagem.

Outra característica importante do CCMP é o fato de apesar do cabeçalho da mensagem não ser cifrada, ele é autenticado pelo CBC-MAC. Isto evita, por exemplo, que um atacante altere o endereço de origem de modo que a estação de destino responda a mensagem para ele (EDNEY; ARBAUGH, 2004).

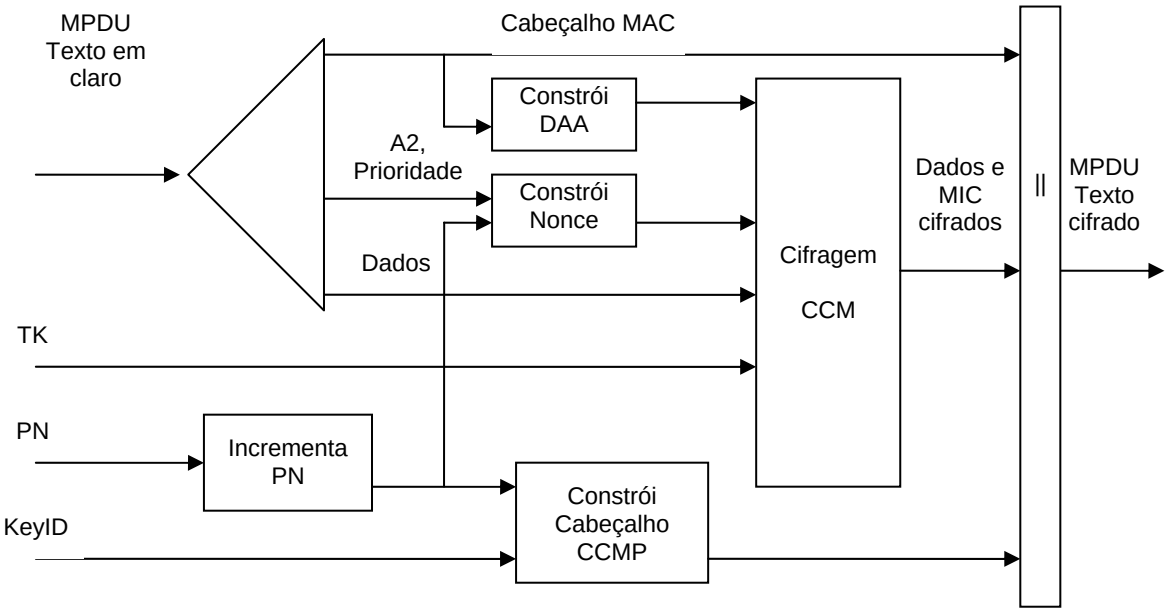

Figura 2.15 – Diagrama de bloco do encapsulação CCMP

A encapsulação CCMP é feita conforme os passos a seguir (IEEE, 2004):

1º) Incrementa o número do pacote, PN (*Packet Number*) para cada MPDU de modo a não repetir PN para a mesma chave temporal (TK). MPDU´s retransmitidas não são modificadas.

2º) Usa o cabeçalho MAC para construir os dados adicionais de autenticação, DAA. Os campos do cabeçalho que podem alterar em retransmissão são zerados no cálculo do DAA.

3º) Constrói o *Nonce* a partir do PN, do campo de endereço 2 (A2), e do campo prioridade do MPDU.

4º) Constrói o cabeçalho CCMP com o novo PN e o identificador da chave (*KeyID*).

5º) Usa a chave temporal, o *nonce*, o DAA e os dados do MPU para gerar o texto cifrado e o MIC.

6º) Forma o MPDU cifrado combinando o cabeçalho original do MPDU, o cabeçalho do CCMP e os dados e MIC cifrados.

2.12.2 Hierarquia de chaves

Diferentemente do TKIP, que possui dois processos que necessitam de segurança e utilizam chaves distintas, o AES-CCMP possui apenas um processo. Assim o número de chaves no AES-CCMP é menor.

Como no WPA, as chaves secretas, também estão dividas em dois grupos: *Pairwise Key Hierarchy* e *Groupwise Key Hierarchy*.

O esquema da *Pairwise Key Hierarchy* para o AES está representado na figura 5.3 (EDNEY; ARBAUGH, 2004).

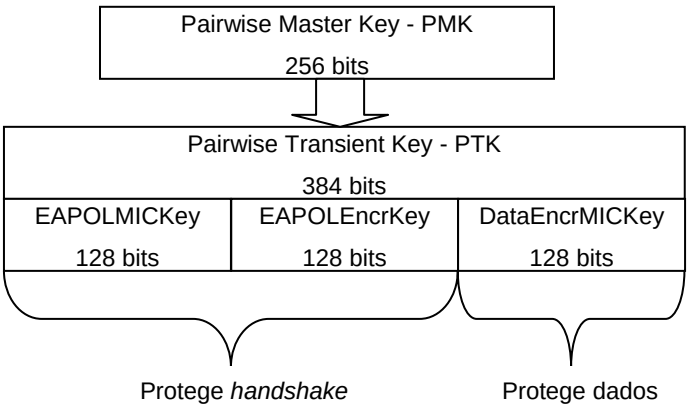

Figura 2.16 – AES *Pairwise Key Hierarchy*

A *Pairwise Key Hierarchy* está dividida em apenas três valores:

- EAPOLEncrKey
- EAPOLMICKey
- DataEncrMICKey

A EAPOLEncKey e a EAPOLMICKey são utilizadas durante o *handshake* (autenticação e autorização) EAPOL, respectivamente para proteger a cifragem de dados e a integridade dos dados.

A DataEncrMICKey é utilizada durante a comunicação de dados *unicast* e para proteger a cifragem de dados e a integridade dos dados.

A *Group Key Hierarchy* está representado na figura 5.4 (EDNEY; ARBAUGH, 2004).

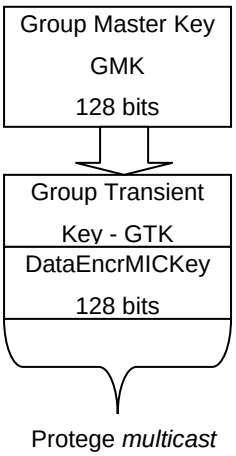

Figura 2.17 – AES *Group Key Hierarchy*

O valor que compõe a GTK é:

- DataEncrMICKey

A DataEncMICKey é utilizada durante a comunicação de dados *multicast* e para proteger a cifragem de dados e a integridade dos dados.

2.13 RSN

O padrão 802.11i apresenta duas definições importantes sobre redes sem fio: RSN e TSN.

RSN (*Robust Security Network*), significa rede de segurança robusta. É definido como “uma rede de segurança que permite apenas a criação RSNA´s” (IEEE, 2004a).

Nessa definição é citada outra definição importante, RSNA. RSNA (*Robust Security Network Association*) é definido como “o tipo de associação usada por um par de estações se o procedimento de estabelecimento de autenticação ou associação entre elas inclui o *handshake* de 4 vias” (IEEE, 2004a).

Sobre a RSNA, Ronald Tögl escreve (TÖGL, 2004):

> **Uma RSNA define um numero de características de segurança tais como mecanismos melhorados de autenticação para estações, algoritmos de gerenciamento de chaves, estabelecimento de chaves criptográficas e dois mecanismos melhorados de encapsulação de dados, fornecendo confidencialidade, chamado CCMP e o TKIP opcional.**

TSN (*Transition Security Network*), significa rede de segurança de transição. É definido como “uma rede de segurança que permite a criação de associações pré-associação de rede de segurança robusta (pré-RSNA´s) bem como RSNA´s.” (IEEE, 2004a).

O importante destas definições é que elas dividem o mundo das redes sem fio 802.11 em duas categorias, as RSN´s, ou seja as redes em que todas as estações utilizam os mecanismos de segurança definidos no padrão 802.11i; e as TSN´s, ou seja, as redes mistas, que permitem estações associadas que não utilizam os mecanismos de segurança do padrão 802.11i.

3 Validação dos mecanismos de segurança

3.1 Ataques ao WEP

Uma implementação prática do ataque de Fluhrer foi proposta por Stubblefield *et al*. (2002). O ataque em sua implementação prática envolve análises matemáticas que vão além da proposta deste trabalho. Contudo, é importante salientar que esses se tornaram a base para ferramentas para quebra de chaves WEP conhecidas, tais como Airsnort e WEPCrack.

Ataques menos complexos, e de eficácia relativa são enumerados por Borisov *et al*. (2001) explorando falhas no algoritmo WEP:

1. Ataque passivo para decifrar o tráfego

Considerando que o vetor de inicialização tem 24 bits, são possíveis 2^{24} valores, isto é, menos de 17 milhões. Assim, em redes com tráfego intenso, o valor do vetor de inicialização certamente irá se repetir em períodos relativamente curtos de tempo – algo em torno de 5 horas para uma rede a 11 Mbps. A repetição do vetor de inicialização, conhecida por colisão, gerará seqüências-chave idênticas. Capturando-se dois textos cifrados com a mesma seqüência e efetuando o ou-exclusivo entre eles obtém-se o ou exclusivo entre os dois textos em claro originais. Isto é demonstrado no exemplo seguir:

(A) 00101000	(B) 10010001
⊕ (S) 00011001	⊕ (S) 00011001
(C) 00110001(A ⊕ S)	(D) 10001000 (B ⊕ S)

(A) 00101000	(C) 00110001
⊕ (B) 10010001	⊕ (D) 10001001
(E) 10111001(A ⊕ B)	(F) 10111001 (A ⊕ S) + (B ⊕ S)

(E) = (F) => (A ⊕ B) = (C ⊕ D) => (A ⊕ B) = (A ⊕ S) + (B ⊕ S)

A intenção deste ataque é decifrar parte de algum texto ou mesmo todo um texto em claro. Para tanto pode ser necessário coletar certa quantidade de ou-exclusivos de textos em claro. O ataque se torna mais fácil se o atacante puder enviar uma mensagem para a rede sem fio – um e-mail, por exemplo – pois assim, tendo o texto em claro poderá calcular a seqüência-chave. Tendo a seqüência-chave para determinado valor do vetor de inicialização poderá decifrar outras mensagens cifradas a partir do mesmo vetor de inicialização.

2. Ataque ativo para injetar tráfego

Conhecendo um texto em claro e seu respectivo texto cifrado, um atacante pode alterar o texto em claro e o texto cifrado da forma correspondente. Assim é possível, por exemplo, alterar comandos enviados a um servidor via telnet.

3. Ataque de ambos os lados

Uma variação do ataque anterior onde o atacante altera o endereço IP de destino de um pacote capturado para o endereço IP de uma máquina de seu controle e o reenvia ao ponto de acesso. Isto é possível pois muitos pontos de acesso estão conectados a redes que possuem saídas para Internet, geralmente através de firewalls. Assim o pacote será recebido como texto em claro – sem cifragem WEP – pelo atacante.

4. Ataque baseado em tabela

Através dos ataques anteriores o atacante obtém uma série de seqüências-chave e seus vetores de inicialização correspondentes criando assim uma tabela. Desta forma poderá decifrar mensagem cifradas com os vetores de inicialização constantes na tabela. Eventualmente poderá obter todos pares de seqüência-chave e vetor de inicialização, podendo então decifrar todo o tráfego.

3.2 Ferramentas de Ataque ao WEP

Com base no ataque FMS e na proposta de implementação prática de Stubblefield, Ioannidis e Rubin (2002), surgiram algumas ferramentas capazes de quebrar a chave WEP. Três dessas são bastante conhecidas: WEPCrack, AirSnort e a mais recente AirCrack.

3.2.1 WEPCrack

Primeira ferramenta a utilizar o ataque FMS.

Apesar de escrita em Perl, linguagem disponível para vários sistemas operacionais, só funciona completamente em ambientes Unix (Linux, BSD e outros).

Utiliza *dumps* de pacotes capturados de rede para quebra da chave secreta WEP. Os *dumps* podem ser gerados com Prismdump ou Ethreal.

Disponível em http://wepcrack.sourceforge.net.

3.2.2 AirSnort

Apesar de ter sido lançado depois de WEPCrack, obteve maior popularidade, por também ser capaz de capturar os dados necessários para quebrar a chave.

Sofreu evoluções em novas versões. Em sua última versão, 0.2.7e, lançada em 9/1/2005, a quebra da chave é feita automaticamente.

Disponível em http://airsnort.shmoo.com.

3.2.3 AirCrack

Conjunto de ferramentas bastante atualizado – versão mais atual, 0.6, lançada em 23/6/2006 – capaz de capturar dados e quebrar a chave secreta WEP.

Disponível em http://www.aircrack-ng.org/doku.php.

3.3 Soluções paliativas

Na tentativa de fazer seus produtos menos sujeitos às falhas do WEP, alguns fornecedores implementaram algumas soluções proprietárias. Além de nenhuma das soluções ter resolvido plenamente os problemas, trouxe mais um: incompatibilidade. As soluções mais interessantes foram (WONG, 2003):

3.3.1 Aumento da chave WEP

Esta foi a primeira solução imaginada pelos fornecedores para aumentar a segurança do WEP. Neste sentido, muitos fornecedores aumentaram a chave secreta para 104 bits, o que ficou conhecido por WEP-128 bits (104 bits da chave secreta mais 24 do vetor de inicialização). Outros foram mais além, como a Agere com 152 bits e a US Robotics com 256 bits.

3.3.2 Chave WEP dinâmica

Alguns fornecedores, como a Cisco e a Microsoft implementaram mecanismos proprietário para a troca automática da chave-secreta WEP. Assim, com a vida útil da chave diminuída seria possível minimizar as chances de quebra da chave secreta.

3.3.3 Utilização de VPN´s

A utilização de VPN´s (*Virtual Private Networks* – Redes Privadas Virtuais) não é propriamente uma solução para as falhas WEP, mas sim uma tentativa de suprir a rede sem fio com um nível de segurança superior ao fornecido pelo WEP.

3.4 Validade do WEP

O padrão 802.11 (IEEE, 2004a) na introdução do WEP diz: "*Wired equivalent privacy* é definida como proteção para usuários autorizados de rede sem fio de escutas casuais".

Por esta definição, pode-se concluir que o objetivo do WEP não é de ser uma proteção muito robusta, capaz de deter *hackers* ou *crackers*. Contudo, mesmo o modesto propósito de deter "escutas casuais" não pôde ser alcançado, pois a quebra da chave secreta pelo ataque FMS deu subsídios à criação de ferramentas para quebra da chave secreta que podem ser utilizadas por usuários com pouco conhecimento de informática.

Assim, o WEP, na prática, se tornou apenas um maneira de desmotivar uma intrusão da rede, ou seja, fazer com que o atacante venha a preferir atacar uma rede sem proteção alguma a perder alguns minutos executando programas de quebra da chave secreta WEP.

3.5 Validade do WPA

Diferentemente do WEP, o WPA conseguiu atingir seus objetivos. Solucionou as falhas apresentadas no WEP e permitiu que os dispositivos legados fossem atualizadas por software evitando assim a necessidade de troca de toda a base de dispositivos instalados.

Além disso, por ter sido criado com base no que já havia sido definido pelo grupo de trabalho 802.11i até aquele o momento, o WPA é também compatível com o padrão 802.11i lançado posteriormente. Assim, mesmo após o lançamento desse padrão, não houve a necessidade de se trocar todos os dispositivos imediatamente para aderir ao padrão. Desta forma o WPA desempenhou bem o papel de padrão de transição.

3.6 Validade do 802.11i

Como era esperado, o padrão 802.11i definiu mecanismos de segurança que solucionaram os problemas apresentados no WEP e ainda definiu um novo conceito de redes sem fio, a RSN.

O uso de CCMP como mecanismo preferencial para encapsulação de dados, no lugar do TKIP, que se mantém como método alternativo, deu maior segurança ao processo por estar baseado em um algoritmo de criptografia, o AES, escolhido por uma criteriosa seleção feita pelo NIST.

Conclusão

A revelação das falhas do WEP e a criação de ferramentas gratuitas capazes de quebrar sua chave tornaram-no ineficaz até mesmo para seu propósito inicial de deter “escutas casuais”.

O grupo criado pelo IEEE para definir um padrão de segurança de redes sem fio confiável, 802.11i, demorou mais do que os consumidores e fabricantes podiam aguardar, forçando a Wi-Fi Alliance a lançar um padrão de transição, o WPA.

O WPA foi definido com base nos padrões que já tinham sido definidos pelo grupo de trabalho 802.11i até aquele instante e teve como premissas resolver os problemas do WEP e permitir, na medida do possível, o *upgrade* dos dispositivos legados através de *software* ou *firmware*. Utilizando um padrão de segurança já reconhecido, o 802.1X, e um mecanismo de segurança desenvolvido especificamente para sua necessidade, o TKIP, o WPA conseguiu cumprir com sua proposta e tornou-se um padrão de transição de grande valor.

O padrão definitivo, 802.11i, acrescentou uma cifragem mais robusta, baseada no AES, aos mecanismos de segurança já definidos pelo WPA. Esse mecanismo, denominado CCMP, permitiu assegurar tanto a confidencialidade quanto a integridade das mensagens.

Ainda mais importante, o padrão 802.11i definiu um novo conceito em redes sem fio, o RSN, ou redes de segurança robusta. Este conceito inclui alguns mecanismos de segurança tais como autenticação melhorada, algoritmo de gerenciamento de chaves, estabelecimento de chave criptográfica e dois mecanismos de encapsulação de dados, o CCMP e, opcionalmente, o TKIP (TÖGL, 2004).

Os mecanismos de segurança do RSN implementam autenticação e cifragem por mensagem, o que não ocorre em redes cabeadas padrão. Apesar de a máxima da segurança

afirmar que “não existe nada 100% seguro”, o padrão 802.11i foi implementado com base em mecanismos robustos e testados por criptonalistas que o tornam confiável o bastante para permitir que as redes sem fio não mais sejam vistas como a parte mais insegura da rede corporativa.

Por este estudo, concluímos que, na forma definida pelo padrão 802.11i, a segurança das redes sem fio não é mais um fator impeditivo para a popularização dessa tecnologia tanto no meio corporativo quanto no doméstico.

Trabalhos Futuros

Este trabalho teve seu foco nos mecanismos de segurança internos do padrão IEEE 802.11. Contudo, uma rede sem fio pode ter sua segurança aumentada pelo uso de mecanismos não definidos pelo padrão. Um desses métodos muito utilizado por fabricantes de dispositivos de rede sem fio é a VPN , que fornece uma camada a mais de segurança à rede.

O uso de *gateways* ou *firewalls* também pode ser considerado para incrementar a segurança. O estudo da segurança efetiva provida por esses mecanismos adicionais pode prover material para trabalhos futuros.

Referências

ABNT. *NBR ISO/IEC 17799*: Tecnologia da Informação – Código de Prática para a gestão da segurança da informação, 1999

ABOBA, B.; BLINK L.; VOLLBRECHT, J.; CARLSON, J.; LEVKOWETZ, H. *IETF RFC 3748: Extensible Authentication Protocol (EAP)*. The Internet Society, 2004.

BORISOV, N.; GOLDBERG, I; WAGNER, D. *Intercepting Mobile Communications: The Insecurity of 802.11*. In: Proceedings of the 7th annual international conference on Mobile computing and networking, p. 180–189. Rome, Italy, 2001.

BORISOV, N.; GOLDBERG, I; WAGNER, D. *Security of the WEP algorithm*. Abr. 2002. Disponível em: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>. Acesso em: 6 ago. 2006 22:50.

EDNEY, J.; ARBAUGH, W. A. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Boston: Addison-Wesley, 2004.

FERGUSON, N. *Re: DOS attack in 802.11i?* 7 nov. 2002. Disponível em: <http://www.mail-archive.com/cryptography@wasabisystems.com/msg03078.html>. Acesso em: 2 set. 2006 15:30.

FLUHRER, S.; MANTIN, I.; SHAMIR, A. *Weakness in Key Scheduling Algorithm of RC4*. In: Eighth Annual Workshop on Selected Areas in Cryptography, 2001.

HE, C.; MITCHELL, J. C. *1 Message Attack on the 4-Way Handshake*, Stanford University, Mai. 2004. Disponível em: <http://www.drizzle.com/_aboba/IEEE/11-04-0497-00-000i-1-message-attack-4-way-handshake.doc>. Acesso em: 1 set. 2006 18:00.

IEEE. *Std 802.11-1997*: Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1997.

____. *Std 802.11i-2004*: Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

____. *Std 802.1X-2004*: Local and metropolitan area networks – Port-Based Network Access Control, 2004.

MOSKOWITZ, R. *Weakness in Passphrase Choice in WPA Interface*, Nov. 2003. Disponível em: <http://www.wifinetnews.com/aschives/002452.html>. Acesso em: 1 set. 2006 18:20.

PEIKARI, C.; FOGIE, S. *Maximum Wireless Security*. Indianapolis: SAMS, 2002.

RSA Security; *RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4.* Set. 2001. Disponível em: <http://www.rsasecurity.com/rsalabs/node.asp?id=2009>. Acesso em: 6 ago. 2006 23:10.

STUBBLEFIELD, A.; IOANNIDIS, J.; RUBIN, A. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. In: Network and Distribution System Security Symposium, 2002.

TANENBAUM, A. S. *Rede de Computadores*. São Paulo: Campus, 2003.

TÖGL, R. *Fixing WEP Robust Security Network with 802.11i.* Set. 2004. Disponível em: <http://www.toegl.co.at/ronald/studium/802.11i-RSN.pdf>. Acesso em: 4 ago. 2006 16:20.

WALKER, J. *Unsafe at Any Key Size: An Analysis of the WEP Encapsulation.* IEEE 802.11. doc 00-362, Out. 2000.

WI-FI ALLIANCE. *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*. 2003.

WOOL A. *A Note in the Fragility of the Michael Message Integrity Code*. IEEE Transactions in Wireless Communication, Vol. 3, No. 5, 2004.

WONG S. *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*. Sans Institute, 2003.