Análise de Segurança em Redes Wireless 802.11x

Pablo de Souza Lacerda

Juiz de Fora, MG
Julho de 2007

Análise de Segurança em Redes Wireless 802.11x

Pablo de Souza Lacerda

Monografia submetida ao corpo docente do Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora, como parte integrante dos requisitos necessários para a obtenção do grau de Bacharel em Ciência da Computação.

Aprovada pela banca constituída pelos seguintes professores:

_____

Prof. Marcelo Lobosco – orientador
Doutor em Eng. Sist. e Comp., UFRJ

_____

Prof. Marcos Ribeiro Quinet de Andrade
Mestre em Ciência da Computação, UFF

_____

Prof. Eduardo Pagani Julio
Especialista em Redes de Computadores, CESJF

Juiz de Fora, MG
Julho de 2007

Resumo

A cada dia as redes sem fio (*wireless networks*) se tornam mais populares, principalmente em virtude da praticidade e mobilidade propiciadas aos seus usuários. Entretanto, o meio não-guiado por onde as informações destas redes trafegam, usando ondas de rádio, é extremamente inseguro, uma vez que os dados estão suscetíveis à escuta e a ataques diversos. O objetivo deste projeto é fazer um estudo detalhado da tecnologia de redes sem fio 802.11, analisando principalmente as questões de segurança. Em particular, estudaremos possíveis fragilidades dos protocolos existentes e faremos um levantamento das ferramentas desenvolvidas especificamente para realizar ataques. Além disso, verificaremos se os mecanismos de defesa disponíveis apresentam soluções eficazes para a segurança das redes.

Palavras-chave: *wireless*, segurança, rede sem fio, 802.11x .

Sumário

1. Introdução.....09

1.1 Contextualização. 09

1.2 Motivação 10

1.3 Visão Geral da Monografia.....11

2. Fundamentos de redes sem fio 802.11 12

2.1 Introdução 12

2.2 Conceitos Básicos 12

2.2.1 Topologia de rede 13

2.3 Padrões atuais 15

2.3.1 Padrão 802.11b 15

2.3.2 Padrão 802.11a 15

2.3.3 Padrão 802.11g 16

2.3.4 Padrão 802.11i 16

2.3.5 Padrão 802.11n 16

2.4 Endereçamento MAC 17

2.5 Criptografia e autenticidade em redes sem fio 17

2.5.1 Wired Equivalent Privacy (WEP) 18

2.5.2 Wi-fi Protected Access (WPA) 18

2.5.2.1 Extensible Authentication Protocol 19

2.5.3 WPA2 ou 802.11i 20

2.6 Conclusão 21

3. Análise dos ataques e vulnerabilidades das redes sem fio 22

3.1 Introdução 22

3.2 Problemas de segurança física 22

3.3 Negação de serviço (*Denial of Service - DoS*).....23

3.4 Mapeamento do ambiente.....23

3.5 Configurações.....24

3.5.1 Configuração aberta.....24

3.5.2 Configuração fechada.....25

3.6 Vulnerabilidades nos protocolos WEP e WPA.....25

3.7 Técnicas e ferramentas de ataque.....25

3.7.1 Access Point Spoofing (Associação Maliciosa) 26
3.7.2 ARP Poisoning 26
3.7.3 MAC Spoofing 26
3.7.4 Wardriving 26
3.7.5 Warchalking 27
3.7.6 Ferramentas de Ataque 28
3.7.6.1 Airtraf 28
3.7.6.2 Netstumbler 29
3.7.6.3 Kismet.....29
3.7.6.4 AirJack.....30
3.7.6.5 Ferramentas para quebra de chaves WEP 31
3.8 Conclusão.....31
4. Estratégias de defesa 32
4.1 Considerações Iniciais 32
4.2 Configurações do concentrador.....32
4.3 Defesa dos equipamentos clientes.....33
4.4 Padrão 802.1x e RADIUS.....33
4.5 Virtual Private Network (VPN).....35
4.6 Firewalls.....36
4.7 Senhas descartáveis (*One-time Password* - OTP).....37
4.8 Certificados digitais.....37
4.9 Token e SmartCard.....38
4.10 Detecção de ataques e monitoramento.....39
4.10.1 wIDS.....39
4.10.2 Garuda.....40
4.10.3 Kismet.....40
4.10.4 Snort – Wireless.....40
4.10.5 Honeypots e Honeynets.....41
4.10.6 AirMagnet.....42
4.11 AirStrike.....44
4.12 Conclusão.....45
5. Conclusão 46
6. Referências Bibliográficas 48

Lista de Figuras

Figura 1 – Topologia de rede no modelo *Ad-Hoc* 14
Figura 2 – Topologia de rede no modelo infra-estrutura 14
Figura 3 – Visão geral sobre os padrões da tecnologia sem fio.....16
Figura 4 – Adicionando *hosts* para efetuar mapeamento.....24
Figura 5 – Exemplo de *Warchalking* 27
Figura 6 – *Airtraf* na tela de varredura.....28
Figura 7 – Visão geral da ferramenta Netstumbler.....29
Figura 8 – *Kismet* em ação.....30
Figura 9 - Simulação de acesso a uma rede sem fio.....34
Figura 10 – Exemplo de uma WLAN com VPN 36
Figura 11 - *Token* de Autenticação.....38
Figura 12 – Topologia do modelo de *wireless honeynet* 42
Figura 13 – Interface do *Airmagnet* 43
Figura 14 – Arquitetura de rede do *AirStrike* 45

Lista de Siglas e Abreviações

AP Access Point

AES Advanced Encryption Standard

BSS Basic Service Set

CRC-32 Cyclic Redundancy Check

D.o.S Denial Of Service

ESS Extended Service Set

ESSID Extended Service Set Identifier

EAP Extensible Authentication Protocol

EAP-LEAP Extensible Authentication Protocol - Lightweight Extensible Authentication Protocol

EAP-TLS Extensible Authentication Protocol - Transport Layer Security

GHz Gigahertz

GPS Global Position System

IAS Internal Authentication Server

IEEE Institute of Electrical and Electronic Engineers

IPSec Internet Protocol Security

IV Vetor de Inicialização

LAN Local Area Network

MAC Media Access Control

Mbps Megabits per second

PEAP Protected Extensible Authentication Protocol

RADIUS Remote Authentication Dial-In User Server

RC4 Route Coloniale 4

SSID Service Set Identifier

TKIP Temporal Key Integrity Protocol

VPN Virtual Private Network

WPA Wi-fi Protected Access

WPA-PSK Wi-Fi Protected Access - Pre-Shared Key

WPA-PSK.TKIP Wi-Fi Protected Access - Pre-Shared Key . Temporal Key Integrity Protocol

WEP Wired Equivalent Privacy

WLAN Wireless Local Area Network

Wi-fi Wireless-fidelity

1 – Introdução

1.1 – Contextualização

Redes sem fio (*wireless networks*) se tornam a cada dia mais populares, principalmente em virtude da praticidade e mobilidade propiciadas aos seus usuários. Nos últimos anos, verificou-se um expressivo aumento tanto no número de dispositivos portáteis com suporte a essa tecnologia quanto no alcance dessas redes. Inúmeros lugares, como salas de conferências, aeroportos e hotéis, oferecem como diferencial aos seus freqüentadores 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. Em ambientes corporativos estas redes são cada vez mais utilizadas como um auxiliar precioso para as LANs (*Local Area Networks*) convencionais, seja por prover vantagens econômicas, seja por prover mobilidade aos usuários e facilidade de instalação (DUARTE, 2003).

A primeira rede sem fio foi criada na Universidade do Havaí, em 1971, para conectar computadores nas quatro ilhas na qual localizavam-se seus *campi* 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 of Eletrical and Electronics 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 mesma a velocidade do 802.11a (ENGST & FLSIESHMAN, 2005).

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).

Inúmeras tecnologias enquadram-se na categoria de redes sem fio. O foco desta monografia será nos padrões 802.11x, conhecidos genericamente como *wi-fi* (abreviação de *wireless fidelity* – fidelidade sem fio, em associação com o termo de áudio *hi-fi*, que significa alta fidelidade de som) .

1.2 – Motivação

A tecnologia de redes sem fio ainda é uma novidade na vida da maioria das pessoas. Trata-se de uma tecnologia de rápida e fácil montagem e instalação, sem requerer conhecimento técnico específico por parte do instalador. Além disso, proporciona grande mobilidade e praticidade aos usuários.

Devido a estas vantagens, as redes de computadores sem fio possuem atualmente um papel muito importante na comunicação de dados. Entretanto, o meio não-guiado por onde as informações destas redes trafegam, usando ondas de rádio, é extremamente inseguro, uma vez que os dados estão suscetíveis à escuta e a ataques diversos (GRÉGIO, 2005).

Ataques às redes sem fio, além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais estas se interconectam. Um fator determinante da segurança em redes sem fio está relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque (DUARTE, 2003).

Estas redes tornaram-se um alvo fácil para pessoas mal intencionadas, desejosas em comprometer sistemas, pois disponibilizam inúmeros atrativos como dificuldade na identificação da origem exata do ataque, imaturidade das opções e protocolos de segurança para esse tipo de tecnologia, facilidade em obter acesso à rede guiada através de uma conexão de rede sem fio e principalmente a falta de conhecimento técnico da maioria dos usuários adeptos desta nova tecnologia (DUARTE, 2003).

Desta forma, as redes sem fio têm sido exaustivamente estudadas e muitos ataques foram desenvolvidos e/ou adaptados para poderem se valer das vulnerabilidades presentes

nestas redes. Além disso, elas apresentam falhas graves de segurança e problemas na implementação e conceituação do próprio padrão 802.11 (DUARTE, 2003). Estes problemas precisam ser solucionados para que não venham a impedir o crescimento vigoroso de sua utilização.

O objetivo deste projeto é fazer um estudo detalhado da tecnologia de redes sem fio 802.11, analisando principalmente as questões de segurança. Em particular, estudaremos as possíveis fragilidades dos protocolos existentes e faremos um levantamento das ferramentas desenvolvidas especificamente para realizar ataques. Além disso, verificaremos se os mecanismos de defesa disponíveis apresentam soluções eficazes para a segurança das redes.

1.3 – Visão Geral da Monografia

Este trabalho está dividido em cinco capítulos. O segundo descreve fundamentos e conceitos básicos das redes em estudo, permitindo uma visão geral dos principais conceitos e preparando o leitor para melhor compreensão dos próximos capítulos.

O terceiro mostra os riscos e vulnerabilidades a que as redes sem fio estão sujeitas. Além disso, descreve técnicas e algumas ferramentas de ataque.

O quarto analisa estratégias de segurança que devem ser aplicadas às redes *wi-fi*, tornando-as mais seguras e menos vulneráveis às inúmeras ferramentas de ataques disponíveis.

Por fim, o quinto faz uma conclusão de tudo que foi estudado e analisado neste trabalho.

2 – Fundamentos de redes sem fio 802.11

2.1 – Introdução

As redes *wireless* não requerem cabos para transmissão dos dados. Elas realizam sua transmissão através de ondas de rádio ou infravermelho, o que permite-as atingir sem muito esforço locais de difícil acesso para redes cabeadas. Todavia, tais redes estão mais suscetíveis a interferências causadas pelo meio externo, já que não possuem nenhuma proteção física no meio onde se propagam.

Existem vários padrões de tecnologia de redes sem fio, como por exemplo o *WiMax/802.16* (longo alcance, rápido) e o *Bluetooth* (curto alcance, lento e baixa potência); entretanto, a prioridade deste estudo será o padrão 802.11.

2.2 – Conceitos Básicos

As redes sem fio são compostas por dois tipos básicos de componentes: os adaptadores de redes, que são interfaces eletrônicas nos computadores dos clientes, e os A*ccess Points* (*APs*), também conhecidos por concentradores, que fornecem os serviços às estações associadas.

Os APs são dispositivos que fazem o gerenciamento da rede, podendo também atuar como uma ponte entre a rede sem fio e a rede guiada (DUARTE, 2003). Dentre as suas principais funções, destacam-se: a autenticação e a associação, que possibilita um dispositivo se manter conectado ao transitar entre áreas de cobertura diferentes. As estações fazem uma varredura para encontrar o AP com melhor qualidade de sinal e se associar a ele.

Um conceito muito utilizado é o de *WLANS* (*Wireless Local Area Networks*), que são as redes locais sem fio.

Basic Service Set (BSS) é um conjunto de estações controladas por um único *Access Point.* O conjunto de um ou mais BSSs interconectados e integrados a uma WLAN, parecendo um único BSS, é chamado de *Extended Service Set* (ESS). O ESS provê maior mobilidade para a rede, sendo que uma estação em movimento pode trocar de *AP* sem a necessidade de se reconectar no processo de troca. Segundo RUFFINO (2005), *Extended Service Set Identifier* (ESSID) é conhecido como o nome da rede. ESSID constitui-se de uma cadeia de caracteres alfanuméricos que deve ser conhecida tanto pelo concentrador como

pelos clientes que desejam conexão. Em geral, o concentrador envia sinais com ESSID, que é detectado pelos equipamentos na região de abrangência, fazendo com que estes enviem um pedido de conexão. Essas informações são conhecidas como *Beacon frames*, sinais enviados pelos concentradores para orientar os clientes.

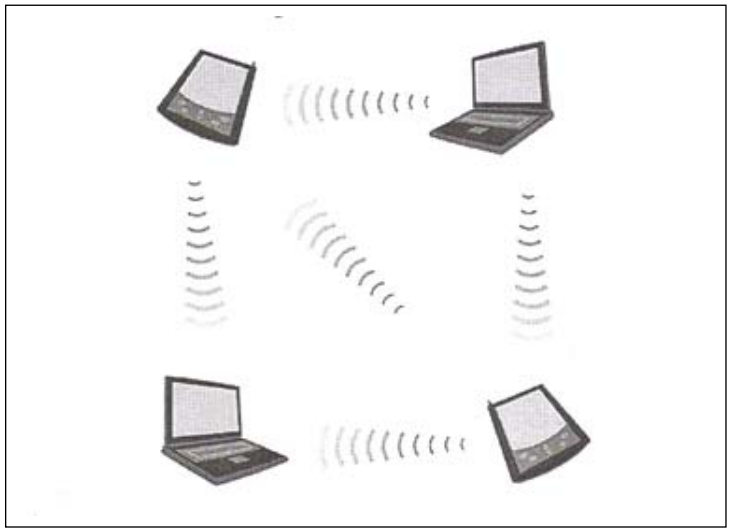
2.2.1 – Topologia de rede

Assim como as redes *Ethernet*, as redes *wi-fi* compartilham o mesmo meio entre todas as estações conectadas a um mesmo concentrador. Portanto, quanto maior o número de usuários, menor será a banda disponível para cada um deles. Essa mesma característica faz com que o tráfego fique visível para todas as interfaces participantes. Desta forma, de forma similar às redes cabeadas, uma estação pode capturar o tráfego não originado em si ou que lhe é destinado (RUFFINO, 2005).

Em termos de organização, o padrão 802.11 estabelece dois modos distintos de operação: *Ad-Hoc* e infra-estrutura.

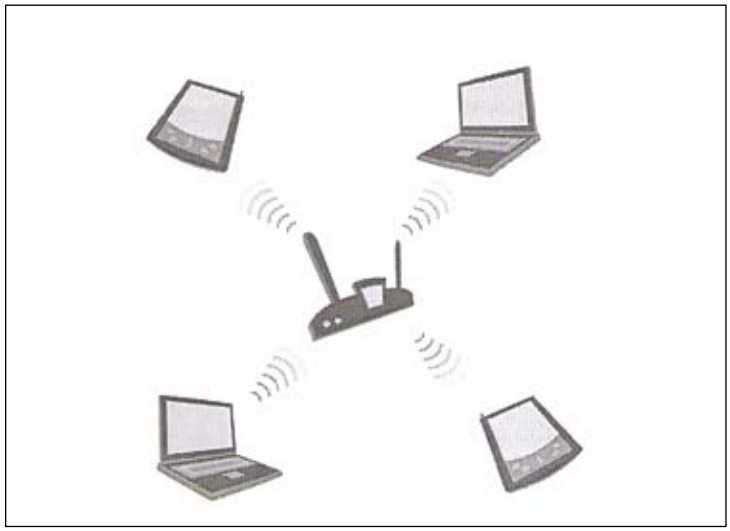
No modo *Ad-Hoc* (Figura 1) os computadores comunicam-se diretamente, sem o intermédio da estação base. Este modo pode ser mais adequado em pequenas redes ou na falta de um concentrador, mas deve-se ressaltar que a ausência do mesmo cria vários problemas de segurança e para a gerência da rede, como a escuta e captura de tráfego. Todavia, pode ser imprescindível para resolver questões rápidas, como por exemplo uma troca de arquivos em um aeroporto. No modo infra-estrutura (Figura 2) há a presença de uma estação base denominada concentrador de acesso, para onde toda a comunicação é dirigida, o que permite controlar todos os itens (autorização, autenticação, controle de banda, filtros de pacote, criptografia) em um único ponto.

Figura 1 – Topologia de rede no modelo *Ad-Hoc*



Fonte: RUFFINO (2005)

Figura 2 – Topologia de rede no modelo infra-estrutura



Fonte: RUFFINO (2005)

2.3 – Padrões atuais

O IEEE é uma associação profissional técnica sem fins lucrativos com cerca de 380 mil membros. Seu objetivo é desenvolver padrões técnicos consensuais nos campos das engenharias elétrica, eletrônica e de computação para uso das indústrias. Um dos seus grupos de trabalho foi denominado 802.11, que reúne uma série de especificações que basicamente definem como deve ser a comunicação entre dispositivos de uma rede sem fio (ENGST & FLSIESHMAN, 2005).

A seguir serão descritos alguns dos padrões 802.11, bem como as semelhanças e diferenças entre eles. A figura 3, no final desta seção, resume algumas destas características para os principais padrões.

2.3.1 – Padrão 802.11b

Entre 1999 a 2001, a principal especificação foi o 802.11b. Este padrão foi muito bem-sucedido, já que as empresas venderam milhões de dispositivos que o suportavam. Ainda é hoje o padrão mais popular e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis. Este padrão permite 11 Mbps (*Megabits per second*) de velocidade de transmissão máxima, porém seu *throughput* real é de 5 Mbps. Ele opera na freqüência de 2,4 GHz (*Gigahertz*) e permite um número máximo de 32 clientes conectados.

2.3.2 – Padrão 802.11a

O surgimento do 802.11a ocorreu em meados de 2002 e tem como principal característica o significativo aumento da velocidade para um máximo de 54 Mbps, mas seu *throughput* real é de 25 Mbps. Outra diferença é a operação na faixa de 5 GHz, uma faixa com poucos concorrentes, porém com menor área de alcance. Permite 64 clientes conectados (RUFFINO, 2005).

Uma excelente vantagem é que este padrão tem 12 canais não sobrepostos que permitem que mais pontos de acesso cubram o mesmo local físico sem interferência de um sobre o outro (ENGST & FLSIESHMAN, 2005).

Infelizmente, devido à utilização da banda de 5 GHz, o 802.11a não é compatível com a base instalada atual (802.11b), pois utilizam freqüências diferentes.

2.3.3 – Padrão 802.11g

O 802.11g opera em 54 Mbps, mas seu *throughput* real é de 20 Mbps. Utiliza as mesmas freqüências de rádio que o 802.11b, o que permite que equipamentos de ambos os padrões (b e g) coexistam no mesmo ambiente.

2.3.4 – Padrão 802.11i

Criado em 2004, este padrão define mecanismos de autenticação e privacidade e vários de seus aspectos podem ser implementados nos protocolos existentes. O padrão inclui o protocolo WPA (*Wi-fi Protected Access*), que foi projetado para fornecer soluções de segurança mais eficientes.

2.3.5 – Padrão 802.11n

Também conhecido como WwiSE (*Word Wide Spectrum Efficiency*), trata-se de um padrão em desenvolvimento cujo principal objetivo é o aumento da velocidade (cerca de 100 a 500 Mbps).

Figura 3 – Visão geral sobre os padrões da tecnologia sem fio.

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	2,4 Ghz	54 Mbps/ 20 Mbps	Sim	2003	Avançando em todos os lugares

Fonte: ENGST & FLSIESHMAN (2005)

2.4 – Endereçamento MAC

Todo dispositivo de rede possui um endereçamento físico, também conhecido por endereçamento MAC (*Media Access Control*). Trata-se de um número único com intuito de identificar de forma unívoca um equipamento em relação a qualquer outro fabricado mundialmente.

Segundo GIMENES (2005), pode-se configurar um concentrador mediante o cadastramento prévio dos endereços MAC dos dispositivos participantes. Esta configuração autentica apenas o equipamento e não o usuário, tornando possível que uma pessoa não autorizada a utilizar a rede a utilize por meio de um equipamento corretamente cadastrado. Além disso, neste método é necessário obter manualmente os endereços físicos e cadastrá-los manualmente no concentrador. Esse mecanismo exigirá sempre alguma manutenção, que será maior ou menor, de acordo com o fluxo de usuários e interfaces que entram e saem do cadastro, porém não deixa de ser uma boa solução para pequenas redes e ambientes com poucas mudanças.

Existem técnicas e ferramentas para se apropriar de um endereço MAC de outra placa ou simplesmente fazer uso de outro que não o original de fábrica. Elas serão detalhadas no capítulo seguinte.

2.5 – Criptografia e autenticidade em redes sem fio

Uma forma de proteção aos dados trafegados na rede é a criptografia. Usando-se criptografia, todos os dados transmitidos ficarão fora de uma ordem lógica e entendível (GIMENES, 2005). Assim, caso um atacante tente obter os dados trafegados na rede, não conseguirá compreendê-los.

Conforme AGUIAR (2005), a criptografia computacional é usada para garantir:

- sigilo: somente os usuários autorizados têm acesso às informações;
- integridade da informação: garantia ao usuário de que a informação está correta;
- autenticação do usuário: é o processo que permite ao sistema verificar a identidade do usuário ou dispositivo com quem está se comunicando.

2.5.1 – Wired Equivalent Privacy (WEP)

Devido à insegurança do meio onde às informações trafegam nas redes 802.11, foi criado inicialmente o protocolo WEP (*Wired Equivalent Privacy*) para fornecer segurança. Este está totalmente disseminado e presente em todos os produtos que estão em conformidade com o padrão *wi-fi*.

Trata-se de um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas (RUFFINO, 2005).

O WEP opera na camada de enlace de dados e é baseado no 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 criptografar os dados. Além disso, o WEP utiliza CRC-32 (C*yclic Redundancy Check*) para calcular o *checksum* da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o *checksum* para garantir que a mensagem não foi alterada (GIMENES, 2005).

Na prática o WEP tem suas falhas e vulnerabilidades, mas não deixa de ser uma camada de proteção adicional.

2.5.2 – Wi-fi Protected Access (WPA)

Diante dos problemas de segurança divulgados para WEP, a *Wi-fi Alliance*, em conjunto com o IEEE, lançou o protocolo WPA. Este protocolo fornece melhor tratamento de segurança que o WEP, ao passo que é compatível com o hardware que roda o WEP. Dessa forma a atualização do WEP para WPA é feita através da atualização do *firmware* dos dispositivos *wi-fi*, não necessitando mudanças na infra-estrutura de hardware (AGUIAR, 2005).

O WPA possui melhores mecanismos de autenticação, privacidade e controle de integridade que o WEP (AGUIAR, 2005).

No WPA, ao contrário do WEP, não está disponível suporte para conexões *Ad-Hoc*. Portanto, essa modalidade de rede sem uso de concentrador não se beneficia dos mecanismos de proteção introduzidos no protocolo WPA na sua primeira versão.

O WPA atua em duas áreas. A primeira é a que substitui o WEP, cifrando os dados e garantindo a privacidade do tráfego, enquanto a segunda autentica o usuário, utilizando para isso padrões 802.1x e EAP (*Extensible Authentication Protocol*).

O WPA utiliza dois tipos de protocolos para cifrar as informações: um voltado para pequenas redes, utilizando uma chave previamente compartilhada (*Pre-shared Key*, ou WPA-PSK), que será responsável pelo reconhecimento do equipamento pelo concentrador. O outro tipo é conhecido como infra-estrutura, que requer ao menos a adição de um servidor de autenticação RADIUS (*Remote Authentication Dial-In User Server*) (RUFINO, 2005).

O método de chave compartilhada é semelhante ao WEP, onde a troca de chaves é feita manualmente, fazendo com que seu uso se torne mais adequado em redes pequenas, onde os participantes estão acessíveis na maior parte do tempo (GIMENES, 2005).

Dentre as novidades do WPA há o protocolo TKIP (*Temporal Key Integrity Protocol*), que é responsável pela troca dinâmica das chaves. No WEP as chaves eram estáticas e seu IV era de apenas 24 bits, passando agora para 48 bits (GIMENES, 2005).

Neste protocolo é utilizada uma chave base de 128 bits chamada de TK (*Temporal Key*). Esta chave é combinada ao endereço MAC do transmissor (TA), criando uma outra chave chamada de TTAK (*Temporal and Transmitter Address Key*), conhecida como "Chave da 1º Fase". A TTAK é combinada com o IV do RC4 para criar chaves diferentes para cada pacote (AGUIAR, 2005).

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. Além disso, ele pode ser programado para alterar o IV a cada pacote, por sessão ou por período, tornando mais difícil a obtenção do mesmo, via captura de tráfego.

2.5.2.1 – Extensible Authentication Protocol (EAP)

Um modelo para autenticação também foi definido no WPA, conhecido como EAP, que utiliza o padrão 802.1x e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital. Este padrão pode ser utilizado em conjunto com outras tecnologias existentes, como o servidor de autenticação RADIUS.

O 802.1x utiliza o protocolo EAP para gerenciar a forma como a autenticação mútua será feita na rede. Ele possibilita a escolha de um método específico de autenticação a ser

utilizado, como senhas, certificado digital ou *tokens* de autenticação. O autenticador não precisa entender o método de autenticação, ele simplesmente transmite os pacotes EAP do usuário a ser autenticado para o servidor de autenticação e vice-versa (AGUIAR, 2005).

Conforme GIMENES (2005), pode-se configurar os APs 802.1X sem fio como clientes RADIUS para que eles enviem solicitações de acesso e mensagens de contas para os servidores RADIUS que executam IAS (*Internal Authentication Server*). O IAS executa a autenticação dos usuários e dispositivos, controlando o acesso à rede por meio de diretivas de acesso remoto centralizado.

Segundo GRÉGIO (2005), existem vários tipos de EAP que dão suporte a diversos métodos de autenticação:

- EAP-LEAP (*LightWeight EAP*): Desenvolvido pelo CISCO, usa o método de *login* e senha para transmitir a identidade do usuário a ser autenticado ao servidor de autenticação.
- EAP-TLS (*Transport Layer Security*): Especificado na RFC 2716. Usa um certificado X.509 para autenticação.
- PEAP (*Protected EAP*): Oferece autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificados nos clientes. Foi adotado pela *Microsoft* no *Windows XP* e *Windows Server 2003*.

2.5.3 –WPA2 ou 802.11i

Conhecido também como 802.11i, o WPA2 foi ratificado pelo IEEE em junho de 2004. Trata-se de um produto disponível por meio da *Wi-fi Alliance.* 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 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, constituindo-se assim em 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 (AGUIAR, 2005).

2.6 – Conclusão

A partir do que foi apresentado neste capítulo, é possível entender as principais características das redes sem fio 802.11, desde topologia de rede à protocolos complexos de criptografia, bem como métodos de autenticação e os padrões atuais disponíveis.

Pode-se concluir que a tecnologia w*ireless* traz um novo paradigma no que diz respeito à comunicação entre os dispositivos de uma rede de computadores, reduzindo custos a nível físico e operacional, evoluindo cada dia mais para uma nova tendência mundial, que já está presente na maioria dos países desenvolvidos e que tem ganhado muita força nos últimos anos nos demais países (UTZIG, 2006).

Essa tecnologia abre novos horizontes e estabelece um novo conceito tecnológico no que diz respeito a todo e qualquer tipo de comunicação entre dispositivos de uma rede de computadores (UTZIG, 2006).

No próximo capítulo serão analisados os riscos, as ameaças, as vulnerabilidades e ferramentas de ataque das redes sem fio.

3 – Análise dos ataques e vulnerabilidades das redes sem fio

3.1 – Introdução

Este capítulo detalhará os riscos e vulnerabilidades a que as redes sem fio estão sujeitas. Além disso, serão apresentadas técnicas de ataques e ferramentas empregadas com este propósito. Entende-se por vulnerabilidade as falhas ou falta de segurança das quais pessoas mal intencionadas possam se valer para invadir, subtrair, acessar ilegalmente, adulterar e destruir informações confidenciais. Além de poder comprometer, corromper e inutilizar o sistema.

Mesmo com os avanços da tecnologia sem fio, os riscos inerentes a esta tecnologia se apresentam de forma significativa e devem ser devidamente analisados e minimizados na implantação de uma rede w*ireless*.

3.2 – Problemas de segurança física

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 e, principalmente, facilitar o acesso não autorizado e outros tipos de ataques (RUFINO, 2005).

Alguns itens devem ser observados para avaliar a abrangência de uma rede sem fio, como o padrão utilizado e a potência dos equipamentos. 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. Essa avaliação é importante, pois um atacante munido de uma interface de maior potência poderá receber sinal a distância não prevista pelos testes de propagação do sinal.

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.

3.3 – Negação de serviço (*Denial of Service - DoS*)

Um ataque de negação de serviço é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Trata-se de um tipo de ataque que não necessita de acesso ou invasão à rede-alvo, mas pode acarretar sérios transtornos dependendo do ambiente envolvido.

Sabe-se na prática que até dispositivos *Bluetooth* conseguem causar retardo a redes *wi-fi*, tornando por vezes inviável o acesso de alguns equipamentos à rede. De acordo com RUFINO (2005) verificou-se em testes de laboratório que dispositivos *Bluetooth* (com alcance de aproximadamente 100 metros), próximos a concentradores *wi-fi*, causam grande interferência (principalmente no padrão 802.11g em baixa velocidade).

3.4 – Mapeamento do ambiente

Uma das primeiras ações realizadas pelos atacantes é fazer um mapeamento do ambiente. Esse procedimento possibilita obter o maior número de informações sobre determinada rede, permitindo conhecer detalhes que lhe permitam lançar ataques de forma mais precisa e com menos riscos de ser identificado. O sucesso de tal ação depende do nível de proteção configurado na rede-alvo (RUFINO, 2005).

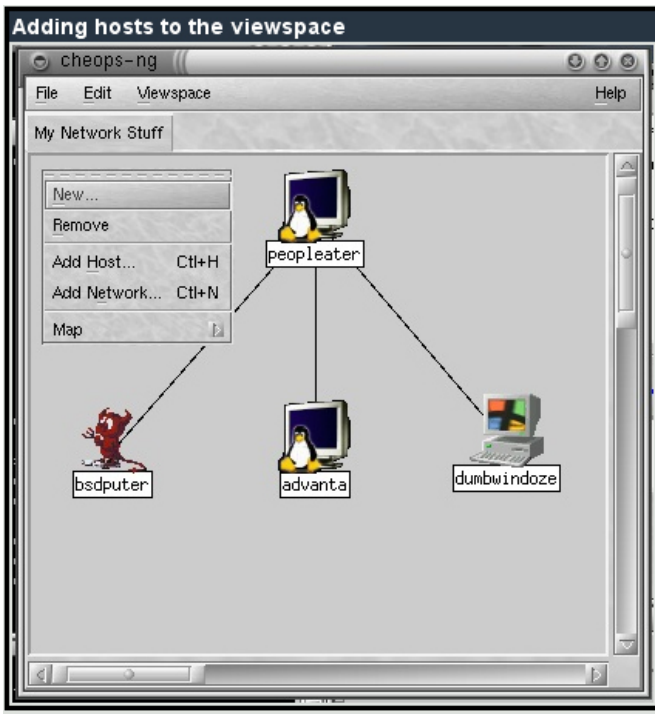
O mapeamento passivo é aquele onde o atacante obtém as informações (IP, sistema operacional, SSID) sem ser reconhecido. Ferramentas tradicionais em rede cabeada, como o p0f, podem realizar essa tarefa: basta ao atacante estar posicionado em uma área coberta pelo sinal da rede-alvo. De posse dessas informações o atacante pode selecionar equipamentos de seu interesse e que estejam vulneráveis (AGUIAR, 2005).

Uma das possibilidades mais interessantes para identificar características e localizar redes sem fio é integrar ferramentas de análise com dispositivos de localização por satélite, conhecidos como GPS (*Global Positioning System*). Desta forma é possível gerar mapas com bom grau de precisão, onde se encontram redes com características de interesse. Um exemplo destas ferramentas é o *GPS Daemon* (GPSD), disponível em várias plataformas abertas como *Linux* e *FreeBSD* (RUFINO, 2005).

Já o mapeamento ativo pode ser tão completo quanto o atacante desejar. Uma excelente ferramenta é o *Cheops-ng*, que não somente identifica graficamente os componentes, como também informa o sistema operacional, tipo/modelo dos equipamentos,

serviços em uso e tempo de resposta a *ping*. A Figura 4 exibe uma das interfaces da ferramenta (CHEOPS-NG, 2007).

Figura 4 – Adicionando *hosts* para efetuar mapeamento.



Fonte: CHEOPS-NG (2007).

3.5 – Configurações

Segundo RUFFINO (2005), existem muitos motivos para que um atacante queira acessar uma determinada rede: obter acesso direto para *Internet*, promover ataques, dentre outros.

3.5.1 – Configuração aberta

De acordo com GIMENES (2005), este tipo de configuração é caracterizado pelo envio do SSID da rede pelo concentrador, ou seja, ele aceita conexões de qualquer dispositivo cuja compatibilidade de padrão seja atendida. Trata-se de uma situação ainda muito comum em ambientes de redes fio. Esta configuração permite o fácil acesso por parte de qualquer usuário.

3.5.2 – Configuração fechada

Neste tipo de configuração, o concentrador não envia o seu SSID, portanto apenas permite a conexão de usuários que sabem o SSID da rede (GIMENES, 2005). Os atacantes terão de promover uma escuta do tráfego para determinar o SSID correto, para depois conectarem-se a rede alvo.

3.6 – Vulnerabilidades nos protocolos WEP e WPA

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 claro a importância dos protocolos WEP e WPA para redes *wireless*. Ainda que sejam úteis para a segurança da rede, eles apresentam vulnerabilidades que serão 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. Além disso, quanto mais pessoas conhecerem a chave, menos seguro será o mecanismo de segurança (DUARTE, 2003).

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. Além disso o IV é transmitido em texto puro, ou seja, sem criptografia, deixando a transmissão de dados mais suscetível a ataques (WARCHALKING, 2006).

Segundo TEWS *et al* (2007), é possível quebrar uma chave WEP de 104 bits em menos de sessenta segundos.

Apesar do WPA ter características de segurança superiores às do WEP, este também está sujeito a ataques de força bruta ou dicionário, onde o atacante testa senha em seqüência ou em palavras comuns. Outro problema seria no armazenamento das chaves, tanto nos clientes quanto nos servidores/concentradores, podendo comprometer a segurança das redes (RUFFINO, 2005).

3.7 – Técnicas e ferramentas de ataque

Segundo GIMENES (2005), não existe nenhuma grande novidade nos ataques às redes sem fio. Grande parte destes ataques não sofreram nenhuma modificação em relação aos ataques às redes cabeadas. Outros, no entanto, tiveram que sofrer algumas modificações a fim de obter melhores resultados. A seguir descrevemos algumas técnicas e ferramentas de ataque utilizadas.

3.7.1 - *Access Point Spoofing* (Associação Maliciosa)

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

3.7.2 – 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 *ARP Poisoning* pode ser disparado de uma estação da WLAN à uma estação guiada. Ou seja, este ataque não fica restrito apenas às estações sem fio (DUARTE, 2003).

3.7.3 – 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.

3.7.4 – 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).

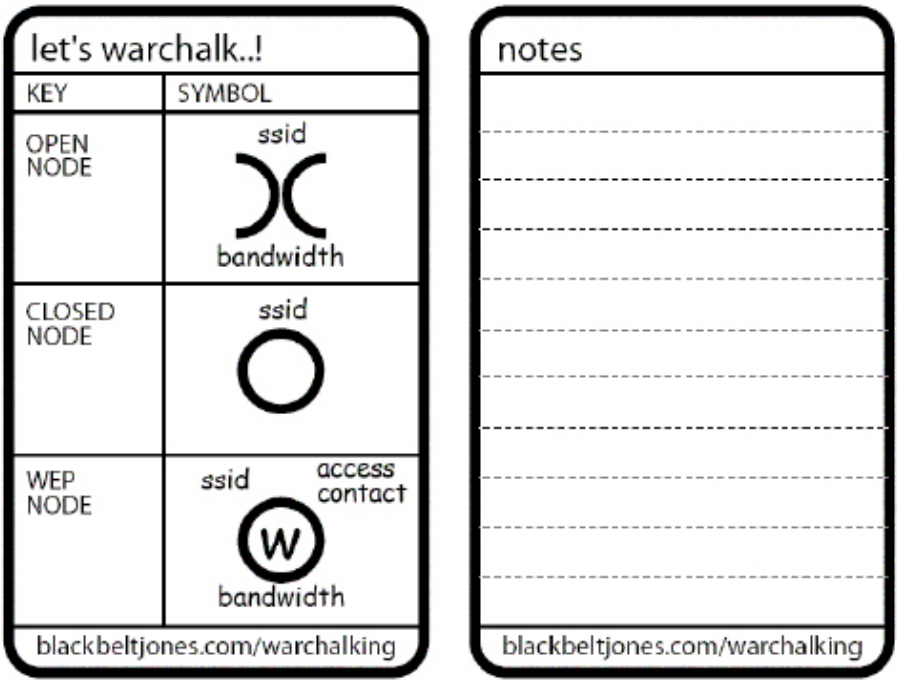
O objetivo deste tipo de ataque é mapear todos os A*ccess Points* encontrados com o auxílio de um GPS.

3.7.5 – Warchalking

Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas de W*ardriving* 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 5. Existem grupos organizados para *warchalking* que se utilizam de símbolos próprios para marcar as redes numa tentativa de mantê-las em segredo (DUARTE, 2003).

Figura 5 – 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).

3.7.6 – Ferramentas de Ataque

Segundo RUFFINO (2005), ao contrário das redes cabeadas, em que fabricantes e modelos das interfaces de rede nada influenciam o comportamento das ferramentas, em redes *wireless* a maior parte das ferramentas dependem de equipamentos específicos e/ou modelos de placas de rede, ou de um padrão (802.11g, por exemplo).

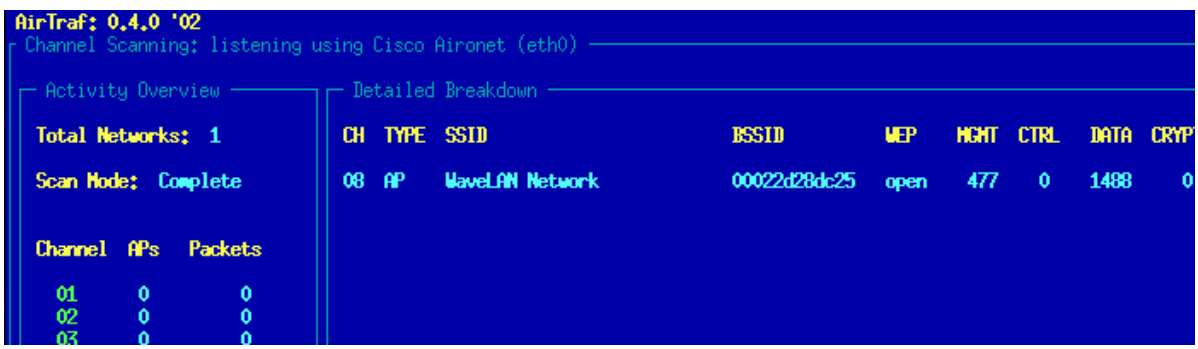
A seguir descrevemos algumas ferramentas gratuitamente disponíveis, suas principais características e objetivos.

3.7.6.1 – Airtraf

Esta ferramenta permite coletar uma grande quantidade de informações sobre as redes identificadas, tais como clientes conectados e serviços utilizados, tudo em tempo real. Além disso, ela "quebra" a chave do protocolo WEP no padrão 802.11b. Ela atua passivamente monitorando as transmissões.

De acordo com RUFFINO (2005), o *Airtraf* é uma ferramenta muito prática para coletar informações sobre redes sem fio. Além de exibir detalhes que são úteis aos atacantes, também pode ser usada por administradores que podem monitorar as atividades das quais são responsáveis.

Figura 6 – *Airtraf* na tela de varredura



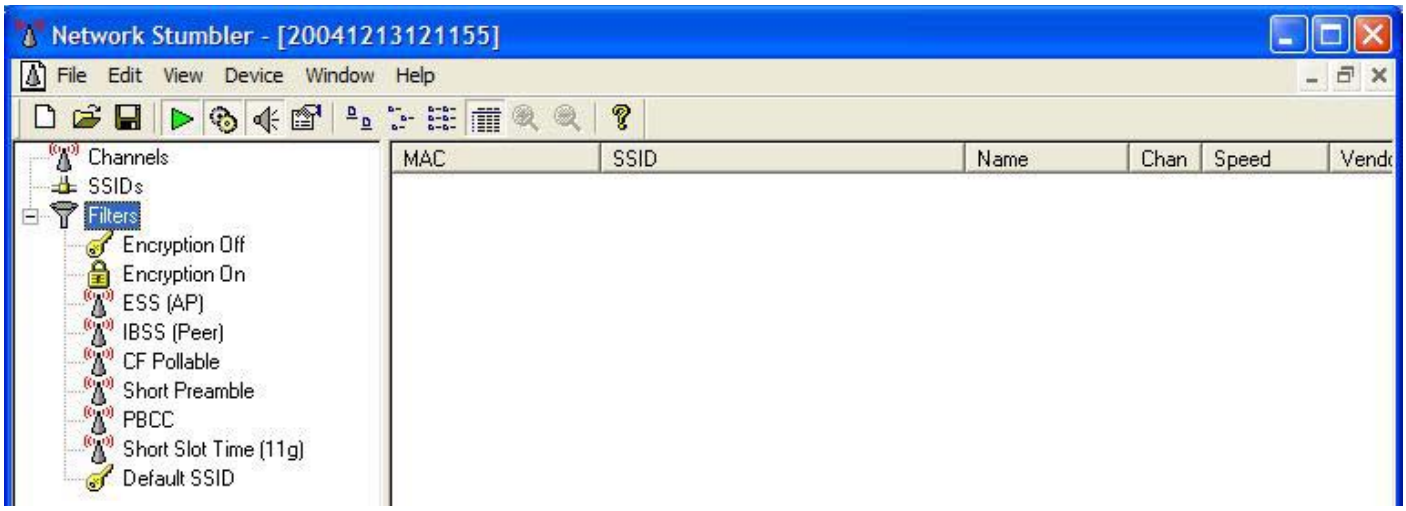
Fonte: AIRTRAF (2004).

3.7.6.2 – Netstumbler

Uma das primeiras ferramentas disponíveis para mapeamento e identificação de redes sem fio em ambiente *Windows*. Ela permite integração com equipamentos GPS, gerando mapas precisos de pontos de acesso rastreados. Além disso, atualmente permite identificar redes em todos os padrões comerciais e aceita uma grande variedade de interfaces de rede (RUFFINO, 2005).

O *Netstumbler* apresenta limitações, como não realizar captura de tráfego e não possuir métodos para quebra de chaves WEP.

Figura 7 – Visão geral da ferramenta *Netstumbler*

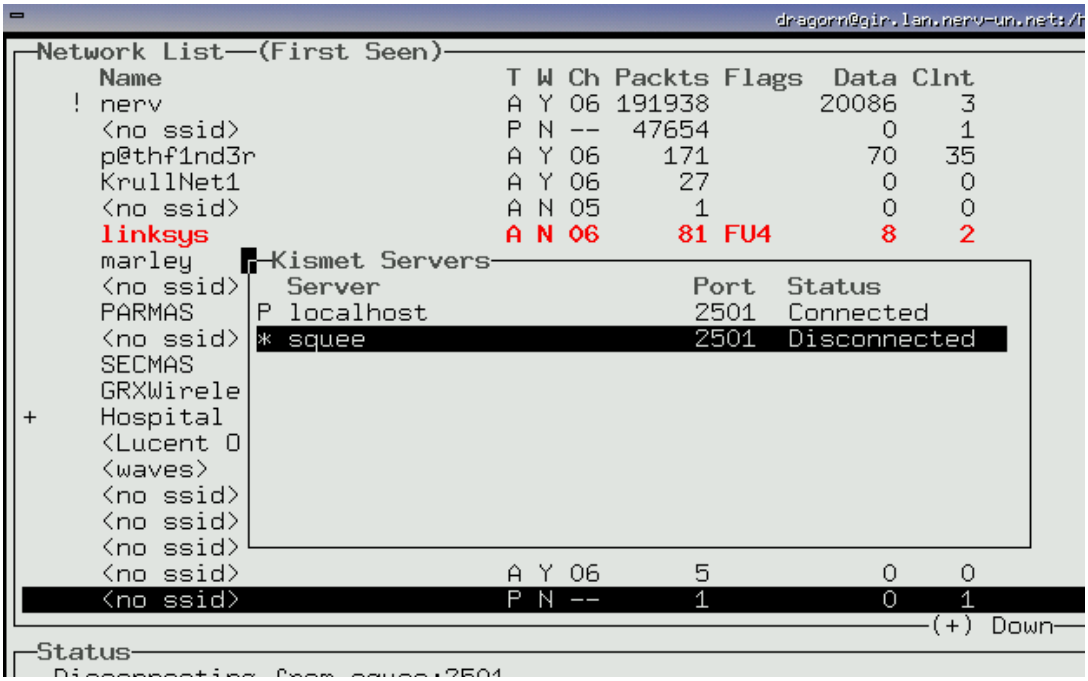


Fonte: NETSTUMBLER (2005)

3.7.6.3 – 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 (KISMET, 2007).

Figura 8 – *Kismet* em ação



Fonte: KISMET (2007)

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.

3.7.6.4 – AirJack

Uma característica interessante desta ferramenta é a facilidade de fazer um ataque do tipo “homem no meio”, que consiste na implantação de falsos concentradores que se interpõem aos concentradores oficiais e, desta forma, passam a receber as informações transmitidas.

3.7.6.5 – Ferramentas para quebra de chaves WEP

Existem várias ferramentas desenvolvidas para decifrar chaves WEP, com maior ou menor grau de eficiência. Geralmente aplicam uma combinação de força bruta ou ataques com dicionário. Dentre elas destacam-se: *Airsnort, WepCrack, WepAttack, AirCrack.*

3.8 – Conclusão

Neste capítulo, foram estudados os riscos e vulnerabilidades inerentes às redes sem fio. Além disso, foram apresentados os principais tipos de ataques, bem como algumas ferramentas de ataque, mostrando suas principais vantagens e desvantagens.

Nota-se a grande quantidade e variedade destas ferramentas disponíveis gratuitamente. Observa-se também a grande especificidade da maioria delas, sendo criadas para um objetivo específico e para modelos de interfaces e padrões determinados.

Diante desta análise, torna-se cada vez mais importante medidas de segurança na implantação de redes sem fio, pois além dos riscos inerentes às redes *wireless,* temos cada vez mais o aprimoramento e o surgimento de novas ferramentas de ataque.

4 – Estratégias de defesa

4.1 – Considerações Iniciais

O uso de redes sem fio permite muito mais flexibilidade e mobilidade aos usuários, porém um fator fundamental vem sendo colocado em segundo plano na implementação dessas redes: a segurança da informação. O uso de estratégias de segurança eficazes é imprescindível, pois há a necessidade de diminuir os riscos e os acessos indevidos à rede (JUNIOR *et al*, 2004).

Para conseguir um nível razoável de segurança é preciso implementar controles externos aos equipamentos. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são fundamentais (JUNIOR *et al*, 2004).

Neste capítulo serão apresentadas estratégias de segurança que devem ser aplicadas às redes *wi-fi*, tornando-as mais seguras e menos vulneráveis as inúmeras ferramentas de ataques disponíveis.

4.2 – Configurações do concentrador

O primeiro passo para tornar a rede mais segura é desabilitar a difusão da informação de SSID (*broadcast* SSID), escondendo assim o nome da rede. Desta forma, apenas clientes que conhecem o nome da rede ao qual o concentrador responde poderiam estabelecer conexão. Todavia existem tipos de ataque que não necessitam conhecer o SSID, como é o caso da escuta do tráfego. Inclusive, ao realizar a escuta, é possível descobrir o SSID da rede-alvo.

Deve-se também modificar o nome ESSID padrão para ao menos retardar um ataque. O administrador deve escolher um nome que não revele nem o equipamento nem a empresa. Segundo RUFFINO (2005), é preciso alertar que o campo INFO é meramente documentável e permite cadastrar informações adicionais, sendo transmitido em texto não criptografado. Portanto, tanto o ESSID como o INFO devem ser usados corretamente, para dificultar ao máximo as ações de um possível atacante.

Alguns concentradores permitem alterar o endereço MAC. Esta mudança evita a identificação imediata do fabricante por parte de um atacante, pois o endereço MAC está diretamente relacionado ao seu fabricante.

A maior parte dos concentradores permite configuração via HTTP e TELNET. Recomenda-se desabilitar essas opções do lado da rede sem fio, para impedir que informações importantes (como usuário e senha) sejam interceptadas por um possível atacante. Esta ação pressupõe que a rede cabeada tenha mecanismos de proteção que possibilitem monitorar e autenticar os usuários, restringindo as configurações do concentrador somente as pessoas devidamente autorizadas (RUFFINO, 2005).

Outra importante medida é fazer os concentradores ignorarem clientes que enviam SSID igual a "ANY". Esta é uma situação que usualmente caracteriza um cliente que busca qualquer concentrador disponível. Como não é possível ter certeza de que se trata realmente de um cliente, esta situação deve ser evitada, já que um atacante pode utilizá-la para ter acesso à rede.

É importante destacar que essas medidas usadas isoladamente não fornecem um bom nível de segurança, por isso devem ser combinadas com outras medidas para que se tornem devidamente eficazes.

4.3 – Defesa dos equipamentos clientes

Um importante mecanismo de defesa é o PSPF (*Publicly Secure Packet Forwarding*), que bloqueia o acesso de um cliente a outros ligados ao mesmo concentrador, evitando ataque direto de um usuário contra outro. Esta configuração equivale à de um *switch,* onde se define uma interface por porta. Entretanto, ao contrário do *switch* onde existe separação física do tráfego, este método não impede a captura dos pacotes. Desta forma, este mecanismo deve ser usado de forma combinada com outras medidas de segurança, para garantir a privacidade dos usuários (RUFFINO, 2005).

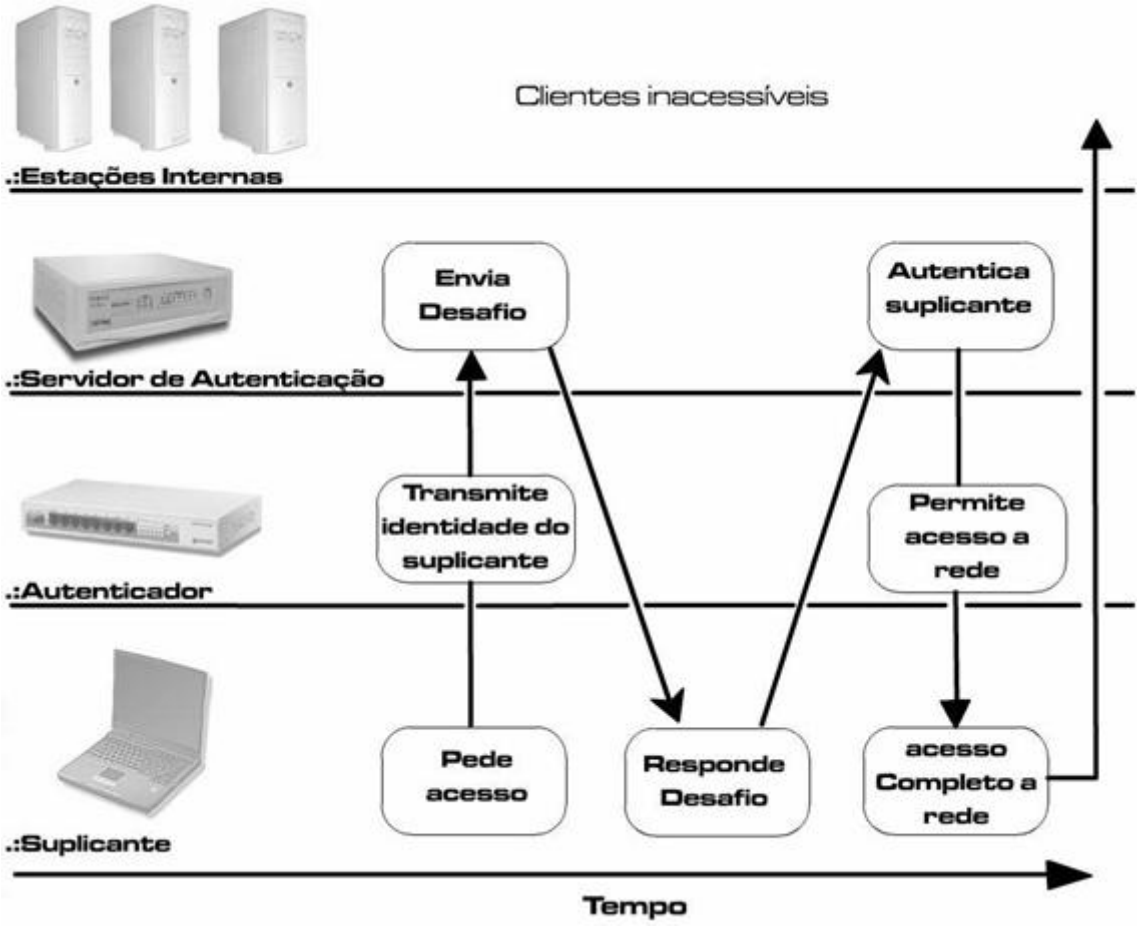
4.4 – Padrão 802.1x e RADIUS

O padrão IEEE 802.1X define métodos de autenticação, que são componentes importantes para aumentar o nível de segurança de uma rede sem fio. Um componente muito utilizado para fazer autenticação é o servidor RADIUS.

Segundo AGUIAR (2005), em um processo de autenticação 802.1x existem 3 participantes:

- O suplicante: usuário a ser autenticado.
- Servidor de autenticação: sistema de autenticação RADIUS, que realiza a autenticação dos clientes cadastrados.
- Autenticador: mediador na transação entre o suplicante e o servidor de autenticação. Geralmente é o AP.

Figura 9 - Simulação de acesso a uma rede sem fio



Fonte: GIMENES (2005)

De acordo com a figura 9, o requisitante (suplicante) pede o acesso, o autenticador transmite a identidade do suplicante para o servidor de autenticação, que por sua vez envia um desafio ao suplicante. O suplicante responde o desafio e o servidor autentica o usuário para que o autenticador permita o acesso à rede (GIMENES, 2005).

O 802.1x utiliza o protocolo EAP para gerenciar a forma como a autenticação mútua será feita na rede. Ele possibilita a escolha de um método específico de autenticação a ser utilizado, como senhas, certificados ou *tokens* de autenticação (AGUIAR, 2005).

O autenticador não precisa entender o método de autenticação, ele simplesmente repassa os pacotes EAP do suplicante para o servidor de autenticação e vice-versa (AGUIAR, 2005).

4.5 – Virtual Private Network (VPN)

Uma opção de segurança para redes sem fio são as VPN (Redes Privadas Virtuais). Segundo JUNIOR *et al* (2004) elas são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações de modo seguro, entre redes corporativas ou usuários remotos. Esta técnica, também chamada de tunelamento, cria "túneis virtuais" de comunicação entre dois pontos, garantindo maior segurança no tráfego das informações transmitidas.

A grande maioria destas redes utilizam o protocolo *IPSec* para construir o canal seguro. A principal função do *IPSec* é fazer o roteamento das mensagens por um túnel cifrado, através da inserção de dois cabeçalhos especiais após o cabeçalho IP de cada mensagem (JUNIOR, 2003).

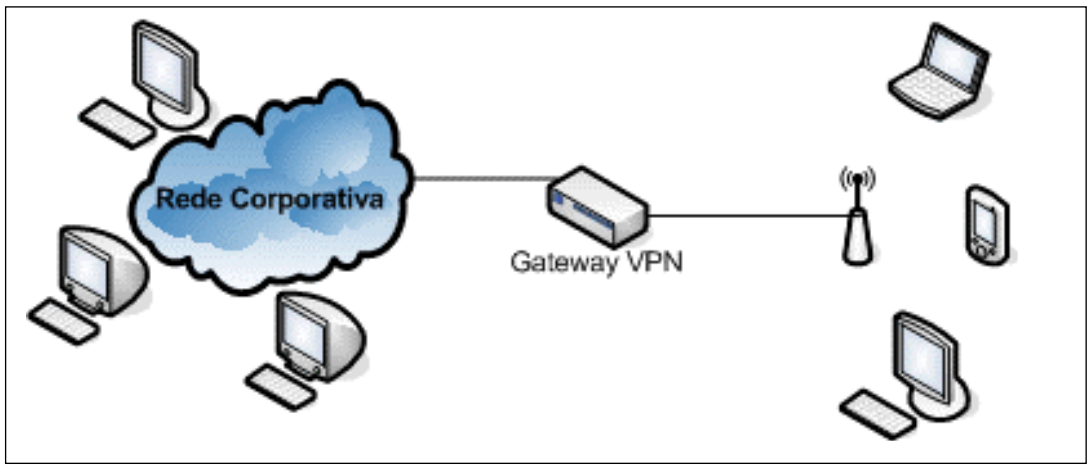
Antes do pacote ser transportado ele é criptografado, de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado viaja através da Internet até alcançar seu destino, onde é decifrado, retornando ao seu formato original (JUNIOR *et al*, 2004).

Além da criptografia, as VPNs oferecem a autenticação dos usuários, outro item de muita importância quando se trata de segurança no tráfego de dados. É feita uma verificação na identidade do usuário, permitindo acesso somente a clientes cadastrados (GIMENES, 2005).

A figura 10 exibe um exemplo de utilização de VPN com dispositivos *wireless*. Neste exemplo os clientes conseguem fazer conexões seguras (com o *IPSec*) para dentro da rede

corporativa, através de *gateway* VPN. Este *gateway* ainda pode ter um *firewall* integrado para filtrar e bloquear o tráfego.

Figura 10 – Exemplo de uma WLAN com VPN.



Fonte: JUNIOR (2003)

As VPNs podem oferecer uma opção segura para transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança (JUNIOR *et al*, 2004).

Todavia, a escolha por este tipo de rede deve ser muito bem analisada, pois podem ocorrer problemas de desempenho e atrasos na transmissão.

4.6 – Firewalls

De acordo com AGUIAR (2005), os *firewalls* são componentes fundamentais para garantir a segurança de uma rede sem fio. Através dele pode-se controlar todo o tráfego de dados que entra e sai da rede, de forma seletiva, de acordo com um conjunto de regras previamente estabelecidas em sua configuração.

O *firewall* também pode assumir o papel de *gateway* entre duas redes, podendo estas redes ser uma *wi-fi* e a outra LAN. Desta forma é possível isolar as duas redes, evitando que pessoas não autorizadas que possuem acesso a uma rede não tenha o mesmo privilégio em acessar à outra. Assim bloqueia-se o tráfego que ocorre do lado *wi-fi* para a LAN e da LAN para *wi-fi* (JUNIOR *et al*, 2004).

Além disso, um *firewall* é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior dos acessos às redes (JUNIOR *et al*, 2004).

4.7 – Senhas descartáveis (*One-time Password* - OTP)

Tratando-se de mecanismos de segurança em redes sem fio, há dois pontos principais a serem protegidos: o conteúdo das informações e o acesso ao equipamento do usuário. O uso da criptografia tenta sanar o primeiro problema, mas se o atacante acessar o equipamento do usuário, a segurança provida pela criptografia tende a ser perdida (RUFFINO, 2005).

Desta forma, cabe ao administrador proteger o equipamento com tecnologias de *firewall,* antivírus, anti-spyware e principalmente fornecer mecanismos de autenticação baseados em senhas descartáveis, *tokens* e cartões processados (*smartcards*) ou fazer uso de dispositivos biométricos (RUFFINO, 2005).

As senhas descartáveis são simples e de fácil implementação. A idéia é permitir que o usuário informe uma senha diferente a cada acesso, tornando ineficiente a captura da senha pela rede, visto que será informada uma senha diferente da atual no próximo acesso (RUFFINO, 2005).

O processo de criação das senhas descartáveis inicia-se quando o servidor envia uma informação como desafio. Este desafio é recebido pelo cliente, que o concatena com a senha secreta. Sobre este valor é aplicada uma função criptográfica, gerando a senha descartável a ser utilizada pelo cliente somente nesta seção. O servidor realiza um cálculo semelhante e verifica se o valor recebido do cliente corresponde ao calculado localmente. Se o valor recebido for válido, o cliente é autorizado a utilizar o sistema.

4.8 – Certificados digitais

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

Estes certificados são sempre lembrados como um dos métodos de autenticação mais seguros, principalmente quando armazenados em dispositivos processados como *tokens* ou cartões.

De acordo com AGUIAR (2005), um certificado digital contém três elementos:

- Informação de atributo: informação sobre o objeto que é certificado. No caso de uma pessoa, o seu nome, nacionalidade, etc.
- Chave de informação pública: esta é a chave publicada na Autoridade Certificadora. O certificado atua para associar a chave pública à informação de atributo.
- Assinatura da Autoridade Certificadora: a Autoridade assina os dois primeiros elementos, validando-os.

Entre os métodos de EAP citados nos capítulos anteriores, alguns permitem o uso de certificados digitais. O mais diretamente associado a esses recursos é o EAP_TLS, que permite autenticar o usuário em função de informações disponíveis nos certificados.

4.9 – Token e SmartCard

Algumas formas de autenticação utilizam dispositivos físicos para armazenarem informações confidenciais como chaves privadas e senhas, na tentativa de impedir uma possível captura no computador do cliente. Como exemplo destes dispositivos podemos citar os *tokens* e os *smartcards.*

O *token* é um dispositivo pequeno, do tamanho de um chaveiro, que pode ser usado para armazenar IDs digitais e dados de autenticação. Para acessar o seu ID digital, basta conectar o *token* a uma porta USB no computador ou dispositivo móvel. O *token* pode incluir um teclado numérico, que permite digitar um número de identificação pessoal (PIN). A figura 11 mostra um *token* de autenticação.

O *Smartcard* 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 11 - *Token* de Autenticação

Fonte: AGUIAR (2005)

4.10 – Detecção de ataques e monitoramento

Segundo RUFFINO (2005), a ação de segurança mais importante é o correto monitoramento do ambiente. Porém, o monitoramento também pode falhar em algum momento. Ao optar em qual setor devem ser aplicados os investimentos em segurança, certamente mecanismos de monitoramento devem ter prioridade, porque eles irão detectar pontos de falha, bem como poderão analisar como um determinado ataque ocorreu ou foi bloqueado.

Um erro comum é o monitoramento apenas dos padrões utilizados no ambiente, propiciando ataques que utilizam exatamente algum padrão não existente.

4.10.1 – wIDS

Esta ferramenta consegue detectar não somente tipos comuns de ataques, mas também irregularidades em geral, como repetidas requisições para associação com um determinado concentrador. O wIDS está disponível para qualquer tipo de placas e *chipsets*, bastando a interface poder entrar em modo monitor (AGUIAR, 2005).

Para RUFFINO (2005), os tipos de tráfego suspeito monitorados por esta ferramenta são:

- Análise do intervalo de tempo entre os BEACONS de cada concentrador encontrado;
- Detecção de requisições provenientes de varredura;
- Detecção da freqüência de requisições de reassociação;

- Detecção de grande volume de requisições de autenticação em um pequeno intervalo de tempo.

4.10.2 – Garuda

É uma ferramenta que facilita a criação e mudança das assinaturas dos pacotes suspeitos analisados. Entretanto somente aceita placas do padrão *aironet* (GARUDA, 2006).

O *Garuda* ainda possibilita a integração com uma base de dados em *MySQL*. Sendo assim, as informações sobre pacotes suspeitos serão armazenadas no banco.

4.10.3 – Kismet

Usualmente aceita como uma ferramenta para varredura e ataque, o *Kismet* agrega mecanismos que o tornam um grande aliado de monitoramento e detecção de ataques (KISMET, 2007). Dentre as suas principais funções, destacam-se:

- Identificação de ferramentas de ataque (*Netstumbler* e *AirJack*);
- Detecção de tráfego irregular;

Visto que a ferramenta pode ser integrada a dispositivo GPS, o *Kismet* informa a localização física de um possível atacante.

4.10.4 – Snort – Wireless

É uma tradicional ferramenta para identificar possíveis ataques baseados em assinaturas, pacotes mal formados e tráfego suspeito (SNORT, 2007). Trata-se de um sistema de detecção de intruso que é capaz de fazer o registro dos pacotes e a análise do tráfego de uma rede em tempo real.

Esta ferramenta consegue executar análise do protocolo e faz combinações que podem detectar uma variedade de ataques, como varredura feita por ferramentas como o *NetStumbler* e a presença não autorizada de um concentrador na área de abrangência da rede (SNORT, 2007).

4.10.5 – Honeypots e Honeynets

Honeypots são redes monitoradas com a finalidade de serem atacadas e comprometidas, para que seja possível analisar as atividades de invasão que sejam efetuadas contra as mesmas. Assim é possível compreender as técnicas utilizadas na realização de ataques a redes de computadores (GRÉGIO, 2005).

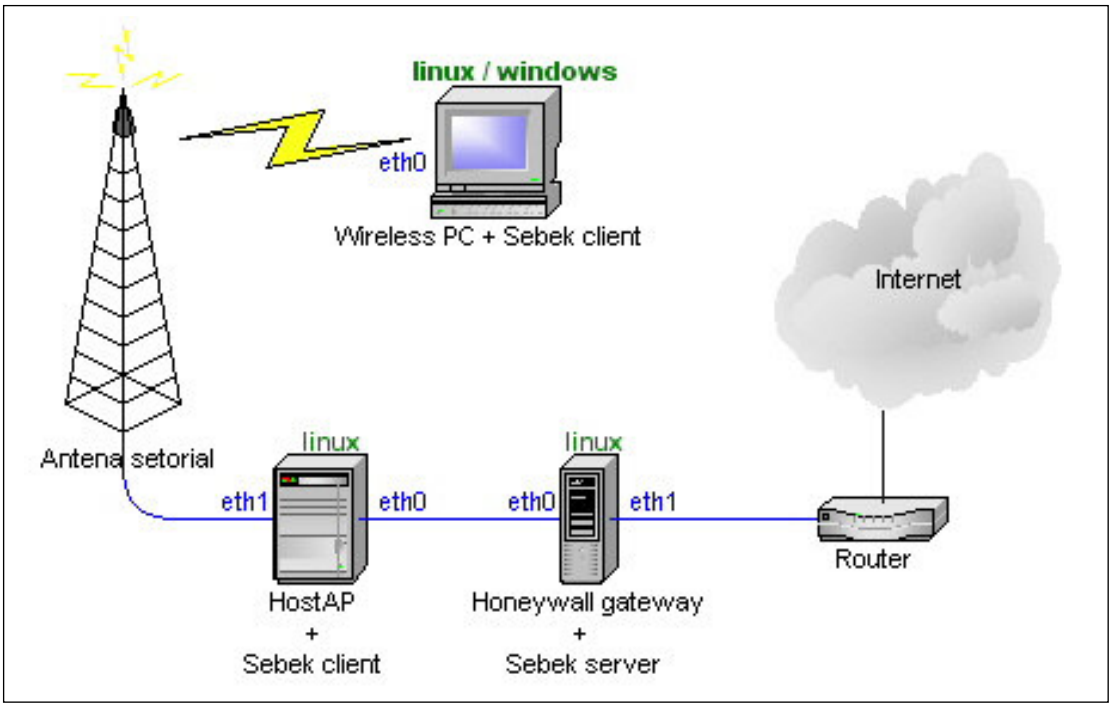
Segundo GRÉGIO (2005), "os *honeypots* podem ser classificados como de alta interação e baixa interação. *Honeypots* de alta interação são aqueles constituídos de um computador com um sistema operacional instalado, simulando um sistema de produção real. Isso permite que um invasor possa interagir totalmente com o sistema atacado e explorar as vulnerabilidades dos programas e serviços em execução neste sistema".

As *honeynets* são um tipo peculiar de *honeypot* de alta interação, mais complexo, consistindo de uma rede real configurada com uma quantia considerável de ferramentas de monitoramento. A tecnologia de *honeynets* evoluiu, tornando a implementação e o gerenciamento mais simples pela combinação do controle e captura de dados em uma só máquina (*honeywall*) (GRÉGIO, 2005).

A detecção de intrusos em redes de computadores sem fio torna possível a compreensão total da metodologia utilizada por um atacante para invadir e comprometer uma rede sem fio, desde o momento em que é realizada a varredura (*scanning*) no concentrador de acesso – o início de um provável ataque – até tentativas de apropriação indevida do mesmo ou negativas de serviço (GRÉGIO, 2005).

Desta forma, os ataques poderão ser estudados minuciosamente para fornecer soluções que minimizem seus efeitos nocivos à utilização segura de uma rede sem fio, protegendo a integridade e confidencialidade dos dados.

Figura 12 – Topologia do modelo de *wireless honeynet.*



Fonte: GRÉGIO (2005).

4.10.6 – AirMagnet

Numa rede *wi-fi* é possível alguém conectar um AP na rede, se passando por outro dispositivo e desta forma capturar todo o tráfego. *Softwares* de monitoramento de sinal como o *AirMagnet* permitem o reconhecimento de dispositivos estranhos conectados à rede, podendo inclusive soar alarmes quando for detectada uma irregularidade (AGUIAR, 2005).

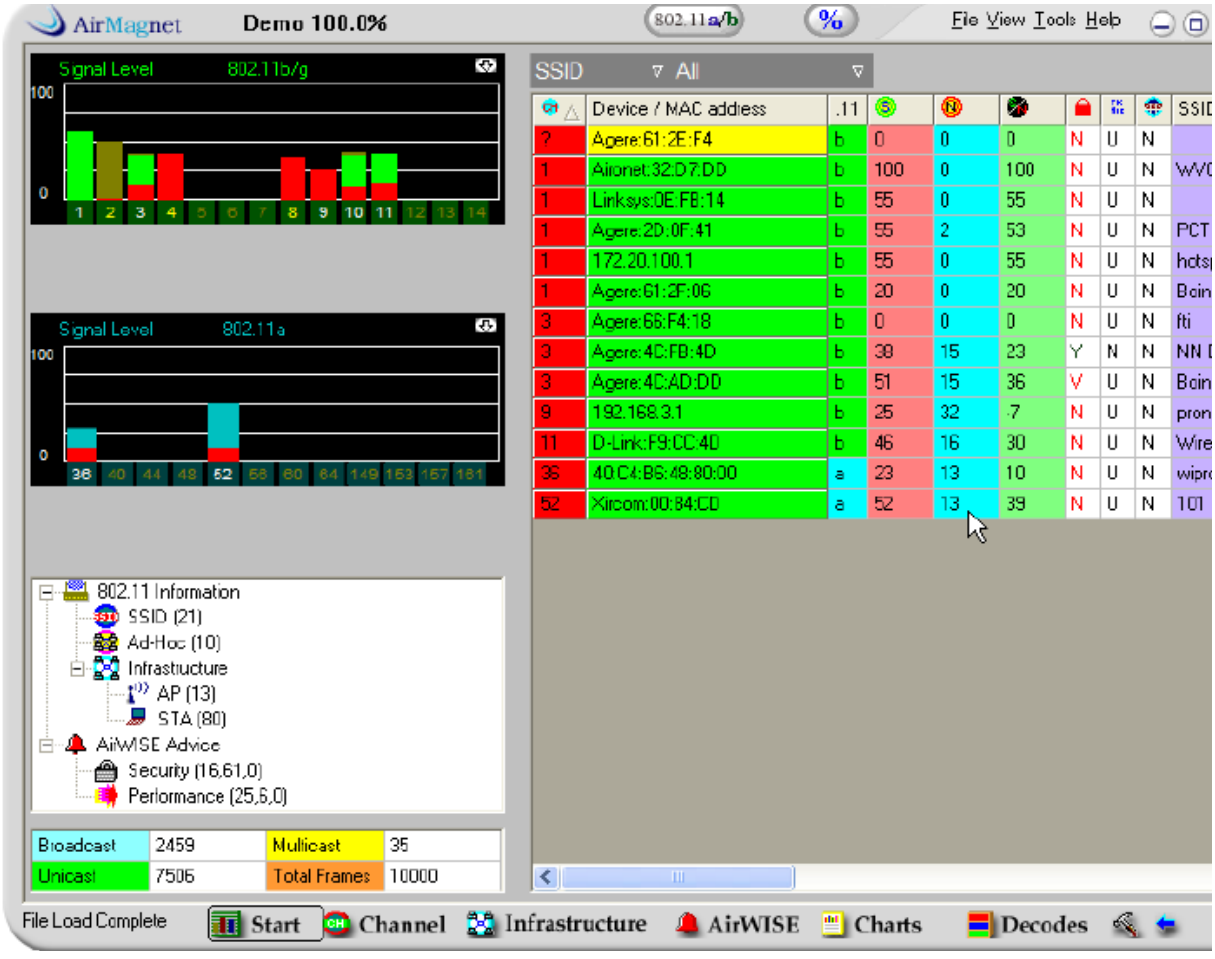
Este *software* é usado para montar e monitorar redes sem fio. Ele ajuda a organizar a forma da rede e sua segurança, com base em rotinas e tarefas que auxiliam o administrador a entender o ambiente WLAN (GOLEMBIEWSKI *et al*, 2006) .

Quando uma WLAN não é projetada de uma forma correta, as conseqüências para a taxa de transmissão e a conectividade podem ser desastrosas, gerando problemas de lentidão (*delay*) na rede. O *AirMagnet* oferece as ferramentas *survey* e *coverage* que dão detalhes dos pontos de acesso e adaptadores de rede *wireless*, avaliando suas condições de cobertura e tráfego. Também traz ferramentas que possibilitam avaliar a qualidade do sinal e identifica possíveis interferências de locais ou equipamentos desconhecidos. Ele gera um mapa de

SSID's (identificadores), com informações de pontos de acesso e estações que estão dentro do alcance da rede (GOLEMBIEWSKI *et al*, 2006).

O *software* ainda oferece arquivos de relatório, que podem ser exportados para o programa Excel, facilitando a criação de gráficos, por exemplo. Abaixo, na figura 13, temos a interface principal do *software*, onde são mostrados os campos com uma lista de SSID's, que são os identificadores dos equipamentos que se encontram no raio de cobertura dos APs. Cada campo compreende o nível de sinal, canal de operação, relação sinal ruído (S/R), se possui ou não criptografia e outras funções (GOLEMBIEWSKI *et al*, 2006).

Figura 13 – Interface do *Airmagnet*



Fonte: GOLEMBIEWSKI *et al* (2006)

4.11 – AirStrike

A arquitetura da WLAN é um aspecto importante para a garantia da segurança dos usuários, do AP e da própria infra-estrutura da rede cabeada. O *AirStrike* tem como compromisso prover segurança durante o acesso a redes sem fio através do ponto de acesso, sem comprometer, com isso, a conectividade dos usuários (AIRSTRIKE, 2007).

O *AirStrike* é uma solução de segurança para redes sem fio (WLAN) baseada no padrão IEEE 802.11a/b/g. Foi fundamentado no sistema operacional *OpenBSD* em conjunto com diversos outros *softwares* de código aberto sobre uma plataforma i386 (AIRSTRIKE, 2007).

Este sistema de segurança gerencia redes sem fio com segurança e confiabilidade, garantindo que somente usuários autorizados terão acesso à rede e que suas mensagens não poderão ser capturadas. Além disso, ele utiliza *softwares* livres para seu funcionamento, possibilitando um desenvolvimento contínuo e facilitando sua integração com os mais variados ambientes de produção (AIRSTRIKE, 2007).

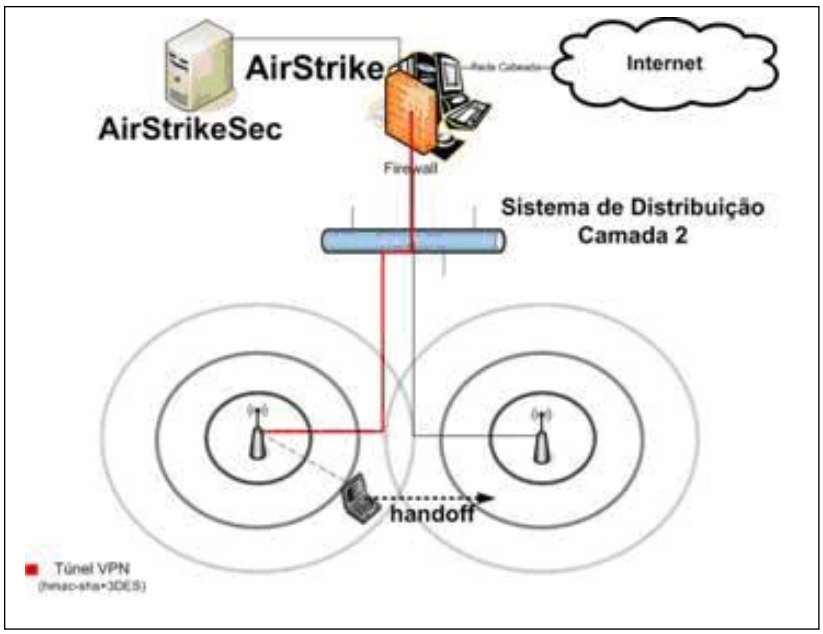
De acordo com AIRSTRIKE (2007), o funcionamento do sistema está relacionado a alguns mecanismos de segurança, como:

- Autenticação: par *login* e senha inseridos no aplicativo cliente.
- Autorização: *firewall*, que através da mudança dinâmica de suas regras permite o acesso seletivo aos recursos da rede.
- Privacidade e Integridade: IPSec, implementação de uma VPN segura.
- *Dead Peer Detection* (DPD) - detecta automaticamente o desligamento de uma estação, e reconfigura as regras de *firewall*.

O *firewall* presente no *gateway* de segurança permite um conjunto restrito de serviços disponíveis às estações da WLAN, dentre eles: DHCP, VPN/IPSec e autenticação. As regras são dinamicamente alteradas após a autenticação de um usuário, de modo a liberar outros serviços ao cliente autenticado. As regras do *firewall* restringem ao máximo a quantidade de portas abertas. Entretanto, o usuário administrador da rede *AirStrike* deve configurar essas regras de acordo com as necessidades do seu ambiente de rede e sua política de segurança AIRSTRIKE (2007).

A figura 14 ilustra a arquitetura deste sistema de segurança.

Figura 14 – Arquitetura de rede do *AirStrike*



Fonte: AIRSTRIKE (2007).

4.12 – Conclusão

Devido a grande instabilidade do meio (ondas eletromagnéticas) onde as informações trafegam, a importância dos mecanismos de segurança para redes sem fio tornou-se o principal foco na utilização deste tipo de rede. Ainda assim, é grande o número de redes totalmente desprotegidas e facilmente alvejadas por atacantes. Tratam-se principalmente de redes domésticas, que sequer habilitam algum recurso de criptografia, mas surpreendentemente algumas redes empresariais são implementadas sem todos os cuidados necessários. Um motivo relevante para esta desproteção seria a facilidade de instalação, aliada a configuração dos equipamentos, que muitas vezes vêm de fábrica sem as medidas de segurança adequadas habilitadas.

Neste capítulo foram apresentadas inúmeras estratégias e medidas de segurança, desde simples configurações nos concentradores até ferramentas especializadas em monitoramento. É importante ressaltar que, para que estas medidas sejam realmente eficazes, elas devem ser usadas de forma combinada, e não isoladamente.

5 – Conclusão

O rápido crescimento das redes w*i-fi* nos últimos anos se deve principalmente a mobilidade propiciada aos usuários, a facilidade de implementação e pela queda de preço dos seus dispositivos. Essa conjunção de fatores vem propiciando uma rápida popularização destas redes, tanto em sua implementação coorporativa quanto pessoal: cada vez mais leigos estão criando redes em suas casas para conectarem dispositivos e compartilharem banda, dados e recursos (AGUIAR, 2005).

Independente do nível de segurança implementado ou possível de ser adotado em redes sem fio, elas sempre apresentarão riscos e vulnerabilidades. Em qualquer caso, o cliente e o concentrador são sempre pontos de possíveis falhas e devem receber atenção especial e constante (RUFFINO, 2005).

Apesar do expressivo avanço e disseminação das redes sem fio, alguns problemas ainda estão sendo solucionados, como é o caso do armazenamento da senha, tanto para o cliente quanto para servidor. Mesmo certificados digitais estão sujeitos a ataques. Como possível solução tem-se o uso de cartões e *tokens* processados, com objetivo de diminuir as possibilidades de fraude e cópia de informações secretas.

O principal problema das redes *wi-fi* refere-se à autenticação, já que outros elementos estão em constante evolução, como algoritmos para criptografia do tráfego, protocolos e freqüências utilizadas. Mesmo com o uso de cartões e *tokens*, há dificuldade de implementação, problemas de escalabilidade e compatibilidade (RUFFINO, 2005).

Outro sério problema em redes sem fio é a facilidade em se praticar ataques do tipo negação de serviço. Não existe solução definitiva para esse problema, porém este pode ser monitorado e com uso de ferramentas adequadas a origem do ataque pode ser facilmente descoberta (RUFFINO, 2005).

Visto que os padrões e protocolos atuais de segurança ainda não são satisfatórios, recomenda-se a utilização de ferramentas de segurança adicionais para aumentar a confiabilidade dos ambientes sem fio. Dentre elas, destaca-se: *Firewalls*, VPNs e *AirMagnet*. A utilização de ferramentas depende muito do tipo de ambiente e recurso a ser utilizado pelos usuários da rede. Não se deve impor que todos os ambientes sem fio tenham os mesmos requisitos de segurança, pois cada um tem objetivos específicos. O uso do *AirMagnet* é indicado por esta ferramenta integrar diversos mecanismos de segurança, como a que realiza o

monitoramento da rede e a detecção de dispositivos estranhos na rede, além de incluir funcionalidades úteis, como a geração de relatórios. Este tipo de *software* constitui-se em um auxiliar precioso para os administradores das redes.

Outra importante recomendação é a constante manutenção e monitoração do ambiente sem fio implementado. Na maioria dos casos é utilizada uma simples configuração dos mecanismos básicos de segurança da rede, sem o posterior acompanhamento do seu estado. Assim cria-se a possibilidade de falhas e vulnerabilidades no ambiente configurado.

Segundo AGUIAR (2005), quando bem projetada, uma rede pode ser tão segura quanto necessário. O que falta é a elaboração de políticas eficientes de segurança nas redes *wireless* que considerem todas as suas particularidades e pontos fracos e que levem em consideração as características do ambiente onde a rede será implantada.

6 - Referências Bibliográficas

AIRSTRIKE. **AirStrike.** 2007 . Disponível em : http://www.airstrike.ravel.ufrj.br/br/conteudo_osistema.htm . Acessado em: 22/06/207

AIRTRAF. **Documentation.** 2004. Disponível em: http://airtraf.sourceforge.net/. Acessado em: 17/05/2007.

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.

CHEOPS-NG. **Description.** 2007. Disponível em: http://cheops-ng.sourceforge.net/index.php . Acessado em: 12/05/2007.

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, Adam; FLEISHMAN, Glenn. **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. 2005

GARUDA. **Documentation.** 2007. Disponível em : http://garuda.sourceforge.net/. Acesssado em: 25/05/2007.

GIMENES, Eder Coral. **Segurança de Redes Wireless.** Mauá, SP. FATEC, 2005, 58p. Trabalho de Conclusão do Curso de Tecnólogo em Informática com ênfase em Gestão de Negócios..

GOLEMBIEWSKI, H. S. D; LUCENA, V. F; SAMPAIO, R. B. **Levantamento da área de cobertura de uma rede wireless 802.11:** um estudo de caso na UNED de Manaus. I Congresso de Pesquisa e Inovação da Rede Norte Nordeste de Educação Tecnológica. Natal – RN, 2006, 15 p.

GRÉGIO, A .R .A. **Wireless Honeynets:** Um Modelo de Topologia para Captura e Análise de Ataques a Redes sem Fio. São José do Rio Preto, SP. UNESP / IBILCE , 2005, 57p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

JUNIOR, A. A. S. C. **Segurança em redes wireless**. Passo Fundo, RS. Universidade de Passo Fundo, 2003, 66p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

JUNIOR, C. A. C; BRABO, G. S; AMORAS, R. A. S. **Segurança em redes wireless padrão IEEE 802.11b:** Protocolos WEP, WPA e análise de desempenho. Belém, PA. Universidade da Amazônia, 2004, 78p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

KISMET. **Documentation.** 2007. Disponível em : http://www.kismetwireless.net/ Acesssado em: 17/05/2007.

NETSTUMBLER. **Documentation** . 2007. Disponível em: http://www.netstumbler.org. Acessado em: 17/05/2007.

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.

SNORT. **The Snort Project.** 2007. Disponível em : http://www.snort.org/. Acesssado em: 25/05/2007.

TEWS, Erik; WEINMANN, Ralf-Philipp; PYSHKIN, Andrei. **Breaking 104 bit WEP in less than 60 seconds.** 2007. 12p.

UTZIG, Jeferson Tiago. **Wireless, uma tendência em comunicação e transporte de informações.** 2006. Disponível em: comp.uniformg.edu.br/plone/artigos2006/ricardo/ Ercomp_Artigo14.doc. Acessado em: 17/05/2007.

WARCHALLING. **Entendendo e vencendo WEP.** 19 de Julho de 2006. Disponível em:https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39&Itemid=2 .Acessado em: 12/05/2007.