

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN**

Carlos Sigmund Meneses Fonseca

ANÁLISE DAS VULNERABILIDADES E ATAQUES ÀS REDES SEM FIO

ANÁLISE DAS VULNERABILIDADES E ATAQUES ÀS REDES SEM FIO

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito obrigatório para a obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto, M.Sc.

**NATAL/RN
2007**

CARLOS SIGMUND MENESES FONSECA

ANÁLISE DAS VUNERABILIDADES E ATAQUES ÀS REDES SEM FIO

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito obrigatório para a obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto, M.Sc.

NATAL/RN

2007

RD 30.285
FARN
BIBLIOTECA
Nº Reg M000750
14, 12, 07

004.72
F743ov
2007
ex 01

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Fonseca, Carlos Sigmund Meneses

Análise das vulnerabilidades e ataques às redes sem fio / Carlos Sigmund Meneses Fonseca. Natal: FARN, 2007.
36 f.

Orientador: Aluizio Ferreira da Rocha Neto (M. Sc.)

Monografia (Especialização em Redes de Computadores) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Redes sem Fio - Wireless – Monografia. 3. Segurança de Redes sem Fio – Monografia. I. Título.

RN/FARN/BC

CDU 004.72

CARLOS SIGMUND MENESES FONSECA

Dedico à minha mãe, mulher de fina flor e coragem que na escola do trabalho e da vida acumulou paciência, amor e perseverança.

ANÁLISE DAS VUNERABILIDADES E ATAQUES ÀS REDES SEM FIO

Monografia apresentada ao curso de Especialização em Redes da Faculdade Natalense para o Desenvolvimento do RN e aprovado em 25 de Maio de 2007, pela banca examinadora composta pelos seguintes membros

Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador

Gleydson Azevedo Ferreira de Lima, M.Sc.
Membro Examinador

DEDICATÓRIA

Dedico à minha mãe, mulher de fina flor e coragem que na escola do trabalho e da vida acumulou paciência, amor e perseverança.

— Ao professor Antônio Ferreira da Rocha Neto, que me ofereceu a oportunidade de galgar mais um passo em meus estudos acadêmicos.

A minha esposa, cômico e amante que sempre está ao meu lado apoiando-me em todos os meus projetos.

A minha mãe, razão de minha existência e exemplo de vitória... agradeço tudo.

AGRADECIMENTOS

Aos meus Avôs, Carlos e Edla, cuja lucidez moral e intelectual me possibilitou liberar das amarras do medo e da insegurança.

Aos meus irmãos que sempre estão ao meu lado

Ao professor Aluizio Ferreira da Rocha Neto, que me ofereceu a oportunidade de galgar mais um passo em meus sonhos acadêmicos.

A minha esposa, cúmplice e amante que sempre esta ao meu lado apoiando-me em todos os meus projetos.

A minha mãe, razão de minha existência e exemplo de vitória....agradeço tudo.....

RESUMO

Esta pesquisa analisa as vulnerabilidades e tecnologias empregadas hoje na utilização de Redes sem fio, seja ela “Domestica” ou “Coorporativa”. As Rede sem fio por se propagarem através de ondas de rádio, e por isso não se limitam ao perímetro onde se encontra o AP (*access point*). Atravessando estruturas como paredes, o sinal pode chegar a alcançar a área externa de uma empresa ou residência, facilitando o acesso indevido. Para se evitar que um *host* obtenha acesso indevido a rede ou capture as informações ali trafegadas, este trabalho apresenta os métodos e ações que podem ser implementados em busca de assegurar uma maior proteção, se utilizando, por exemplo, de criptografia como o WEP (*Wired Equivalency Privacy*), o WPA (*Wi-Fi Protected Access*), para assegurar a confiabilidade das informações. Também são abordados métodos para assegurar a autenticidade dos usuários, como o baseado em um servidor RADIUS (*Remote Authentication Dial-In User Server*), que autentica os usuários que podem acessar a rede através do protocolo 802.1x.

Palavras-chaves: Redes sem fio. Vulnerabilidades. Segurança. WEP. WPA. RADIUS.

ABSTRACT

This research analyzes the vulnerabilities and technologies in the use of wireless networks, been it a home or corporate network. The wireless network propagates through radio waves, and therefore is not limited to the perimeter of the AP (access point). Crossing structures as walls, the signal can arrive to reach the external area of a company or residence, being facilitated the improper access. To prevent itself there that one host gets improper access the net or captures the passed through information, this work presents the methods and actions that can be implemented in search to assure a bigger protection, if using, for example, cryptography as WEP (Wired Equivalency Privacy), WPA (Wi-Fi Protected Access), to assure the trustworthiness of the information. Also they are boarded methods to assure the authenticity of the users, as the based on RADIUS (Remote Authentication Dial-In User Server), which authenticates the users who can have access the net through the protocol 802.1x.

Key-Words: Wireless Networks. Vulnerabilities. Security. WEP. WPA. RADIUS

SUMÁRIO

1	INTRODUÇÃO.....	11
1.1	OBJETIVOS.....	12
1.1.1	<i>Objetivos Específicos.....</i>	<i>12</i>
1.2	ORGANIZAÇÃO DO TRABALHO.....	12
2	REFERENCIAL TEÓRICO.....	13
2.1	REDES WIRELESS.....	13
2.2	PADRÃO 802.11.....	14
2.3	COMPONENTES.....	16
2.4	MODOS DE OPERAÇÃO.....	16
2.5	SEGURANÇA DE REDES WIRELESS.....	17
2.5.1	<i>Posicionamento Físico.....</i>	<i>18</i>
2.5.2	<i>Configurações.....</i>	<i>19</i>
2.5.3	<i>MAC Address.....</i>	<i>19</i>
2.5.4	<i>Criptografia.....</i>	<i>21</i>
2.5.5	<i>Autenticação.....</i>	<i>24</i>
2.5.6	<i>Fundamentos do 802.1x.....</i>	<i>27</i>
2.6	SOFTWARES COMPLEMENTARES.....	28
2.6.1	<i>Firewall.....</i>	<i>28</i>
2.6.2	<i>Monitoramento da Rede Wi-Fi.....</i>	<i>29</i>
3	VULNERABILIDADES EXPLORADAS NAS REDES WIFI.....	30
3.1	WEP.....	30
3.2	ACCESS POINT SPOOFING (ASSOCIAÇÃO MALICIOSA).....	30
3.3	ENVENENAMENTO ARP.....	31
3.4	SPOOFING.....	32
3.5	ATAQUES DE NEGATIVA DE SERVIÇO.....	32
3.6	WLAN SCANNER (ATAQUES DE VIGILÂNCIA).....	33
3.7	WARDRIVING.....	33
3.8	WARCHALKING.....	34
4	MÉTODOS DE ACESSO SEGURO.....	36
4.1	RADIUS.....	36
4.1.1	FUNDAMENTOS.....	37
4.2	VPN.....	38
5	ANÁLISE DE RESULTADOS.....	39
6	CONCLUSÃO.....	41
	REFERÊNCIAS.....	42
	GLOSSÁRIO.....	45

LISTA DE FIGURAS

FIGURA 1: CLASSIFICAÇÃO PELA ABRANGÊNCIA DAS REDES SEM FIO	13
FIGURA 2: REDE SEM FIO NO MODO DE INFRA-ESTRUTURA	17
FIGURA 3: REDE SEM FIO NO MODO <i>Ad Hoc</i>	17
FIGURA 4: VANTAGENS E DESVANTAGENS DOS TIPOS DE EAP	25
FIGURA 5: SIMULAÇÃO DE ACESSO A UMA REDE SEM FIO.	28
FIGURA 6: SÍMBOLOS DO <i>WARCHALKING</i>	34

CRC-32	<i>Cyclic Redundancy Check</i>
D.o.S	<i>Denial Of Service</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
EFS	<i>Encrypted File System</i>
ESS	<i>Extended Service Set</i>
EAP	<i>Extensible Authentication Protocol</i>
EAP-LEAP	<i>Extensible Authentication Protocol - Lightweight Extensible Authentication Protocol</i>
EAP-TLS	<i>Extensible Authentication Protocol - Transport Layer Security</i>
EAP-TTLS	<i>Extensible Authentication Protocol - Tunnelled Transport Layer Security</i>
FTP	<i>File Transfer Protocol</i>
GHz	<i>Gigahertz</i>
JAS	<i>Journal Authentication Server</i>
ICP	<i>Infra-estrutura de chaves públicas</i>
IEE	<i>Institute of Electrical and Electronic Engineers</i>
ICV	<i>Integrity Check Value</i>
IPSec	<i>Internet Protocol Security</i>
ISM	<i>Industrial, Scientific and Medical</i>
LAN	<i>Local Area Network</i>
MAC	<i>Media Access Control</i>
Mbps	<i>Megabits per second</i>
MIC	<i>Message Integrity Code</i>
MS-CHAPv2	<i>Microsoft Challenge-Handshake Authentication Protocol v. 2</i>
NDSAPI	<i>NetBIOS Extended User Interface</i>
NetBIOS	<i>Network Basic Input/Output System</i>
OSI	<i>Open Systems Interconnection</i>

LISTA DE ABREVIACÕES

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

PCI	<i>Peripheral Component Interconnect</i>
PCMCIA	<i>Personal Computer Memory Card International Association</i>
PEAP	<i>Protected Extensible Authentication Protocol</i>
RADIUS	<i>Remote Authentication Dial-In User Server</i>
RC4	<i>Route Coloniale 4</i>
SSID	<i>Service Set Identifier</i>
STA	<i>Stations</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
USB	<i>Universal Serial Bus</i>
VPN	<i>Virtual Private Network</i>
WPA	<i>Wi-Fi Protected Access</i>
WPA-PSK	<i>Wi-Fi Protected Access - Pre-Shared Key</i>
WPA-PSK.TKIP	<i>Wi-Fi Protected Access - Pre-Shared Key.Temporal Key Integrity Protocol</i>
WEP	<i>Wired Encryption Protocol</i>
WLAN	<i>Wireless Local Area Network</i>
WLL	<i>Wireless Local Loop</i>
WMAN	<i>Wireless Metropolitan Area Network</i>
WPAN	<i>Wireless Personal Area Network).</i>
WWAN	<i>Wireless Wide Area Network</i>
Wi-Fi	<i>Wireless-Fidelity</i>
WiMAX	<i>Worldwide Interoperability for Microwave Access</i>
TI	<i>Tecnologia da Informação</i>

1 INTRODUÇÃO

No decorrer dos últimos anos a utilização de redes sem fio vem sendo cada vez mais utilizada para prover conectividade dentro das empresas e grandes corporações. Estas redes são cada vez mais utilizadas como auxílio para LANS convencionais, seja por prover uma alternativa economicamente viável, seja por prover taxas de transmissão compatíveis a redes cabeadas. Além também de servirem como links entre as empresas e os clientes.

Em contra partida ao crescimento da rede sem fio, as tecnologias de segurança para este novo cenário ainda não conseguem garantir uma confiabilidade plena. Segundo ENGST & FLSIESHMAN (2005) as redes sem fio tiveram seu início a partir de um projeto que conectavam as universidades do Havai aos computadores de quatro ilhas. As redes sem fio 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. (ENGST & FLEISHMAN, 2005)

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 frequência do 802.11b. (ENGST & FLEISHMAN, 2005)

As redes sem fio hoje é uma realidade, seu futura, caberá ao desenvolvimento de novas tecnologias que garantam velocidade, maior propagação e principalmente segurança dos dados nela trafegados.

A partir da diminuição dos custos e simplificação nas configurações por parte dos fabricantes de dispositivos sem fio seu uso é cada vez maior. O problema é que esta facilidade na implementação acarretou por permitir que usuários sem qualificação e conhecimento instalassem estas redes sem nenhuma preocupação com a segurança dos dados nela trafegados. Hoje qualquer garoto munido de um notebook e uma latinha de batata frita transformada em antena e um bom software de análise de rede pode estar bisbilhotando o tráfego de dados nas redes sem fio.

Esta monografia tem o intuito de abordar as questões relevantes a segurança nas tecnologias de rede sem fio, no que diz respeito às vulnerabilidades e formas de ataque. Também será mostrado os principais métodos utilizados no desenvolvimento de uma rede sem fio segura.

1.1 OBJETIVOS

Este trabalho tem como objetivo analisar as principais vulnerabilidades de segurança em uma rede sem fio baseada no padrão IEEE 802.11. Como também destacar os principais modelos de segurança hoje utilizados.

1.1.1 Objetivos Específicos

- Realizar pesquisa dos principais protocolos de segurança e autenticação utilizados;
- Analisar o uso de protocolos de autenticação WEP, WPA EAP;
- Pesquisar as novas propostas de segurança e tecnologia em rede sem fio;
- Pesquisar métodos de autenticação como o 802.1x;
- Apresentar uma metodologia que possa agregar os principais métodos de segurança em redes sem fio;

1.2 ORGANIZAÇÃO DO TRABALHO

O seguinte projeto divide-se em 6 capítulos, incluindo a introdução, objetivos e uma breve visão do projeto e a metodologia que foi utilizada.

O capítulo 2 apresenta o referencial teórico o qual fala o que são as redes sem fio, seus padrões, redes wireless, os métodos de segurança existentes e as principais ferramentas, como criptografias, lista de endereços MAC e autenticação.

No capítulo 3 e 4 é mostrado alguns tipos de ataques hoje utilizados contra uma rede sem fio. Como também os métodos de acesso seguro, utilizando VPN e servidores de autenticação RADIUS.

No capítulo 5 é mostrado as análises dos resultados da pesquisa desenvolvida

E por fim, o capítulo 6 no qual são apresentadas as conclusões do desenvolvimento do projeto.

2 REFERENCIAL TEÓRICO

2.1 REDES WIRELESS

A palavra Wireless é originária do inglês *wire* (fio, cabo) e *less* (sem). Hoje qualquer conexão para transmissão de dados através de tecnologia de rádio pelo ar e sem a utilização de cabos é chamada de Wireless. Por sua extrema facilidade de instalação e uso é cada vez mais freqüente seu uso nos dias de hoje.

Existem vários tipos e padrões de redes wireless, como por exemplo, o WiMax, Bluetooth, Wi-Fi (Wireless Fidelity), InfraRed (Infravermelho). (ARTHAS, 2007)

Encaixam-se 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). (ARTHAS, 2007)

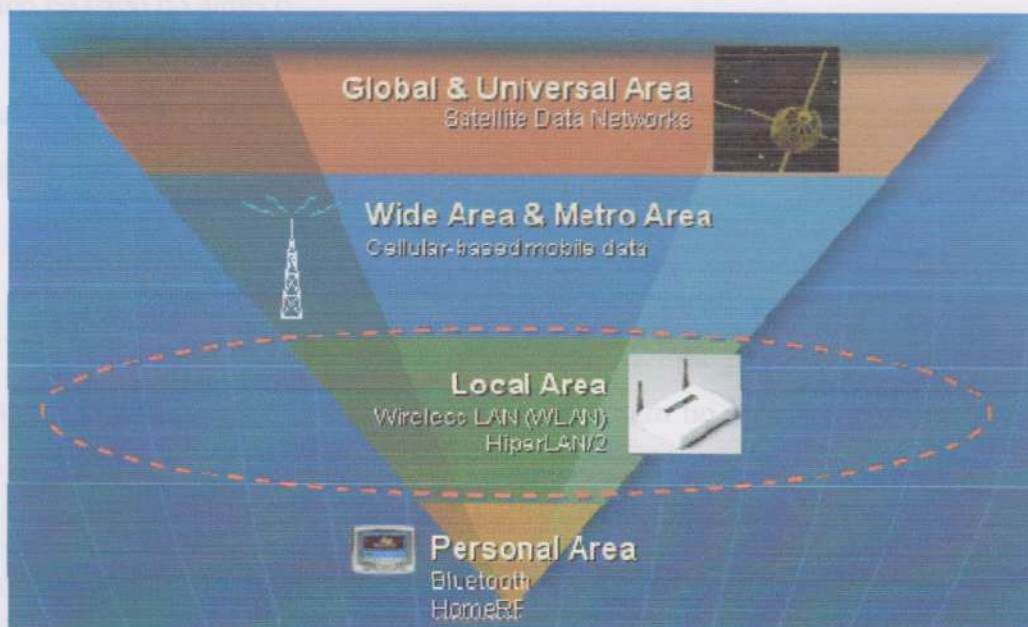


Figura 1: Classificação Pela Abrangência das Redes Sem Fio

Fonte: Microsoft (2007)

Em busca de áreas de cobertura maiores e mais velocidade nas transmissões sem fio que outra tecnologia virou alvo dos laboratórios, o WiMAX, que utiliza o padrão IEEE 802.16d, foi ratificado em Dezembro de 2001 e foca basicamente as faixas de frequências situadas entre 10GHz e 66GHz cobrindo uma distância de 50 quilômetros quadrados a uma velocidade nominal de 75 Mbps. No Brasil os testes com WIMAX estão sendo realizados nas áreas de São Paulo a Cidade de Outro Preto em Minas Gerais. Hoje outras tecnologias neste padrão se destacam como: MIMO Tecnologia de rede sem fio que emprega várias antenas para transmitir dados, MESH Redes descentralizadas, capazes de se auto-configurar e a mais recente originaria dos laboratórios coreanos a WIBRO que acessa dados em movimento.

Conforme engst ; flsieshman (2005), a grande vantagem em instalar uma rede sem fio é a mobilidade. Há alguns anos, um cenário onde permitia-se que as pessoas pudessem desfrutar da conectividade de uma rede sem a necessidade de fios era um tanto quanto futurista. Hoje a realidade mudou.

As redes sem fio nos proporcionam a mesma conectividade de uma rede cabeada comum dentro do perímetro de alcance da rede, 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.

Segundo matéria publicada na revista INFO Exame (Coleção 2005 – *Wi-Fi*) pela jornalista Débora FORTES (2005), várias empresas estão começando a criar políticas de uso de notebooks e PDA's em redes wireless.

2.2 PADRÃO 802.11

O IEEE 802.11 (*Institute of Eletrical and Eletronic Engineers*) é um conjuntos de padrões de mercado para tecnologias de rede local sem fio (WLAN) compartilhadas. São eles:

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

IEEE 802.11b: descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Este 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 802.11g: descreve o mais recente padrão para redes sem fio. Atua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps.

IEEE 802.11i: trata-se um grupo de trabalho que está ativamente definindo 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 802.11e: fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e 802.11a. Os melhoramentos incluem a capacidade multimídia feito possível com a adesão da funcionalidade de qualidade de serviços (QoS – *Quality of Service*), como também melhoramentos em aspectos de segurança. Isto significa a habilidade de oferecer vídeo e áudio à ordem (*on demand*), serviços de acesso de alta velocidade a Internet e Voz sobre IP (VoIP – *Voice over Internet Protocol*). Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

Segundo arthas (2004), os grupos do IEEE que estão desenvolvendo outros protocolos são:

Grupo 802.11d – Está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O corrente protocolo 802.11 só define operações WLAN em alguns países).

Grupo 802.11f – Está a desenvolver *Inter-Access Point Protocol* (Protocolo de acesso entre pontos), por causa da corrente limitação de proibir *roaming* entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.

Grupo 802.11g – Estão a trabalhar em conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.

Grupo 802.11h – Está em desenvolvimento do espectro e gestão de extensões de potência para o 802.11a do IEEE para ser utilizado na Europa.

2.3 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 vêm 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*.

2.4 MODOS DE OPERAÇÃO

Infrastructure mode – É usado para conectar os computadores que tem adaptadores de rede sem fio, também conhecidos como clientes sem fio, a uma rede com fio existente. Por exemplo uma residência ou um escritório de pequena empresa pode ter uma rede Ethernet existente. Com o modo de infra-estrutura, os notebooks ou outros computadores de mesa que não possuam uma conexão Ethernet com fio podem ser conectados perfeitamente à rede existente. Um nó de rede conhecido como ponto de acesso (AP) sem fio é usado para conectar as redes com e sem fio. A figura 2 demonstra o exemplo citado.

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

2.5 SEGURANÇA DE REDES WIRELESS

Grças aos investimentos crescentes na tecnologia sem fio nos últimos anos é cada vez maior o número de instituições e empresas que estão aderindo a esta tecnologia. Com

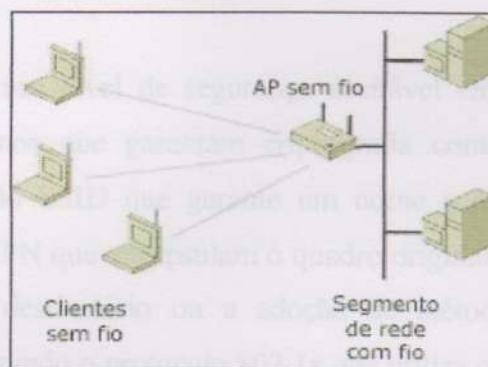


Figura 2: Rede sem fio no modo de infra-estrutura

Fonte: Microsoft Brasil (2007)

Ad-Hoc mode – É usado para conectar clientes sem fio diretamente, sem a necessidade de um ponto de acesso (AP) sem fio ou uma conexão a uma rede com fio existente. Segundo documentação da Microsoft uma rede AD-HOC pode ter até 9 clientes trocando dados entre se.

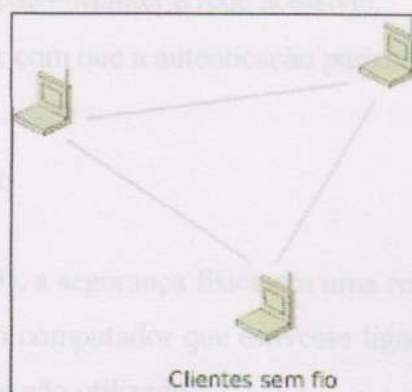


Figura 3: Rede sem fio no modo *Ad Hoc*

Fonte: Microsoft Brasil (2007)

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

2.5 SEGURANÇA DE REDES WIRELESS

Graças aos investimentos crescentes na tecnologia sem fio nos últimos anos é cada vez maior o número de instituições e empresas que estão aderindo a esta tecnologia. Com

isto, também houve um aumento no risco com a segurança do tráfego de informações que circulam nestas redes.

Para garantirmos um nível de segurança aceitável em uma rede sem fio, esta deverá possuir mecanismos que garantam criptografia como: WEP ou WPA. Uma identificação da rede pelo SSID que garante um nome a rede e em um nível mais avançado, utilização de VPN que encapsulam o quadro original em uma espécie de túnel, ligando diretamente ao destinatário ou a adoção de métodos de autenticação com servidores RADIUS, utilizando o protocolo 802.1x que utiliza o EAP como meio de fazer o pacote de conversação de autenticação entre diversos componentes da solução e gerar as chaves usadas para autenticação do cliente para fazer uso da rede.

Segundo DUARTE (2003), uma rede sem fio para que possa estar segura 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.

2.5.1 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)

Hoje, para ter acesso a uma rede sem fio, basta estar munido de software de monitoramento e equipamentos que possam capturar os sinais desta rede.

Então para diminuir o acesso não permitido a rede sem fio é importante a posição do *Access Point*, para que as ondas eletromagnéticas fiquem centralizadas, minimizando a área coberta pela rede fora do perímetro desejado.

2.5.2 Configurações

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

Após 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. (RUFINO, 2005)

Praticamente todos os aparelhos possuem uma configuração padrão de fábrica, desde o SSID (*service set identifier*), endereços IPs e senhas, por tanto, o acesso indevido a rede se torna fácil e simples. Existem 2 tipos de configurações: (RUFINO, 2005)

2.5.2.1 Configuração Aberta

De acordo com rufino (2005), este tipo de configuração é caracterizado pelo envio do SSID da rede pelo concentrador, 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)

2.5.2.2 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)

2.5.3 MAC Address

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 Interconnection*). (GUERRA, 2002)

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. (GUERRA, 2002)

Pode-se configurar um concentrador 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 frequentes dependendo da alternância entre os usuários. Outra coisa, este método só é bem utilizado em redes que tenham um numero pequeno de STA's, já que o trabalho de cadastramento é manual.

Para se conectar a uma rede *wi-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 plugá-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 *Netwrok Address*.

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.

2.5.4 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. Os métodos de criptografia usados em uma rede wireless são:

2.5.4.1 WEP

O *Wired Equivalency Privacy* (WEP), segundo a Microsoft, é o método criptográfico usado nas redes wireless 802.11. O 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 (*Cyclic 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 que traz 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, 2007)

Segundo rufino (2005), alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. 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)

2.5.4.2 WPA

O WPA foi produzido pela Wi-Fi Alliance como estratégia para unificar e aperfeiçoar a segurança usada na rede sem fio. O WPA reúne uma série de recursos de segurança amplamente considerados como sendo os métodos mais seguros disponíveis atualmente para proteger as WLANS. O WPA suporta a criptografia robusta, o que torna a descoberta das chaves de criptografia bem menos viável.

De acordo com Eduardo PRADO, Comunidade *Wireless* Brasil (2005), 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 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*, especifica 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.” (SUPPORT MICROSOFT, 2007)

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. (SUPPORT MICROSOFT, 2007)

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. (SUPPORT MICROSOFT, 2007)

2.5.4.3 WPA2

De acordo com (MICROSOFT, 2005), 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, 2007).

2.5.5 Autenticação

O EAP é um padrão IETF (Internet Engineering taskforce) para efetuar a autenticação. Ele pode ser usado com uma variedade de diferentes métodos de autenticação com base em senhas, certificados de chaves públicas ou outras credenciais.

Como o EAP é um método de autenticação conectável, existe uma variedade de diferentes tipos EAP a escolher. Os melhores tipos de EAP normalmente utilizam a criptografia para proteger a conversação de autenticação e pode gerar dinamicamente as chaves usadas para a criptografia durante o processo.

As diferentes soluções de segurança para WLANS fundamentadas no 802.1x oferecem tipos diferentes de EAP com níveis variáveis de proteção. Estes incluem tanto soluções baseadas em padrões como soluções proprietárias e estas soluções possuem níveis variáveis de suporte entre os fornecedores de sistemas operacionais e de hardware de rede. A autenticação e o acesso a rede fundamentados no 802.1x e o EAP compõem uma segurança significativa a uma rede sem fio.

Outro tipo de autenticação oferecido pela Microsoft ao PEAP (EAP Protegido). Ele foi projetado para portar os tipos de EPA dentro de um canal protegido por TLS e requer um certificado baseado em servidor. O EAP também gera chaves dinamicamente para criptografar o tráfego sem fio durante o processo de autenticação. A Microsoft oferece suporte ao Windows para usar o MSCHAPv2 para fazer autenticação de senha segura dentro do PEAP.

A figura a seguir ilustra os tipos de EAP que podem ser usados em uma infraestrutura 802.1X da Microsoft e as vantagens e desvantagens de cada tipo.

Recurso	PEAP	EAP-TLS	MD5
Autenticação mútua	Autenticação mútua	Autenticação mútua	Sem autenticação mútua
Chaves dinâmicas (rechaveamento)	Gerado durante a autenticação	Gerado durante a autenticação	Sem chaves dinâmicas (rechaveamento): depende de chaves estáticas.
Nível de tecnologia de segurança	Autenticação mais segura por senha	Autenticação mais segura	Tecnologia de baixa segurança
Proteção da credencial de usuário	Protegido pelo túnel TLS (<i>Transport Layer Security</i>)	Autenticação por certificados	Aberto a ataques de dicionário
Facilidade de implementação	Com suporte amplo e oferecido originalmente nos clientes Windows.	Requer uma PKI (Infra-estrutura de Chave Pública). Com suporte amplo e oferecido originalmente nos clientes Windows.	Simples, porém não recomendado para uso sem fio.
Flexibilidade de credenciais	Qualquer EAP aprovado com túnel TLS, inclusive senhas baseadas em EAP – MSCHAPv2.	Somente certificados digitais	Somente senha

Figura 4: Vantagens e desvantagens dos tipos de EAP

Fonte: Microsoft (2004)

O tipo de EAP recomendado para executar a autenticação de cliente por certificados é o EAP-TLS e o tipo de EAP recomendado para executar a autenticação de cliente por senha é o MSCHAPv2 (EAP-Microsoft Challenge-Handshake Authentication Protocol

versão 2) com o PEAP (*Protected Extensible Authentication Protocol*), também conhecido como PEAP-EAP-MSCHAPv2. (MICROSOFT, 2007)

O 802.1x oferece autenticação bem mais forte do que a de sistema aberto ou de chave compartilhada. A solução recomendada pela Microsoft é usar o EAP-TLS e certificados digitais para autenticação. Para usar a autenticação EAP-TLS em uma rede sem fio, deverá ter uma infra-estrutura de autenticação que consiste de um domínio do Active Directory, servidor RADIUS e um CAs (Autoridade de certificação) para emitir certificados para os servidores RADIUS e clientes sem fio. Esta infra-estrutura é apropriada para grandes empresas e organizações, mas não é viável para residências ou pequenas empresas devido aos custos envolvidos.

A autenticação 802.1X por senha é suficiente para empresas pequenas que não possuem atualmente uma infra-estrutura de certificado adequada e não precisam de certificados para outras finalidades, como o uso do EFS (*Encrypted Sistem Files* ou Sistema de Arquivos Criptografados), VPN (Rede Virtual Privada), etc. Como alternativa, a autenticação 802.1X por senha pode ser vista como uma tecnologia provisória para a obtenção do controle de acesso 802.1X à WLAN durante o planejamento de uma infra-estrutura de certificado futura. (MICROSOFT, 2004)

No entanto, os custos envolvidos na aquisição de um ou mais certificados de servidor de um terceiro confiável devem ser ponderados com cuidado em comparação com o valor que uma infra-estrutura de certificado poderá trazer para uma empresa. Estas orientações foram desenvolvidas para ajudá-lo a obter uma solução de autenticação de cliente por certificados que usa o EAP-TLS (*Encrypted Sistem Files - Transport Layer Security*) com custo e esforço mínimo. (MICROSOFT, 2004)

Segundo Fernando Veríssimo (2003), há vários tipos de EAP que são usados hoje em dia, dentre eles:

1. EAP-LEAP – (*Extensible Authentication Protocol-Lightweight Extensible Authentication Protocol*) Esse padrão foi desenvolvido pela CISCO. EAP-LEAP usa um par *login/senha* para transmitir a identidade do suplicante para o servidor RADIUS para autenticação.

2. EAP-TLS - Esse padrão foi descrito na RFC 2716. EAP-TLS (*Extensible Authentication Protocol - Transport Layer Security*) usa um certificado X.509 para autenticar.

3. EAP-TTLS - Esse é um padrão desenvolvido pela Funk Software. EAP-TTLS (*Extensible Authentication Protocol - Tunneled Transport Layer Security*) é uma opção

alternativa ao EAP-TLS. Enquanto o servidor de autenticação identifica a si mesmo ao cliente com um certificado de servidor, o suplicante usa um par *login/senha* para se identificar.

4. EAP-PEAP (*Protect EAP*) - Outro padrão desenvolvido para prover autenticação mútua segura. O padrão foi desenhado para superar algumas vulnerabilidades existentes em outros métodos EAP.” (VERÍSSIMO, 2003)

Há um caso especial na implementação do IEEE 802.1X chamado de Pré-compartilhamento. Em ambientes pequenos (ambientes domésticos ou pequenas empresas), um servidor de autenticação pode não estar disponível. Então uma chave pré-estabelecida é usada. A chave é de conhecimento do suplicante e do autenticador. Uma autenticação parecida com a que acontece no WEP então é feita entre esses dois participantes. (VERÍSSIMO, 2003)

2.5.6 Fundamentos do 802.1x

Há 3 participantes em uma transação usando o 802.1X:

- O suplicante - Um usuário ou um cliente que quer ser autenticado. Ele pode ser qualquer dispositivo sem fio.
- O servidor de autenticação - Um sistema de autenticação, tipo RADIUS, que faz a autenticação dos clientes autorizados.
- O autenticador - O dispositivo que age como um intermediário na transação, entre o suplicante e o servidor de autenticação. O ponto de acesso, na maioria dos casos.

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.

2.6 SOFTWARES COMPLEMENTARES

2.6.1 Firewall

Um firewall pode ser definido como uma coleção de componentes ou mesmo um sistema colocado entre duas redes de comunicação que possui as seguintes propriedades:

- Todo o tráfego de dentro para fora dessa rede e vice-versa deve passar pelo firewall.

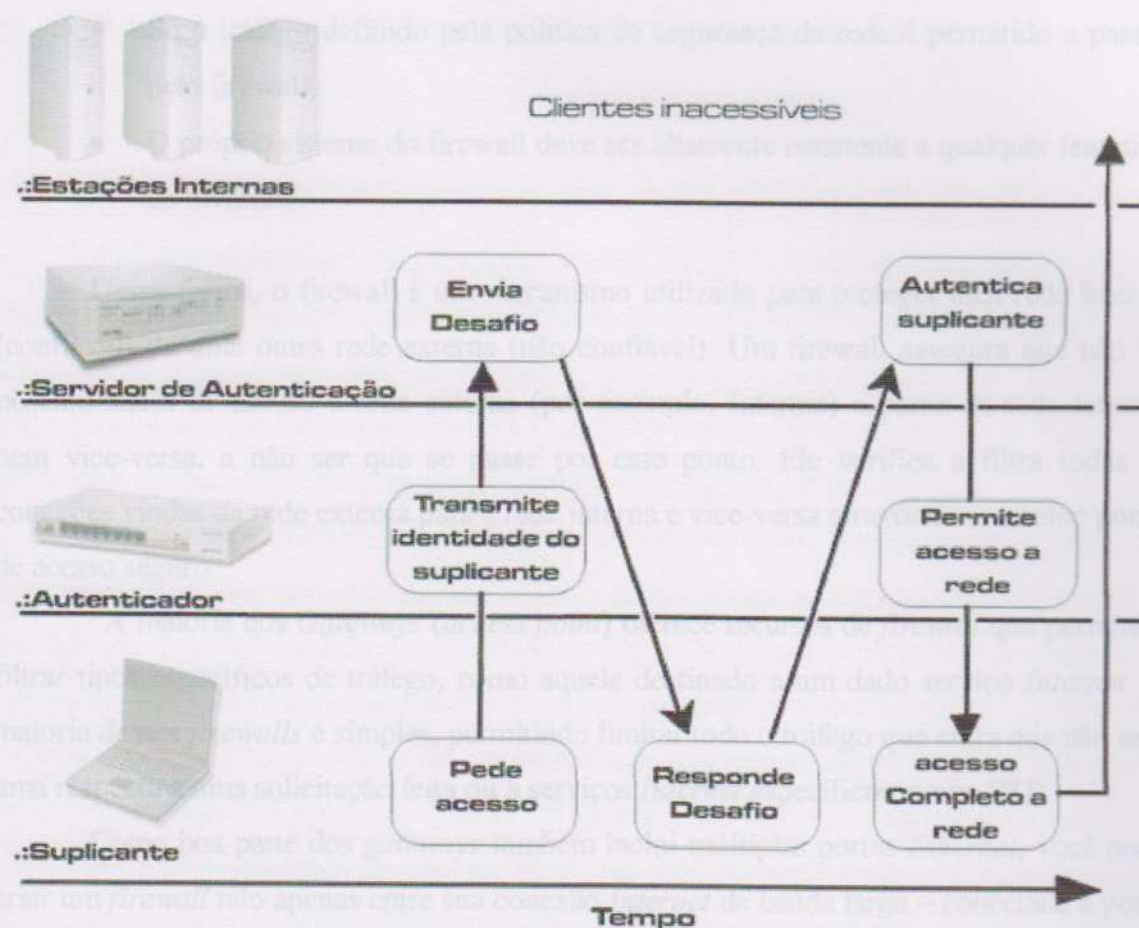


Figura 5: Simulação de acesso a uma rede sem fio.

Fonte: Lockabit (2006)

Na figura 5, 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.

2.6 SOFTWARES COMPLEMENTARES

2.6.1 Firewall

Um firewall pode ser definido como uma coleção de componentes ou mesmo um sistema colocado entre duas redes de comunicação que possui as seguintes propriedades:

- Todo o tráfego de dentro para fora dessa rede e vice-versa deve passar pelo firewall;

- Só o tráfego definido pela política de segurança da rede é permitido a passar pelo firewall;
- O próprio sistema do firewall deve ser altamente resistente a qualquer tentativa de invasão.

Dessa forma, o firewall é um mecanismo utilizado para proteger uma rede interna (confiável) de uma outra rede externa (não confiável). Um firewall assegura que não há possibilidades de acesso à rede externa (por exemplo, Internet) a partir da rede interna, nem vice-versa, a não ser que se passe por esse ponto. Ele verifica e filtra todas as conexões vindas da rede externa para a rede interna e vice-versa através de um único ponto de acesso seguro.

“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)

2.6.2 Monitoramento da Rede Wi-Fi

“Da mesma forma que muitos administradores monitoram o seu ambiente de rede convencional (com o uso de IDS, 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.” (CERT, 2003)

3 VULNERABILIDADES EXPLORADAS NAS REDES WI-FI

3.1 WEP

Um dos principais das principais vulnerabilidades é utilizar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes de uma determinada rede. Caso seja necessário a troca desta chave o processo poderá ser trabalhoso e em alguns casos inviável (caso seja em provedores de acesso em locais públicos e em locais que tenham grande número de estações por exemplo).

O protocolo WEP diz que deve existir uma chave conhecida por ambos os lados da comunicação, porém não indica (nem sugere) de que forma a distribuição da chave deve ser feita. E é na dificuldade de distribuir as chaves que reside um dos problemas deste protocolo. Em redes pequenas e pouco moveis (pequenos escritórios e de uso doméstico), tal fato não seja a ser um problema, porem ainda assim exige administração. Entretanto, em ambientes maiores e/ou com grande mobilidade, isto pode ser impossível de ser feito. Caso haja real necessidade de uso do WEP, tal ação possivelmente será feito de forma pouco segura, já que muitas pessoas tem de conhecer a chave. E mesmo que a distribuição seja realizada da forma mais segura possível, uma chave é exponencialmente menos secreta tanto quanto forem as pessoas (neste caso, equipamentos) que a conhecerem, visto que equipamentos podem ser perdidos, atacados e compartilhados. (RUFINO, 2005)

3.2 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)

Esta associação maliciosa consta de duas máquinas com dispositivos para redes sem fio e segue o seguinte conjunto de passos:

- A vítima envia pacotes de *Probe Request* (pacotes que busca conexão com um *access point*) à procura de *access points* para conexão;
- O atacante, com o auxílio de um *software* de conexão, se passa por um *access point*;
- A vítima requisita a associação e se associa ao atacante;
- O atacante responde com as informações de rede necessárias como endereço IP;

- O atacante envia uma requisição de NET USE;
- A vítima responde com LOGIN;
- Qualquer vulnerabilidade de qualquer serviço do cliente pode ser agora explorada.

Nesta explanação, 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)

3.3 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 vítima. (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 homem-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)

3.4 SPOOFFING

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

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 *Spoofing*, existe o MAC *Spoofing* 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)

3.5 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. (MARTINS, 2003)

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 radiofrequência 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. (MARTINS, 2003)

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. (MARTINS, 2003)

3.6 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. (MARTINS, 2003)

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. (MARTINS, 2003)

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. (MARTINS, 2003)

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. (MARTINS, 2003)

3.7 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, 2007)

Muitas *homepages* como o "wardriving.com" dão instruções detalhadas de como efetuar o *wardriving*. Outras como a "*wardriving is not a crime*" tem como principal objetivo fazer apologia ao *wardriving*. Chama atenção o fato de existir uma distribuição *WarLinux* (<http://warlinux.sourceforge.net/>) concebida única e exclusivamente para *wardriving*. (BABOO, 2007)

3.8 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, (ARTHAS, 2004)

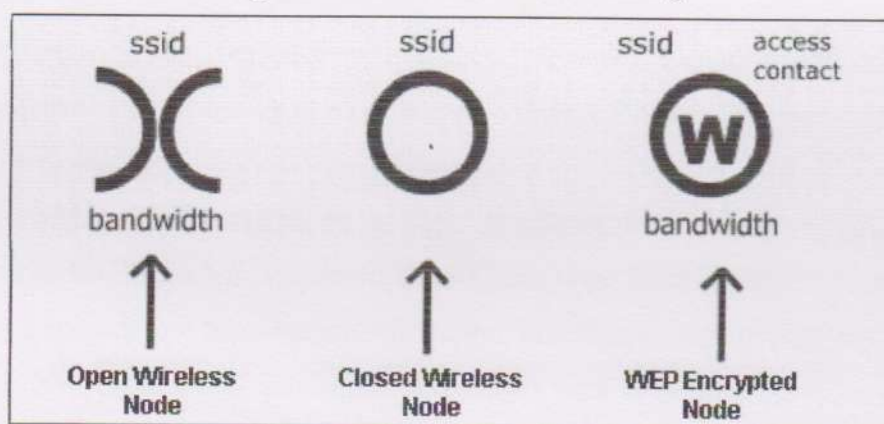
Este tipo de ataque tem como objetivo encontrar redes sem fio através de técnicas de *wardriving* e marcar estas redes através da pichação de muros e calçadas com símbolos específicos. (BABOO, 2005)

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.

A Figura 6 mostra um exemplo dos símbolos utilizados nesta ação.

Figura 6: 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 control* (chave WEP utilizada) e a *bandwidth* (velocidade da rede).

4.1 RADIUS

O protocolo RADIUS foi desenvolvido pela empresa Livingston, mais tarde passou a pertencer a empresa Lucent Technologies e hoje faz parte dos padrões em desenvolvimento no IETF (Internet Engineering Task Force). O protocolo pode ser utilizado de forma integrada a diversos serviços garantindo segurança e restrição no acesso a uma rede. Este método é formado pelas seguintes entidades:

Um usuário, agente que deseja ter acesso a uma terminando serviço na rede autenticada;

Um servidor de acesso a rede, responsável por entrar em contato com o servidor RADIUS requisitando a autenticação do usuário;

O servidor RADIUS, que realiza a identificação do usuário validando seus dados e for fim uma base de dados onde as informações necessárias para o RADIUS identificar o usuário. Este banco poderá estar no próprio servidor RADIUS ou em outra máquina.

4.1.1 Funcionamento

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 aguardada por um determinado tempo, porém caso esta mensagem não chegue, o cliente poderá encaminhar uma nova requisição para o mesmo servidor ou para um servidor RADIUS alternativo. (ALBUQUERQUE, 2003)

Quando recebe uma requisição a primeira ação do servidor é validar o cliente RADIUS o qual encaminhou a mensagem de requisição, evitando desta 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. (ALBUQUERQUE, 2003)

4 MÉTODOS DE ACESSO SEGURO

4.1 RADIUS

O protocolo RADIUS foi desenvolvido pela empresa Livingston, mais tarde passou a pertence a empresa Lucent Technologies e hoje faz parte dos padrões em desenvolvimento no IETF (Internet Engineering Task Force). O protocolo pode ser utilizado de forma integrada a diversos serviços garantindo segurança e restrição no acesso a uma rede. Este método é formado pelas seguintes entidades:

Um usuário, aquele que deseja ter acesso a uma determinado serviço na rede autenticada;

Um servidor de acesso a rede, responsável por entrar em contato como servidor RADIUS requisitando a autenticação do usuário.

O servidor RADIUS, que realiza a identificação do usuário validando seus dados e for fim uma base de dados onde as informações necessárias para o RADIUS identificar o usuário. Este banco poderá estar no próprio servidor RADIUS ou em outra máquina.

4.1.1 Funcionamento

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. (ALBUQUERQUE, 2003)

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. (ALBUQUERQUE, 2003)

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. (ALBUQUERQUE, 2003)

4.2 VPN

Virtual Private Network ou Rede Privada Virtual é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a *Internet*. (SANTOS, 2001)

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. (CARRIÓN, 2003)

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. (CARRIÓN, 2003)

“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.” (CARRIÓN, 2003)

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.

Uma rede *wifi* utilizando, por exemplo, o padrão IEEE 802.11g obtém velocidade nominal de 54mbps com um alcance, também nominal, de 100m.

Para se estabelecer uma rede sem fio é preciso no mínimo, no modo estruturado, um *Access Point* (AP) e um dispositivo (USB, PCI, PCMCIA) que acesse o AP.

Este tipo de rede é excelente para locais onde uma rede cabeada comum não se encaixaria, obrigando a mudar todo o layout do local.

Mobilidade é a palavra chave que caracteriza este tipo de rede.

Porém, é um novo ambiente, onde novos tipos de ataques surgem, exigindo então a criação de mecanismos de defesa para esta aplicação.

É aconselhável evitar que o sinal da rede sem fio ultrapasse os limites físicos do local onde ela opera, evitando que um atacante se posicione fora dos limites físicos do local, aumentando assim o conforto do mesmo.

Para evitar que o sinal saia dos limites físicos a posição do AP é essencial, existem locais onde não há como evitar este tipo de falha, mas é uma preocupação a ser estudada.

Nesta monografia foram apresentadas três tipos de cenários que poderão ser utilizados para garantir a segurança da rede sem fio:

- * *Uma casa ou pequena empresa que devido a custos não pode possuir servidores de domínio e autenticação através de servidor RADIUS utilizando o protocolo 802.1x. O modelo indicado é chamado de chave pré-compartilhada (WPA-PSK). A chave pré-compartilhada é configurada no AP sem fio em cada cliente sem fio. A chave de criptografia WPA-PSK inicial é derivada do processo de autenticação, que verifica ao tempo o cliente sem fio quanto o AP sem fio estão configurados com a mesma chave pré-compartilhada. É importante dizer que cada chave de criptografia inicial é exclusiva e que o protocolo de criptografia utilizado na configuração cliente é o TKIP (Protocolo de integridade da chave temporária).*
- * *Médias empresas que podem possuir um controlador de domínio e um servidor RADIUS e suas estações de serviço utilizam uma plataforma de sistema operacional que suporte WPA. Poderá ser utilizado tanto autenticação o EAP-PEAP com o TTAP-MS-CHAPv2, o acesso sem fio seguro pode ser obtido com a instalação de certificado adquirida em um servidor RADIUS e a utilização de credenciais de nome e senha para autenticação.*

5 ANÁLISE DE RESULTADOS

Uma rede *wi-fi* utilizando, por exemplo, o padrão IEEE 802.11g obtém velocidade nominal de 54mbps com um alcance, também nominal, de 100m.

Para se estabelecer uma rede sem fio é preciso no mínimo, no modo estruturado, um *Access Point* (AP) e um dispositivo (USB, PCI, PCMCIA) que acesse o AP.

Este tipo de rede é excelente para locais onde uma rede cabeada comum não se encaixaria, obrigando a mudar todo o layout do local.

Mobilidade é a palavra chave que caracteriza este tipo de rede.

Porém, é um novo ambiente, onde novos tipos de ataques surgem, forçando então a criação de mecanismos de defesa para esta aplicação.

É aconselhável evitar que o sinal da rede sem fio ultrapasse os limites físicos do local onde ela opera, evitando que um atacante se posicione fora dos limites físicos do local, aumentando assim o conforto do mesmo.

Para evitar que o sinal saia dos limites físicos a posição do AP é essencial, existem locais onde não há como evitar este tipo de falha, mas é uma precaução a ser estudada.

Nesta monografia foram apresentadas três tipos de cenários que poderão ser utilizados para garantir a segurança da rede sem fio:

- *Uma casa ou pequena empresa que devido a custos não pode possuir servidores de domínio e autenticação através de servidor RADIUS utilizando o protocolo 802.1x.* O modelo indicado é chamado de chave pré-compartilhada (WPA-PSK), a chave pré-compartilhada é configurada no AP sem fio em cada cliente sem fio. A chave de criptografia WPA-PSK inicial é derivada do processo de autenticação, que verifica se tanto o cliente sem fio quanto o AP sem fio estão configurados com a mesma chave pré-compartilhada. É importante dizer que cada chave de criptografia inicial é exclusiva e que o protocolo de criptografia utilizado na configuração cliente é o TKIP (Protocolo de integridade de chave temporária)
- *Médias empresas que podem possuir um controlador de domínio e um servidor RADIUS e suas estações de serviço utilizem uma plataforma de sistema operacional que suporte WPA.* Poderá ser utilizado como autenticação o EAP-PEAP com o PEAP-MS-CHAPv2, o acesso sem fio seguro pode ser obtido com a instalação de certificado adquirido em um servidor RADIUS e a utilização de credenciais de nome e senha para autenticação.

- *Em grandes empresas e organizações que possuem recursos significativos para implementar um projeto de segurança de grande porte.* Deverá ser criada uma infra-estrutura de autenticação que consiste em pelo menos um domínio do *Active Directory*, servidor *RADIUS (Remote Authentication Dial-In User Service)* e *CAs (Autoridade de Certificação)* para emitir certificados para o servidor *RADIUS* e clientes sem fio.

6 CONCLUSÃO

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 canaletas especiais. Devido a esta facilidade, o uso deste tipo de rede atrai cada vez mais usuários.

Entretanto, sua implementação deverá ser acompanhada de métodos que garantam uma segurança a partir do tipo de projeto proposto e levando em consideração o número de equipamentos, usuários e tamanho da organização.

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 nesta pesquisa, ou seguindo as orientações do fabricante é possível se obter um nível satisfatório de segurança, respeitando as limitações técnicas e econômicas dos usuários, empresas ou organizações.

CERT: *Práticas de Segurança para Administradores de Redes Internet*, 4.13.6.

Monitoração da Rede IPDefeat, 2003. Disponível em: <http://www.cert.br>. Acessado em 20 de março de 2007.

DUARTE, Luiz Otávio. *Análise de Vulnerabilidades e Ataques Incrrentes a Redes Sem Fio IEEE 802.11s*. Monografia (Trabalho de Conclusão do Curso de Bacharel em Ciência da Computação). - UNESP, São José do Rio Preto, 2003. Disponível em: <http://www.apostilando.com>. Acessado em 14 de março de 2007.

ENGST, Adam, FLEISHMAN, Glenn. *Kit de Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh*. 2 ed. São Paulo: Pearson Makron Books, 2005.

REFERÊNCIAS

- ALBUQUERQUE, Luciano Renovato de. **Uma Visão Geral do Funcionamento do Protocolo RADIUS**. 2003. Disponível em: <http://www.lockabit.coppe.ufrj.br>. Acessado em 14 de fevereiro de 2007
- ARTHAS, Kael. Tutorial Wireless. 2004. Disponível em <http://www.babooforum.com.br>. Acessado em: 02 de março de 2007
- BALIEIRO, Silva. Na Rua Com As Redes Sem Fio. São Paulo. **INFO Exame**, ano 19, n 218, P.: 46-48, maio de 2004.
- CARDOSO, Rogério. **WLANS São Inseguras?**. Disponível em <http://www.ciscoredacaovirtual.com>. Acessado em 02 de março de 2007
- CARRIÓN, Demetrio de Souza Diaz. **Implementação De Um Ponto De Acesso Seguro Para Redes 802.11b Baseado No Sistema Operacional OPENBSD**. Monografia (Trabalho de Conclusão do Curso de Engenharia Elétrica) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2003. Disponível em: <http://www.ravel.ufrj.br> . Acessado em 20 de março de 2007.
- CERT. **Práticas de Segurança para Administradores de Redes Internet**, 4.13.6. Monitoração da Rede *Wireless*. 2003. Disponível em: <http://www.cert.br>. Acessado em 20 de março de 2007
- DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Monografia (Trabalho de Conclusão do Curso de Bacharel em Ciência da Computação). - UNESP, São José do Rio Preto, 2003. Disponível em: <http://www.apostilando.com> . Acessado em 14 de março de 2007.
- ENGST, Adam; FLEISHMAN, Glenn. **Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh**. 2 ed: São Paulo.: Pearson Makron Books., 2005.

FORTES, Débora. **A Explosão Das Redes Sem Fio**. São Paulo. INFO Exame Coleção *Wi-Fi*, P. 7-13, Abril. 2005. Acessado em 08 de março de 2007

GUERRA, André Roberto. **Entendendo os Protocolos**. 2002. Disponível em: <http://www.clubedasredes.eti.br/> . Acessado em: 19 de fevereiro de 2007.

MARTINS, Marcelo. **Protegendo Redes Wireless 802.11b**. 2003. Rio de Janeiro. Disponível em: <http://www.modulo.com.br> . Acessado em 16 de fevereiro de 2007 fevereiro de 2007

MICROSOFT. **Configurando Redes Sem Fio IEEE 802.11 Com Windows XP Para Residências e Pequenas Empresas**. 2005. Disponível em <http://www.microsoft.com/brasil> . Acessado em 03 de abril de 2007.

MICROSOFT. **Decisão sobre uma Estratégia de Rede sem Fio Protegida**. 2004. Disponível em: <http://www.microsoft.com/brasil> . Acessado em 04 de abril de 2007.

MICROSOFT. **Usando o 802.1X e a Criptografia Para Proteger WLANs**. Disponível em: <http://www.microsoft.com/brasil> . Acessado em 25 de março de 2007

MICROSOFT. **Visão Geral da Atualização de Segurança WPA Sem Fio no Windows XP**. 2005. Disponível em: <http://support.microsoft.com> . Acessado em 04 de abril de 2007.

PRADO, Eduardo. **Segurança em WLAN**. 2004. Disponível em: <http://www.wirelessbrasil.org> . Acessado em 08 de abril de 2007

RUFINO, Nelson Murilo de Oliveira. **Segurança de Redes Sem Fio**. São Paulo. Novatec, 2005.

SANTOS, Luiz Carlos. **Como funciona a VPN?**. 2001. Disponível em: <http://www.clubedasredes.eti.br>. Acessado em 17 de março de 2007

SANTOS, Luiz Carlos. **Uma Combinação Ideal, DSL/Cable Modem e WLAN**. 2003. Disponível em: <http://www.clubedasredes.eti.br> . Acessado em: 19 de abril de 2007

SYMANTEC. **Implementando Uma LAN Sem Fio Segura**. 2003. Disponível em:

<http://www.symantec.com> . Acessado em 08 de março de 2007

TEIXEIRA, Edson Rodrigues Duffles. **Tutoriais: Banda larga e VOIP**. 2005. Disponível

em: <http://www.teleco.com.br> . Acessado em: 04 de fevereiro de 2007.

VERÍSSIMO, Fernando. **O Problema de Segurança em Redes Baseadas no Padrão**

802.11. 2003. Disponível em: <http://www.lockabit.coppe.ufrj.br> . Acessado em 06 de fevereiro de 2007

GLOSSÁRIO

Autenticador	Equipamento que transmite a identidade do usuário para o servidor de autenticação.
<i>Bluetooth</i>	Conexão de rede sem fio de curto alcance.
<i>Backdoor</i>	Programa que permite a ação remota de um hacker sobre um computador infectado.
<i>Checksum</i>	Forma de detectar a consistência dos dados.
<i>Desktops</i>	Microcomputadores de mesa.
<i>Defacers</i>	Pessoas que alteram páginas de Internet alheias sem a devida autorização.
<i>Ethernet</i>	Tecnologia de interconexão para redes locais (LAN) baseada em envio de pacotes.
<i>Firmware</i>	<i>Software</i> embarcado, software que controla o <i>hardware</i> diretamente.
FTP	<i>File Transfer Protocol</i> . Protocolo de transferência de arquivo utilizado na Internet.
<i>Gateways</i>	Porta de ligação entre redes, interligando redes internas com outras internas ou com externas.
<i>Hardware</i>	Parte física do computador.
<i>Hosts</i>	Máquinas pertencentes à uma rede (computadores, <i>notebooks</i> , palms).
ISM	Faixas de frequência destinada a equipamentos que não necessitam de licenciamento da Agência Nacional de Telecomunicações – ANATEL.
<i>Laptop</i>	Computador portátil.
<i>Notebook</i>	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 <i>hosts</i> ligados entre si.
Servidor, <i>Server</i>	Máquina que atua servindo uma rede (dados, Internet)

<i>Software</i>	Seqüência de instruções a serem executadas no tratamento, direcionamento e manipulação de dados ou informações.
<i>Suplicante</i>	Usuário que deseja obter acesso à rede.
<i>Wireless</i>	Comunicação sem fio.