UNIVERSIDADE DO SAGRADO CORAÇÃO

JÚLIO CÉZAR DUARTE DRUMOND

ANÁLISE COMPARATIVA ENTRE OS PROTOCOLOS DE SEGURANÇA WEP, WPA E WPA2

BAURU
2009

JÚLIO CÉZAR DUARTE DRUMOND

ANÁLISE COMPARATIVA ENTRE OS PROTOCOLOS DE SEGURANÇA WEP, WPA E WPA2

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título de Bacharel em Ciência da Computação, sob orientação do Prof. Henrique Pachioni Martins.

BAURU
2009

Lista de Figuras

Figura 1– Associação entre canal e respectiva freqüência 16
Figura 2 – Diagrama de bloco WEP 21
Figura 3 – Autenticação WEP 22
Figura 4 – Exemplo WEP 23
Figura 5 - Exemplo de log 24
Figura 6 - Resultado 25
Figura 7 - Comando 25
Figura 8 – Autenticação 802.1x 28
Figura 9 – Exemplo de Warchalking 37
Figura 10 – Tela do AIRCRAK-NG 38
Figura 11 – Tela do xterm 39
Figura 12 – Imagem do Aicrack 40
Figura 13 - Imagem do Aircrak 40
Figura 14 – Imagem do Aircrack 41
Figura 15 – Imagem do Aircrack 41

Lista de Quadros

Quadro 1 – Probabilidades em espionar em localizações diferentes.....10
Quadro 2 – Comparativo WEP e WPA2 33

SUMÁRIO

1 INTRODUÇÃO 6
2 JUSTIFICATIVA 7
3 OBJETIVOS 8
3.1 Objetivo Geral 8
3.2 Objetivo Específico 8
4 WIRELLES 9
4.1 História 9
4.2 Probabilidades de Ataques 10
4.3 Vantagens e Desvantagens das Redes sem Fio 11
4.4 Formas de Segurança nas Redes sem Fio 11
5 WI-FI: LANs SEM FIO 802.11 16
5.1 Padrões Atuais 16
5.2 Padrão 802.11b 16
5.3 Padrão 802.11a 17
5.4 Padrão 802.11g 17
5.5 Padrão 802.11i 17
5.6 Padrão 802.1n 17
5.7 Padrão 802.1x 18
6 PROTOCOLOS DE SEGURNAÇA WEP, WPA E WPA2 19
6.1 WEP 19
6.1.1 Criptografia 19
6.1.2 Quebra de Chaves WEP 23
6.2 Análise e Performance de Rede *Jperf* 25
6.3 Vulnerabilidades WEP e WPA 25
6.4 WPA 26
6.4.1 Uso de senhas pequenas ou de fácil adivinhação 27
6.4.2 Autenticação no WPA 27
6.4.3 Criptografia de Dados 29
6.4.4 Integridade dos Dados 30
6.5 WPA2 32
6.5.1 Criptografia e Decriptografia WPA2 33
7 Técnicas e Ferramentas 36
7.1 *Access Point Spoofing* (Associação Maliciosa) 36
7.2 ARP *Poisoning* 36
7.3 MAC *Spoofing* 36
7.4 Wardriving 36
7.5 Warchalking 37
8 Ferramentas de quebra 38
8.1 Kismet 38
8.2 AirCrack 38
9 RESULTADOS 39
10 CONSIDERAÇÕES FINAIS 43
REFERÊNCIAS BIBLIOGRÁFICAS 44

RESUMO

As redes sem fio estão cada vez mais presentes em nosso dia a dia. Esta tecnologia nos proporciona mobilidade, resposta mais rápidas, extensão do trabalho e lazer para lugares que antes não eram habituais. Mas todas estas facilidades estão estreitamente condicionadas à questão da segurança. Neste trabalho é feito uma comparação entre dois protocolos de segurança – WEP, WPA e WPA2, disponíveis para redes wireless. Um aspecto crítico se tratando de segurança em redes sem-fio, é a garantia de trafego seguro dos dados diante de um possível ataque e a integridade dos pacotes.

Este trabalho faz um estudo dos métodos criptográficos e através de testes feitos com software de gerenciamento de trafego de rede, será feito uma comparação entre os métodos criptográficos. Com este estudo comparativo, teórico e prático, serão apresentados os principais ataques, as principais vulnerabilidades e suas respectivas soluções e as ferramentas que são utilizadas em cada caso.

Palavras-chave: Wireless, Segurança, WEP, WPA, WPA2.

ABSTRACT

Wireless Network are more and more present in our day. This technology provides us more mobility, quick answers, work extension and leisure for places that before were not habitual. But all this facilities are narrowly conditioned to security matter. In this work is made comparison between three security protocol – WEP, WPA and WPA2, available to wireless network. A critical aspect when we talk about security in wireless networks, is the guarantee that data will traffic in safety in a possible attack and integrity of the packages. This graduation work does a study of the cryptographic methods and after tests done with network traffic management software, it will be made a comparison between the cryptographic methods. In this comparative study, theoretical and practical, it will be presented the main attacks, the main vulnerabilities and their respective solutions and tools that are used in each case.

Key-words: Wireless, Security, WEP, WPA, WPA2.

1 INTRODUÇÃO

Os avanços nas comunicações nos últimos anos possibilitaram o surgimento de várias tecnologias para atender as reais necessidades dos usuários. Hoje em dia, o mercado está apostando em uma das mais surpreendente e revolucionária tecnologia: a tecnologia *Wireless*.

Uma das tecnologias que mais despertou e ainda desperta interesse sobre as pessoas e também sobre as empresas e organizações, devido a sua fácil mobilidade, fácil maneira de ser instalada e proporcionar uma fácil manutenção.

Devido ao grande crescimento no uso das redes sem fio em vários lugares como hotéis, empresas, e também nas casas, houve então, uma enorme preocupação dentro da segurança que essas redes apresentam.

A tendência no mundo todo é a de se criar cada vez mais, redes mistas, onde os trechos são mais distantes e com um acesso difícil utilizando-se das redes sem fio.

Dentro desse propósito serão mencionadas neste trabalho, formas de segurança que podem ser aplicadas, utilizando-se de combinações de seguranças existentes para essa rede como *firewall*, controle de acesso e criptografias. Também serão mencionadas as formas e as ferramentas de segurança que podem ser usadas nas estruturas das redes wireless.

Iremos mostrar também algumas ferramentas que são usadas para localizar e fazer varreduras nas redes sem fio, algumas com recursos que podem ser utilizados para invasão e outras que somente localizam e trazem informações sobre as redes e pontos de acesso.

2 JUSTIFICATIVA

Dentro da tecnologia de redes sem fio, comparando e analisando as vantagens e desvantagens dos protocolos de segurança estudados, serão finalizados com os experimentos e análises dos índices de segurança que são aplicados nesta tecnologia, mostrando os riscos de vulnerabilidade. Esse trabalho será feito para que usuários dessa tecnologia venham se prevenir dos ataques em suas redes, utilizando-se das seguranças necessárias, tornando assim, o uso das redes *wireless* mais segura tanto em ambientes domésticos, como nos corporativos. Serão estudados dentro deste contexto, as possíveis falhas de segurança dentro de uma rede sem fio, sendo que, em hipótese alguma, não teremos o intuito de invadir e explorar possíveis falhas nas redes.

3 OBJETIVOS

3.1 Objetivo Geral

Fazer uma análise comparativa entre os protocolos de segurança WIRED EQUIVALENT PRIVACY (WEP), WI-FI PROTECTED ACCESS (WPA) e WI-FI PROTECTED ACCESS 2 (WPA2), sugerir mecanismos adequados para o uso correto de segurança através dos protocolos e implementar técnicas para a melhoria do uso das redes sem fio, para que estes possam ser usados de maneira segura nas pequenas empresas, ou até mesmo em ambientes domésticos.

3.2 Objetivo Específico

- Fazer um comparativo dos protocolos de segurança mencionados;
- Analisar as possíveis falhas de segurança das redes sem fio;
- Indicar formas de segurança para essas redes.

4 WIRELLES

4.1 História

Redes sem fio (*wireless network*) tem se tornado mais popular a cada dia, principalmente pela sua praticidade e mobilidade na qual oferece aos seus usuários. Nos últimos anos houve um aumento expressivo no número de dispositivos portáteis e suporte a essa tecnologia. Hoje em inúmeros lugares, como salas de conferências, aeroportos e hotéis oferecem como diferencial a seus clientes a possibilidade de acessar a internet a partir de seus dispositivos móveis (RUFINO, 2005).

O uso de redes sem fio não se restringe a ambientes públicos, pois seu uso em ambientes corporativos está cada vez mais utilizado como um auxiliar precioso para as LANs (*Local Área Networks*) convencionais, provendo vantagens econômicas e mobilidade aos usuários (DUARTE, 2003).

A primeira rede sem fio foi criada na Universidade do Havaí, em 1971, para conectar computadores nas quatro ilhas na qual se localizavam seus campos sem utilizar cabos telefônicos. As redes sem fio ingressaram no ramo da computação pessoal nos anos 80. Algumas das primeiras redes sem fio não utilizavam rádio, mas transceptores (uma combinação de transmissor e receptor) infravermelhos. Todavia tais redes nunca obtiveram sucesso porque a sua radiação não pode atravessar a maioria dos objetos físicos (ENGST & FLSIESHMAN, 2005)

Redes sem fio baseadas em ondas de rádio ganharam destaque no início dos anos 90, quando os processadores tornaram-se rápidos o suficiente para gerenciar dados transmitidos e recebidos por meio de conexões de rádio. Porém, somente em 1999 o IEEE (*Institute and Eletrical and Eletronics Engineers*) consolidou o padrão 802.11b. Em meados de 2002 o padrão 802,11a foi ratificado, superando significativamente o 802,11b em termos de velocidade, infelizmente, devido à utilização da banda de 5 GHz, o 802.11a não é compatível com os milhões de dispositivos 802,11b atualmente em utilização, o que contribui para sua baixa aceitação. No final de 2002 surgiu o 802.11g, totalmente compatível com o 802.11b e com a mesma velocidade dos 802.11a (ENGST & FLSIESHMAN, 2005).

As redes wireless seguem os mesmos princípios que guiam todos os dispositivos sem fio. Um transceptor envia sinais através de ondas de radiação eletromagnética, que se

propagam a partir de uma antena, esta recebe sinais propagados nas freqüências corretas e desejadas (ENGST & FLSIESHMAN, 2005).

4.2 Probabilidades de Ataques

Segundo ENGST e FLSIESHMAN (2005) quando estamos recebendo ou enviando algo em redes sem fio, devemos primeiramente observar e analisar onde estamos utilizando essas redes sem fio, pois dependendo de onde estamos, existirá a probabilidade de alguém vir a se conectar com a sua rede e de espionar seus procedimentos nessa rede. Pode ser provável que usemos as redes sem fio em uma ou mais localizações (**Quadro 1**).

Local	***Detalhes***	***Probabilidade de espionar***
Rural/longe	Em sua casa e distante de outras casas	Extremamente baixa
Longo alcance	Sobre um link ponto a ponto de longo alcance com um ISP ou vizinho sem fio	Baixa, devido à natureza direcional da maioria dos links ponto-a-ponto
Afastado do centro urbano (populoso ou não)	Na sua casa em uma área urbana densa ou com pelo menos várias outras casas perto	Moderadamente alta, particularmente se tiver vizinhos high-tech, mas ataques reais são improváveis
Utilização diversificada	Em uma vizinhança residencial e comercial de utilização diversificada	Moderadamente alta, visto que empresas são alvos mais atraentes e são mais prováveis de utilizar redes sem fio
Vizinhança de espaço público	Em uma vizinhança próxima a um estacionamento público ou onde as pessoas podem estacionar na rua	Alta, visto que redes comunitárias recebem alta utilização por uma população anônima e diversa
Edifício comercial	Em um edifício comercial tendo várias empresas ou um estacionamento próximo e dentro do campo de visão	Muito alta, devido à proximidade e à atratividade de alvos
Roaming (itinerante)	Na estrada, em aeroportos, cafés, hotéis e outras localizações	Moderadamente alta, devido à facilidade de monitoração, mas de risco relativamente baixo porque ninguém sabe como observar seus dados particulares

Quadro 1 - Probabilidade de espionar em localizações diferentes
Fonte: Engst e Fleishman (2005)

4.3 Vantagens e Desvantagens das Redes sem Fio

As redes sem fio apresentam as seguintes vantagens:

-Flexibilidade: dentro da área de cobertura, uma determinada estação pode se comunicar sem nenhuma restrição. Além disso, permite que a rede alcance lugares onde os fios não poderiam chegar (COLUNGA, 2008).

-Facilidade: a instalação pode ser rápida, evitando a passagem de cabos através de paredes, canaletas e forros, portanto uso mais eficiente do espaço físico (COLUNGA, 2008).

-Vantagens como: melhor utilização dos investimentos em tecnologias existentes como laptops, rede de dados e voz, aplicativos, agilidade nas respostas aos clientes (COLUNGA, 2008).

-Diversas topologias: podem ser configuradas em uma variedade de topologias para atender a aplicações específicas. As configurações são facilmente alteradas, facilidade de expansão, manutenção reduzida (COLUNGA, 2008).

Em contrapartida, apresentam as seguintes desvantagens:

-Qualidade de serviço: a qualidade do serviço provido ainda é menor que a das redes cabeadas. Tendo como principais razões para isso a pequena banda passante devido às limitações da rádiotransmissão e a alta taxa de erro devido à interferência (COLUNGA, 2008).

-Custo: o preço dos equipamentos de Redes sem Fio é mais alto que os equivalentes em redes cabeadas (COLUNGA, 2008).

-Segurança: intrinsecamente, os canais sem fio são mais suscetíveis a interceptores não desejados. O uso de ondas de rádio na transmissão de dados também podem interferir em outros equipamentos de alta tecnologia, como por exemplo, equipamentos utilizados em hospitais. Além disso, equipamentos elétricos podem são capazes de interferir na transmissão acarretando em perdas de dados e alta taxa de erros na transmissão (COLUNGA, 2008).

-Baixa interferência de dados: embora a taxa de transmissão das Redes sem Fio esteja crescendo rapidamente, ela ainda é muito baixa se comparada com as redes cabeadas (COLUNGA, 2008).

4.4 Formas de Segurança nas Redes sem Fio

Segurança em redes wireless ainda é um assunto tratado de forma muito delicada, tanto pelos que são usuários da tecnologia, quanto pelos os fabricantes de equipamentos. Segurança, apesar de ser um item fundamental em qualquer projeto de rede, ainda é tratada

com certo descaso por aqueles que estão montando uma pequena rede. Apesar dos recursos de segurança atuais não serem 100% invioláveis, é sempre bom garantir, ao máximo, que seu ambiente e possíveis dados estejam bem guardados.

A segurança é o calcanhar de Aquiles das tecnologias wireless atuais, principalmente o Wi-Fi. Se já era difícil garantir e proteger redes convencionais, imagine conseguir essa façanha com informações voando pelo ar, de um lado para outro. Por ainda não ser uma tecnologia 100% segura, todas medidas de segurança adicionais, mesmo que simples, são bem-vindas.

Qualquer pessoa, sem muito conhecimento avançado sobre o assunto, pode adotar medidas básicas para melhorar a segurança de uma rede wireless, o que muitas vezes acaba não acontecendo, criando assim, um verdadeiro paraíso para curiosos e intrusos, muitas vezes conhecidos como hackers.

Para dificultar ao máximo invasões indesejadas em sua rede particular e manter vizinhos bisbilhoteiros longe dos seus arquivos, você pode tomar algumas precauções que veremos a seguir.

1) Utilizar a encriptação de dados é a melhor coisa que você pode fazer para começar a melhorar sua segurança. O método de encriptação mais comum é o WEP (*wired equivalent privacy*), que lhe permite criar chaves de 64, 128 ou 265 bits. Outros métodos, como o WPA (*Wi-Fi Protected Access*), também podem ser utilizados, sempre levando em consideração que a encriptação, apesar de ser um item fundamental, não é a garantia de uma rede impenetrável. O novo protocolo Wi-Fi 802.11i especificado pelo IEEE há pouco tempo, além das chaves convencionais, também traz o sistema AES (*Advanced Encryption Standard*) que demonstra ser um grande avanço no que diz respeito ao *Wi-Fi* e seu futuro. Sem dúvidas, uma rede com dados encriptados, provavelmente espantará 99% dos curiosos de plantão, já que a quebra de chaves de 256 bits ainda não é uma tarefa para qualquer um.

2) SSID (*service set identifier*) é o nome do seu ponto de acesso, que equipamentos visitantes precisam saber para conectar-se a ele. Pontos de acesso costumam vir com SSIDs padrão de fábrica: nomes como *Linksys*, *Default*, *3Com*, são alguns dessa longa lista. Um SSID padrão como esses pode ser uma informação bastante útil para quem está tentando invadir uma rede wireless, afinal, sabendo qual a marca e modelo de determinado aparelho, fica fácil arriscar e tentar encontrar o endereço IP, usuário e senha do mesmo. Um SSID padrão geralmente significa que a rede foi configurada por alguém com muita pressa e/ou pouco conhecimento.

3) Uma vez com o SSID padrão em mãos, é muito simples chegar ao endereço IP, pelo qual é possível ter acesso ao módulo de administrador do aparelho. Cada fabricante tem um padrão de endereço IP que é configurado de fábrica, ou quando é dado reset no aparelho, por isso é importante habilitar a senha do módulo administrador do seu ponto de acesso. Com a senha habilitada, mesmo que o invasor consiga o número IP do seu ponto, ele não terá como ir adiante e entrar no módulo de administração, conseguindo informações valiosas para quem está atacando.

4) Se possível, defina no *hotspot* quais são os endereços MAC das máquinas autorizadas a se conectar(muitos equipamentos permitem isso). Também limite o número de endereços IPs fornecidos pelo servidor DHCP do seu ponto.

5) O envio do nome SSID pelo sinal é bastante útil nos casos onde o acesso do ponto é aberto ao público, pois quem se conecta precisa saber o nome do SSID para efetuar a conexão. Em redes sem visitantes (apenas computadores que raramente mudam) é possível desligar o envio do SSID pelo sinal, informando manualmente esse nome aos dispositivos autorizados a conectar-se ao ponto. Dessa forma, um estranho pode até saber que a sua rede está ali, mas terá isso como um desafio a mais na hora de invadir o seu ambiente. Caso a sua opção de broadcast de SSID esteja habilitada, o ideal então é mudar o nome padrão para algum outro.

6) Este, talvez, seja o ponto onde a maioria acaba por pecar ao instalar uma rede sem fio. A maior parte dos aparelhos permite que você configure a força do sinal, reduzindo ao máximo os sinais que ultrapassam os limites físicos de seu ambiente, impedindo que ele chegue ao alcance do vizinho curioso. O ideal é ir abaixando o sinal aos poucos e testando nos vários pontos da casa ou ambiente. Assim, você dificulta ao máximo uma invasão via rádio, já que a grande maioria dos curiosos de plantão não vai estar equipada com antenas direcionais de alto ganho.

7) Todos os pontos acima estão relacionados aos estágios a serem vencidos antes do invasor alcançar o seu computador. A instalação de uma *firewall* (*software* ou *hardware*) no computador reforça ainda mais a segurança, impedindo o acesso de pessoas indesejadas, mesmo que elas tenham vencido todos os estágios anteriores. Caso sua rede wireless precise de um nível de segurança maior que a alcançada através das medidas acima, isso indica que ela precisa ser desenhada e implementada por especialistas. Redes para escolas, locais públicos, médias e grandes empresas, condomínios, etc, precisam ser muito bem projetadas. O projeto de uma rede com tamanha importância ou proporções leva em conta fatores como clima e topografia, tarefa que é executada por empresas especializadas.

Uma rede *Wi-Fi* básica pode ser montada rapidamente em sua residência ou escritório. Porém, muitos proprietários de imóveis não estão cientes de todas as opções disponíveis para tornar sua rede melhor. Considere as idéias descritas neste artigo que podem melhorar a capacidade, o desempenho e a segurança de sua rede sem fios de sua casa ou escritório.

Muitos proprietários de imóvel ouviram falar de equipamentos básicos de *Wi-Fi*, como roteadores e placas de redes Wireless. Há uma verdadeira explosão de novos modelos de roteadores e adaptadores que vêm expandindo os limites de velocidade e recursos como *firewall*, gerenciamento remoto, servidor *web* e muito mais. O equipamento pode precisar ser substituído por modelos mais rápidos, mais confiáveis e mais compatíveis. As pessoas também esquecem de considerar algumas das novas aplicaçõe s de redes sem fio, tais como os servidores de impressão sem fio. Em vez de se conformar com uma rede sem fios de segunda linha, faça uma pesquisa e adquira o material certo a um bom preço.

Algumas pessoas se apressam em montar sua rede *Wireless* e depois de pronta percebem que algumas áreas do prédio não são atendidas. Outros até conseguem fazer a rede funcionar corretamente, mas de repente, ao atender um telefone sem fio ou ligar o microondas a rede trava. Outros ainda sofrem em silêncio com uma rede de fraco desempenho, mas corrigir esses problemas pode ser muito simples, muitas vezes bastando mudar a posição do Access Point para um ponto mais alto e central dentro do prédio.

Os equipamento *Wi-Fi* podem transmitir vários canais diferentes. A maioria dos roteadores e Access Points funcionam no mesmo número de canal programado de fábrica, competindo pelo mesma faixa de frequência, e a maioria das pessoas nem mesmo sabe que podem mudar isso. Porém, se você estiver enfrentando interferência de outros equipamentos sem fios, simplesmente mudar o canal *Wi-Fi* já pode resolver o problema em definitivo.

Os roteadores *Wireless* contêm trechos de software embutidos chamado *firmware*. Uma versão desse *firmware* é instalada no roteador pelo fabricante, e este trabalha normalmente bem quando o dispositivo é instalado inicialmente. Porém, muitos roteadores oferecem também atualizações periódicas de *firmware* que oferecem novos recursos. Atualizar o *firmware* pode melhorar o desempenho, aumentar a segurança e melhorar a confiabilidade do equipamento. À medida que passa o tempo, mantenha o *firmware* de seu roteador e adaptador atualizado periodicamente.

Não importa em que parte de sua residência ou escritório o *Access Point* esteja instalado, às vezes o sinal da rede sem fios simplesmente não será forte o bastante. A probabilidade desse problema aumenta à medida em que aumentam as distâncias e o número

de obstruções como paredes de tijolo entre o roteador e um cliente *Wi-Fi*. A melhor maneira de resolver este problema é melhorar a antena do *Access Point*. Alguns *Access Points* não suportam esta opção, mas os com antenas destacáveis suportam. Outra opção envolve instalar um dispositivo adicional chamado repetidor, mas envolve perda de desempenho.

Você pode ajustar a potência do sinal emitido pelo *Access Point*, aumentando ou reduzindo o nível de sinal de acordo com sua necessidade. O mesmo se dá com os adaptadores *Wi-Fi*. Geralmente os *Access Points* vêm de fábrica com 75% de sua potência de transmissão.

Muitos proprietários de imóveis consideram sua rede sem fios um sucesso quando o compartilhamento da conexão à *Internet* funciona. Porém, se as funções de segurança não forem habilitadas outras pessoas podem usar sua conexão sem que você sequer saiba disso. Por isso, ative os recursos de criptografia de seu *Access Point* e dos adaptadores de rede *Wi-Fi*.

Seguindo essas dicas você poderá tirar o máximo de sua rede *Wireless* em sua casa ou escritório (AURELIO,2005).

5 WI-FI: LANs SEM FIO 802.11

5.1 Padrões Atuais

O *Institute of Electrical and Eletronics Engineers* (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio. Um desses grupos de trabalho foi denominado 802.11, que reúne uma série de especificações que basicamente definem como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes. Ao longo do tempo foram criadas várias extensões, onde foram incluídas novas características operacionais e técnicas. O padrão 802.11 original (também conhecido como *Wi-Fi*), em termos de velocidade de transmissão, provê, no máximo, 2Mbps, trabalhando com a banda de 2,4 GHz (RUFINO, 2005).

5.2 Padrão 802.11b

Opera na freqüência de 2,4 GHz e usa somente DSSS. Permite um número máximo de 32 clientes conectados. Há limitação em termos de utilização de canais, sendo ainda hoje o padrão mais popular e com maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis (RUFINO, 2007).

Na figura 1 conta a associação entre canal e a respectiva freqüência:

Canal	Freqüência	Canal	Freqüência
1	2,412	8	2,447
2	2,417	9	2,452
3	2,422	10	2,457
4	2,427	11	2,462
5	2,432	12	2,467
6	2,437	13	2,472
7	2,442	14	2,484

Figura 1– Associação entre canal e respectiva freqüência
Fonte: Rufino (2005)

5.3 Padrão 802.11a

Segundo Rufino (2007) o padrão 802.11a tem como sua principal característica um aumento significativo da velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo). Porém, pode operar com velocidades mais baixas. Poe oferecer também, um aumento na quantidade de clientes conectados (64) e ainda no tamanho da chave usada com WEP, podendo chegar em alguns casos, a 256 bits. O maior problema relacionado com a expansão do desse padrão, é a incompatibilidade com a base instalada (802.11b), pois esse padrão usa faixas de freqüência diferentes.

5.4 Padrão 802.11g

Este padrão é mais recente que os comentados anteriormente e equaciona a principal desvantagem do 802.11a, que é utilizar a faixa de 5GHz e não permitir interroperação com 802.11b. Além disso, o 802.11g incorpora várias das características positivas do 802.11a, como utilizar também modulação OFDM e velocidade a cerca de 54 Mb nominais (RUFINO, 2007).

5.5 Padrão 802.11i

O principal protocolo de rede definido neste padrão é chamado RSN (*Robust Security Network*), que permite meios de comunicação mais seguros que os difundidos atualmente. Está inserido neste padrão também o protocolo WPA, que foi desenhado para prover soluções de segurança maios robustas, em relação ao padrão WEP, além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES (*Advanced Encrypton Standard*) (RUFINO, 2007).

5.6 Padrão 802.1n

Segundo Rufino (2007) este tipo de padrão também pode ser conhecido como WwiSE (*World Wide Spectrum Efficiency*). Este padrão está em desenvolvimento, e o seu principal foco é o aumento da velocidade (cerca de 100 a 500 Mbps). Também existe o desejo do aumento da área de cobertura. Relacionado com os padrões atuais, existem poucas mudanças, sendo que a mais significativa é a modificação de OFDM, conhecida como MIMO-OFDM

(*Multiple Input, Multiple Out-OFDM*). Outra vantagem é a compatibilidade retroativa com os padrões atuais.

5.7 Padrão 802.1x

Mesmo não sendo projetado para redes sem fio, até por ter sido definido anteriormente a esses padrões, o 802.1x possui características que são complementares a essas redes, pois permite autenticação baseada em métodos já consolidados como o RADIUS (*Remote Authentication Dial-in User Service*), de forma escalável e expansível. Desta maneira é possível promover um único padrão de autenticação, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas e discadas etc.), e manter a base de usuários em repositório único, quer seja em banco de dados convencional, LDAP ou qualquer outro reconhecido pelo servidor de autenticação (RUFINO, 2007).

É importante notar que para essa infra-estrutura funcionar, basta que os componentes – concentrador, servidor RADIUS e outros opcionais, como: LDAP, Active Directory, banco de dados convencionais etc. – estejam interligados por meio de uma rede. A localização física de cada elemento tem pouca importância (RUFINO, 2007).

Em se tratando de redes sem fio, a mecânica é semelhante: só estará apto a fazer uso dos serviços da rede o usuário (e/ou equipamento) que estiver devidamente autenticado no servidor RADIUS. O 802.1x pode utilizar vários modelos de autenticação no modelo EAP (*Extensible Authentication Protocol*), que define formas de autenticação baseadas em usuário e senha, senhas descartáveis (*One Time Password*), algoritmos unidirecionais (*hash*) e outros que envolvam algoritmos criptográficos (RUFINO, 2007).

6 PROTOCOLOS DE SEGURNAÇA WEP, WPA E WPA2

6.1 WEP

A segurança de uma rede sem fio é muito importante, especialmente para a hospedagem de aplicativos e de informações valiosas. Por exemplo, redes transmitindo números de cartão de crédito para verificação ou armazenando informações sensíveis definitivamente precisam ter sua segurança reforçada. Nesses casos, você deve ser proativo na proteção de sua rede contra ataques de segurança. Quando ativamos o *Access Point* com os parâmetros originais de fábrica, todos os equipamentos com adaptadores *Wi-Fi* em sua área de cobertura poderão se conectar a ele e visualizar os dados sendo transmitidos. Isso podem permitir que hackers violem seu sistema ou roubem dados sigilosos. A primeira medida para evitar esse problema é ativar WEP em sua rede. WEP, sigla para protocolo de segurança de redes sem fio padrão 802.11, é um padrão opcional de criptografia e compressão que está disponível na maioria das placas de interface de rede e nos elementos ativos, tais como *Access Points*. Quando implementamos uma rede *Wirelles*, devemos estar bem atentos à ativação do WEP para melhor a segurança (LIMA, 2006).

Como as informações trafegam livremente em uma rede wireless, teria que existir um controle externo. Sendo assim surgiu o WEP que controla a criptografia e a autenticação. Baseado em *Shared Secrets* ou Senhas Compartilhadas, que são configuradas ponto a ponto de acesso. O padrão WEP foi desenvolvido pelo *Institute of Electrical and Electronics Engineers* (IEEE), cujo objetivo é proporcionar proteção para redes sem-fio que cumpram o padrão 802.11 (MARTINS, 2003).

O WEP se propôs a atender as seguintes necessidades:

Confiabilidade: Segurança e confidencialidade da informação transmitida.

Autenticação: Necessidade de ter um método para garantir a autenticação de um novo dispositivo válido.

Integridade: Garantir que os dados transmitidos chegariam ao outro lado da rede sem sofrer alterações (MARTINS, 2003).

6.1.1 Criptografia

O WEP atua na camada dois (enlace) do modelo Interconexão de Sistemas

Abertos/*Open Systems Interconnection* (ISO/OSI), criado com o objetivo de possibilitar o uso de criptografia para transmissão dos dados, autenticação na rede sem-fio e controle de integridade dos dados (MARTINS, 2003).

O algoritmo usado pelo WEP é o RC4, que é um algoritmo de chave simétrica desenvolvido por *Ron Rivest*. O RC4 criptografa os dados a partir de uma chave fixa de 40 bits ou 104 bits predefinida nos dispositivos. Esta chave é combinada com uma seqüência de 24 bits conhecida por *Inicialization Vector* (IV), formando uma chave de 64 ou 128 bits (MARTINS, 2003).

Criando assim uma seqüência de bits pseudo-aleatória que através de operações XOR (OU EXCLUSIVO), geram os dados criptografados. O IV é modificado para cada pacote enviado. Ao chegar ao receptor utiliza a chave criada e aplica o processo inverso ao da criptografia. O CRC-32 é mais um recurso do WEP, que é uma função que detecta erros, realiza cálculos sobre os dados transmitidos e gera um resultado ICV, enviado junto à mensagem para o receptor. Ao receber a mensagem, o receptor realiza os mesmos cálculos e compara os resultados. Se os resultados forem verdadeiros, ou seja, a mensagem não foi alterada e nem corrompida no trajeto (VERÍSSIMO, 2003).

Esta técnica toma uso da seguinte propriedade da operação binária XOR:

$$A \oplus B \oplus B = A$$

Deste modo, se tomar o texto limpo, executar a operação binária XOR com a seqüência de chaves, e então executar mais uma vez o XOR com a seqüência binária, retornará ao texto limpo. Finalmente, o receptor compara o CRC recebido com o CRC calculado por si para validar a integridade. Na figura 2 existe um gráfico que demonstra o diagrama do bloco WEP.

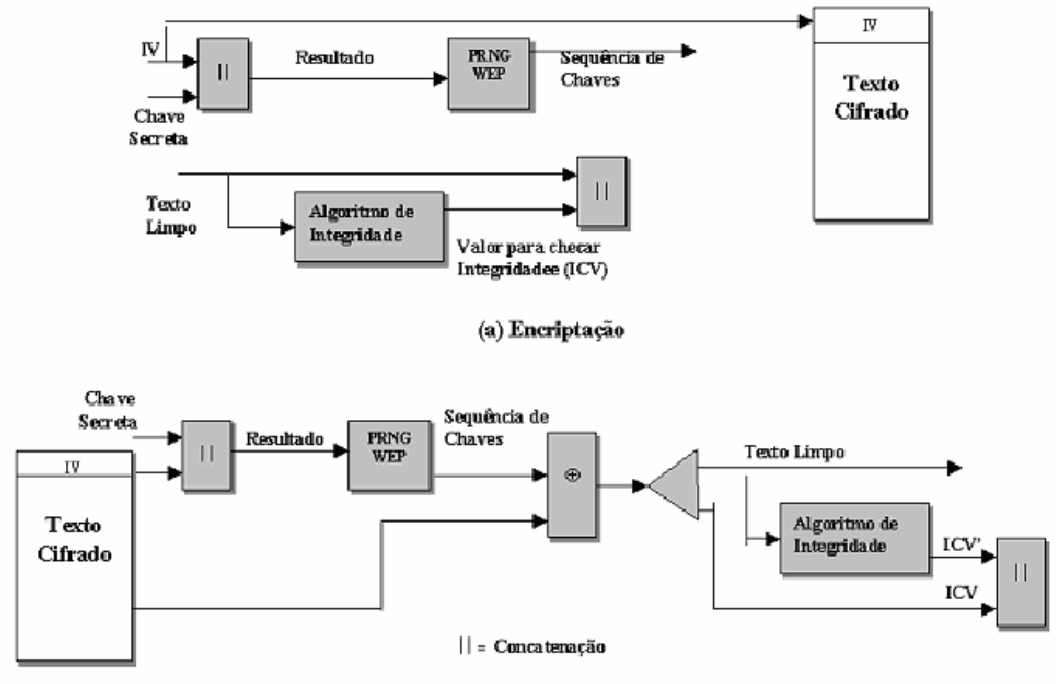

Figura 2 – Diagrama de bloco WEP
Fonte: Martins (2003)

Nas redes *Wi-Fi*, a autenticação pode ocorrer de dois modos sendo que um deles não usa a criptografia. Sem a utilização da criptografia o acesso pode ser aberto ou fechado. O acesso é aberto quando os APs da rede enviam pacotes em *broadcast* para que os clientes *Wi-Fi* detectem a rede. Estes contêm informações como o *Service Set Identifier* (SSID) da rede, canal de comunicação utilizado. Este método é utilizado nos *HotSpots*. Este método ocorre com o WEP desabilitado e o envio do SSID em *broadcast* habilitado. Torna-se um acesso fechado quando o SSID não é enviado em broadcast, dessa forma o cliente tem que ter o conhecimento do SSID para poder se conectar a rede. Neste método, o envio do SSID em *broadcast* é desabilitado. Ambos são extremamente vulneráveis, o método aberto permite só a conexão com a rede, já no método fechado podem ser usados softwares que monitoram os canais de transmissão em busca de informações sobre a rede como o SSID. Exemplos destes tipos de softwares são o *NetStumbler*, *AirCrack* e *KisMAC*. O método que utiliza criptografia consiste em configurar chaves pré-estabelecidas nos clientes sem-fio. Através desta chave compartilhada e com o IV, a criptografia é processada com o algoritmo RC4. Este método autentica os clientes no AP, mas não autentica no cliente, deixando de ter a garantia de que o AP é ou não autorizado (MARTINS, 2003).

A Figura 3 mostra o funcionamento do método de autenticação Desafio/Resposta.

Figura 3 – Autenticação WEP
Fonte: Martins (2003)

O WEP foi muito criticado por suas falhas nos mecanismos de segurança, deixando assim de ter credibilidade. No padrão WEP a chave criptográfica K é a mesma utilizada por todos os hosts da rede, e é através do IV que o RC4 varia esta chave. O problema é que o IV de 24 bits é muito pequeno e a quantidade de combinações diferentes possíveis é de 2**24. Como o IV varia para cada pacote, o IV começará a repetir seus valores. Além disso, o WEP não define como irá ocorrer a variação do IV, isso acaba ficando como decisão de cada fabricante. Quando o fabricante utiliza a repetição pelo método de incrementar seqüencialmente o IV, essa ação torna-se muito perigosa, pois é fácil prever os valores assumidos através do cálculo de quando o IV começará a repetir seu valor e então utilizar o mesmo IV em conjunto com a chave de rede. Especialistas em segurança recomendam a troca das chaves secretas das redes *Wi-Fi* periodicamente para aumentar a segurança (VERÌSSIMO, 2003).

Torna-se um problema, já que a nova chave deve ser configurada em cada host da rede individualmente. Isto se torna pouco prático e até mesmo impossível em redes grandes (VERÌSSIMO, 2003).

Outra falha refere-se a seu mecanismo de garantia de integridade, o CRC-32, que por ser uma função linear e não possuir chave, o torna suscetível a ataques. Outra falha do CRC-32, pelo fato deste não usar chaves, é a possibilidade de se descobrir seqüências, e através destas, burlar a autenticação (VERÌSSIMO, 2003).

Habilitando a criptografia WEP a comunicação passará a ser criptografada e somente quem tiver acesso à chave criptográfica terá acesso à sua rede. A opção WEP pode ser ativada no painel de configuração do AP. Usado ainda hoje, utiliza o algorítmo *Ron Code* 4 (RC4) para criptografar os pacotes que serão trocados numa rede sem fio a fim de tentar garantir confidencialidade aos dados de cada usuário. Além disso, utiliza-se também o *Cyclic Redundancy Code* 32 (CRC-32) que é uma função detectora de erros que ao fazer o checksum de uma mensagem enviada gera um *Integrity Check Value* (ICV) que deve ser conferido pelo receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida e/ou alterada no meio do caminho. Essa tecnologia de encriptação tem dois padrões: 64 e 128 bits. O padrão 64 bits é suportado por toda interface *Wireless Fidelity* (*WI-FI*), já o 128 bits é mais seguro porém não é suportado por todos os produtos. Para ser habilitado todos os componentes da rede devem suportar o padrão, caso isso não aconteça os nós de 64 bits não entrarão na rede (MORIMOTO, 2005).

A WEP foi projetada para agir meramente como uma porta trancada, impedindo que os invasores penetrem no tráfego da rede sem fio; outras medidas destinam-se a sustentar essa linha inicial de defesa. A WEP basicamente criptografa todos os dados que fluem por uma rede sem fio, impedindo que os invasores espionem da rede, como mostra a figura 4 (ENGST & FLEISHMAN, 2005).

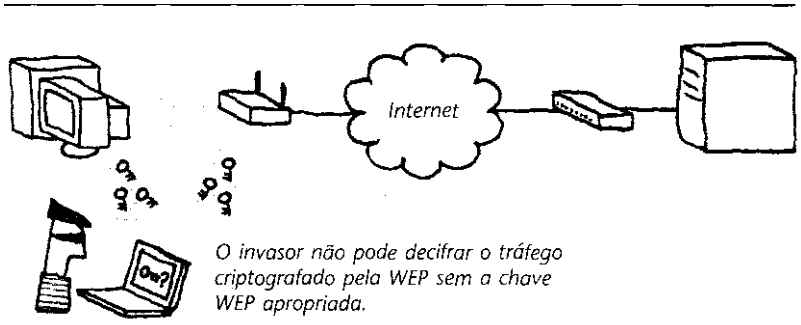

Figura 4 – Exemplo WEP
Fonte: Engst e Fleishman (2005)

6.1.2 Quebra de Chaves WEP

Na rede mundial de computadores acha-se um grande número de ferramentas que fazem o trabalho de quebra de chaves, tanto em virtude de testes no caso de um administrador

de redes, quanto no caso de um hacker que o utiliza para invasão. Geralmente é utilizado a combinação de força bruta e ataques baseados em exploração de vulnerabilidades. Entre as ferramentas conhecidas temos:

- *WepCrack*
- *WepAttack*
- *Airsnort*
- *Wep_tools*
- *Weplab*
- *AirCrack*

Na experiência será utilizado o *AirCrack*, que é considerado uma boa ferramenta para quebra de chaves WEP. Para usá-lo é necessário capturar alguns pacotes da rede com outras ferramentas (*Kismet*, *Ethereal* ou *Tcpdump*).

Posteriormente, o *AirCrack* trabalhará com base no arquivo gerado para descobrir a chave. A descoberta ocorrerá conforme o número de pacotes capturados.

Exemplo:

A rede foi configurada com uma chave WEP de 64 bits, 42:4B:3F:28:50.

Após coleta de trafego o programa gera um arquivo de Log com os resultados da operação realizada. Neste exemplo foi gerado um arquivo de 300 Mega Bytes (MB), como mostra a figura 5. O comando utilizado foi:

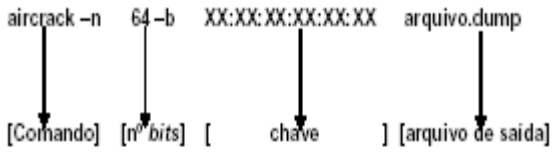

Figura 5 - Exemplo de log
Fonte: Engst e Fleishman (2005)

Após o programa computar por 47 segundos, foi gerado o resultado abaixo (Figura 6):

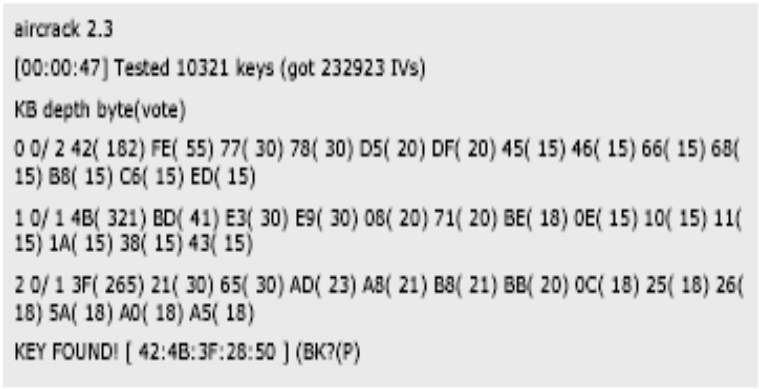

Figura 6 - Resultado
Fonte: Engst e Fleishman (2005)

6.2 Análise e Performance de Rede *Jperf*

Para a análise de desempenho de rede de cada um dos protocolos de autenticação, será utilizado o software *Jperf*, que mede a velocidade real da banda da rede. Através dos logs e gráficos gerados pelo software, é possível analisar qual o protocolo de autenticação tem o melhor desempenho. O servidor foi configurado com o nome HALFORD e a porta 5001 foi aberta para conexão, com pacotes de envio de 16K e tempo de 300 segundos equivalente a 5 minutos para todos os protocolos. Quando o comando RUN é acionado, o programa executa o seguinte comando mostrado na figura 7:

```
iperf -c HALFORD -P 1 -i 1 -p 5001 -l 16K -f k -t 300 -L 5001
```

Figura 7 - Comando
Fonte: Engst e Fleishman (2005)

Sendo que:

- iperf -c name_pc – conexão com máquina remota para medição da banda;
- p – porta de acesso na máquina remota;
- l 16k – tamanho do pacote enviado;
- t 300 – tempo de envio em segundos.

6.3 Vulnerabilidades WEP e WPA

Vulnerabilidades são as falhas ou falta de segurança nas quais pessoas mal intencionadas possam invadir, subtrair, acessar ilegalmente, adulterar e destruir informações confidenciais. Mesmo com os avanços da tecnologia, os riscos inerentes a esta tecnologia se

apresentam de forma significativa e devem ser devidamente analisados e minimizados na implantação da rede. Aspectos antes irrelevantes, como o posicionamento de determinados componentes de rede, agora devem ser cuidadosamente estudados sob o risco de comprometer o bom funcionamento da rede. Alguns itens devem ser observados para avaliar a abrangência de uma rede sem-fio, como o padrão utilizado e a potência dos equipamentos (RUFINO, 2005).

Por exemplo, o padrão 802.11a atinge distâncias menores que o 802.11b ou 802.11g. A maioria dos concentradores permitem selecionar valores intermediários de potência, caso o administrador ache necessário (RUFINO, 2005).

Desta forma, segundo Gimenes (2005), o posicionamento dos componentes pode ser determinante na qualidade e segurança da rede. É regra geral que quanto mais ao centro estiver o concentrador, melhor será o aproveitamento pelas estações do sinal transmitido por ele. Se as ondas de radiofreqüência se propagam pelo ar, então nada mais normal do que serem passíveis de captura. Caso as informações não estejam devidamente cifradas, não somente o tráfego pode ser copiado, como seu conteúdo pode ser conhecido. Dessa forma, fica clara a importância dos protocolos WEP e WPA para redes wireless. Ainda que sejam úteis para a segurança da rede, eles apresentam vulnerabilidades aqui descritas. O protocolo WEP utiliza uma chave única e estática conhecida por ambos os lados da comunicação. Caso precise trocar a chave, o processo pode ser inviável, dependendo do tamanho da rede. Outro problema do WEP é o pequeno tamanho do IV, que não é suficiente para evitar a repetição em uma rede com tráfego elevado, o que facilita a quebra das chaves.

Segundo Tews, Weinmann e Pyshkin (2007), é possível quebrar uma chave WEP de 104 bits em menos de sessenta segundos. Apesar de o WPA ter características de segurança superiores às do WEP, este também está sujeito a ataques de força bruta ou dicionários, onde o atacante testa senha em seqüência ou em palavras comuns.

6.4 WPA

A despeito de o WPA ter características de segurança superiores às do WEP, ainda assim apresenta algumas vulnerabilidades já reportadas e que devem ser conhecidas para que o seu impacto possa ser minimizado (RUFINO, 2007).

6.4.1 Uso de senhas pequenas ou de fácil adivinhação

Apesar desta vulnerabilidade não ser específica do protocolo WPA, este também está sujeito a ataques de força bruta ou dicionário, onde o atacante testa senhas em sequência e/ou em palavras comuns (dicionário) (RUFINO, 2007).

No caso do WPA, senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque. É muito comum fabricantes usarem senhas pequenas (de 8 a 10 posições) imaginando que o administrador irá modificá-las quando colocar o equipamento em produção, porém, isso não ocorre na prática, o que torna redes mesmo com WPA tão ou mais vulneráveis que redes que utilizam WEP (RUFINO, 2007).

Não há até o momento muitas ferramentas publicamente disponíveis que promovam ataques de força bruta e/ou dicionários para ataques ao WPA. A *KisMac*, utiliza em plataforma Maços X, a partir da versão 0.11a passou a incorporar essa funcionalidade (RUFINO, 2007).

6.4.2 Autenticação no WPA

Com o 802.11, a autenticação 802.1X é opcional. Já no WPA, a autenticação 802.1X é obrigatória. A autenticação com WPA é uma combinação de sistema aberto e autenticação 802.1X, que utiliza duas fases:

- 1ª fase: utiliza autenticação de sistema aberto e indica ao cliente sem-fio que ele pode enviar quadros para o AP sem-fio.
- 2ª fase: utiliza 802.1X para executar uma autenticação no nível do usuário.

Ele provê controle de acesso baseado em porta e autenticação mútua entre os clientes e os APs através de um servidor de autenticação. A figura 8 mostra a transação de autenticação 802.1x, onde existem três entidades participantes:

- **Suplicante:** usuário a ser autenticado.
- **Servidor de autenticação:** sistema *Remote Authentication Dial In User Service* (*Radius*) que faz autenticação de clientes autorizados.
- **Autenticador:** intermediário na transação entre o suplicante e o servidor de autenticação.

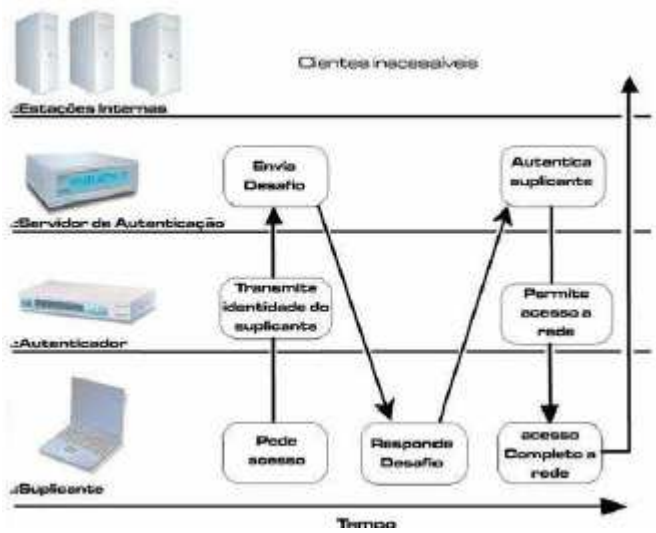

Figura 8 – Autenticação 802.1x
Fonte: Santos (2003)

Os passos de uma transação de autenticação ocorrem da seguinte forma:

1. Um suplicante inicia uma conexão com o autenticador. O autenticador detecta a inicialização e abre a porta para o suplicante. Todavia, todo o tráfego, exceto o relativo à transação 802.1X, é bloqueado.
2. O autenticador pede a identidade ao suplicante.
3. O suplicante responde com a sua identidade.
4. O autenticador passa a identidade a um servidor de autenticação.
5. O servidor de autenticação autentica a identidade do suplicante, e envia uma mensagem de ACCEPT ao autenticador.
6. O autenticador então abre o tráfego ao suplicante.
7. O suplicante pede a identidade do servidor de autenticação.
8. O servidor de autenticação responde com a sua identidade.
9. O suplicante autentica o servidor de autenticação e só então os dados começam a trafegar.

O 802.1x utiliza o protocolo *Extensible Authentication Protocol* (EAP) para gerenciar a forma como a autenticação mútua será feita. Através de um framework generalizado, possibilita a escolha de um método específico de autenticação a ser utilizado como senhas, certificado *Public Key Infrastructure* (PKI) ou *tokens* de autenticação. O autenticador não precisa entender o método de autenticação, ele apenas repassa os pacotes EAP do suplicante para o servidor e vice-versa (SANTOS, 2003).

Existem vários tipos de EAP que dão suporte a diversos métodos de autenticação:

- EAP-LAP (*LightWeight* EAP): Desenvolvido pelo CISCO, usa o método de login e senha para transmitir a identidade do suplicante ao servidor de autenticação.
- EAP-TLS (*Transport Layer Security*): Especificado na *Request for Comments* 2716 (RFC 2716), usa um certificado X.509 para autenticação TLS.
- PEAP (*Protected* EAP): Autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, mas não exige certificados nos clientes. Foi adotado pela Microsoft no Windows XP e Windows Server 2003.
- EAP-TTLS (*Tunneled Transport Layer Security*): É uma extensão do EAP-TLS, pois utiliza a conexão segura TLS para trocar informações adicionais entre o cliente e o servidor. Oferece autenticação mútua e unidirecional, na qual apenas o servidor é autenticado. Ambientes pequenos, onde um servidor de autenticação pode não estar disponível, é usada uma chave pré-estabelecida que é conhecida pelo autenticador e suplicante, e a autenticação ocorre de forma parecida com o WEP, gerando problema de segurança (SANTOS, 2003).

6.4.3 Criptografia de Dados

Ao analisar soluções para os problemas de criptografia do WEP, o *Task Group i* (TGI) encontrou problemas na criação de um protocolo mais robusto para substituir o WEP. Os problemas são:
- Baixo poder de processamento dos chips existentes: Os algoritmos deveriam ser leves para poderem ser executados nos dispositivos que rodavam o WEP.
- Necessidade de manter compatibilidade com o padrão *Wi-Fi*.

A solução foi a utilização do TKIP que é um protocolo de geração de chaves temporais, que apenas poderia ser implementado nos equipamentos já existentes desde que eles tivessem suporte à atualização de firmware. O algoritmo de escalonamento de chaves TKIP surgiu de uma idéia proposta por Russ Housley (RSA *Security*) e Doug Whiting (HIFN) ao IEEE. Foi sugerida por Ron Rivest uma função geradora de chaves para derivar chaves de uma chave base. Rivest propôs a utilização de algoritmos conhecidos como o *Message-Digest Algorithm* 5 (MD5), porém, preferiram não utilizar o MD5 por este ter o custo computacional elevado. Optaram pelo TKIP por ser mais simples e exigir menos processamento. No TKIP, é utilizada uma chave base de 128 bits chamada de Temporal Key (TK). Esta chave é combinada ao endereço *Media Access Control* (MAC) do transmissor *Transmitter Address* (TA), criando uma outra chave chamada de Temporal and *Transmitter Address Key* (TTAK),

conhecida como "Chave da 1º Fase". A TTAK é combinada com o IV do RC4 para criar chaves diferentes para cada pacote. O TKIP faz com que cada estação da rede tenha uma chave diferente para se comunicar com o AP, uma vez que a chave é gerada com o endereço MAC das estações. O problema da repetição de chaves devido à repetição do IV é resolvido ao passo que a TK é alterada sempre que o IV assumir seu valor inicial (SANTOS, 2003).

6.4.4 Integridade dos Dados

O mecanismo utilizado pelo WPA, para garantir a integridade das informações é o algoritmo Michael. Este realiza um cálculo sobre os dados gerando 64 bits. O Michael Integrity Code (MIC) é inserido entre a porção de dados e o ICV de 32 bits no frame 802.11. A diferença principal entre o algoritmo Michael e o CRC-32 é que o primeiro calcula o valor de integridade sobre o cabeçalho do frame também enquanto que o segundo só calcula o valor de integridade sobre a carga de dados e o Michael utiliza chaves para calcular o MIC. Ele previne ataques de repetição que são em que frames repetidos, capturados pelo atacante, são enviados com o intuito de ganhar acesso ou alterar dados da rede. O algoritmo Michael introduz um contador de frames em cada frame, e através deste contador que o ataque de repetição é prevenido. O algoritmo Michael requer pouco processamento e, portanto não precisa de atualização de hardware só de firmwares (SANTOS, 2003).

O processo de criptografia, decriptografia e controle de integridade do WPA ocorre em conjunto. O WPA precisa dos seguintes valores para criptografar, decriptografar e proteger a integridade dos dados da rede sem-fio:

- O IV, que é iniciado em 0 e incrementado para cada quadro subseqüente.
- A chave de criptografia de dados (para tráfego em *unicast*) ou a chave de criptografia de grupo (tráfego em *multicast* ou de difusão).
- O endereço de destino *Destiny Address* (DA) e o endereço de origem Source Address (SA) do quadro sem-fio.
- O valor do campo *Priority* (Prioridade), que é definido como 0 e é reservado para objetivos futuros de *Quality of Service* (QoS).
- A chave de integridade de dados (para tráfego em unicast) ou a chave de integridade de grupo (tráfego em multicast ou de difusão).

O processo ocorre da seguinte forma:

- O IV, o DA e a chave de criptografia de dados são inseridos em uma função de combinação de chave WPA, que calcula a chave de criptografia por pacote.
- O DA, SA, *Priority* (Prioridade), os dados (a carga 802.11 não criptografada), e a chave de integridade de dados são inseridos no algoritmo de integridade de dados Michael para produzir o MIC.
- O ICV é calculado da soma de verificação do CRC-32.
- O IV e a chave de criptografia por pacote são inseridos na função RC4 Pseudo- *Random Number Generator* (PRNG) para produzir um *keystream* do mesmo tamanho que os dados, o MIC e o ICV.
- O *keystream* passa por uma operação de XOR com a combinação de dados, do MIC e do ICV para produzir a parte criptografada da carga 802.11.
- O IV é adicionado à parte criptografada da carga 802.11 no campo IV e o resultado é encapsulado com o cabeçalho e informações finais sobre o 802.11 (THE CABLE GUY, 2004).

A figura 6 mostra o processo de decriptografia do WPA para um quadro de dados *unicast*.

O processo ocorre da seguinte forma:

- O valor IV é extraído do campo IV na carga do quadro 802.11 e inserido junto com o DA e a chave de criptografia de dados na função de combinação de chave, produzindo a chave de criptografia por pacote.
- O IV e a chave de criptografia por pacote são inseridos na função RC4 PRNG para produzir um *keystream* do mesmo tamanho que os dados criptografados, o MIC e o ICV.
- O *keystream* é XORed com dados criptografados, MIC e ICV para produzir dados não criptografados, MIC e ICV.
- O ICV é calculado e comparado ao valor do ICV não criptografado. Se os valores do ICV não coincidirem, os dados serão descartados silenciosamente.
- O DA, o SA, os dados e a chave de integridade de dados são inseridos no algoritmo de integridade Michael para produzir o MIC.
- O valor calculado do MIC é comparado ao valor do MIC não criptografado. Se os valores do MIC não coincidirem, os dados serão descartados. Se os valores do MIC coincidirem, os dados serão passados para as camadas de rede superiores para processamento.

O WPA é uma solução intermediária para corrigir as falhas do WEP. Ele fornece um maior grau de segurança que o WEP. O WPA implementa parte dos recursos do 802.11i na medida que não necessita de novos hardwares.

6.5 WPA2

O WPA corrigiu vários erros do WEP, porém seu desempenho teve uma queda significativa em termos de estabilidade, por isso, surgiu o WPA2 com a promessa de ser a solução definitiva de segurança e estabilidade para as redes sem-fio do padrão Wi-Fi. A principal mudança entre o WPA2 e o WPA é o método criptográfico utilizado. Enquanto o WPA utiliza o TKIP com o RC4, o WPA2 utiliza o *Advanced Encyptation Standart* (AES) em conjunto com o TKIP com chave de 256 bits, que é um método muito mais poderoso. A AES permite a utilização de chaves de 128, 192 e 256 bits, constituindo assim uma ferramenta poderosa de criptografia. A utilização de chave de 256 bits no WPA2 é padrão. Com a utilização do AES, introduziu-se também a necessidade de novo hardware, capaz de realizar o processamento criptográfico. Os novos dispositivos WPA2 possuem um co-processador para realizar os cálculos da criptografia AES. O AES é um cifrador em blocos que criptografa blocos de 16 bits de cada vez, e repetindo várias vezes um conjunto definido de passos que trabalha com chave secreta que opera com um número fixo de bytes. O AES é reversível, o procedimento utilizado para criptografar os dados, é utilizado para decriptografá-los. O AES trabalha com operações de XOR entre os blocos e a chave, organiza o bloco em uma matriz e realiza trocas circulares em cada linha e promove uma mistura entre as colunas da matriz (BERENT, 2005).

Para controle de integridade e autenticação, o WPA2 trabalha como o WPA. No quadro 2, um comparativo entre WEP e WPA2, demonstrando o quanto o WEP é falho em relação WPA2 (BERENT, 2005).

Ponto fraco do WEP	Como o ponto fraco é abordado pelo WPA2
O IV (vetor de inicialização) é muito pequeno	No CCMP do AES, o IV foi substituído por um campo de Número do pacote e duplicou em tamanho, para 48 bits.
Integridade dos dados fraca	O cálculo da soma de verificação criptografada pelo WEP foi substituído pelo algoritmo CBC-MAC do AES, que foi criado para fornecer uma integridade dos dados forte. O algoritmo CBC-MAC calcula um valor de 128 bits, e o WPA2 usa os 64 bits de ordem superior como um MIC (código de integridade da mensagem). O WPA2 criptografa o MIC com a criptografia do modo de contador do AES.
Usa a chave mestra em vez de uma chave derivada	Como o WPA e o protocolo TKIP (Temporal Key Integrity Protocol), o CCPM do AES usa um conjunto de chaves temporais derivadas de uma chave mestra e de outros valores. A chave mestra é derivada do processo de autenticação do 802.1X do EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) ou do PEAP (Protected EAP).
Sem rechaveamento	O CCMP do AES faz o rechaveamento automaticamente para derivar novos conjuntos de chaves temporais.
Sem proteção contra reexecução	O CCMP do AES usa um campo de Número do pacote como contador para fornecer proteção contra reexecução.

Quadro 2 – Comparativo WEP e WPA2
Fonte: Berent (2005)

6.5.1 Criptografia e Decriptografia WPA2

O processo ocorre da forma que o *Counter* CBC-MAC *Protocol* (CCMP) do AES utiliza o *Cipher Block Chaining Message Authentication Code* (CBC-MAC) para calcular o MIC e o modo de contador do AES para criptografar a carga do 802.11 e o MIC. Para calcular o valor de um MIC, o CBC-MAC do AES usa o seguinte processo:

1. Criptografa um bloco inicial de 128 bits com o AES e a chave de integridade de dados. Isso produz um resultado de 128 bits (Resultado1).
2. Executa uma operação OR (XOR) exclusiva entre Resultado1 e os 128 bits de dados seguintes pelos quais o MIC está sendo calculado. Isso produz um resultado de 128 bits (XResultado1).
3. Criptografa o XResultado1 com o AES e a chave de integridade de dados. Isso produz o Resultado2.
4. Executa um XOR entre Resultado2 e os 128 bits de dados seguintes. Isso produz o XResultado2.

Os passos 3-4 se repetem para os blocos de 128 bits adicionais dos dados. Os 64 bits de ordem superior do resultado final são o MIC do WPA2.

O bloco inicial é um bloco de 128 bits. O cabeçalho MAC é o cabeçalho MAC 802.11 com os valores dos campos que podem ser alterados em trânsito definidos como 0. O cabeçalho CCMP tem 8 bytes e contém o campo número do pacote de 48 bits e campos adicionais. Os bytes de preenchimento (definidos como 0) são adicionados para garantir que a parte do bloco de dados inteiro até os dados de texto sem formatação seja um número

integral de blocos de 128 bits. Os dados são as partes de texto sem formatação (não criptografados) da carga do 802.11. Os bytes de preenchimento (definidos como 0) são adicionados para garantir que a parte do bloco de dados do MIC que inclui os dados de texto sem formatação seja um número integral de blocos de 128 bits.

- O campo Sinalizador (8 bits) é definido como 01011001 e contém vários sinalizadores.
- O campo Prioridade (8 bits) é reservado para finalidades futuras e é definido como 0.
- O Endereço de origem (48 bits) é do cabeçalho MAC 802.11
- O Número do pacote (48 bits) é do cabeçalho CCMP.
- O comprimento dos dados de texto sem formatação em bytes (16 bits).

O algoritmo de criptografia do modo de contador do AES usa o seguinte processo:

1. Criptografa um contador inicial de 128 bits com o AES e a chave de criptografia de dados. Resultado de 128 bits (Resultado1).
2. Executa uma operação OR (XOR) exclusiva entre Resultado1 e o primeiro bloco de 128 bits dos dados que estão sendo criptografados. Isso produz o primeiro bloco criptografado de 128 bits.
3. Incrementa o contador e o criptografa com o AES e a chave de criptografia de dados. Isso produz o Resultado2.
4. Executa um XOR entre Resultado2 e os 128 bits de dados seguintes. Isso produz o segundo bloco criptografado de 128 bits.

O modo de contador do AES repete as etapas 3-4 para os blocos de 128 bits adicionais de dados. Para o bloco final, o modo de contador do AES executa o XOR do contador criptografado com os bits restantes. Contador não é o mesmo que o valor do contador de 128 bits usado no algoritmo de criptografia do modo de contador do AES. Para criptografar um quadro de dados em *unicast*, o WPA2 usa o seguinte processo:

1. Insere o bloco inicial, o cabeçalho MAC 802.11, o cabeçalho CCMP, o comprimento dos dados e campos de preenchimento no algoritmo CBC-MAC com a chave de integridade de dados para produzir o MIC.
2. Insere o valor do contador inicial e da combinação dos dados com o MIC calculado no algoritmo de criptografia do modo de contador do AES com a chave de criptografia de dados para produzir os dados criptografados e o MIC.
3. Adiciona o cabeçalho CCMP contendo o Número do pacote à parte criptografada da carga do 802.11 e encapsula o resultado com o cabeçalho e as informações finais do 802.11. Para decriptografar um quadro de dados em unicast e verificar a integridade dos dados:

1. Determina o valor do contador inicial a partir dos valores nos cabeçalhos do 802.11 e do CCMP.
2. Insere o valor do contador inicial e a parte criptografada da carga do 802.11 no algoritmo de decriptografia do modo de contador do AES com a chave de criptografia de dados para produzir os dados decriptografados e o MIC. Para a decriptografia, o modo de contador do AES executa o XOR do valor do contador criptografado com o bloco de dados criptografados, produzindo o bloco de dados decriptografados.
3. Insere o bloco inicial, o cabeçalho MAC 802.11, o cabeçalho CCMP, o comprimento dos dados e campos de preenchimento no algoritmo CBC-MAC do AES com a chave de integridade de dados para calcular o MIC.
4. Compara o valor calculado do MIC com o valor do MIC não criptografado. Se os valores do MIC não corresponderem, o WPA2 descartará os dados silenciosamente. Se os valores do MIC corresponderem, o WPA2 passará os dados para as camadas de rede superiores para processamento.

7 Técnicas e Ferramentas

7.1 *Access Point Spoofing* (Associação Maliciosa)

A associação maliciosa ocorre quando um atacante, passando-se por um *Access Point*, ilude outro sistema de maneira a fazer com que este acredite estar se conectando em uma WLAN real (DUARTE, 2003).

7.2 ARP *Poisoning*

Redireciona o tráfego para o impostor via falsificação/personificação do endereço MAC. É um ataque de camada de enlace de dados que só pode ser disparado quando um atacante está conectado na mesma rede local que a vítima. Um ataque que se utilize de *Address Resolution Protocol* (ARP) *Poisoning* pode ser disparado de uma estação da WLAN à uma estação guiada. (DUARTE, 2003).

7.3 MAC *Spoofing*

Os dispositivos para redes sem-fio possuem a particularidade de permitir a troca do endereço físico. Com isso, atacantes mal intencionados podem capturar um endereço MAC válido de um cliente, trocar seu próprio endereço pelo do cliente e utilizar a rede.

7.4 Wardriving

Utilizam-se neste tipo de ataque equipamentos configurados para encontrar tantas redes sem-fio quantas aquelas que estiverem dentro da área de abrangência do dispositivo de monitoramento (AGUIAR, 2005).

7.5 Warchalking

Este tipo de ataque tem como objetivo encontrar redes sem-fio através de técnicas de Wardriving e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. Estes símbolos guiam outros atacantes, informando-lhes as características da rede (DUARTE, 2003).

Alguns dos símbolos utilizados por estes atacantes podem ser observados na figura 8. Existem grupos organizados para warchalking que se utilizam de símbolos próprios para marcar as redes numa tentativa de mantê-las em segredo (DUARTE, 2003).

A figura 9 mostra uma lista de símbolos usados por atacantes que utilizam o *warchalking*.

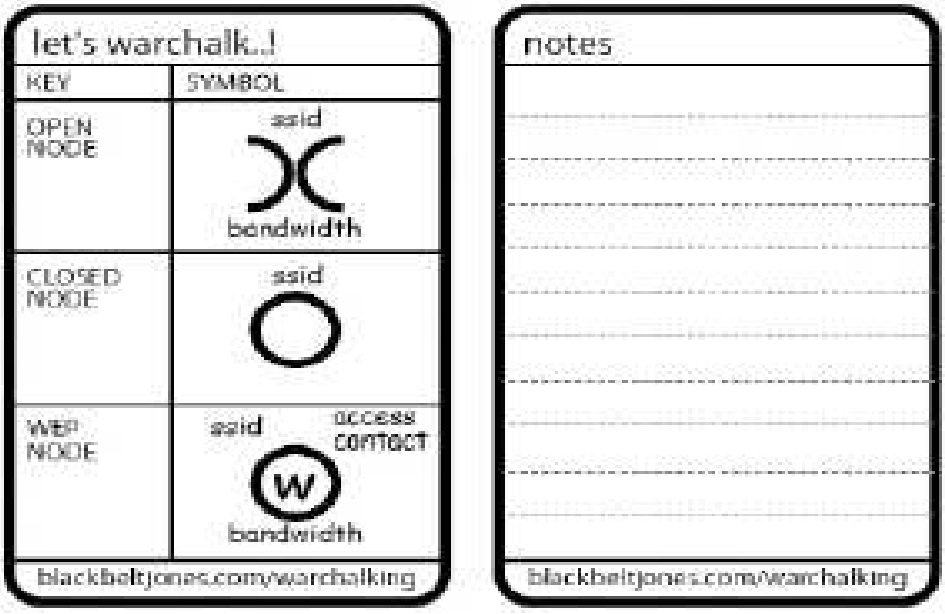

Figura 9 – Exemplo de Warchalking
Fonte: Duarte (2003)

- O primeiro símbolo identifica uma rede *Wi-Fi* aberta, descrevendo seu SSID (nome da rede) e sua largura da banda.
- O segundo símbolo identifica uma rede fechada, descrevendo apenas o SSID (nome da rede).
- O terceiro símbolo identifica uma rede protegida pelo protocolo de criptografia WEP, junto com o SSID (nome da rede), o *Access Contact* (chave WEP utilizada) e a largura da banda (velocidade da rede).

8 Ferramentas de quebra

A seguir algumas ferramentas disponíveis que foram usadas para testes, e suas principais características e objetivos.

8.1 Kismet

É uma das ferramentas com maior velocidade de atualizações e adição de novas funcionalidades. O *Kismet* pode ser utilizado com diferentes finalidades: no mapeamento de redes, na captura de tráfego e na localização via GPS.

Todo o tráfego das redes em análise pelo *Kismet* vai sendo armazenado em um arquivo, mas também pode ser visto em tempo de captura e utilizado de forma imediata por um possível atacante (KISMET, 2007).

A única falha desta excelente ferramenta é não atuar diretamente na quebra de chaves WEP.

8.2 AirCrack

É um programa que pode recuperar chaves uma vez que os pacotes de dados suficientes tenham sido capturado. Ele implementa o ataque FMS padrão juntamente com algumas otimizações como ataque *Korek*, assim como todo ataque PTW nova, tornando o ataque muito mais rápido comparado a outras ferramentas de quebra WEP. Na verdade essa ferramenta é um conjunto para auditoria de redes sem fio.

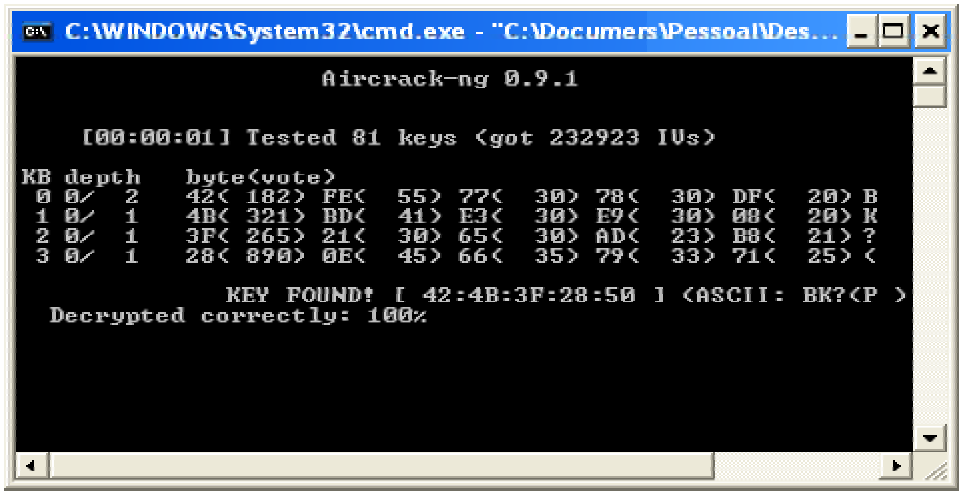

Figura 10 – Tela do AIRCRAK-NG

9 RESULTADOS

Através dos estudos e testes avaliados, os resultados apresentados neste trabalho apresenta os seguintes estudos comparativos dos protocolos:

WEP

Devido esse protocolo ter sido o primeiro a ser criado, ele apresenta uma grande vulnerabilidades. Existem dois parâmetros que servem de entrada para o algoritmo RC4 são a chave secreta k de 40 bits ou 104 bits e um vetor de inicialização de 24 bits. Depois desses dois parâmetros, o algoritmo passa a gerar uma seqüência criptografada RC4 (k,v).

Acontece que no protocolo WEP, a chave secreta é a mesma utilizada por todos os usuários da mesma rede, devemos ter um vetor de inicialização diferente para cada pacote a fim de evitar a repetição de uma mesma seqüência RC4. Essa repetição de seqüência é extremamente indesejável pois pode dar margem a ataques bem sucedidos e conseqüente descoberta de pacotes por eventuais intrusos (figura 11).

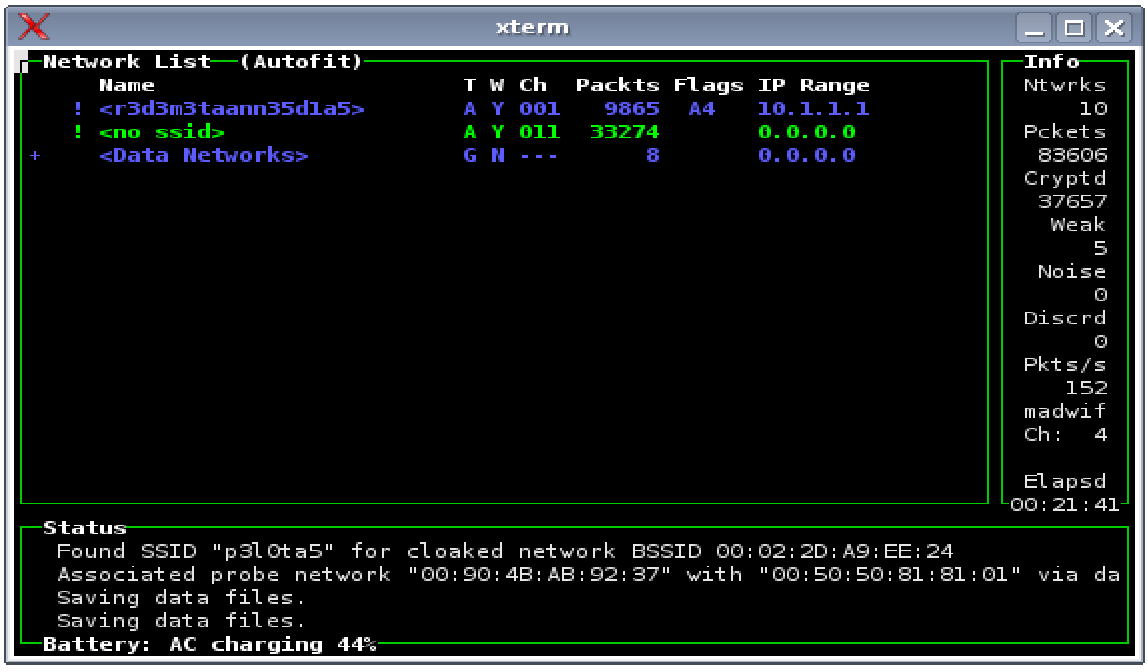

Figura 11– Tela do xterm

A figura 12, o *Kismet* nos mostras quais foram as redes encontradas, onde foi selecionada a rede “minharede” para serem feitos os nossos testes. Depois que selecionamos a rede , os dados da mesma foram salvos em um arquivo de extensão .dump.

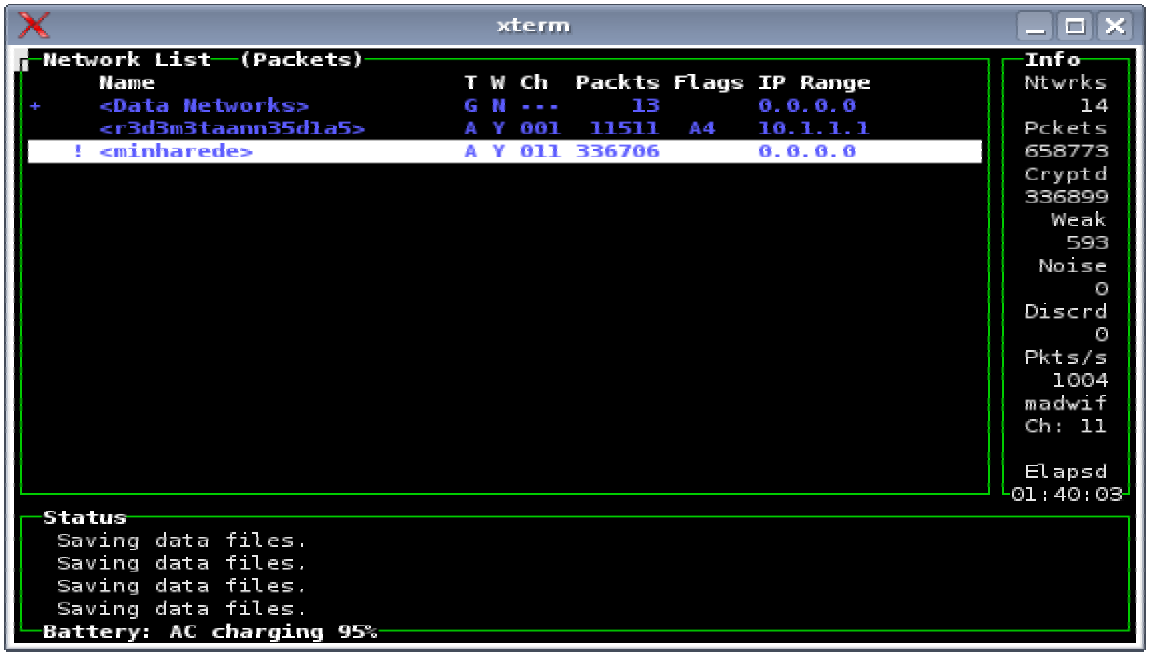

Figura 12 – Imagem xterm

Depois de salvo o arquivo .dump, ele foi inserido no *Aircrack*, para que os dados extraídos da rede “minharede” pudessem ser analisados (figura 13).

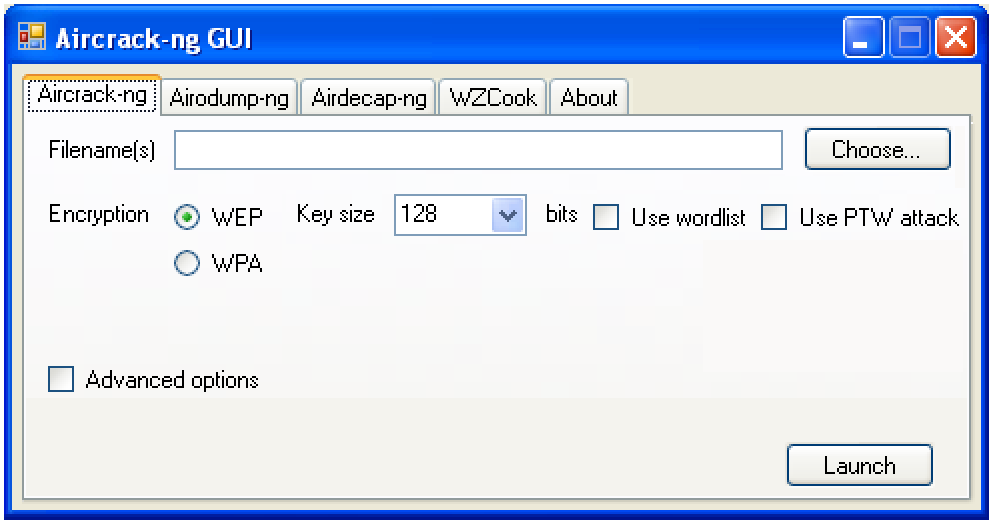

Figura 13 – Imagem do Aicrack

Essa figura (figura 14) nos mostra os dados que estão sendo analisados pelo *Aircrack*, que detectou os MAC´s da rede, ESSID, e também o tipo de protocolo utilizado na segurança, que no caso é o protocolo WEP.

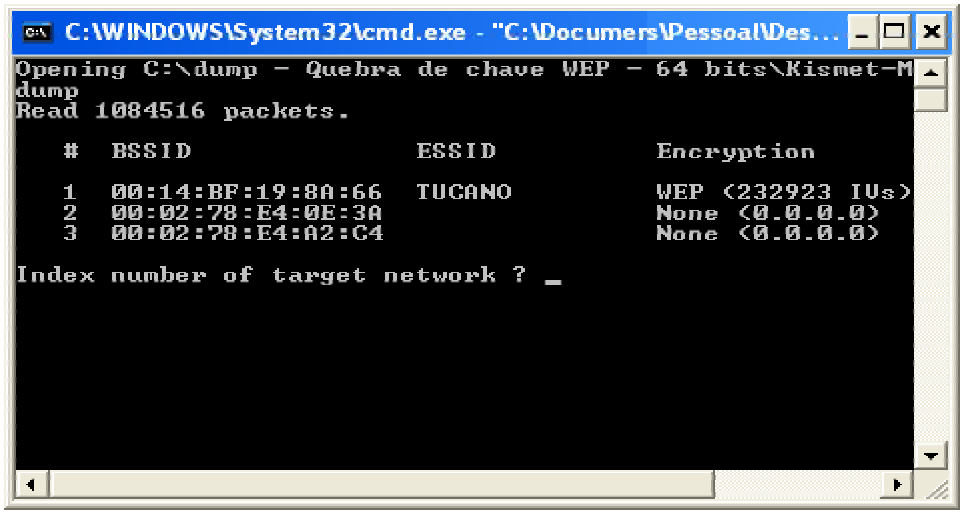

Figura 14 – Imagem do Aircrack

Essa figura (figura 15) nos mostra as chaves de criptografia encontradas, através do trafego de pacotes da rede.

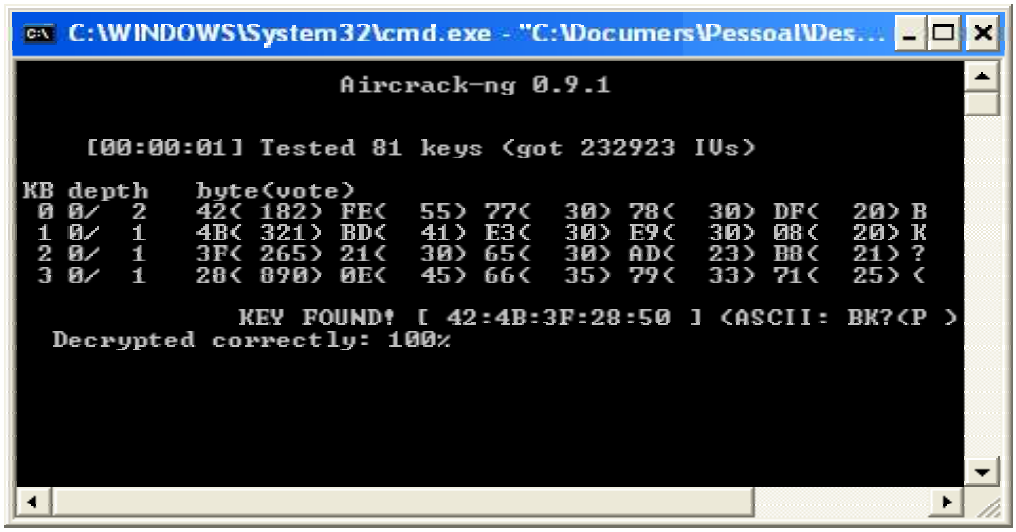

Figura 15 – Imagem do Aircrack

WPA

Um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves, além de contar com uma tecnologia de autenticação de usuários.

Utiliza criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros.

Uma das principais características que diferencia o WEP do WPA, é a chave de criptografia dinâmica, que utiliza a mesma chave repetidamente. Esta característica do WPA, ao contrário do WEP, é muito importante porque não exige que se digite manualmente as chaves de criptografia.

Nos testes realizados não foi possível a quebra da criptografia WPA e também a invasão, isso acontece pois é utilizado uma criptografia dinâmica,

WPA2

Na criptografia do protocolo WPA2 é utilizado o AES (Advanced Encryptation Standart) junto com o TKIP com chave de 256 bits, onde este pode ser considerado um método bem mais poderoso do que o do protocolo WPA, onde este protocolo utilizava o TKIP com o RC4. O AES permite ser utilizada chave de 128, 192 e 256 bits, o padrão no WPA2 é 256 bits, sendo assim, é considerada uma ferramenta muito poderosa de criptografia. Portanto, perante essa tecnologia, os testes que feitos mostrou que não foram possíveis as quebras das chaves criptografadas.

10 CONSIDERAÇÕES FINAIS

Através desse trabalho realizado, podemos concluir que as redes sem fio são de importante necessidade para os usuários, sendo este profissional ou não. Porém, o uso dessa tecnologia ainda nos mostra um fator muito crítico na parte de sua segurança.

Dentro desse estudo comparativo dos protocolos WEP, WPA e WPA2, chegou-se a conclusão de que o protocolo WEP, adota praticamente, as mesmas maneiras de segurança utilizadas nas redes cabeadas.

Analisando o uso do protocolo WEP, foram encontradas diversas falhas, onde as mesmas poderiam ser vasculhadas, exploradas e até mesmo, publicadas na internet.

Devido à essa vulnerabilidade, os engenheiros da IEEE, procuraram por apresentar outros tipos de protocolos, que continham várias soluções para se corrigirem os problemas dentro do WEP, surgindo assim, o protoclo WPA e o WPA2, onde estes garantiram, entre muitas coisas: confidenciabilidade e integridade.

O estudo realizado neste trabalho, será e grande valor para que os usuários das redes sem fio, já que foram encontrados maneiras de segurança para que os usuários de redes sem fio, à nível profissional ou não, ao se conectar e usar suas redes, possam fazê-la de uma maneira mais segura.

REFERÊNCIAS BIBLIOGRÁFICAS

AURELIO, M. **7 Dicas Para Melhorar Sua Rede Wireless em Casa e no Escritório.** Disponível em http://www.malima.com.br/blog/blog_commento.asp?blog_id=18. Acessado em 05/09/2009.

BERENT, A. **AES (Advanced Encryption Standard) Simplified.** Disponível via URL em: http://www.infosecwriters.com/text_resources/pdf/AESbyExample.pdf. Acessado em 02/06/2009.

COLUNGA, M. **Vantagens e Desvantagens das redes sem fio.** 2008. Disponível em http://redeswirelessdf.blogspot.com/2008/05/vantagens-e-desvantagens-das-redes-sem.html. Acessado em: 11/05/2009.

DUARTE, L.O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** São José do Rio Preto, SP. UNESP / IBILCE , 2003, 55p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

ENGST, A.; FLEISHMAN, G. **Kit do Iniciante em Redes Sem Fio:** O guia prático sobre redes *Wi-Fi* para Windows e Macintosh. 2ª ed.: São Paulo. Ed.: Pearson Makron Books.

GIMENES, E. C. **Segurança de Redes Wireless**. Mauá, SP. FATEC, 2005. Trabalho de Conclusão do Curso de Tecnólogo em Informática com ênfase em Gestão de Negócios.

KISMET. **Documentation**. Disponível via URL em: http://www.kismetwireless.net/. Acessado em 02/06/2009.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet:** Uma abordagem top-down. 3ª ed.: São Paulo. Ed.: Pearson Addison Wesley, 2007.

LIMA, M. A. **WEP:** O que é – Como funciona – É seguro. 2006. Disponível em http://www.malima.com.br/blog/blog_commento.asp?blog_id=29. Acessado em 11/05/2009.

MARTINS, M. **Protegendo Redes Wireless 802.11b**. Disponível em http://www.planetarium.com.br/noticias/2003/3/1/104802279/protegendo_redes_wireless.pdf. Acessado em 02/06/2009.

MORIMOTO, C. **WEP.** 2005. Disponível em http://www.guiadohardware.net/termos/wep. Acessado em 12/05/2009.

RUFINO, N.M.O. **Segurança em Redes sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**.** São Paulo: Novatec, 2005.

SANTOS, I. C. **WPA: A evolução do WEP**. Disponível via URL em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=70. Acessado em 02/06/2009.

TEWS, E.; WEINMANN, R.; PYSHKIN, A. **Breaking 104 bit WEP in less than 60 seconds**. 2007.

THE CABLE GUY. **Wi-Fi Protected Access (WPA) Overview**. Disponível via URL em: http://www.microsoft.com/technet/community/columns/cableguy/cg0303.mspx. Acessado em 02/06/2009.

VERÍSSIMO, F. **Em defesa de Rivest**. Disponível via URL em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos?id=55. Acessado em 29/05/2009.