Faculdade de Tecnologia de Americana
Curso de Processamento de dados

SEGURANÇA EM REDES WIRELESS

BRUNO REGONHA

Americana, SP
2010

Faculdade de Tecnologia de Americana
Curso de Processamento de dados

SEGURANÇA EM REDES WIRELESS

BRUNO REGONHA

brunoregonha@gmail.com

Monografia apresentada a FATEC Americana, como parte dos requisitos para obtenção do título de Tecnólogo em Processamento de Dados, sob orientação da Prof. Esp. Nelson Gonçalves Júnior

Americana, SP
2010

BANCA EXAMINADORA

Prof. Esp. Nelson Gonçalves Júnior (Orientador)

Prof. Irineu Ambrozano Filho

Prof. José Renato Siqueira Lopes

Epígrafe

“Um telégrafo sem fio não é difícil de entender. O telégrafo normal é como um gato muito longo. Você puxa o rabo em New York e ele mia em Los Angeles. A tecnologia sem fio é a mesma coisa, só que sem o gato”. (EINSTEIN, Albert)

Agradecimentos

Agradeço a minha mãe, Luzia e principalmente meu pai, Luiz Fernando, por sempre acreditarem em mim e no meu potencial, sempre me apoiando e me fornecendo tudo o que eu precisava para concluir este trabalho.

Agradeço ao meu orientador, Prof. Esp. Nelson Gonçalves Junior, pelo suporte dado na elaboração, me auxiliando a corrigir e melhorar este trabalho.

Agradeço aos meus amigos por estarem sempre ao meu lado, me dando apoio e força em todos os momentos que precisei.

Agradeço também a todos aqueles que participaram diretamente e indiretamente deste trabalho.

Dedicatória

Dedico esta monografia a todos aqueles que me ajudaram, de uma forma ou de outra, a chegar até aqui.

Resumo

O presente texto conceitua as redes sem fio (wireless), focando sua segurança. O rápido crescimento desse tipo de rede nos últimos anos é comparado com o crescimento da Internet nas últimas décadas. As redes do padrão 802.11x têm sido amplamente adotadas por instituições e empresas com a finalidade de economia em infra estrutura de cabeamento, além de prover interligação, maior mobilidade e flexibilidade para redes locais. Em contrapartida, mesmo com a ratificação de novos protocolos e surgimento de novas soluções, ainda existem algumas preocupações adicionais em segurança que são inerentes a um meio de comunicação sem fio. Assim, neste trabalho serão tratados os tipos de ataques existentes em redes sem fio, focalizando os padrões IEEE 802.11, e as formas de prevenções e detecções para as mesmas.

Palavras-chave: segurança, redes sem fio, WLAN.

Abstract

The present text conceptualizes the wireless networks, focusing on their security. The fast growth of this kind of networks in last years is compared with growth of Internet in last decades. The standard 802.11 networks had been largely adopted in institutions and companies with the purpose of economy in cables infra-structure, beyond to offer connection, more mobility and more flexibility to local networks. However, even with ratifications of new protocols and development of new solutions, there are some additional concerns about security that are inherent to a wireless communication environment. So, in this work will be treated kind of attacks that exists in wireless networks, focusing on standards IEEE 802.11, and ways to prevent and detect tothem.

Key-words: security, wireless networks, WLAN.

Sumário

Lista de Figuras

.

Lista de Abreviações

AP	*Access Point*
ARP	*Address Resolution Protocol*
AES	*Advanced Encryption Standard*
BSS	*Basic Service Set*
CRC-32	C*yclic Redundancy Check*
D.o.S	*Denail Of Service*
DHCP	*Dynamic Host Configuration Protocol*
EFS	*Encripted File Sistem*
ESS	*Estended Service Set*
EAP	*Extensible Authentication Protocol*
EAP-LEAP	*Extensible Authentication Protocol - Lightweight Extensible Authentication Protocol*
EAP-TLS	*Extensible Authentication Protocol - Transport Layer Security*
EAP-TTLS	*Extensible Authentication Protocol - Tunneled Transport Layer Security*
FTP	*File Transfer Protocol*
GHz	Gigahertz
IAS	*Internal Authentication Server*
ICP	Infra-estrutura de chaves públicas
IEEE	*Institute of Eletrical and Eletronic Engineers*
ICV	*Integrity Check Value*
IPSec	*Internet Protocol Security*
ISM	*Industrial, Scientific and Medical*
LAN	*Local Area Network*
MAC	*Media Access Control*
Mbps	*Megabits per second*
MIC	*Message Integrity Code*
MSCHAPv2	Microsoft *Challenge–Handshake Authentication Protocol* v. 2
NetBEUI	*NetBIOS Extended User Interface*
NetBIOS	*Network Basic Input/Output System*

OSI	*Open Systems Interconection*
PCI	*Peripheral Component Interconnect*
PCMCIA	*Personal Computer Memory Card International Association*
PEAP	*Protected Extensible Authentication Protocol*
RADIUS	*Remote Authentication Dial-In User Server*
RC4	*Route Coloniale* 4
SSID	*Service Set Identifier*
STA	*Stations*
TKIP	*Temporal Key Integrity Protocol*
USB	*Universal Serial Bus*
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 Encriptation Protocol*
WLAN	*Wireless Local Area Network*
WLL	*Wireless Local Loop*
WMAN	*Wireless Metropolitan Area Network*
WPAN	*Wireless Personal Area Network*.
WWAN	*Wireless Wide Area Network*
Wi-Fi	*Wireless-Fidelity*
WiMAX	*Worldwide Interoperability for Microwave Access*

1. Introdução

As redes sem fio têm conquistado gradativamente o mercado da comunicação devido à diminuição dos custos, sua facilidade de implementação e a flexibilidade de uso, que permitiram sua rápida disseminação. Segundo ENGST & FLEISHMAN (2005) iniciou-se de um projeto que ligou as universidades do Havaí em 1971, que conectavam os computadores de quatro ilhas. Elas entraram para o uso da computação pessoal em 1980, quando a idéia de compartilhar dados entre computadores começava a se tornar popular.

As primeiras redes sem fio baseadas em ondas de rádio ganharam notoriedade no início dos anos 90, quando os processadores se tornaram mais rápidos a ponto de suportar tal aplicação. As redes existentes na época eram patenteadas e incompatíveis, por isso, no meio da década de 90 as atenções se voltaram para o novo modelo do IEEE (*Institute of Eletrical and Eletronic Engineers*), o 802.11.

Em 1999 o IEEE finalizou o padrão 802.11b (11Mbps a 2,4GHz). Em 2002, foi distribuído ao mercado o 802.11a (54Mbps a 5GHz), que é incompatível com o padrão 802.11b. No mesmo ano, foi ratificado o padrão 802.11g (54Mbps a 2,4GHz), que opera na mesma velocidade do 802.11a e na mesma freqüência do 802.11b. (ENGST & FLEISHMAN, 2005). E posteriormente o IEEE aprovou oficialmente a versão final do padrão para redes sem fio 802.11n.

Apesar da facilidade de uso deste tipo de rede, suas vulnerabilidades devem ser tratadas de forma a melhorar a proteção da rede.

O **objetivo geral** foi demonstrar como atua uma rede sem fio baseada no padrão IEEE 802.11, demonstrando suas vulnerabilidades e as principais ferramentas de defesa, que podem variar de soluções simples até as mais estruturadas e custosas.

Como **objetivos específicos** devido à simplicidade de uso e de configuração, a segurança tem sido o elemento mais preocupante neste tipo de rede, pois uma pessoa mal intencionada pode obter acesso de modo fácil utilizando uma antena, por exemplo, feita com uma lata tubular com papel alumínio e *softwares* específicos para cada situação.

Para evitar que haja acessos indevidos, este trabalho descreve algumas das ferramentas utilizadas para conter as vulnerabilidades da rede sem fio baseada no padrão IEEE 802.11.

O **método científico** de pesquisa utilizado foi a pesquisa documental, fazendo-se através de referências bibliográficas disponíveis em livros, *sites* e artigos *online*.

O trabalho foi estruturado em cinco capítulos, sendo que o capítulo 1 trata-se de uma introdução ao trabalho, mostrando sua contextualização, objetivo, uma visão geral do trabalho e a metodologia utilizada.

O capítulo 2 conceitua o que são as redes sem fio, seus padrões e componentes.

O capítulo 3 aborda a segurança das redes sem fio, demonstrando os métodos de segurança existentes e as principais ferramentas, como criptografias, lista de endereços MAC e autenticação.

O capítulo 4 descreve alguns tipos de ataques existentes contra redes sem fio, demonstrando como cada um ocorre. Aborda também os métodos de acesso seguro, utilizando VPN e servidores de autenticação RADIUS.

O capítulo 5 se reserva as considerações finais, com base nas informações conseguidas a partir dos estudos realizados nos capítulos anteriores.

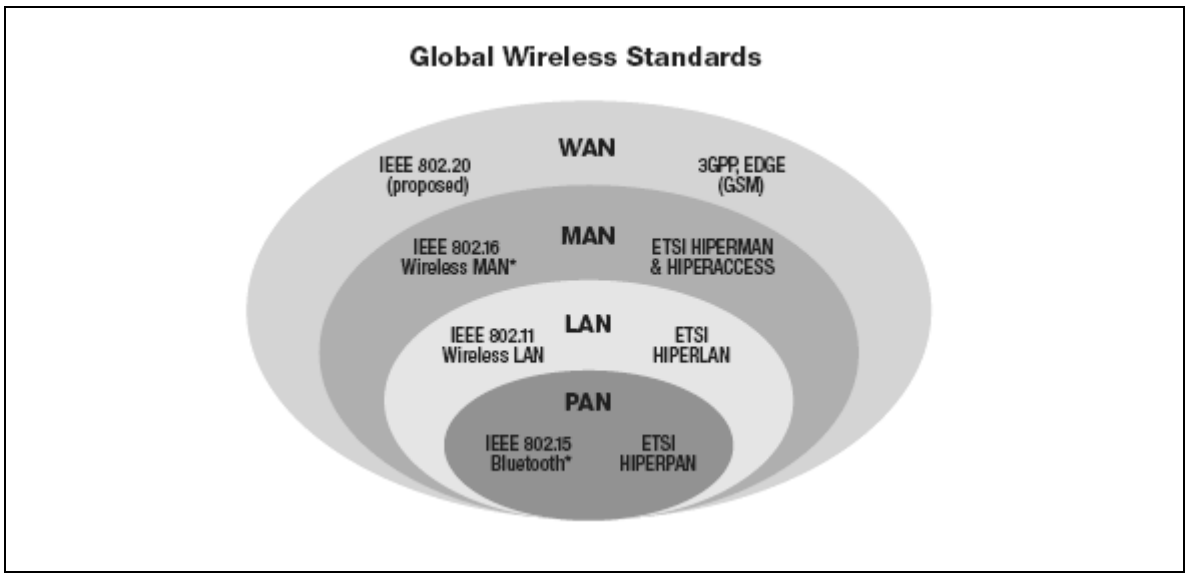
2. Redes Wireless

A palavra wireless, traduzindo significa sem fios (wire: fio, cabo); (less: sem). Portanto caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Existem vários tipos e padrões de redes *wireless*, como por exemplo, o *WiMax, Bluetooth*, *Wi-Fi(Wireless Fidelity)*, *InfraRed*(Infravermelho).

Uma rede *wireless* é reconhecida por ser sem fio, pois o transmissor e o receptor estão se comunicando sem a presença de fios, no nosso caso, por ondas de rádio. (ENGST & FLEISHMAN, 2005)

Se encontram nessa categoria os seguintes tipos de rede: Locais Sem Fio ou WLAN (*Wireless Local Area Network*), Redes Metropolitanas sem Fio ou WMAN (*Wireless Metropolitan Area Network*), por exemplo o WiMAX (*Worldwide Interoperability for Microwave Access*), Redes de Longa Distância sem Fio ou WWAN (*Wireless Wide Area Network*), redes WLL (*Wireless Local Loop*) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (*Wireless Personal Area Network*).

Figura 1: Classificação Pela Abrangência das Redes Sem Fio



Fonte: TEIXEIRA (2005)

Segundo TEIXEIRA (2005), o WiMAX, que utiliza o padrão IEEE 802.16, foi ratificado em Dezembro de 2001, estava focando basicamente as faixas de freqüências situadas entre 10GHz e 66GHz considerando sempre aplicações com linha de visada, obtendo até 34Mbps.

Conforme ENGST & FLEISHMAN (2005), a grande vantagem em instalar uma rede sem fio é a mobilidade. Há alguns anos, essa visão de conectividade sem fios era um tanto quanto futurista, mas hoje a realidade mudou, e tornando possível que aquele e-mail que não poderia esperar por resposta possa ser respondido no meio de uma reunião ou até mesmo no meio do almoço.

2.1 Padrão 802.11

Segundo RUFINO (2005), existem alguns padrões, definidos pelo IEEE (*Institute of Eletrical and Eletronic Engineers*), quando se discute a configuração de uma WLAN:

IEEE 802.11a: é o padrão que descreve as especificações da camada de enlace e física para redes sem fio que atuam na freqüência de 5GHz. Apesar de ter sido firmado em 1999 não existem muitos dispositivos que atuam nesta freqüência.

IEEE 802.11b: inclui aspectos da implementação do sistema de rádio e também inclui especificação de segurança. Esta descreve o uso do protocolo WEP (*Wired Equivalency Privacy)*. Trabalha na ISM de 2.4 GHz e prove 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.

IEEE 802.11d: habilita o hardware de 802.11 a operar em vários países aonde ele não pode operar hoje por problemas de compatibilidade, por exemplo, o IEEE 802.11a não opera na Europa.

IEEE 802.11e: agrega qualidade de serviço (QoS) às redes IEEE 802.11. Em suma, permite a transmissão de diferentes classes de tráfego, além de trazer o recurso de *Transmission Oportunity* (TXOP), que permite a transmissão em rajadas, otimizando a utilização da rede.

IEEE 802.11f: recomenda prática de equipamentos de WLAN para os fabricantes de tal forma que os Access Points (APs) possam interoperar. Define o protocolo IAPP (Inter-Access-Point Protocol).

IEEE 802.11g: baseia-se na compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 54 Mbps. Funciona dentro da frequência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens também são as velocidades. Usa autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia dinâmica (método de criptografia TKIP e AES). Torna-se por vezes difícil de configurar, como Home Gateway devido à sua frequência de rádio e outros sinais que podem interferir na transmissão da rede sem fio.

IEEE 802.11h: versão do protocolo 802.11a (Wi-Fi) que vai ao encontro com algumas regulamentações para a utilização de banda de 5 GHz na Europa. O padrão 11h conta com dois mecanismos que optimizam a transmissão via rádio: a tecnologia TPC permite que o rádio ajuste a potência do sinal de acordo com a distância do receptor; e a tecnologia DFS, que permite a escolha automática de canal, minimizando a interferência em outros sistemas operando na mesma banda.

IEEE 802.11i: trata-se um grupo de trabalho que foi criado para definir uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e 802.11g.

IEEE 802.11n: IEEE aprovou oficialmente a versão final do padrão para redes sem fio 802.11n. Vários produtos 802.11n foram lançados no mercado antes de o padrão IEEE 802.11n ser oficialmente lançado, e estes foram projetados com base em um rascunho (draft) deste padrão. Há a possibilidade de equipamentos IEEE 802.11n que chegaram ao mercado antes do lançamento do padrão oficial serem incompatíveis com a sua versão final. Basicamente todos os equipamentos projetados com base no rascunho 2.0 serão compatíveis com a versão final do padrão 802.11n. Além disso, os equipamentos 802.11n possivelmente precisarão de um upgrade de firmware para serem 100% compatíveis com o novo padrão. As principais especificações técnicas do padrão 802.11n incluem: - Taxas de transferências disponíveis: de 65 Mbps a 600 Mbps. - Método de transmissão: MIMO-OFDM - Faixa de freqüência: 2,4 GHz e/ou 5 GHz.

2.2 Componentes

A topologia de uma rede IEEE 802.11 é composta pelos seguintes elementos:

BSS - *Basic Service Set* - corresponde a uma célula de comunicação *wireless*.

STA - *Stations* - são as estações de trabalho que comunicam-se entre si dentro da BSS.

AP - *Access Point* - funciona como uma *bridge* entre a rede *wireless* e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS. Existem APs que também atuam como roteador, possibilitando o compartilhamento de *Internet* pelos outros micros da rede. Eles vêem de fábrica como servidores DHCP (*Dynamic Host Configuration Protocol*), facilitando a obtenção de um endereço IP na rede. Também conhecido como concentrador.

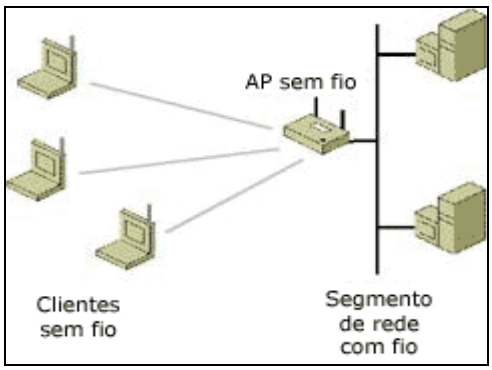
Bridge - Faz a ligação entre diferentes redes, por exemplo, uma rede sem fio para uma rede cabeada convencional..

ESS - *Extended Service Set* - consiste de várias células BSS vizinhas que se interceptam e cujos AP estão conectados a uma mesma rede tradicional. Nestas condições uma STA pode movimentar-se de um BSS para outro permanecendo conectada à rede. Este processo é denominado *Roaming*.

Dois modos de operação são previstos:

Infrastructure mode - quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS).

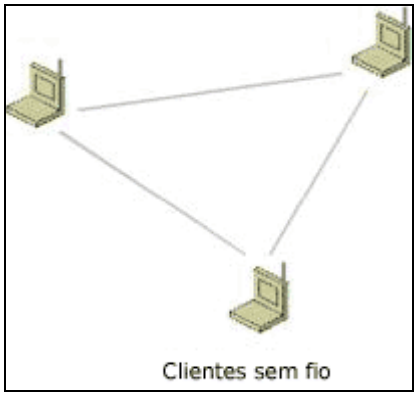
Figura 2: Rede sem fio no modo de infra-estrutura



Fonte: Microsoft Brasil (2004)

Ad-Hoc mode - quando não existe AP e as estações se comunicam entre si diretamente. Este modo não é recomendado pelo padrão.

Figura 3: Rede sem fio no modo *Ad Hoc*



Fonte: Microsoft Brasil (2004)

Existem vários tipos de hardwares para acessar uma rede sem fio, como placas USB (externas), placas PCI(internas) e adaptadores de placas *Ethernet*.

3. Segurança de Redes Wireless

A explosão das redes sem fio não é nenhuma surpresa para as empresas atuais. Isso se deve ao grande aumento de produtividade que as tecnologias sem fio proporcionam o que é difícil de ser ignorado. Em um recente estudo, a Gartner descobriu que funcionários com *notebooks* atingiram um aumento de produtividade de meia hora a três horas, comparado aos usuários de *desktops*. Quando a conexão sem fio é adicionada a esses notebooks, ocorre um aumento de até 11 horas de produtividade adicional por semana.

Porém, as redes sem fio vêm também acompanhadas de desvantagens significativas e talvez a segurança seja a principal delas. A segurança é um dos três maiores problemas enfrentados por gerentes de TI, com relação às redes sem fio e computação remota.

Os principais problemas de segurança com relação aos sistemas sem fio incluem:

- Intercessão de transmissão sem fio à medida que viaja via aérea.
- Perda de um dispositivo portátil, comprometendo os dados nele contidos.
- "Relacionamentos de confiança" quando os dispositivos sem fio são usados para comércio (por exemplo, para a o envio de pedidos ou compras).

Para lidar com esses problemas, as empresas precisam determinar procedimentos muito específicos para o uso de dispositivos sem fio, incluindo as funções para as quais os mesmos podem ser usados, o que pode ou não ser armazenado e qual a tecnologia de segurança que deve estar instalada, para evitar que os dados sejam comprometidos, no caso de roubo do dispositivo.

A definição de políticas e padrões para os dispositivos sem fio é imprescindível. Por exemplo, sempre que uma LAN sem fio for ativada, a tecnologia VPN deve ser implementada. Além disso, notebooks com recursos sem fio devem ter proteção antivírus e de *firewall* instaladas.

Mas a segurança não termina aí. Uma rede sem fio pode realizar transmissões em distâncias muito além de um prédio, permitindo a qualquer um que esteja por perto ou até mesmo passando perto de uma instalação, espreitar dados. Só é necessária uma antena potente e um software de hacker facilmente disponível no mercado.

A rede deve estar operante e garantir:

- Confiabilidade – O sinal transmitido pela rede pode ser captado por qualquer receptor atuante na área em que o sinal estiver ativo.
- Integridade da Informação – Garantir que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor.
- Disponibilidade da Rede – Manter a rede acessível.
- Autenticidade – Fazer com que a autenticação para o acesso à rede ocorra.

3.1 Posicionamento Físico

Segundo RUFINO (2005), a segurança física em uma rede cabeada era constituída em proteger o acesso físico a um computador que estivesse ligado à rede ou mesmo, proteger ou desativar um ponto de rede não utilizado.

Para este tipo de segurança, basta proteger o acesso das pessoas, mas, em uma rede sem fio, onde os dados trafegam pelo ar, o perímetro a ser coberto pela segurança seria de metros e metros, as vezes, além das paredes da empresa. (RUFINO, 2005)

Para acessar uma rede sem fio, basta estar munido de dispositivos de acesso a ela e se posicionar de forma a obter um sinal cuja potência permita uma conexão.

Para ajudar a minimizar o problema de acesso não permitido, algo a se levar em conta quando se for construir uma rede sem fio é a posição do *Access Point*, para que as ondas eletromagnéticas fiquem centralizadas, minimizando a área coberta pela rede fora do perímetro desejado. (RUFINO, 2005)

3.2 Configurações

Os concentradores, também conhecidos por *Access Point*, são, em geral, pré-configurados ainda na fábrica, para facilitar a instalação da rede. (RUFINO, 2005)

A instalação da rede, por falta de conhecimento ou simplesmente por desatenção e despreocupação, as pessoas não alteram as configurações de fábricas dos concentradores.

As configurações de fábricas não habilitam os mecanismos de segurança, tornando o tráfego da rede mais vulnerável a um ataque. Praticamente todos os aparelhos possuem uma configuração padrão de fábrica, desde de o SSID (*Service Set Identifier*), endereços IPs e senhas, por tanto, o acesso indevido a rede se torna fácil e simples. (RUFINO, 2005)

3.2.1 Configuração Aberta

De acordo com RUFINO (2005), este tipo de configuração é caracterizado pelo envio do SSID da rede pelo AP, ou seja, ele aceita conexões de qualquer pessoa cuja compatibilidade de hardware seja atendida.

Ao requisitar conexão, o concentrador possui um servidor DHCP (*Dynamic Host Configuration Protocol*), provendo um endereço IP válido para a rede, liberando o acesso à ela. (RUFINO, 2005)

3.2.2 Configuração Fechada

Neste modo de configuração, o concentrador não envia o seu SSID, portanto, só permitindo conexão aqueles que souberem o SSID da rede. (RUFINO, 2005)

Para um atacante, basta “escutar” o tráfego desta rede para determinar seu SSID correto, podendo assim acessar a mesma. (RUFINO, 2005)

3.3 Endereçamento Físico

Outra forma de proteção de acesso a uma rede *wi-fi*, segundo RUFINO (2005), é definir os endereços físicos acessíveis a esta.

Endereçamento físico, também conhecido por endereçamento MAC, faz parte da camada de Enlace do modelo OSI (*Open Systems Interconection*).

Todo dispositivo de rede possui um endereçamento físico (*Media Access Control*). Antigamente, os endereços físicos não eram únicos, os fabricantes produziam placas cujos endereços físicos eram iguais, ocasionando alguns conflitos. Atualmente, todo dispositivo de rede possui um endereço físico único.

Pode-se configurar um AP para receber conexões apenas dos endereços físicos definido pelo administrador. Este dispositivo 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 que tem o acesso liberado à mesma. (RUFINO, 2005)

Existem algumas desvantagens em utilizar este tipo de autenticação, pois, é necessário obter manualmente os endereços físicos e cadastrá-los manualmente no concentrador. (RUFINO, 2005)

Além de trabalhoso, as alterações podem ser mais freqüentes dependendo da alternância entre os usuários.

Para se conectar a uma rede *w-fi* é necessário ter um dispositivo que atenda os padrões da rede, como placas PCI (internas), adaptadores USB, adaptadores *Ethernet* e cartões e placas PCMCIA. Em geral, estes dispositivos são portáteis e removíveis, ou seja, uma pessoa mal intencionada pode obter um *hardware* que tem permissão para acessar a rede e pluga-lo em seu computador, obtendo assim, o acesso a rede.

Outra desvantagem é que por obtenção do tráfego, que contem o endereço MAC dos dispositivos, o atacante com um endereço físico válido de acesso à rede pode renomear o endereço físico de sua placa e obter o acesso. (RUFINO, 2005)

Para alterar o endereço físico no *Windows* (somente as versões 2000, XP e 2003), segundo RUFINO (2005), utiliza-se o caminho: conexões de rede, propriedades da rede local, configurar, avançado e *NetwrokAddress*.

Um outro modo de obter um endereço MAC válido é utilizar a força bruta, testando repetidamente endereços MAC aleatórios, podendo criar uma lista de acesso para determinada rede.

3.4 Criptografia

Uma forma de proteção aos dados trafegados na rede é a criptografia. Caso um atacante tente obter os dados trafegados na rede, a criptografia vai cuidar de deixar todos os dados fora de uma ordem lógica e entendível. (ENGST & FLEISHMAN, 2005)

3.4.1 WEP

O *Wired Equivalency Privacy* (WEP) opera na camada de enlace de dados e fornece criptografia entre o cliente e o *Access Point*. O WEP 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.

O WEP trouxe como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o SSID e a lista de endereços físicos permitidos, também conhecido por endereço MAC (*Media Access Control*).

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão *WI-FI*, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede. (MICROSOFT , 2004)

Segundo RUFINO (2005), alguns programas largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede captando alguns pacotes. Como disse o WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas por softwares como *AirSnort* ou *WEPCrack*. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.

O WEP vem desativado na maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que será preciso definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. Nas estações a chave, assim como o endereço SSID e outras configurações de rede podem ser definidas através de outro utilitário, fornecida pelo fabricante da placa. (RUFINO, 2005)

3.4.2 WPA

Com os problemas de segurança no WEP, a *Wi-Fi Alliance* adiantou a parte de autenticação e certificação elaboradas para o 802.11i e liberou o protocolo WPA (*Wi-Fi Protected Access*).

Apesar de avanços terem ocorridos nesse protocolo, a maioria deles requer novos elementos na infra-estrutura da rede e ainda deve trabalhar em conjunto com outros protocolos, como o 802.1x.

Na versão 1 do WPA não há suporte à conexões *Ad-Hoc*, portanto, apenas as redes utilizando um concentrador podem fazer uso deste recurso.

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

O WPA2 foi ratificado em meados de 2004 corresponde a versão final do WPA, a diferença entre WPA e WPA2 e que o WPA utiliza o algoritmo RC4 o mesmo sistema de encriptação utilizado no WEB o TKIP (*Temporal Key Integrity Protocol*), enquanto o WPA2 se basea na criptografia (*Advanced Encryption*

Standard) mais segura que a TKIP, mas exige mais processamento e algumas placas mais antigas não suportam o WPA2 nem mesmo atualizado a firmware.

3.4.2.1 Mecanismos de Criptografia WPA

O WPA (*Wi-Fi Protected Access*) possui diferentes modelos de segurança, adaptável ao tipo do uso em que ele será implementado, uma para aplicações pequenas, como redes domésticas e pequenos escritórios, utilizando uma chave previamente compartilhada (Pré-shared key ou WPA-PSK), sendo responsável pelo reconhecimento do aparelho. Outro método é conhecido como infra-estrutura, adicionando um servidor RADIUS (*Remote Authentication Dial-In User Server*) para autenticação, podendo ainda necessitar de uma infra - estrutura de chaves públicas (ICP), caso se utilize certificados digitais para autenticar usuários. (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 melhor adequado em redes pequenas onde os participantes estão acessíveis na maior parte do tempo. Não existem ainda problemas divulgados nos protocolos usados com WPA-PSK.TKIP, responsável pela troca dinâmica das chaves. (RUFINO, 2005)

O protocolo TKIP (*Temporal Key Integrity Protocol*) é o responsável pelo gerenciamento da troca de chaves, no WEP as chaves eram estáticas e seu vetor de inicialização era de apenas 24bits, passando agora para 48bits. (RUFINO, 2005)

O TKIP pode ser programado para alterar o vetor de inicialização a cada pacote, por sessão ou por período, tornando mais difícil a obtenção do mesmo via captura de tráfego.

“Com 802.11 e WEP, a integridade dos dados é fornecida por um valor de verificação de integridade, o ICV (*Integrity Check Value*) de 32-bit que aparece com a carga útil 802.11 e é criptografado com WEP. Embora o ICV esteja criptografado, pode-se alterar os bits na carga criptografada e atualizar o ICV criptografado sem ser detectado pelo receptor.

Com WPA, um método conhecido como *Michael,* específica um novo algoritmo que calcula um código de integridade da mensagem, o MIC (*Message*

Integrity Code) de 8 bytes usando os recursos de cálculo disponíveis nos dispositivos existentes. O MIC está localizado entre a parte de dados do quadro 802.11 do IEEE e o ICV de 4 bytes. O campo MIC é criptografado com os dados do quadro e o ICV.

Michael também ajuda a fornecer proteção à reexecução. Para ajudar a evitar ataques de repetição, é usado um novo contador de quadros no IEEE 802.11." (MICROSOFT, 2004)

No WPA também foi inserido um modelo para autenticação de usuários, conhecido como EAP (*Extensible Authentication Protocol*), que utiliza o padrão 802.11x 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. (MICROSOFT, 2004)

Uma das vantagens em se utilizar equipamentos adicionais para a autenticação do usuário é de ter uma base centralizada, onde todos os métodos de acesso (não apenas *wi-fi*, mas cabeadas e/ou discadas também) utilizem a mesma forma, sem a necessidade de manter uma sincronização. (MICROSOFT, 2004)

3.4.3 Criptografia WPA2

De acordo com a publicação da Microsoft (2004) WPA2 é uma certificação de produto disponível por meio da *Wi-Fi Alliance* que certifica equipamentos sem fio como sendo compatíveis com o padrão 802.11i. O WPA2 oferece suporte aos recursos de segurança obrigatórios adicionais do padrão 802.11i que não estão incluídos em produtos que oferecem suporte ao WPA. Com o WPA2, a criptografia é realizada com o AES (*Advanced Encryption Standard*), que também substitui o WEP por um algoritmo de criptografia bem mais forte. Como o TKIP do WPA, o AES permite a descoberta de uma chave de criptografia de difusão ponto a ponto inicial exclusiva para cada autenticação, bem como a alteração sincronizada da chave de criptografia de difusão ponto a ponto para cada quadro. Como as chaves AES são descobertas automaticamente, não há necessidade de

se configurar uma chave de criptografia para o WPA2. O WPA2 é a modalidade de segurança sem fio mais forte.

Como talvez não seja possível agregar suporte AES por meio de uma atualização de *firmware* ao equipamento existente, o suporte a AES é opcional e depende do suporte ao *driver* do fornecedor. (MICROSOFT, 2004)

3.5 Softwares Complementares

3.5.1 *Firewall*

Segundo Luiz Carlos dos Santos, *firewall* é o mecanismo de segurança interposto entre a rede interna e a rede externa com a finalidade de liberar ou bloquear o acesso de computadores remotos aos serviços que são oferecidos em um perímetro ou dentro da rede corporativa. Este mecanismo de segurança pode ser baseado em hardware, software ou uma mistura dos dois.

A função do *firewall* é bloquear tráfego malicioso, que poderia colocar em risco os computadores da rede. Eles examinam o tráfego a fim de procurar por certos padrões ou se tem por alvo recursos vulneráveis. O trafego que possui os padrões definidos são descartados para que não cheguem ao seu destino final. (ENGST & FLEISHMAN, 2005)

"A maioria dos *Gateways* (*access point*) oferece recursos de *firewall* que permitem filtrar tipos específicos de tráfego, como aquele destinado a um dado serviço *Internet*. A maioria desses *firewalls* é simples, permitindo limitar todo o tráfego que entra que não seja uma resposta a uma solicitação feita ou a serviços *Internet* específicos, como FTP.

Como boa parte dos *gateways* também inclui múltiplas portas *Ethernet*, você pode criar um *firewall* não apenas entre sua conexão *Internet* de banda larga – conectada à porta de rede remota – e seus computadores e dispositivos sem fio, mas também entre a rede sem fio e quaisquer máquinas conectadas a portas *Ethernet* da rede local (LAN) no *gateway*". (ENGST & FLEISHMAN, 2005)

3.5.2. Monitoramento da Rede *Wi-Fi*

Da mesma forma que muitos administradores monitoram o seu ambiente de rede convencional (com o uso de IDSs, por exemplo), a monitoração da rede *wireless* também é importante. Essa monitoração pode detectar:

- Clientes conectados em um dado instante (em horários improváveis ou simplesmente para acompanhamento);
- Instalação de APs não autorizados;
- Dispositivos que não estejam usando WEP;
- Ataques contra os clientes *wireless*;
- Acessos não autorizados;
- Mudanças de endereços MAC;
- Mudanças de canal;
- DoS.

4. Vulnerabilidades e Métodos de Acesso Seguros

4.1 Vulnerabilidades Exploradas nas Redes Wi-Fi

"Não existe nenhuma grande novidade nos ataques às redes sem fio. Grande parte destes ataques não sofreu nenhuma modificação em relação aos ataques às redes cabeadas. Outros, no entanto, tiveram que sofrer algumas modificações a fim de obter melhores resultados.

Como as redes cabeadas tradicionais têm sido atacadas de maneira impiedosa durante mais de trinta anos e com o crescimento da *Internet* muitas destas redes desenvolveram excelentes mecanismos de defesa.

Podemos citar como exemplo de uma política de defesa bem estabelecida o uso de um *firewall* propriamente configurado. Entretanto, se esta mesma instituição possuir uma rede sem fio mal configurada atrás deste *firewall*, todos os cuidados tomados com a rede cabeada poderão se tornar ineficientes. Seria mais ou menos como se existisse um *backdoor* instalado nesta rede.

Atualmente, dificilmente existe alguma rede WLAN que não tenha ou não venha a sofrer de pelo menos um tipo de ataque. Tais ataques não são limitados a instituições, mas também têm como alvo os consumidores domésticos, visto o crescente uso de equipamentos sem fio por consumidores domésticos. A seguir, são apresentados os ataques mais comuns e os que mais se destacam atualmente nas redes sem fio ". (BABOO, 2005)

4.1.1 Access Point Spoofing (Associação Maliciosa)

A associação maliciosa ocorre quando um atacante, passando-se por um *access point*, engana um outro sistema de maneira a fazer com que este acredite estar se conectando a uma WLAN real. (BABOO, 2005)

O atacante tenta se valer de uma vulnerabilidade do NETBEUI - NetBIOS Extended User Interface (Interface de Usuário Estendida NetBIOS) - que permite compartilhamento de arquivos e impressoras em sistemas Windows. Entretanto a partir do passo quatro, qualquer vulnerabilidade existente no cliente pode ser explorada pelo atacante.

Existe uma sutil diferença entre fazer a associação maliciosa através da utilização de um *software* ou da associação através de redes *Ad Hoc*. Diferença esta existente na grande difusão dos riscos em se manter um dispositivo configurado para atuar em *Ad Hoc*. Com isso, muitos usuários e até mesmo sistemas operacionais evitam este tipo de conexão, permitindo somente conexões em sistemas de infra-estrutura básica ou sistemas infra-estruturados. (BABOO, 2005)

4.1.2 Envenenamento ARP

O ataque de envenenamento (ARP *Poisoning*) do protocolo de resolução de endereços (ARP, *Address Resolution Protocol*) não é um ataque novo, porém a forma de concepção dos *access points* e a implicação da arquitetura de rede gerada por este *access point* faz com que esta rede seja particularmente vulnerável a esta forma de ataque. 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 vitima. (BABOO, 2005)

Deste modo, este tipo de ataque se limita às redes que estejam conectadas por *hubs*, *switches* ou por *bridges*. Deixando de fora as redes conectadas por roteadores e *gateways*. (BABOO, 2005)

A maioria dos *access points* disponíveis hoje no mercado atuam como um *bridge* entre a rede cabeada e a rede sem fio. Desta forma, um ataque que utilize-se de ARP *Poisoning*, como é o caso do ataque do homen-no-meio, pode ser disparado de uma estação da WLAN a uma estação cabeada. Ou seja, abre-se caminho, através da rede sem fio, a um ataque à rede cabeada. (BABOO, 2005)

Este tipo de ataque utiliza-se de pacotes de ARP *reply* para fazer o *cache poisoning*. O atacante, um *host* C, envia um pacote de ARP *reply* para B dizendo que o IP de A aponta para o endereço MAC de C. De maneira semelhante envia um pacote de ARP *reply* para A dizendo que o IP de B aponta para o endereço MAC de C. Como o protocolo ARP não guarda os estados, os *hosts* A e B assumem que enviaram um pacote de ARP *request* pedindo estas informações e assumem os pacotes como verdadeiros. (BABOO, 2005)

A partir deste ponto, todos os pacotes trocados entre os *hosts* A e B necessariamente passam por C. Portanto o *host* C deve se encarregar de reenviar os pacotes para os devidos destinos após capturá-los. (BABOO, 2005)

4.1.3 MAC Spoofing

Existem muitas instituições que criam listas de acesso para todos os dispositivos explicitamente permitidos à conexão. Estas instituições costumam fazer este controle através do endereço MAC da placa do cliente, banindo desta forma o acesso de outras placas não autorizadas. (RUFINO, 2005)

Entretanto, é sabido que os dispositivos usados nas redes sem fio possuem uma particularidade: a de permitir a troca do endereço físico. Desta maneira, qualquer atacante mal intencionado pode capturar através de técnicas de *Eavesdrooping & Espionage* um endereço MAC válido de um cliente, efetuar a troca de seu próprio endereço pelo do cliente e utilizar a rede como um usuário autorizado. (RUFINO, 2005)

Além deste tipo de MAC *Spoffing*, existe o MAC *Spoffing* da placa de rede cabeada dos *access points*. Ou seja, os *access points* são capazes de trocar seus endereços MAC das placas de redes tradicionais. Assim, nem mesmo os *firewalls* internos a LAN forneceriam segurança suficiente contra este tipo de ataque. (BABOO, 2005)

4.1.4 Ataques de Negativa de Serviço

Também conhecido por D.o.S (*Denail Of Service*), cujo próprio nome indica tornar algum recurso ou serviço indisponível. Em redes sem fio estes ataques podem ser tão perturbadores quanto maior sua sofisticação.

Estes ataques podem ser disparados de qualquer lugar dentro da área de cobertura da WLAN. Como as redes 802.11b e 802.11g trabalham na radiofreqüência de 2.4 GHz e esta é utilizada por fornos microondas, aparelhos de monitoramento de crianças e recentemente por telefones sem fio, estes produtos

podem facilitar os ataques de negativa de serviço, através da inserção de ruídos a partir destes aparelhos nas redes sem fio. (RUFINO, 2005)

No entanto, *hackers* podem se utilizar de técnicas mais sofisticadas para gerar algum tipo de ataque. Um exemplo é o de quando um hacker se passar por um access *point* com o mesmo SSID e endereço MAC de um outro *access point* válido e inunda a rede com pedidos de dissociação. Como estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se reassociarem. Desta maneira, os usuários desta rede passam a não poder ficar muito tempo conectados a ela. (RUFINO, 2005)

4.1.5 WLAN Scanner (Ataques de Vigilância)

Mesmo não sendo considerado ataque para muitos estudiosos, pode se tornar um ataque com um grau de comprometimento muito grande dependendo da finalidade para a qual se utiliza este tipo de ataque.

É conhecido por ataque de vigilância porque consiste em se percorrer a cidade ou o local onde se deseja invadir, observando se existe ou não uma WLANs sendo usada. Para efetuar este tipo de ataque, não existe a necessidade de nenhum equipamento especial. Apenas um dispositivo sem fio. (RUFINO, 2005)

O que se pretende através deste tipo de ataque é encontrar fisicamente os dispositivos de redes sem fio para que, numa outra etapa posterior, estes dispositivos possam ser invadidos. Podendo ainda ter sua configuração retornada à configuração padrão ou ainda ser roubado. (RUFINO, 2005)

Neste caso um hacker pode invadi-lo, conseguindo gerar ataques dentro da porção guiada da rede, representando assim um grande risco a exposição de equipamentos.

4.1.6 Wardriving

Wardriving é uma forma de ataque muito parecida com a anterior. Modifica-se somente a forma de como as WLANs são encontradas. Neste tipo de ataque

são utilizados equipamentos configurados para encontrar o máximo de redes sem fio que estiverem dentro da área de abrangência do dispositivo de monitoramento. (BABOO, 2005)

Muitas *homepages* como o "wardriving.com" dão instruções detalhadas de como efetuar o *wardriving*. Outras como a "*wardriving is not a crime*" tem como tem como principal objetivo fazer apologia ao *wardriving*. Chama atenção o fato de existir uma distribuição *WarLinux* (http://sourceforge.net/projects/warlinux/) concebida única e exclusivamente para *wardriving*.

4.1.7 Warchalking

Inspirado em prática surgida na Grande Depressão norte-americana, quando andarilhos desempregados (conhecidos como "*hobos*") criaram uma linguagem de marcas de giz ou carvão em cercas, calçadas e paredes, indicando assim uns aos outros o que esperar de determinados lugares, casas ou instituições onde poderiam conseguir comida e abrigo temporário.

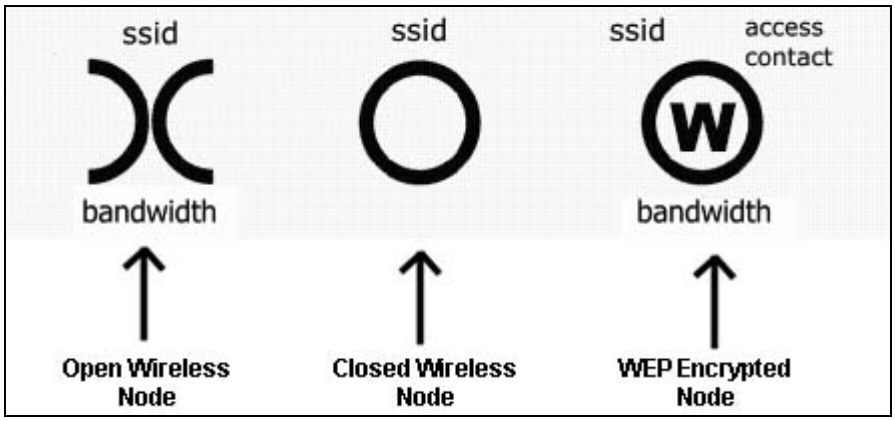
Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas de *wardriving* e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. (BABOO, 2005)

Isto para que outros atacantes possam de antemão saber quais as características da rede. Existem grupos organizados para *warchalking* que utilizam-se de símbolos próprios para marcar as redes numa tentativa de mantê-las em segredo. (BABOO, 2005)

Existem também grupos rivais que tentam encontrar e pichar o maior número de redes possível para ganhar mais status. Seriam como os grupos de *defacers* de páginas da *Web*, mas realizados fisicamente.

Segue um exemplo dos símbolos utilizados nesta ação.

Figura 4: Símbolos do *Warchalking*



Fonte: Communication Services Incorporated (CSI). (2005)

O primeiro símbolo significa uma rede *wi-fi* aberta, descrevendo seu SSID (nome da rede) e sua *Bandwidth* (largura da banda, a velocidade que se obtém dessa rede).

O segundo símbolo significa uma rede fechada, descrevendo apenas o SSID (nome da rede).

O terceiro símbolo descreve uma rede protegida pelo protocolo de criptografia WEP, junto com o SSID (nome da rede), o *access contact* (chave WEP utilizada) e a *bandwidth* (velocidade da rede).

4.2 Métodos de Acesso Seguros

4.2.1 VPN

Virtual Private Network ou Rede Privada Virtual é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a *Internet*.

O sigilo do tráfego da rede, a autenticação inicial dos usuários, a integridade das mensagens da rede sem fio serão garantidos através da implementação de uma VPN segura, para tanto utiliza-se do protocolo IPSec a fim de garantir a privacidade virtual da rede e a segurança das eletrônicas que por ela passam.

Nesta arquitetura todo o tráfego entre as estações e o AP é encriptado independente do destino dos pacotes enviados pelas estações. A VPN poderia ser configurada de forma que somente alguns pacotes com endereços de destino definidos fossem encriptados.

No estabelecimento de um túnel IPSec (*Internet Protocol Security*) todo o pacote IP é protegido e todas as mensagens provenientes das estações saem com o endereço do AP como endereço de destino. Garante-se com esta última característica uma privacidade maior para os usuários, dificultando a análise passiva do tráfego da rede.

O servidor VPN pode se tornar um gargalo. Todo o acesso do cliente WLAN será canalizado pelo servidor. Os dispositivos VPN tradicionalmente atendem muitos clientes remotos de baixa velocidade. Ser solicitado a controlar a taxa de transferência de um grande número de clientes que funcionam na velocidade total da LAN significará que muitos dispositivos VPN não conseguirão atender mais de poucas dezenas ou centenas de clientes. (MICROSOFT, 2004)

O foco deste trabalho se prende a estudar métodos e processos que tornam uma comunicação sem fio no padrão IEEE 802.11. Uma VPN pode ser usada para qualquer tipo de meio de transmissão de dados (redes cabeadas, *wi-fi*, infravermelho, etc), portanto, para proteger as informações de uma rede *wi-fi* recomenda-se que se utilize dos protocolos de criptografia específicos para este

tipo de rede (WEP ou WPA), pois possuem um determinado nível de segurança e não causam tanto impacto a performance da rede quanto uma VPN causa.

4.2.2 RADIUS

O primeiro passo é realizado pelo usuário que deseja acessar a rede, encaminhando uma mensagem contendo seu *login* e senha para o cliente RADIUS (*Remote Authentication Dial-In User Server*).

Ao receber a mensagem do usuário o cliente RADIUS gera uma requisição contendo os dados do usuário, encaminhando-a para o servidor RADIUS. Uma mensagem de resposta é aguarda por um determinado tempo, porém caso essa mensagem não chegue, o cliente poderá encaminhar uma nova requisição para o mesmo servidor ou para um servidor RADIUS alternativo. (MICROSOFT, 2007)

Quando recebe uma requisição a primeira ação do servidor é validar o cliente RADIUS o qual encaminhou a mensagem de requisição, evitando dessa forma que um “falso” cliente consiga realizar alguma operação. Tratando-se de um cliente válido, os dados referentes ao usuário, encaminhados na requisição, serão verificados. Não apenas seu *login* e senha, mas também a porta através da qual o usuário entrou em contato com o cliente RADIUS será validada. (MICROSOFT, 2007)

Após validar as informações a respeito do usuário o servidor RADIUS encaminha uma resposta para o cliente, negando o acesso caso as informações não sejam válidas, ou permitindo o acesso a rede caso contrário. Quando o servidor permite o acesso encaminha junto a resposta enviada ao cliente, os direitos e permissões referentes ao tipo/nível de acesso permitido ao usuário em questão. (MICROSOFT, 2007)

5. Considerações finais

A partir da apresentação e análise dos dados, este trabalho conclui que uma rede sem fio é de extrema facilidade de uso e configuração, possibilitando uma mobilidade excelente que pode ser utilizada como diferencial para as empresas.

Sua implantação é simples, descartando a necessidade de grandes reformas onde uma rede cabeada precisaria estar passando fios por paredes ou caneletas especiais, devido a esta facilidade, o uso deste tipo de rede atrai cada vez mais usuários.

Como todo ambiente lógico não é totalmente seguro, as redes sem fio têm suas vulnerabilidades, atualmente existem vários processos que ajudam a tornar um ambiente *Wireless* seguro, mesmo não garantindo que a rede seja totalmente segura.

É importante ressaltar que utilizar uma rede sem fio requer maior preocupação com a segurança para se garantir uma maior privacidade dos dados ali trafegados, pois o meio em que ela trafega é o ar, potencializando que uma pessoa mal intencionada possa usufruir do sinal fora do perímetro físico, atravessando paredes e invadindo o meio externo, facilitando a ação do sujeito.

Qualquer barreira levantada contra o invasor é melhor do que simplesmente deixar a rede aberta e totalmente vulnerável.

Esta pesquisa não encontrou motivos para não utilizar uma rede sem fio, elas são versáteis e úteis em muitos casos, desde que se faça uso de seus métodos e ações para garantir a privacidade das informações transitadas e aumentar a sensação de que o ambiente sem fio é seguro.

Utilizando os métodos explanados no capítulo 6.1, ou seguindo as orientações do fabricante é possível se obter um nível satisfatório de segurança, respeitando as limitações técnicas e econômicas do usuário.

6. Referencial Bibliográfico

BABOO, Fórum. **5. Ataques às Redes Sem Fio**. 2005. Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=335352 . Acessado em: 16/04/2010.

CERT. **Práticas de Segurança para Administradores de Redes *Internet*,** 4.13.6. Monitoração da Rede *Wireless*. 2003. Disponível em: http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#sec2 . Acessado em: 17/04/2010.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão do Curso de Bacharel em Ciência da Computação. UNESP São José do Rio Preto. 2003. Disponível em: http://www.apostilando.com/download.php?cod=230&categoria=Redes . Acessado em: 06/04/2010.

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.

INCORPORATED, Communication Services. **Warchalking**; 2005. Disponível em: http://www.1csi.com/warchalking.html. Acessado em: 18/04/2010.

MICROSOFT. **Protocolo RADIUS.** 2007. Disponível em: http://technet.microsoft.com/pt-br/library/cc781821(WS.10).aspx . Acessado em: 14/04/2010.

MICROSOFT. **Visão Geral da Atualização de Segurança WPA Sem Fio no Windows XP.** 2005. Disponível em: http://support.microsoft.com/kb/815485/pt-br . Acessado em: 16/04/2010.

RUFINO, Nelson Murilo de Oliveira. **Segurança de Redes Sem Fio**. 1ª ed. São Paulo: Ed.: Novatec, 2005.

SYMANTEC. **Implementando Uma LAN Sem Fio Segura.** 2003. Disponível em: http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html . Acessado em: 18/04/2010.

TEIXEIRA, Edson Rodrigues Duffles. **Tutoriais: Banda larga e VOIP.** 2005. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp . Acessado em: 08/04/2010.

VERÍSSIMO, Fernando. **O Problema de Segurança em Redes Baseadas no Padrão 802.11.** 2003. Disponível em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=82 . Acessado em: 10/04/2010.

7. Glossário

Autenticador	Equipamento que transmite a identidade do usuário para o servidor de autenticação.
Bluetooth	Conexão de rede sem fio de curto alcance.
Backdoor	Programa que permite a ação remota de um hacker sobre um computador infectado.
Checksum	Forma de detectar a consistência dos dados.
Desktops	Microcomputadores de mesa.
Defacers	Pessoas que alteram páginas de Internet alheias sem a devida autorização.
Ethernet	Tecnologia de interconexão para redes locais (LAN) baseada em envio de pacotes.
Firmware	*Software* embarcado, software que controla o *hardware* diretamente.
FTP	*File Transfer Protocol*. Protocolo de transferência de arquivo utilizado na *Internet*.
Gateways	Porta de ligação entre redes, interligando redes internas com outras internas ou com externas.
Hardware	Parte física do computador.
Hosts	Máquinas pertencentes à uma rede (computadores, *notebooks*, palms).

ISM	Faixas de freqüência destinada a equipamentos que não necessitam de licenciamento da Agência Nacional de Telecomunicações – ANATEL.
Laptop	Computador portátil.
Notebook	Computador portátil.
NetBEUI	Versão melhorada do NetBIOS
NetBIOS	É uma interface que fornece às aplicações de rede um serviço de transmissão orientado à conexão
Pacotes	Estrutura de dados unitária que circula numa rede de computadores.
Rede	Dois ou mais *hosts* ligados entre si.
Servidor, *Server*	Máquina que atua servindo uma rede (dados, *Internet*)
Software	Seqüência de instruções a serem executadas no tratamento, direcionamento e manipulação de dados ou informações.
Suplicante	Usuário que deseja obter acesso à rede.
Wireless	Comunicação sem fio.