UNIVERSIDADE DO SAGRADO CORAÇÃO

RAFAEL CREPALDI LEITE

ANALISE DAS VULNERABILIDADES E POSSÍVEIS ATAQUES AS REDES SEM FIO

BAURU
2009

RAFAEL CREPALDI LEITE

ANALISE DAS VULNERABILIDADES E POSSÍVEIS ATAQUES AS REDES SEM FIO

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. Esp. Henrique Pachioni Martins.

BAURU
2009

LISTA DE SIGLAS

AES Advanced Encryption Standard
AP Access Point
CPU Central Processor Unit
CRC-32 Cyclic Redundancy Check
dBi Decibel Isotrópico
DSS Direct Sequence Spread Spectrum
EAP Extensible Autentication Protocol
ESSID Extended Service Set Identifier
GHz Gigahertz
GPS Global Positioning System
IEEE Institute and Eletrical and Eletronics Engineers
I/O Input/Output
MAC Media Aceess Control
Mbps Megabits per Second
MIMO Multiple-input multiple-output
OFDM Direct Sequence Spread Spectrum
OTP One time password
PIC Peripheral Interface Controllers
RADIUS Remoto Authentication Dial-In User Server
RC4 Route Coloniale 4
TK Temporal Key
TKIP Temporal Key Integrity Protocol
TTAK Temporal and Tramsmitter Adres Key
WEP Wired Equivalent Privacy
WLAN Wireless Local Area Network
WPA Wi-fi Protected Access
WPA-PSK Wi-Fi Protected Access - Pre-Shared Key
WwiSE Word Wide Spectrum Efficiency

Lista de Figuras

Figura 1 - Modo de Operação AD-Hoc 16

Figura 2 - Topologia modelo infra-estrutura 16

Figura 3 - Simulação de acesso a rede sem fio 24

Figura 4 – Smartcard 25

Figura 5 – Pontos de Invasão 26

Figura 6 - Exemplo de *Warchalking* 27

Figura 7 - Ferramenta Airtraf fazendo varredura 29

Figura 8 - Ferramenta Netstumbler 30

Figura 9 - Kismet capturando redes 31

Figura 10 - Esboço de uma antena comum 32

Figura 11 - Irradiação da antena Ominidirecional 34

Figura 12 - Antena omnidirecional Fonte: HYPERLINK (2008) 35

Figura 13 - Antena parabólica 36

Figura 14 - Antena setorial 36

Figura 15 - Antena Yagi 37

Figura 16 - Kismet em modo de monitoramento 39

Figura 17 - Redes encontradas pelo Kismet 40

Figura 18 - Inserção do Arquivo .dump no AirCrack 40

Figura 19 - AirCrack analisando a rede 41

Figura 20 - Chave Descriptografada 41

Lista de Quadros

Quadro 1 - Visão sobre os padrões IEEE 802.11 19

Sumário

LISTA DE SIGLAS **3**

1 INTRODUÇÃO **11**

2 JUSTIFICATIVA **12**

3 OBJETIVOS **13**

3.1 OBJETIVO GERAL 13
3.2 OBJETIVOS ESPECÍFICOS 13

4 WIRELESS **14**

4.1 HISTÓRIA SOBRE WIRELESS 14
4.2 VANTAGENS 15
4.3 TOPOLOGIA 15
4.3.1 AD-HOC *15*
4.3.2 Infra-Estrutura *16*
4.3.3 Padrões IEEE 802.11 ..... *16*
4.3.4 Padrões IEEE 802.11b *17*
4.3.5 Padrões 802.11a. *17*
4.3.6 Padrão 802.11g *17*
4.3.7 Padrão 802.11i *18*
4.3.8 Padrão 802.1n *18*
4.4 CRIPTOGRAFIA 19
4.4.1 WEP *20*
4.4.2 WPA *21*
4.4.2.1 EAP 22
4.4.3 WPA2 ou 802.11i *22*
4.5 SEGURANÇA 23
4.5.1 Firewall *23*
4.5.2 Métodos de Autenticação *23*
4.5.3 Senhas Descartáveis (OTP) *24*
4.5.4 Certificação Digital *24*
4.5.5 Tokens e Smartcards *25*
4.5.6 Detecção de ataques e monitoramento *26*
4.5.7 Segurança Fisica *26*
4.6 VULNERABILIDADE 26
4.6.1 Mapeamento do ambiente *27*
4.7 FERRAMENTAS E TÉCNICAS DE ATAQUE 27
4.7.1 WarChalking *27*
4.7.2 WarDriving *28*
4.7.3 WarFlying *28*
4.7.4 Access Point Spoofing (Associação Maliciosa) *28*
4.7.5 MAC Spoofing *28*
4.7.6 ARP Poisoning *28*
4.7.7 2.8.7 Airtraf *29*
4.7.8 Airsnort *29*
4.7.9 Netsumbler *29*
4.7.10 Airjack *30*
4.7.11 AirSnarf *30*
4.7.12 Kismet *30*
4.7.13 Ferramentas para quebra de chaves WEP *31*

5 ANTENAS 32
5.1 CONCEITUANDO ANTENAS 32
5.2 CARACTERÍSTICAS BÁSICAS DAS ANTENAS 33
5.3 ANTENA YAGI-UDA 33
5.4 TIPOS DE ANTENAS 34
5.4.1 Antena Ominidirecional 35
5.4.2 Antenas Direcionais 35
5.4.3 Antena Parabólica 36
5.4.4 Antena Setorial 36
5.4.5 Antena Yagi 37
5.5 USOS DE ANTENAS 37
6 METODOLOGIA 38
7 RESULTADOS E DISCUSSÃO 39
8 CONSIDERAÇÕES FINAIS 44
REFERÊNCIAS 45

AGRADECIMENTOS

Agradeço a Deus por me dar forças, me guiar e me fortalecer em todos os momentos da minha vida.

A Minha mãe e meu pai, meus orgulhos, e quem são os responsáveis por ser quem eu sou. Sem vocês nada disso seria possível.

A Adriana e todos meus amigos por me ajudarem a seguir em frente mesmos nos momentos mais difíceis.

A Minha Tia Maria Alba, Ir. Vilma, mesmo que sempre distantes me deram apoio e acreditaram em mim.

Ao meu orientador Prof. Esp. Henrique Pachioni Martins, pela paciência e atenção.

RESUMO

As redes *Wireless* tem sido adotadas por corporações e pessoas para suas tarefas cotidianas, haja em vista que o ganho de produtividade, gerado pela mobilidade e flexibilidade encontradas nesses novos equipamentos sem fio, tem proporcionado grandes vantagens operacionais. No entanto, existem questões de segurança importantes que devem ser consideradas ao se utilizar essa nova tecnologia. Com o intuito de prover mais uma fonte de referência, este projeto estuda as vulnerabilidades de segurança, as formas e ferramentas de ataques existentes nas redes sem fio atuais.

Palavras Chave: wireless, redes sem fio, vulnerabilidades, segurança .

ABSTRACT

Wireless networks have been adopted by corporations and individuals for their daily tasks, there is a view that gains in productivity, generated by the mobility and flexibility found in these new wireless devices, has provided great operational advantages. However, there are security issues that must be considered when using this new technology. In order to provide a source of reference, this project studies the security vulnerabilities, ways and tools of existing attacks on wireless networks today.

Keywords: wireless, wireless networks, vulnerabilities, security.

“A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original.”
Albert Einstein

1 INTRODUÇÃO

No mundo moderno, em que os avanços tecnológicos proporcionam, a cada dia, alterações no modo de utilização das comunicações, as atenções estão voltadas para a mobilidade e flexibilidade de novas formas. Com tais exigências uma das que mais desperta interesse em pessoas e organizações é a tecnologia *Wireless.*

No primeiro capitulo será abordado a história e introdução das redes wireless, partindo de sua criação até as utilizações atuais, algumas de suas vantagens, as topologias que podem ser aplicadas na estruturação da rede, os tipos de protocolos disponíveis, e formas de seguranças que podem ser aplicadas, como firewall e controle de acesso, criptografias e controle de MAC.

Ainda neste capitulo serão abordadas as formas e ferramentas aplicadas nas estruturas das redes wireless, e também algumas ferramentas que são utilizadas para localizar e varrer as redes sem fio.

No segundo capítulo será descrito o conteúdo sobre antenas e a abordagem dos tipos de antenas usadas na comunicação *wireless,* suas características e utilização, dependendo do modelo da antena.

Os capítulos apresentados possuem bases bibliográficas fundamentais para a estudo das redes, e analise da segurança empregada, e simula possíveis ataques nas falhas encontradas.

2 JUSTIFICATIVA

Devido a falta de materiais acadêmicos e científicos sobre o analise das vulnerabilidades das redes sem fio.

3 OBJETIVOS

3.1 Objetivo Geral

Este foi realizado com intuito de identificar das redes sem fio, e possíveis falhas de segurança, simulando invasões em cima das falhas encontradas.

3.2 Objetivos Específicos

- Captura e analise as redes sem fio;
- Analisar a vulnerabilidade e segurança nas redes sem fio encontradas;
- Simular ataques através das falhas encontradas;

4 WIRELESS

4.1 História Sobre Wireless

Segundo Rufino (2005), as redes sem fio, em particular redes Wi-Fi, Indiscutivelmente se tornam a cada dia mais populares, sendo inegável a conveniência de sua utilização em lugares como conferências , aeroportos, cafés e hotéis. A praticidade e mobilidade que as redes sem fio proporcionam em ambientes corporativos e também domésticos são consideráveis .

> O que é mais surpreendente sobre uma rede sem fio é seu poder, considerando a simplicidade subjacente. Na rede sem fio não há nada que seja tão exclusivo, em termos tecnológicos, mas a combinação de diferentes aspectos da computação e da transmissão torna-a uma escolha atraente e até mesmo alude às raízes da revolução social à medida que as pessoas se comunicam entre si por meio de maneiras novas e mais móveis que nunca (ENGST , FLSIESHMAN, 2005).

Ainda o mesmo autor ressalta que a primeira rede sem fio foi desenvolvida na Universidade do Havaí, em 1971, para conectar computadores nas quatros ilhas sem utilizar cabos telefônicos. As redes sem fio entraram no reino da computação pessoal nos anos 80, quando a idéia de compartilhar dados entre computadores começava a tornar –se popular. Algumas das primeiras redes sem fio não utilizavam rádio; em vez disso, contavam com transceptores infravermelhos. Infelizmente, o infravermelho nunca deslanchou porque sua radiação não pode atravessar a maioria dos objetos físicos.

> 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 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 do 802.11a (ENGST , FLSIESHMAN, 2005).

4.2 Vantagens

Algumas vantagens das redes sem fio podem ser resumidas:

- Mobilidade: Aumenta a produtividade do usuário com a conveniência de permitir-lhes conectar-se sem fio à rede a partir de qualquer lugar dentro da faixa do ponto de acesso (PANZUTO, 2008).
- Distribuição rápida e flexível: rede cabeada com a facilidade de anexar um ponto de acesso a uma conexão de rede de alta velocidade (PANZUTO, 2008).
- Redução do Custo Agregado: Redes sem fio, por serem de fácil instalação são também de fácil expansão, tendo também manutenção reduzida, sendo mais compensador que as redes cabeadas (MATHIAS, 2003)

4.3 TOPOLOGIA

4.3.1 AD-HOC

Segundo Panzuto (2008) o termo "ad hoc" (Figura 1) é geralmente entendido como algo que é criado ou usado para um problema específico ou imediato. Do Latin, ad hoc, significa literalmente "para isto", um outro significado seria: "apenas para este propósito", e dessa forma, temporário .

O mesmo autor ainda ressalta que os nós ou nodos numa rede ad hoc se comunicam sem conexão física entre eles criando uma rede "on the fly", na qual alguns dos dispositivos fazem parte da rede apenas durante a duração da sessão de comunicação, ou, no caso de dispositivos móveis ou portáteis, por enquanto que estão a uma certa proximidade do restante da rede

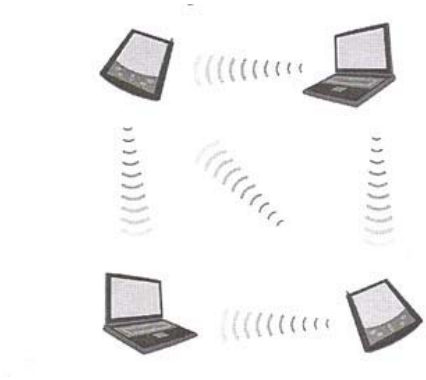

Figura 1 - Modo de Operação AD-Hoc
Fonte: RUFINO (2005).

4.3.2 Infra-Estrutura

A infra-estrutura (Figura 2) há a necessidade de um concentrador de acesso, para que todo tráfego da rede sem fio passe por ele. O mesmo pode efetuar controles como autorizações, autenticações, controle de banda, filtros de pacotes, criptografias (PANZUTO, 2008)

Figura 2 - Topologia modelo infra-estrutura
Fonte: RUFINO (2005).

4.3.3 Padrões IEEE 802.11

> O IEEE é uma associação sem fins lucrativos de profissionais técnicos com cerca de 380 mil membros. O objetivo dessa associação é estabelecer padrões técnicos nos campos das engenharias, elétricas, eletrônicas e computação para uso industrial. Um dos mais conhecidos grupos é o 802.11 que apresenta uma série de especificações que define o uso da comunicação entre dispositivos de uma rede sem fio (ENGST & FLSIESHMAN, 2005).

4.3.4 Padrões IEEE 802.11b

Segundo Rufino (2005) o primeiro subpadrão definido permite 11 Mbps de velocidade de transmissão máxima, porém pode comunicar-se a velocidades mais baixas, como 5,52 ou mesmo 1 Mbps. Opera na freqüência de 2,4 GHz e usa somente DSSS. Permite um nímero Maximo de 32 clientes conectados. Foi ratificado em 1999 e definiu padrões de interoperabilidades bastante semelhante aos da rede Ethernet. 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. Porém, está claro que esse padrão chegou ao limite e já está sendo preterido em novas instalações e em atualizações do parque instalado.

4.3.5 Padrões 802.11a.

Rufino (2005) também ressalta que após definido os padrões 802.11 e 802.11b e tentando resolver os problemas existentes nestes, o 802.11a tem como principal característica o significativo aumento da velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo), mas podendo operar em velocidades mais baixas. Outra diferença é a operação na faixa de 5 GHz, uma faixa com poucos concorrentes porém com menor área de alcance. Oferece também aumento significativo na quantidade de clientes conectados (64) e ainda no tamanho da chave usada com WEP, chegando em alguns casos a 256 bits (mas possui compatibilidade com os tamanhos menores, como 64 e 128 bits) . Finalmente , adora o tipo de modulação OFDM, diferentemente do DSSS usado no 802.11b. Outra vantagem deste padrão consiste na quantidade de canais não sobrepostos disponíveis, um total de 12, diferentemente dos 3 canais livres disponíveis nos padrões 802.11b e 802.11g, o que permite cobrir uma área maior e mais densamente povoada, em melhores condições que outros padrões.

4.3.6 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 5 GHz e não permitir interrupção com o 802.11b. O fato de o 802.11g operar na mesma faixa (2,4 GHz) permite até que equipamentos de ambos padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática do parque instalado. 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, 2005).

4.3.7 Padrão 802.11i

Esse padrão foi criado em 2004, com a definição de mecanismos de autenticação e privacidade, podendo ser implementado nos padrões existentes, o mesmo inclui o WPA como objetivo de oferecer soluções seguras e eficientes .

4.3.8 Padrão 802.1n

> Também conhecido como WWiSE este é um padrão em desenvolvimento, cujo foco principal é o aumento da velocidade (cerca de 100 a 500 Mbps). Paralelamente, deseja-se aumento da área de cobertura. Em relação aos padrões atuais há poucas mudanças. A mais significativa delas diz respeito a uma modificação de OFDM, conhecida como MIMO-OFDM(Multiple Input, Multiple Out-OFDM). Outra Característica deste padrão é a compatibilidade retroativa com os padrões vigentes atualmente. O 802.11n pode trabalhar com canais de 40 Mhz, também, manter compatibilidade com os 20 MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 135 Mbps (RUFINO, 2005).

No quadro abaixo seguem informações referentes as topologias IEEE :

Padrão	**Freqüência**	**Throughput Bruto/real**	**Compatível com o 802.11b**	**Ano em que se tornou real**	**Tendência à adoção**
802.11b	2,4 Ghz	11 Mbps/ 5 Mbps	Sim	1999	Diminuindo em computadores, avançando na eletrônica mais barata
802.11ª	5 Ghz	54 Mbps/ 25 Mbps	Não	2002	Empresas adotando lentamente, sem consumidores
802.11g	2,5 Ghz	54 Mbps/ 20 Mbps	Sim	2003	Avançando em todos os lugares

Quadro 1 - Visão sobre os padrões IEEE 802.11
Fonte: ENGST & FLSIESHMAN (2005).

4.4 Criptografia

Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados. Para solucionar esses problemas, o WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. Porém, dados a diversidade e os ambientes onde uma rede sem fio pode existir (ambientes domésticos, pequenos escritórios, pequenas e grandes indústrias, etc.), pensou-se ser razoável que o WPA tivesse também diferentes modelos de segurança para ter melhor aderência às diferentes necessidades (RUFINO, 2005).

Os protocolos usados para cifrar as informações podem ser dois tipos: um voltado para pequenas redes e de uso doméstico, onde existirá uma chave compartilhada previamente (Pre-shared key, ou WPA-PSK), conhecida como master, que será responsável pelo reconhecimento do equipamento pelo concentrador, e outro é conhecido como infra-estrutura, que exigirá, ao menos, a figura de um servidor de autenticação (RADIUS), portanto um equipamento adicional. Poderá, ainda, necessitar de uma infra-estrutura de chaves públicas (ICP), caso utilize certificados digitais para promover a autenticação do usuário (RUFINO, 2005).

Segundo (GUIMARÃES, 2001), a criptografia computacional como se conhece protege o sistema quanto a ameaça de perda de confiabilidade, integridade , é utilizada para garantir:

- Sigilo : Somente os usuários autorizados tem acesso à informação;
- Integridade : Garantia que o usuário tem de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente;
- Autenticação do usuário : Processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que se alega ser;
- Autenticação do remetente: Processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem;
- Autenticação do destinatário : Consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário;
- Autenticação de atualidade : Consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas;

4.4.1 WEP

O protocolo WEP foi criado para fornecer uma segurança no inicio das redes sem fio. Hoje ele é o mais disseminado e está presente em todos os equipamentos de padrão *wireless*.

Segundo Rufino (2005), esse protocolo utiliza-se de algoritmos simétricos, ou seja, existe uma chave que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens transmitidas nessa rede *wireless*.

> Esse protocolo trabalha na camada de enlace de dados e se baseia método criptográfico RC4 (*Route Coloniale* 4) da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado com a *secret shared key* para formar uma chave de 64 ou 128 bits que é usada para fazer a criptografia. O WEP utiliza o CRC-32 (*Cyclic Redundancy Check*) que serve para calcular o *checksum* da mensagem, que é incluso nos pacotes, visando à segurança dos dados. O receptor ao analisar o pacote recalcula o *checksum* para garantir que as mensagens não foram alteradas no seu percurso (GIMENES, 2005).

Apesar de o WEP ser bastante utilizado para tornar a comunicação de uma rede sem fio mais segura, muitas falhas são apontadas. Uma das vulnerabilidades desse protocolo está associada à reutilização do vetor de inicialização (IV).

> Outra vulnerabilidade do WEP está relacionada ao CRC-32. Como seu algoritmo de garantia de integridade é linear, possibilita que modificações sejam feitas no pacote sem que sejam detectadas. Uma das grandes fraquezas do WEP é a falta de gerenciamento de chaves, pois o padrão WEP não especifica como deve ser a distribuição das chaves (ANDRADE et al, 2003).

4.4.2 WPA

Aguiar (2005) afirma devido a alguns problemas de segurança do protocolo WEP, o WPA surgiu de uma aliança ente a *Wi-fi Alliance,* e o IEEE, para fornecer um tratamento melhor na segurança do WEP, e o mesmo é totalmente compatível com os *hardwares* que rodam WEP. Sendo assim a atualização do WEP para o WPA tem que ser feita através de atualização do *firmware* dos dispositivos sem fio, sem a necessidade de alteração da infra-estrutura de *hardware* .

> Também atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP) utilizando para isso, padrões 802.1x e EAP (RUFINO, 2005).

No WPA possui o protocolo TKIP, que é responsável pela troca dinâmica das chaves, sendo que no WEP as chaves são estáticas e possuía seu IV de apenas 24 bits e esse protocolo trabalha com 48 bits (GIMENES, 2005).

> Neste protocolo se utiliza uma chave base de 128 bits denominada TK , que é combinada com o endereço MAC do transmissor, criando uma chave chamada TTAK (*Temporal and Tramsmitter Adres Key*), que é combinada com o IV do RC4 criando chaves diferentes para cada pacote transmitido (AGUIAR, 2005).

O Mesmo autor afirma que o TKIP fornece uma chave diferente para cada estação da rede para se comunicar com o concentrador, quando a chave é gerada com o endereço MAC das estações. esse protocolo TKIP pode também ser programado para alterar o IV para cada pacote, podendo ser definido por sessão ou por período, dificultando assim a obtenção que trafegam nessa rede.

4.4.2.1 EAP

Segundo PANZUTO (2008) EAP é um protocolo de segurança da camada 2 (camada do endereço MAC) que existe no estágio de autenticação do processo de segurança, e junto com as outras medidas de segurança discutidas até aqui, fornece uma terceira camada de segurança para a rede sem fio. Usando o 802.1x, quando um dispositivo solicita a um AP, os seguintes passos ocorrem no EAP:

- O ponto de acesso exige informações de autenticação do cliente.
- O usuário fornece então a informação solicitada de autenticação.
- O AP encaminha então a informação de autenticação fornecida pelo cliente para um servidor padrão RADIUS para autenticação e autorização.
- Após a autorização do servidor RADIUS, o cliente é permitido conectar-se a transmitir dados.

4.4.3 WPA2 ou 802.11i

Para Aguiar (2005) protocolo foi ratificado pelo IEEE em 2004, tratando de um produto disponível por meio da *Wi-fi Alliance.* A diferença entre o WPA2 e o WPA e sua criptografia utilizada. O WPA utiliza o TKIP com o RC4, já o WPA2 utiliza o AES (*Advanced Encryption Standard*) em conjunto com o TKIP com chave de 256 bits, que é um método de criptografia muito mais poderoso. O AES permite a utilização de chaves de 128, 192 e 256 bits, que constituem assim uma ferramenta poderosa de criptografia. A chave de 256 bits no WPA2 é padrão. A utilização do AES necessita de um novo *hardware*, que seja capaz de realizar o processo criptográfico, pois em dispositivos mais recentes é necessário possuir um co-processador para realizar os cálculos da criptografia

4.5 Segurança

> Com a flexibilidade e mobilidade oferecida aos usuários de rede sem fio, um fator fundamental é a implementação de uma segurança da informação. A utilização de estratégias de segurança eficaz e imprescindível, pois há a necessidade de diminuir os riscos de acessos por pessoas indevidas a essa rede. Para conseguir um nível de segurança é preciso implementar controles externos aos equipamentos, como configurações adequadas, criptografia, autenticação e monitoramento dos acessos à rede sem fio. (PANZUTO, 2008).

4.5.1 Firewall

Para Andrade (2003) O *firewall* é um servidor de Proxy que filtra todo o tráfego que passa por ele, através da rede, nos dois sentidos, com base nas regras de sua configuração. O *firewall* pode estar localizado no *gateway* entre os pontos de acesso da rede sem fio com a rede com fio. Assim, o firewall isola as duas redes, com fio e sem fio, evitando assim que pessoas não autorizadas que consigam acesso a uma rede tenham acesso à outra. Um *firewall* localizado no *gateway* protege a rede de invasores externos, porém não protege dos invasores que estão no mesmo lado da rede, pois os nós não são isolados uns dos outros. Um invasor pode ter acesso aos arquivos que estão na mesma rede e ler os arquivos que estão compartilhados.

4.5.2 Métodos de Autenticação

O método de autenticação do padrão IEEE 802.1X (Figura 3) são componentes importantes para aumentar o nível de segurança da rede sem fio. O servidor RADIUS é um componente muito utilizado para fazer autenticação.

Aguiar (2005) ressalta que em um processo de autenticação 802.1x existem 3 participantes:

- O Suplicante: usuário
- Servidor de autenticação: sistema de autenticação RADIUS, que realizará a autenticação do usuário cadastrado.
- Autenticador: mediador na transação entre o suplicante e o servidor de autenticação. Geralmente é o AP.

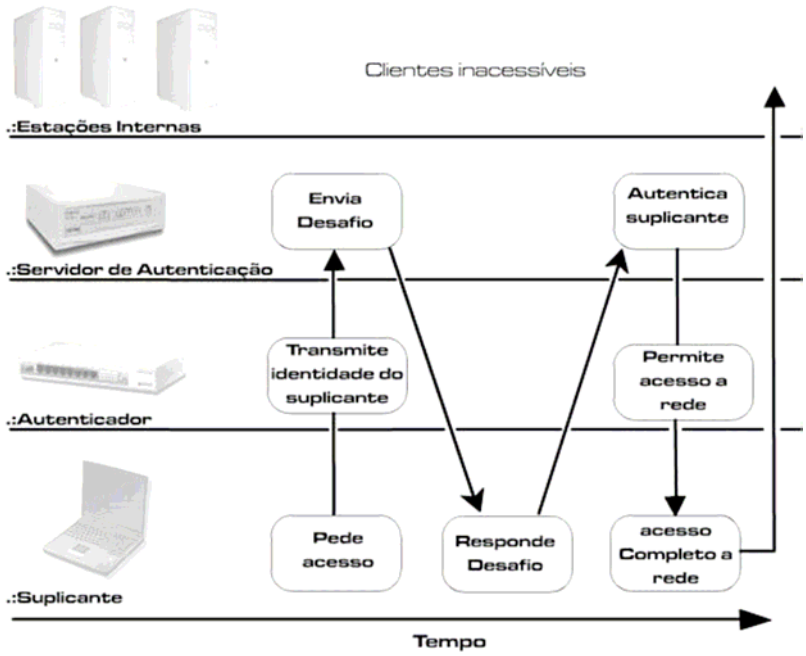

Figura 3 - Simulação de acesso a rede sem fio

Fonte: GIMENES (2005)

Gimenes (2005) ressalta que na Figura 3, o suplicante pede o acesso para o autenticador o qual transmite uma identidade do suplicante para o servidor de autenticação, que por sua vez inicia um desafio para o suplicante. Ao responder o desafio o servidor autentica o usuário para que o autenticador libere o acesso a rede .

4.5.3 Senhas Descartáveis (OTP)

Segundo Rufino (2005) Uma das soluções mais simples e de fácil implementação é o uso de senhas descartáveis (*OTP)*. A intenção é permitir que o usuário informe uma senha diferente a cada acesso, tornando inócua a captura da senha pela rede, já que para um novo acesso será necessário informar um senha diferente da atual.

4.5.4 Certificação Digital

Aguiar (2005) afirma que os certificados digitais associam a identidade de alguém a um par de chaves eletrônicas (privadas e públicas) que, usadas em conjunto, fornecem a comprovação da identidade desta pessoa. É uma versão eletrônica (digital) de uma Carteira de Identidade.

Estes certificados são os métodos mais seguros, principalmente quando armazenados em dispositivos processados como *tokens* ou cartões. Que segundo Aguiar (2005) um certificado digital contém três elementos:

- Informação de atributo: informação sobre o objeto que é certificado se for uma pessoa o seu nome, nacionalidade, etc.
- Chave de informação pública: essa é a chave pública na Autoridade Certificadora. O certificado atua para associar a chave pública a informação de atributo.
- Assinatura da Autoridade Certificadora: a Autoridade assina os dois primeiros elementos, validando-os.

4.5.5 Tokens e Smartcards

Tokens e *Smartcards* são dispositivos físicos utilizados para armazenar informações como chaves privadas e senhas, na tentativa de impedir uma possível captura dessas informações na rede (AGUIAR, 2005).

O *token*, pequeno dispositivo, do tamanho de um chaveiro, utilizado para armazenar identificação digital e dados para a autenticação, para acessar tais informações é necessário conectar o *token* a uma porta USB, do computador ou do dispositivo (AGUIAR, 2005).

O *Smartcard* (Figura 4) é um dispositivo portátil (cartão) que possui uma CPU, uma porta I/O e memória não volátil que só pode ser acessada pela CPU do cartão. Este dispositivo fornece um nível alto de segurança (AGUIAR, 2005).

Figura 4 – Smartcard
Fonte: WIKIMEDIA (2207)

4.5.6 Detecção de ataques e monitoramento

> Nenhuma ação de segurança é mais importante que o correto monitoramento do ambiente. Quaisquer que sejam os métodos de proteção utilizados, este não são infalíveis, mesmo os mais robustos. Na verdade, o monitoramento também pode falhar em algum momento e, ao se escolher para onde devem ir os investimentos em segurança, certamente recursos de monitoramento devem ter prioridade, pois irão detectar os pontos de falha e poderão explicar como um determinado ataque, bem-sucedido não, ocorreu (RUFINO, 2005).

4.5.7 Segurança Fisica

Rufino (2005) ressalta que aspectos antes irrelevantes, como posicionamento dos equipamentos de rede, agora devem ser cuidadosamente estudados, sob o risco de comprometer o bom funcionamento da rede e, principalmente, facilitar o acesso indevido de pessoas não autorizadas e outros tipos de ataques.

> Um item que deve ter uma maior atenção É verificar o padrão utilizado e a potência dos equipamentos, pois o padrão 802.11a atinge uma distância menor que o 802.11b ou 802.11g. As maiorias dos concentradores possibilitam selecionar valores intermediários de potência, no caso de o administrador achar necessário poderá receber sinal a distância não prevista pelo teste de propagação do sinal (GIMENES, 2005).

4.6 Vulnerabilidade

De acordo com (SÊMOLA, 2003), o conceito de vulnerabilidade é definido por fraqueza, fragilidade ou deficiência de um ativo, podendo assim ser explorado por uma ameaça, ou até permitindo que a ameaça ocorra, por se expor, afetando um ou mais princípios efetivos de segurança da informação, conforme Figura 5.

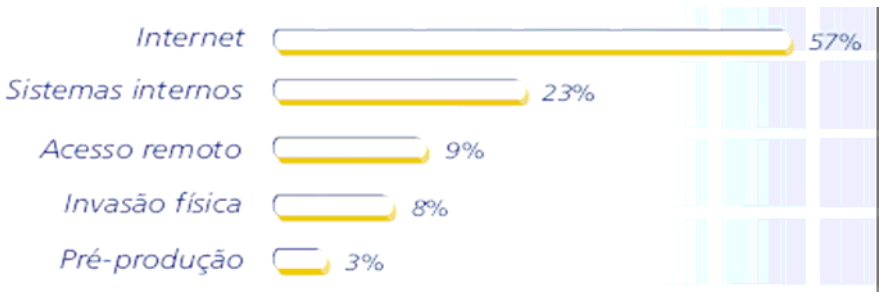

Figura 5 – Pontos de Invasão
Fonte: PITTIGLIANI & AGUIAR (2008)

4.6.1 Mapeamento do ambiente

> Umas das primeiras ações realizadas pelos atacantes é, sem dúvida, promover um mapeamento do ambiente. Esse procedimento possibilita obter o maior número de informações sobre uma determinada rede, permitindo conhecer detalhes que lhe permitam ataques de forma mais precisa e com menos riscos de ser identificado. Tal ação pode ter maior ou menor grau de êxito, dependendo dos mecanismos de proteção existentes na rede-alvo (RUFINO,2005)

4.7 Ferramentas e técnicas de ataque

Segundo Rufino (2005), a maioria dos ataques para redes sem fio podem ser efetuados utilizando ferramentas específicas, porém todo arsenal acumulado e já disponível para redes convencionais não pode ser desprezado, sob pena de conceder vantagem significativa a um possível atacante.

4.7.1 WarChalking

Para Panzuto (2008), WarChalking (Figura 6) é uma prática oriunda da intenção de dizer aos companheiros onde podem obter uma conexão sem fio gratuita em uma rede corporativa ou privada, e através de símbolos indicam se o ponto de acesso sem fio é considerado “aberto” ou “fechado”, indicado tanto por dois semicírculos de costas um para o outro, ou por um círculo comum, respectivamente, e qual o tipo de segurança protege o ponto de acesso.

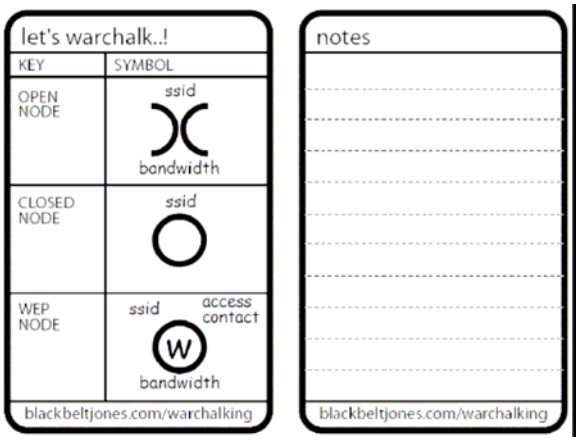

Figura 6 - Exemplo de *Warchalking*

Fonte: DUARTE (2003)

4.7.2 WarDriving

> WarDriving simplifica o encontro de redes sem fio abertas e aumenta dramática e exponencialmente a área de busca. O ato de WarDriving é simples: você apenas dirige por aí buscando por redes sem fio. Parte do apelo é que você agora pode usar sistemas GPS conectados ao seu laptop, que por sua vez é energizado pelo seu carro. Isso torna o ato de WarDriving preciso e potencialmente compensadora para os que buscam a sua rede sem fio, porque eles podem cobrir uma área muito maior com veículo (PANZUTO, 2008).

4.7.3 WarFlying

> WarFlying (i.e.WarStorming) é apenas a busca de redes sem fio enquanto se voa de planador. Entretanto, já que não há muitas pessoas que possuem acesso a um planador e as ferramentas necessárias para se executar o WarFlying, as ocorrências de WarFlying serão menores dos que as do WarDriving (PANZUTO, 2008).

4.7.4 Access Point Spoofing (Associação Maliciosa)

Essa associação maliciosa é quando o atacante se passa por um *Access Point,* iludindo outro sistema de maneira que acreditem que estão conectados a uma WLAN real (DUARTE, 2003).

4.7.5 MAC Spoofing

É quando o atacante se apodera de um endereço MAC de um cliente da rede, e utiliza-se disto para poder participar da mesma rede, sabendo que esses equipamentos sem fio têm a possibilidade da troca do endereço físico (PANZUTO, 2008)

4.7.6 ARP Poisoning

Para Duarte (2003) este é um ataque de camada de enlace de dados que somente pode ser disparado quando o atacante já está conectado na mesma rede local da vítima. Este ataque pode ser disparado de uma estação da WLAN à uma estação guiada, sendo assim, o ataque não fica restrito apenas às estações sem fio.

4.7.7 2.8.7 Airtraf

Aitraf (figura 7) permite coletar uma vasta quantidade de informações sobre as redes identificadas, tais como clientes conectados, serviços utilizados e várias totalizações, tudo em tempo real (RUFINO, 2005).

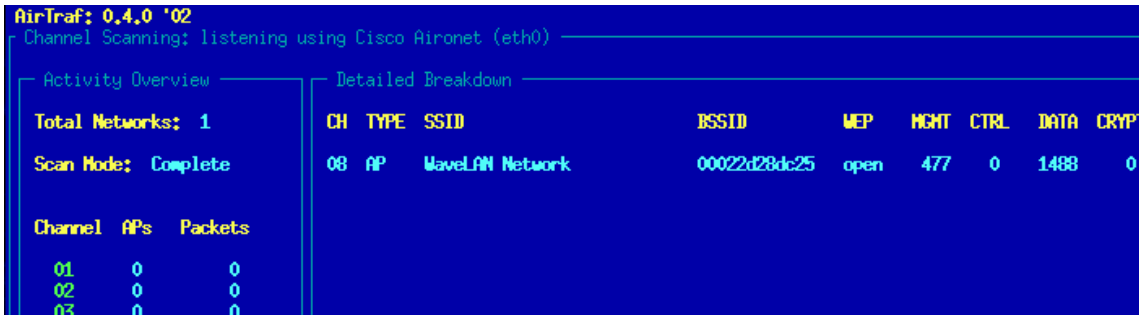

Figura 7 - Ferramenta Airtraf fazendo varredura

Fonte: AIRTRAF (2002).

4.7.8 Airsnort

Segundo autor acima com algumas limitações em termos de quantidades de placas e *chipsets* diretamente suportados (Orinoco/Proxim, Prims2 e, mais recentemente, Atheros), essa popularidade talvez seja, em parte, explicada por conta desses padrões de placas. Uma vantagem desta ferramenta em relação às demais é que mesmo que um padrão de placa não seja suportado diretamente, é possível colocá-la manualmente em modo monitor e escolher o item **Other** na opção **Driver Type.**

4.7.9 Netsumbler

Uma das primeiras ferramentas disponíveis para mapeamento e identificação de redes sem fio em ambiente, o *Netsumbler* (Figura 8) possui algumas características úteis, como permitir integração com equipamentos GPS.

Por meio dela é possível identificar as redes, seus nomes, endereços MAC e outras informações, tais como nível de sinal de propagação de cada rede detectada (RUFINO, 2005).

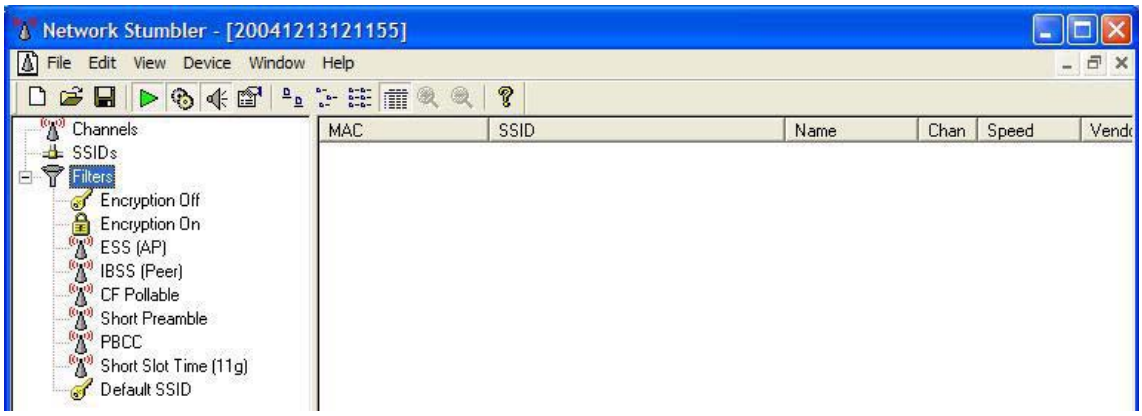

Figura 8 - Ferramenta Netstumbler

Fonte: NETSTUMBLER (2008)

4.7.10 Airjack

Trata-se de outra ferramenta disponível para fazer passar por um concentrador e, com isso, obter informações dos clientes que venham a se conectar a ele. A maior parte das funcionalidades presentes no *Airjack* estão presentes nos cartões que este suporta (Prism2 e Orinoco), como a capacidade de operar em modo infra-estrutura, tal qual um concentrador (RUFINO, 2005).

4.7.11 AirSnarf

As operadoras de telefonia e empresas privadas estão passando a oferecer possibilidades de conexão em locais públicos em vários pontos do país. Essa facilidade de acesso tem atraído muitos clientes e a tendência é que a adesão à serviços desse tipo aumente rapidamente. Porém, existem algumas vulnerabilidades associadas a esses serviços, como a possibilidade de montagem de um falso concentrador emlocais muito movimentados e coletar nomes e senhas dos usuários que tentarem utilizar esse serviço(RUFINO, 2005).

4.7.12 Kismet

Esta ferramenta possui uma atualização constante em suas funcionalidades. O Kismet (Figura 9) pode ser utilizado para o mapeamento de redes, captura de tráfego e localização por GPS. Toda análise do Kismet pode ser armazenada em arquivo ou visto em tempo real (KISMET, 2007).

Essa ferramenta não apresenta quebra de chave WEP.

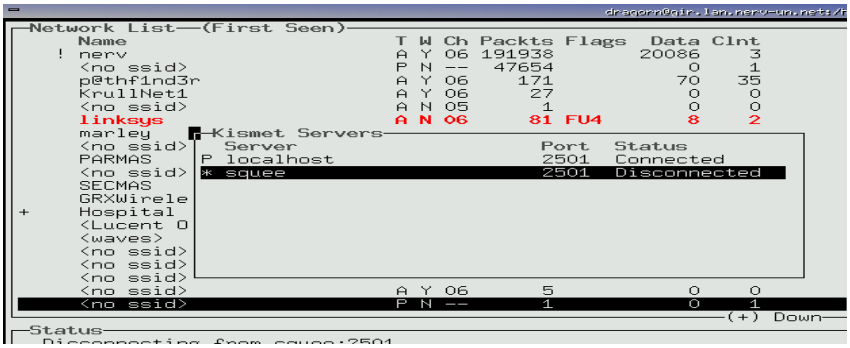

Figura 9 - Kismet capturando redes

Fonte: KISMET (2007)

4.7.13 Ferramentas para quebra de chaves WEP

Algumas ferramentas oferecem grandes recursos para quebra dessa chave, utilizando-se também de combinação de força bruta e ataques de dicionário, mas algumas podem ser destacadas como a *Airsnort, WepCrack, WepAttack, AirCrack* (PANZUTO, 2008).

5 ANTENAS

Segundo Silva (2006) as antenas podem ser definidas como um dispositivo com a capacidade de radiar e receber ondas eletromagnéticas. Essa característica de radiação difere-se a cada tipo de antena, pois dependem da forma física e dos materiais utilizados em sua construção, fatores fundamentais na distribuição dos campos elétricos e magnéticos.

> Todos os pontos de acesso e placas sem fio têm antenas que são embutidas ou que são conectados a uma tomada especial para antena. Entretanto, determinado o tamanho desses dispositivos, particularmente as diminutas placas sem fio, há um limite quanto ao alcance que essas antenas fornecem (ENGST , FLEISHMAN, 2005).

5.1 Conceituando antenas

Segundo Gomes (1985), antenas consistem de um dispositivo equipado de condutores, geralmente dispostos em pares, sendo alimentados por uma linha de transmissão, denominada de dipolos, que é a capacidade de produzir ondas eletromagnéticas no espaço livre a partir de uma corrente elétrica variável no tempo, onde por sua vez gera um campo magnético variável no tempo induzindo assim a formação de um campo elétrico variável no tempo, conforme mostra a Figura 10.

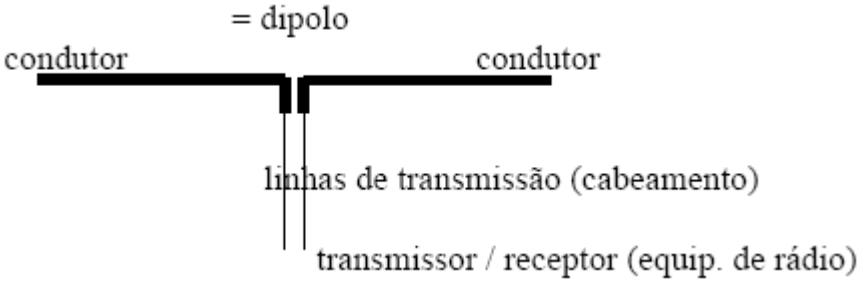

Figura 10 - Esboço de uma antena comum

Fonte: MAIA (2000)

As antenas possuem um sentido de “mão-dupla” onde é possível transmitir e receber ondas e a unidade de grandeza física (MAIA, 2000).

5.2 Características básicas das antenas

Segundo Maia (2000), algumas características que compreendem a construção e a aplicação das antenas buscando um melhor desempenho e seu comportamento satisfatório tanto para ambientes internos como externos, alguns parâmetros são dispostos:

- Diagramação de Irradiação
- Ângulo de Abertura
- Eficiência
- Diretividade
- Ganho
- Relação Frente-Costa
- Resistência a Irradiação
- Largura de Faixa
- Potencia Recebida
- Polarização
- Área Física x Área Utilizada
- Ruídos Incidentes nos Sistemas de Antenas RF

5.3 Antena Yagi-Uda

> A antena Yagi foi apresentada no Japão pelo engenheiro S.Uda, sendo introduzida no mundo ocidental pelo engenheiro H. Yagi, logo conhecida como Yagi-Uda. Este tipo de antena utiliza-se dos mesmo princípios do dipolo de meia-onda, e vários dipolos curtos, colocados em seqüência afim de dar direção e radiação desejada (MAIA, 2000).

Gomes (1985) afirma que esta antena foi chamada de antena radiante, pois seu conjunto de elementos paralelos em ordem, feito usualmente de alumínio, tubo ou aço inoxidável em forma de varetas, sendo que um ou mais destes elementos é condutor, e outros são parasitados. Estes elementos estão alinhados em algum plano podendo ser orientado horizontalmente, verticalmente ou inclinado.

5.4 Tipos de antenas

> Antenas na tecnologia *wireless* são de extrema importância, pois a mesma é a responsável pela velocidade e qualidade de transmissão dos dados. As antenas que por padrão são utilizadas nos pontos de acesso apresentam uma área de cobertura de 30 metros em espaços fechados onde existem paredes e outros obstáculos e em torno de 150 metros em áreas abertas, mas com o avanço tecnológico é possível utilizar-se de antenas mais sofisticadas para melhorar sua performance de transmissão de dados (MORIMOTO, 2008).

O Mesmo autor ainda ressalta que as antenas padrões dos pontos de acessos são chamadas de dipolo ou ominidirecionais pois sua irradiação (Figura 11) segue em todas as direções, permitindo a conexão em qualquer ponto em volta do ponto de acesso, ou seja, cobre uma área de 360º.

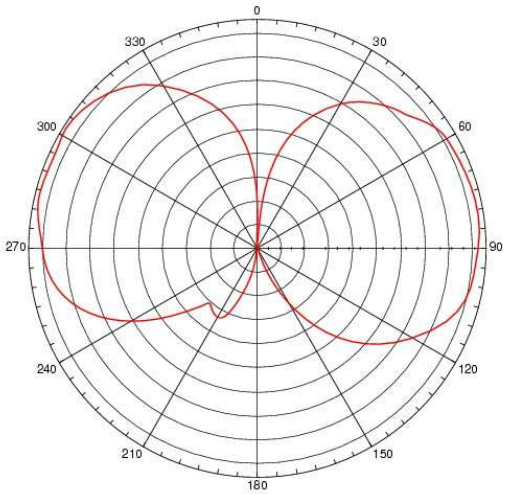

Figura 11 - Irradiação da antena Ominidirecional

Fonte: MORIMOTO (2008).

Segundo Morimoto (2008), a potência de uma antena é medida em dBi , sendo que uma antena que apresenta um ganho de 10 dBi é o que equivale a um aumento de 10 vezes a potência de um equipamento podendo exceder a área de cobertura padrão do ponto de acesso.

Antenas geralmente concentram sinais em determinadas direções, sendo assim quanto mais o sinal é concentrado maior é o ganho, de forma que quanto maior a antena maior é o ganho (MORIMOTO, 2008).

> O ganho da antena é medido em dBi, já a potência de transmissão é medida em dBm (*decibel milliwatt*). O padrão de comparação de potência de transmissão é de 1 *milliwatt* e corresponde a 0 dBm, que partindo disso cada vez é dobrada a potência do sinal, são somados aproximadamente 3 decibéis, já que dentro dessa escala apresenta um aumento de sinal duas vezes mais forte (MORIMOTO, 2008).

5.4.1 Antena Ominidirecional

Morimoto (2008) afirma que as antenas ominidirecionais (Figura 12) cobrem 360º no plano horizontal, são indicadas e com melhor performance em áreas bem amplas, ou aplicações multipontos, onde essa antena é utilizada de estação de base, com estações remotas ao seu redor. Uma desvantagem dessa antena é a exposição de ruídos na transmissão do sinal, pois uma vez que seu sinal cobre um grau de 360º dependendo da potência do equipamento pode colidir com sinais de outras bases transmissoras podendo afetar a performance do seu sinal como do sinal invadido.

Figura 12 - Antena omnidirecional
Fonte: HYPERLINK (2008)

5.4.2 Antenas Direcionais

Antena direcional tem a concentração do seu sinal em uma única direção. Esse sinal pode ter alcance curto e amplo ou longo e estreito. Quanto mais o sinal for estreito maior a distância alcançada (MORIMOTO, 2008).

5.4.3 Antena Parabólica

O autor acima ainda afirma que essa antena emite o sinal em forma de cone, é indicada para aplicações de longa distância. Seu modelo em *grid* (grelha), conforme mostra a figura 13, são menos suscetíveis a ação dos ventos em razão dos mesmos passarem pela sua estrutura, pois dessa forma evita que seu posicionamento seja alterado, tendo a necessidade de um novo ajuste. Seu sinal chega em torno de 40 a 50 km em condições visuais perfeitas.

Figura 13 - Antena parabólica

Fonte: HYPERLINK (2008).

5.4.4 Antena Setorial

Antenas setoriais (Figura 14) têm seu formato amplo e plano cobrindo um ângulo de 90º, são normalmente montadas em paredes podendo seu uso ser interno e externo. Esse tipo de antena é usada para interligação de prédios ou uma área de cobertura de no máximo 8km de distância dependendo do equipamento (MORIMOTO, 2008).

Figura 14 - Antena setorial

Fonte: HYPERLINK (2008).

5.4.5 Antena Yagi

Para Morimoto (2008) as antenas yagi (figura 15) possuem um melhor ganho de sinal, mas sua capacidade de cobertura é pequena, normalmente num raio de 24 x 30 graus, podendo ser mais estreito. Ela apresenta um ganho de 14 a 19 dBi bem superior as setoriais. Essas antenas são utilizadas para cobrir algumas áreas especificas que estejam muito distantes do ponto de acesso ou utilizadas para conectar redes distantes, tendo à necessidade de ambas as antenas estarem apontadas exatamente uma para a outra, podendo fechar links de até 25 km e que representa 150 vezes seu alcance inicial .

Figura 15 - Antena Yagi
Fonte: HYPERLINK (2008)

5.5 Usos de antenas

Segundo (ENGST & FLEISHMAN, 2005) adicionando uma antena externa a um dispositivo de rede sem fio, você pode estender o alcance do dispositivo de dezenas de metros para alguns ou até dezenas de quilômetros. Há duas principais razões por que é recomendável estender o alcance de sua rede.

6 METODOLOGIA

Como proposta para o presente estudo, inicialmente foi realizada uma pesquisa bibliográfica onde segundo Domingues; Heubel; Abel (2003) as pesquisas devem conter assuntos gerais e particulares podendo ser localizadas em diversas fontes de pesquisas como periódicos livros e materiais digitais .

Concluída a pesquisa, foi escolhido um local experimental para a busca dos sinais *wireless*.

Utilizando o sistema Kismet, as redes encontradas foram salvas em um arquivo com a extensão .dump. O arquivo foi inserido no programa AirCrack para analise das vulnerabilidades na segurança aplicada, em cima destas vulnerabilidades encontradas foram simulados ataques sem intuito de danificar a rede.

7 RESULTADOS E DISCUSSÃO

Perante aos estudos bibliográficos e testes realizados, os resultado encontrados no presente trabalho nos mostram as vulnerabilidades dos seguintes protocolos:

WEP

Como foi o primeiro protocolo criado apresenta muitas vulnerabilidades em sua segurança. 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. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (k,v).

Porém, como no 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 dá margem a ataques bem sucedidos e conseqüente descoberta de pacotes por eventuais intrusos.

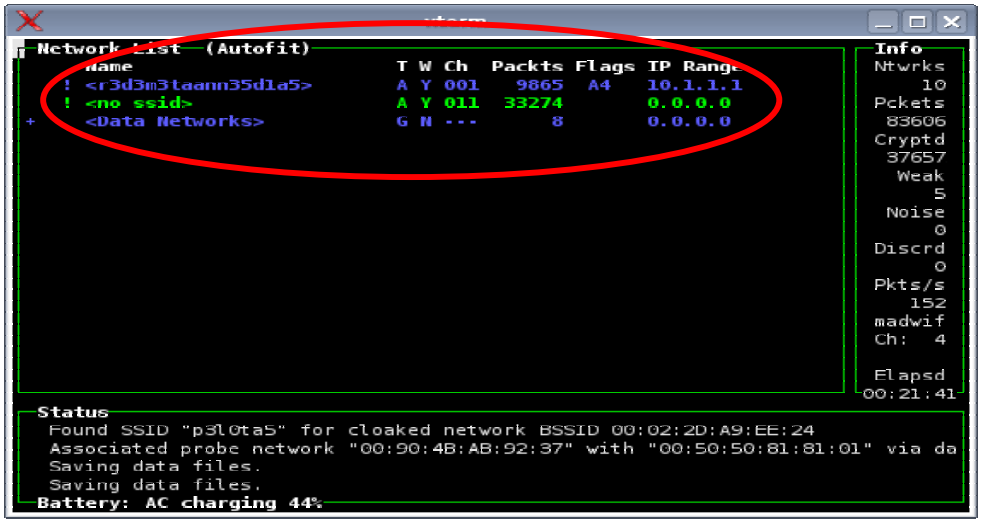

Figura 16 – Kismet em modo de monitoramento

Na Figura 16, podemos ver os testes realizados com o sistema Kismet, onde utiliza a placa de rede em modo de monitoramento .

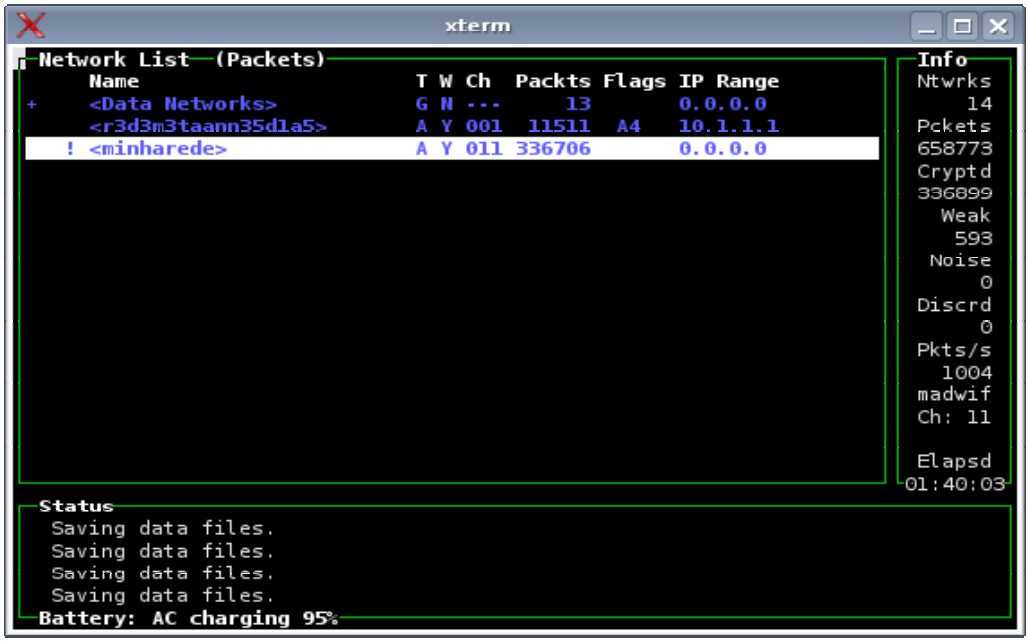

Figura 17 – Redes encontradas pelo Kismet

Na Figura 17, o Kismet nos mostra as redes encontradas no alcance da antena, neste caso foi selecionada a rede “minharede” para os testes. Depois de selecionada a rede , os dados da mesma foram salvos em um arquivo .dump.

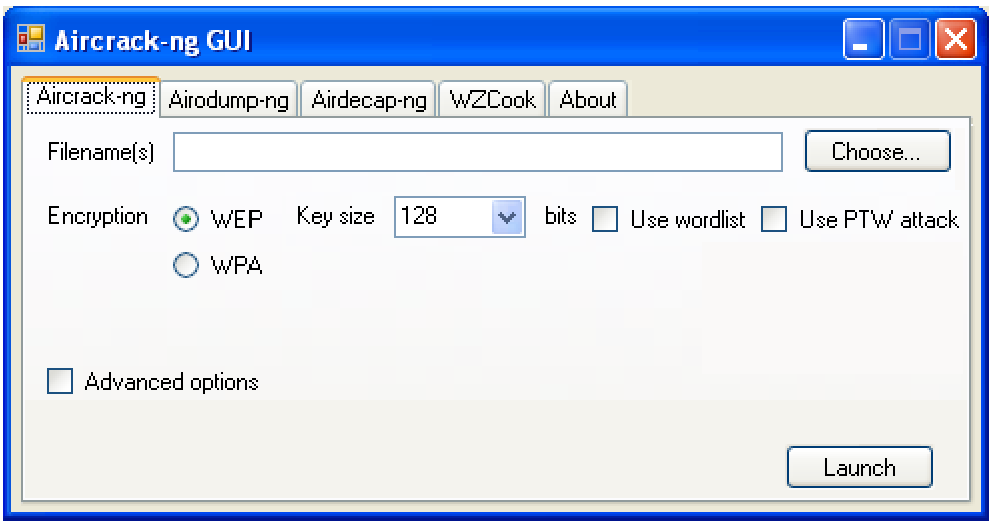

Figura 18 - Inserção do arquivo .dump no Aircrack

O Arquivo .dump foi inserido no Aircrack (Figura 18), para que os dados extraídos da rede “minharede” fossem analisados.

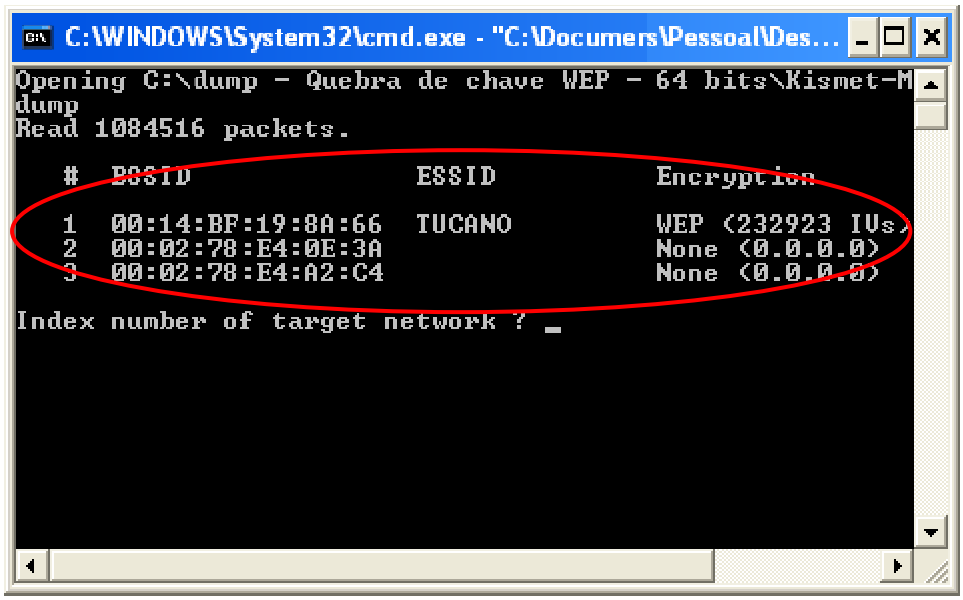

Figura 19 – AirCrack analisando a rede

A Figura 19 nos mostra os dados sendo analisados pelo Aircrack, que detectou os MAC´s da rede, ESSID, e o tipo de protocolo utilizado na segurança, neste caso o protocolo WEP.

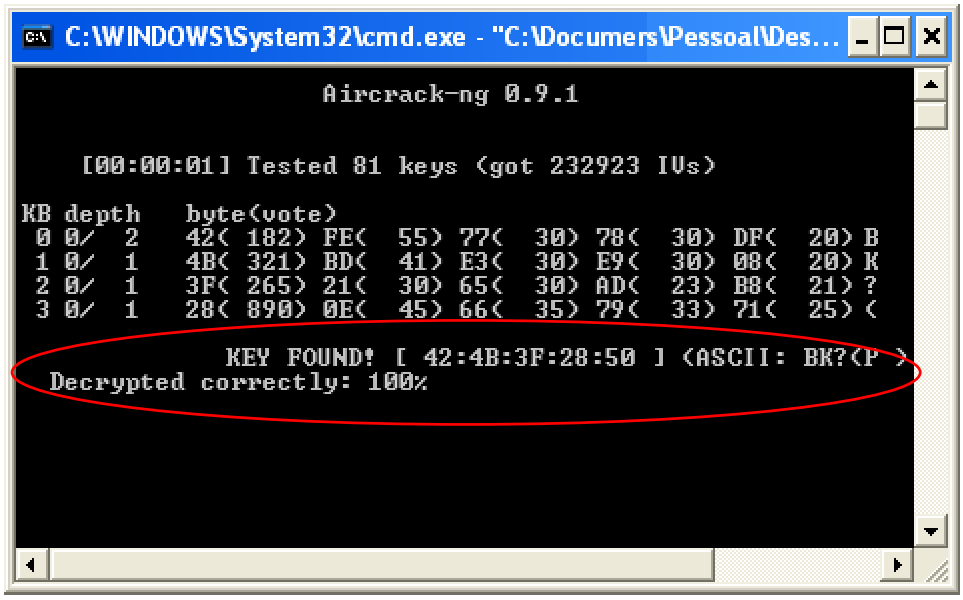

Figura 20 – Chave descriptografada

A Figura 19 nos mostra as chaves de criptografia encontradas, através do trafego de pacotes da rede.

WPA

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, 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.

A chave de criptografia dinâmica é uma das principais diferenças do WPA em relação ao WEP, que utiliza a mesma chave repetidamente. Esta característica do WPA também é conveniente porque não exige que se digite manualmente as chaves de criptografia ao contrário do WEP.

Por utilizar uma criptografia dinâmica, nos testes realizados não foi possível a quebra da criptografia WPA e invasão.

WPA2

Em sua Criptografia utiliza o AES (Advanced Encryptation Standart) junto com o TKIP com chave de 256 bits, um método mais poderoso que o WPA que 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, uma ferramenta muito poderosa de criptografia. Diante dessa tecnologia de segurança, nos testes não foram possíveis quebras das chaves criptografadas.

8 CONSIDERAÇÕES FINAIS

Neste capítulo, foram analisadas as vulnerabilidades inerentes as redes sem fio. Mostrando como estas vulnerabilidades podem ser exploradas e como um eventual atacante pode se valer destas para comprometer o sistema alvo.

Foi mostrado também testes realizados em um ambiente experimental montado para a validação de algumas das vulnerabilidades através de ferramentas desenvolvidas para invasão de redes sem fio, ferramentas que estão disponíveis na Internet e são de domínio público.

Como visto neste trabalho, as vulnerabilidades presentes nas redes sem fio podem causar prejuízos a corporações ou pessoas. Por isso, medidas para minimizar as vulnerabilidades, devem ser desenvolvidas e seguidas para que perdas com eventuais ataques sejam diminutas.

É de grande valia, um moderado, continuado e atualizado estudo sobre as redes *wireless*, uma vez que, diariamente, novas vulnerabilidades internas e ameaças externas vêm conturbar o fantástico mundo *wireless.*

REFERÊNCIAS

AGUIAR, P.A. F. **Segurança em Redes WI-FI.** Montes Claros, MG. Universidade Estadual de Montes Claros, 2005, 79p. Monografia defendida para obtenção do grau de Bacharel em Sistemas de Informação.

AIRTRAF. **Documentation.** 2002. Disponível em: http://airtraf.sourceforge.net. Acessado em: 20/03/2008.

ANDRADE et al, L. D. **Análise das vulnerabilidades de segurança existentes nas redes sem fio: Um estudo de caso projeto WLACA.** Disponível na Internet: http://www.cci.unama.br/margalho/artigos/wlaca.pdf. Acessado em: 09/05/2009

DOMINGUES, M.; HEUBEL, M.T.C.D.; ABEL, I.J.; **Base metodológica para o trabalho científico para alunos iniciantes.** Bauru, SP:Edusc, 2003. 188p.

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, 58p.

GOMES, A.T. **Telecomunicações: transmissão e recepção AM - FM: Sistemas pulsados**. Ed. Érica, 2ª ed. São Paulo, 1985.

GUIMARÃES. C. R. **Criptografia para Segurança de Dados.** Uberlândia, MG. Centro Universitário do Triângulo, 2001, 31p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

HYPERLINK. **Antenas.** 2008. Disponível em: http://www.hyperlinktech.com/category.aspx?id=73. Acessado em 21/04/2008.

KISMET. **Documentation.** 2007. Disponível na Internet: http://www.kismetwireless.net/ . Acessado em: 01/05/2009.

MAIA, W.L.G. **Um estudo de Viabilidade de Links de Rádio Freqüência para Integração de Redes de Computadores na UFACNet e Região do Acre.** Florianópolis, SC. Universidade Federal de Santa Catarina, 2000, 191p. Dissertação de Mestrado para a obtenção do grau de Mestre em Ciência da Computação.

MATHIAS, A.P.; **IEEE 802.11 – Redes Sem Fio.** Disponível na Internet. www.gta.ufrj.br/grad/00_2/ieee/ . 01/05/2009.

MORIMOTO, C.E. **Redes Wireless.** 06 de fevereiro de 2008. Disponível em: http://www.guiadohardware.net/tutoriais/alcance-antenas-conectores-potencia/. Acessado em: 17/04/2008.

NETSTUMBLER. **Documentation.** 2008. Disponível em: http://www.netstumbler.org/. Acessado em : 30/04/2008.

PANZUTO, P. S. **Criação de uma Antena Tipo Yagi-Uda para Análise de Sinal *Wireless:* Um *hardware* para rotacionamento em 360º utilizando microcontrolador PIC16F84A para análise de *software* de captura de sinais *wireless e cálculo de alcance utilizando a fórmula matemática de Fresnel.*** Bauru, SP. Universidade do Sagrado Coração, 2008. Monografia defendida para obtenção do grau Bacharel em Ciência da Computação.

PITTIGLIANI, C . C; AGUIAR, F.C FLEXSECURITY: **Um Framework para segurança da informação.** Tubarão, SC. Universidade do Sul de Santa Catarina, 2007, 121p. Monografia defendida para obtenção do grau Tecnólogo em Redes de Computadores.

RUFINO, N.M.O. **Segurança em Redes sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**.** São Paulo: Novatec, 2005. 224p.

SÊMOLA, Marcos, **Gestão da Segurança da informação**: Aplicada ao Security Officer / Marcos Sêmola / Módulo Security Solutions S. A., Rio de Janeiro, Editora Elsevier / Editora Campos, 2003; Trabalho de Conclusão do Curso de Tecnólogo em Informática com ênfase em Gestão de Negócios.

WIKIMEDIA. **SmartCard.** 2007. Disponível em : http://upload.wikimedia.org/wikipedia/commons/0/05/Smartcard_CAM.jpg. Acessado em : 09/05/2009