

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES**

ANÁLISE DE VULNERABILIDADES EM REDE SEM FIO

Análise de Vulnerabilidades em Rede Sem Fio

JANAINA SAIONARA RODRIGUES DE OLIVEIRA

Janaina Saionara Rodrigues de Oliveira

Graduada em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador:

Gleydson de Azevedo Ferreira Lima

**NATAL/RN
2007**

NATAL/RN
2007

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES**

ANÁLISE DE VULNERABILIDADES EM REDE SEM FIO

JANAINA SAIONARA RODRIGUES DE OLIVEIRA

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

Orientador:

Gleydson de Azevedo Ferreira Lima

**NATAL/RN
2007**

FARN

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES

ANÁLISE DE VULNERABILIDADES EM REDE SEM FIO

JANAINA SAIONARA RODRIGUES DE OLIVEIRA

Monografia apresentada ao curso de
em Redes de
da Faculdade
Natalense para o Desenvolvimento do
Rio Grande do Norte como requisito
obtenção do título de
em Redes de

RB 30.263

FARN

BIBLIOTECA

Nº M.00730

14/12/07

M

004.72

045a

2007

22.01

NATAL/RN
2007

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES

ANÁLISE DE VULNERABILIDADES EM REDE SEM FIO

JANAINA SAIONARA RODRIGUES DE OLIVEIRA

Monografia apresentada ao Curso de Especialização em Redes de Computadores da
Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, aprovada
em de de pela Comissão de Avaliação de Processos

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Oliveira, Janaina Saionara Rodrigues de

Análise de vulnerabilidades em rede sem fio: segurança de redes sem fio /
Janaina Saionara Rodrigues de Oliveira. – Natal: FARN, 2007.
53 f.

Orientador: Gleydson de Azevedo Ferreira Lima (M. Sc.)

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

1. Redes sem Fio – Monografia. 2. Segurança de Redes – Monografia. 3.
Vulnerabilidade das Redes – Monografia. I. Título.

RN/FARN/BC

CDU 004.72

Aluísio Ferreira da Rocha Neto, M.Sc.

Examinador

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES

ANÁLISE DE VULNERABILIDADES EM REDE SEM FIO

JANAINA SAIONARA RODRIGUES DE OLIVEIRA

Monografia apresentada ao Curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, aprovada em ____ de ____ de ____, pela banca examinadora composta pelos seguintes membros:

Gleydson de Azevedo Ferreira Lima, M.Sc.

Orientador

Aluizio Ferreira da Rocha Neto, M.Sc.

Examinador

RESUMO

ABSTRACT

A tecnologia 802.11 para rede sem fio tem sido amplamente utilizada por instituições e empresas com a finalidade de economia de infra-estrutura de cabeamento, além de prover interligação, maior mobilidade e flexibilidade para redes locais. Em contrapartida, existem algumas preocupações adicionais em segurança que são inerentes a um meio de comunicação sem fio.

Este trabalho apresenta uma descrição da forma de funcionamento do padrão IEEE 802.11, especificando as características envolvendo a segurança neste tipo de ambiente. São descritos alguns mecanismos de segurança de redes sem fio. Os mecanismos de segurança implementados, identifica as falhas associadas aos mesmos, e propõe melhorias que possibilitam a elevação do nível de segurança de redes locais sem fio.

A segurança de redes locais sem fio representa um novo desafio para a segurança da informação.

The security of wireless local area networks represents a new challenge in the information

PALAVRAS-CHAVE: Redes sem fio, segurança, criptografia.

KEY WORDS: Wireless, security, cryptography.

ABSTRACT

The 802.11 technology for wireless has been widely deployed by institutions and enterprises in order to don't spend money with cabling infra-structure, providing more intercommunication and great mobility and flexibility to the local networks. Nevertheless, there are several additional worries about security inherent to wireless medium.

This work describes how the standard IEEE 802.11 works, specifying the security in this kind of environment. Some of the most usual security techniques on computer networks, such as wireless, are described. The security mechanisms implemented in the wireless local area networks, identify the vulnerabilities associated with them, and propose a set of improvements which possibility rising the security level of the wireless local area networks.

The security of wireless local area networks represents a new challenge in the information security field.

KEY-WORDS: Wireless, security, cryptography.

ÍNDICE DE FIGURAS

FIGURA 01 – OS PAPEIS NO 802.1X	12
FIGURA 02 – Rede Infraestruturada	13
FIGURA 03 – Rede Ad-Hoc	14
FIGURA 04 – Como as ondas de rádio viajam pelo espaço	17
FIGURA 05 – Interrupção	30
FIGURA 06 – Intersecção	31
FIGURA 07 – Modificação	31
FIGURA 08 – Fabricação	31
FIGURA 09 – Warchalking.....	34
2.2 AUTENTICAÇÃO DE USUÁRIOS COM O 802.1X	15
2.3 TIPOS DE REDES SEM FIO	17
2.4 APLICAÇÕES DE REDES SEM FIO	18
2.5 OUTROS ASPECTOS DAS REDES SEM FIO	20
2.6 SISTEMAS DE SEGURANÇA	22
2.6.1 Falhas de segurança	22
3 ANÁLISE DAS VULNERABILIDADES	24
3.1 VULNERABILIDADES	24
3.2 MECANISMOS DE SEGURANÇA	26
3.2.1 Endereçamento MAC	26
3.2.2 Wired Equivalent Privacy (WEP)	27
3.2.3 WPA Protected Access (WPA)	28
3.3 RISCOS E AMEAÇAS	28
3.3.1 Riscos Internos	29
3.3.2 Riscos Externos	30
3.3.3 Vulnerabilidades nos protocolos	31
3.4 TÉCNICAS E FERRAMENTAS DE ATAQUE	33
3.4.1 Ataques mais comuns nas redes sem fio	37
3.4.2 Ferramentas para redes sem fio	40
3.5 MÉTODOS DE DEFESA	45
3.5.1 ESSID	43
3.5.2 Substituição do endereço MAC	45
3.5.3 Autenticação	46
3.5.4 PSPP	46
3.5.5 Utilização do 802.1X e RADIUS	46
3.5.6 WEP	47
3.5.7 Utilização do 802.11i	47
3.5.8 WPA	47
3.5.9 Uso de Criptografia	47
3.5.10 Certificados digitais	47

SUMÁRIO

1	INTRODUÇÃO.....	10
1.1	MOTIVAÇÕES	10
1.2	OBJETIVOS	11
1.3	ORGANIZAÇÃO DO TRABALHO	11
2	FUNDAMENTAÇÃO TEÓRICA.....	12
2.1	PADRÕES DA TECNOLOGIA SEM FIO	12
2.1.1	Padrão 802.11b	13
2.1.2	Padrão 802.11a	13
2.1.3	Padrão 802.11g	14
2.1.4	Padrão 802.11i	14
2.1.5	Padrão 802.11n	15
2.2	AUTENTICAÇÃO DE USUÁRIOS COM O 802.1X.....	15
2.3	TIPOS DE REDES SEM FIO.....	17
2.4	APLICAÇÕES DE REDES SEM FIO	18
2.5	OUTROS ASPECTOS DAS REDES SEM FIO	20
2.6	SISTEMAS DE SEGURANÇA	22
2.6.1	Falhas de segurança	22
3	ANÁLISE DAS VULNERABILIDADES.....	24
3.1	VULNERABILIDADES	24
3.2	MECANISMOS DE SEGURANÇA.....	26
3.2.1	Endereçamento MAC	26
3.2.2	<i>Wired Equivalent Privacy (WEP)</i>	27
3.2.3	<i>Wi-Fi Protected Access (WPA)</i>	28
3.3	RISCOS E AMEAÇAS	29
3.3.1	Riscos Internos.....	29
3.3.2	Riscos Externos	31
3.3.3	Vulnerabilidades nos protocolos.....	33
3.4	TÉCNICAS E FERRAMENTAS DE ATAQUE	35
3.4.1	Ataques mais comuns nas redes sem fio.....	37
3.4.2	Ferramentas para redes sem fio	40
3.5	MÉTODOS DE DEFESA.....	45
3.5.1	ESSID	45
3.5.2	Substituição do endereço MAC	45
3.5.3	Autenticação	46
3.5.4	PSPF	46
3.5.5	Utilização do 802.1x e RADIUS	46
3.5.6	WEP	47
3.5.7	Utilização do 802.11i.....	47
3.5.8	WPA	47
3.5.9	Uso de Criptografia.....	48
3.5.10	Certificados digitais.....	49

3.5.11	Monitoramento do ambiente.....	49
3.5.12	Mantendo a rede sem fio segura.....	50
4	CONCLUSÃO.....	51
	REFERÊNCIAS BIBLIOGRÁFICAS	53

No mundo real, as pessoas interessadas em segurança podem redirecionar os ataques de fora das portas ou tirar o nome da empresa da porta da frente. Outros colocam grandes letreiros "Entrada Proibida!". Essas abordagens não impedem que invasores penetrem e infiltrem-se, mas são análogas a várias abordagens comuns para proteger uma rede sem fio.

A segurança de uma rede sem fio é muito importante, especialmente para a integridade de serviços e de informações valiosas. Por exemplo, redes transmitindo números de cartões de crédito para verificação ou armazenando informações sigilosas, definitivamente precisam ter sua segurança reforçada.

O objeto principal do trabalho é fornecer uma visão abrangente das características e peculiaridades de redes em fio, como também fornecer o entendimento das vulnerabilidades comuns associadas à tecnologia, seus riscos e as possibilidades de uso com maior segurança.

1.1. MOTIVAÇÕES

Por ser uma tecnologia relativamente recente, muitas vulnerabilidades podem ser identificadas e outras ainda serão descobertas. É justamente explorando estas vulnerabilidades que atacantes se infiltram nas redes sem fio. A forma comum de utilização para explorar estas vulnerabilidades é através do uso de ferramentas desenvolvidas especificamente para esta finalidade.

Ataques direcionados às redes sem fio além de comprometer os recursos locais, podem comprometer os recursos de outras redes com as quais esta se interconecta. Outro fator determinante da segurança em redes sem fio é relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque.

Sabe-se que os ataques dirigidos às redes sem fio podem ser identificados e as contornadas, porém para serem tomadas efetivamente, é necessário que haja a análise das vulnerabilidades inerentes às redes 802.11x.

1 INTRODUÇÃO

A popularidade das redes sem fio se deve a sua flexibilidade e mobilidade. No entanto, existem alguns riscos de segurança que surgem como resultado direto do modo como as WLANs (*Wireless Local Area Network* - Redes Locais sem Fio) funcionam.

No mundo real, as pessoas interessadas em segurança podem remover os números de rua das casas ou tirar o nome da empresa da porta da frente. Outras colocam grandes letreiros "Entrada Proibida!". Essas abordagens não impedem que assaltantes penetrem e infelizmente são análogas a várias abordagens comuns para proteger uma rede sem fio.

A segurança de uma rede sem fios é muito importante, especialmente para a hospedagem de serviços e de informações valiosas. Por exemplo, redes transmitindo números de cartão de crédito para verificação ou armazenando informações sigilosas, definitivamente precisam ter sua segurança reforçada.

O objeto principal do trabalho é fornecer uma visão abrangente das características e peculiaridades de redes em fio, como também fornecer o entendimento das vulnerabilidades comuns associadas à tecnologia, seus riscos e as possibilidades de uso com maior segurança.

1.1 MOTIVAÇÕES

Por ser uma tecnologia relativamente recente, muitas vulnerabilidades podem ser encontradas e outras ainda serão descobertas. É justamente explorando estas vulnerabilidades que atacantes se infiltram nas redes sem fio. A forma comumente utilizada para explorar estas vulnerabilidades é através do uso de ferramentas desenvolvidas especificamente para esta finalidade.

Ataques direcionados às redes sem fio além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais esta se interconecta. Outro fator determinante da segurança em redes sem fio é relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque.

Para que os ataques dirigidos às redes sem fio possam ser identificados e as contramedidas possam ser tomadas eficazmente, é necessário que haja a análise das vulnerabilidades inerentes às redes 802.11x.

2ª FUNDAMENTAÇÃO TEÓRICA

1.2 OBJETIVOS

A análise das vulnerabilidades é voltada ao estudo das falhas de segurança presentes na estruturação dos protocolos 802.11x. Soma-se a esta análise, outra onde se leva em consideração a comunicação entre os dispositivos de rede sem fio.

O estudo das técnicas utilizadas para explorar estas vulnerabilidades também é realizado. Com este estudo, é identificado o grau de conhecimento do atacante, informações de vulnerabilidades ainda não conhecidas e formas eficazes de se identificar quando algum destes ataques está sendo disparado contra determinada rede.

2.1 PADRÕES DA TECNOLOGIA SEM FIO

1.3 ORGANIZAÇÃO DO TRABALHO

O trabalho está organizado da seguinte forma: O capítulo 2 ilustra a conceituação teórica necessária sobre o funcionamento de redes sem fio e seus protocolos, conceitos importantes como tipos de redes sem fio, mecanismos de autenticação, aplicações e sistemas de segurança são estudados para um melhor entendimento de suas vulnerabilidades.

No capítulo 3, serão estudadas as principais ferramentas utilizadas para explorar as falhas das redes sem fio. Serão mostrados também os riscos e ameaças, as vulnerabilidades nos protocolos, as técnicas e ferramentas de ataques a redes desprotegidas e os principais métodos de defesa às redes sem fio.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica é necessária para o entendimento deste trabalho, o qual baseia-se na análise das vulnerabilidades e dos ataques inerentes a redes sem fio 802.11x.

São ilustrados conceitos fundamentais das redes sem fio, tais como os padrões dessa tecnologia, tipos de redes sem fio, suas aplicações, etc.

Por fim, são apresentados importantes aspectos sobre segurança de computadores e redes, tomando como parâmetro principal a segurança de redes sem fio, apontando quais características são desejáveis *a priori*.

2.1 PADRÕES DA TECNOLOGIA SEM FIO

Independentemente do contexto, uma comunicação bem-sucedida só pode acontecer se todas as partes interessadas estiverem falando a mesma linguagem. No mundo das redes, essa linguagem é chamada de *especificação*, e se for objeto de um acordo por um número suficiente de partes interessadas ou se receber um selo de aprovação por um órgão da indústria, essa especificação poderia evoluir e se tornar um *padrão*.

Quando fala-se de redes sem fio, estamos nos referindo a uma família de padrões que funcionam conjuntamente: equipamentos que suportam um dos padrões sempre são compatíveis com outros dispositivos que suportam o mesmo padrão.

De acordo com RUFINO (2005, p. 26), o *Institute of Electrical and Electronics Engineers* (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio. Um desses grupos de trabalho foi denominado 802.11, que reúne uma série de especificações que basicamente definem como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes móveis. Ao longo de tempo foram criadas várias extensões, onde foram incluídas novas características operacionais e técnicas. O padrão 802.11 original (também conhecido como Wi-Fi), em termos de velocidade de transmissão, provê, no máximo, 2 Mbps, trabalhando com a banda de 2,4 GHz.

A família 802.11 conta com as principais extensões (ou sub padrões) descritas na ordem que foram especificadas.

2.1.1 Padrão 802.11b

O primeiro sub padrão a ser definido permite 11 Mbps de velocidade de transmissão máxima, porém pode comunicar-se a velocidades mais baixas, como 5,5, 2 ou mesmo 1 Mbps. Opera na frequência de 2,4 GHz e usa somente DSSS (*Direct Sequence Spread Spectrum – espalhamento espectral por sequência direta para transmitir e receber dados*). Permite um número máximo de 32 clientes conectados. Foi ratificado em 1999 e definiu padrões de interoperabilidade bastante semelhante aos da rede Ethernet. Há limitação em termos de utilização de canais, sendo ainda hoje o padrão mais popular e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis. Porém, está claro que esse padrão chegou ao limite e já está sendo evitado em novas instalações e em atualizações do parque instalado.

2.1.2 Padrão 802.11a

Definido após os padrões 802.11 e 802.11b e tentando resolver os problemas existentes nestes, o 802.11a tem como principal característica o significativo aumento da velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo), mas podendo operar em velocidades mais baixas. Outra diferença é a operação na faixa de 5 GHz, uma faixa com poucos concorrentes, porém com menor área de alcance. Oferece também aumento significativo na quantidade clientes conectados (64) e ainda no tamanho da chave usada com WEP (*Wired Equivalent Privacy - Privacidade equivalente à das redes com fios*), chegando em alguns casos a 256 bits (mas possui compatibilidades com os tamanhos menores, com 64 e 128 bits). Finalmente, adota o tipo de modulação OFDM (*Orthogonal Frequency Division Multiplexing/Modulation – modo de transmissão com capacidade de identificar interferências e ruídos, permitindo troca de ou isolamento de uma faixa de frequência, ou mudar a velocidade de transmissão*), diferentemente do DSSS usado no 802.11b. Outra vantagem deste padrão consiste na quantidade de canais não sobrepostos disponíveis, um total de 12, diferentemente dos 3 canais livres disponíveis nos padrões 802.11b e 802.11g, o que permite cobrir uma área maior e mais densamente povoada, em melhores condições que outros padrões.

2.1.3 Padrão 802.11g

Esse padrão é mais recente que os comentados anteriormente e equaciona a principal desvantagem do 802.11a, que é utilizar a faixa de 5 GHz e não permitir interoperação com 802.11b. O fato de o 802.11g operar na mesma faixa (2,4 GHz) permite até que equipamentos de ambos os padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática do parque instalado. Além disso, o 802.11g incorpora várias das características positivas do 802.11a, como utilizar também modulação OFDM e velocidade a cerca de 54 Mb nominais.

O 802.11g tem várias medidas intermediárias para velocidade, assim não se cai de uma velocidade em 54 Mb diretamente para 11 Mb ou um mais lenta.

De fato, que pode ser um pouco mais lento que uma rede 802.11a equivalente na mesma situação. Isso ocorre porque o 802.11g deve manter a compatibilidade com dispositivo 802.11b, que utilizam um método diferente de codificação de dados nas ondas de rádio, e o overhead de gerenciar quais dispositivos em uma rede 802.11b / 802.11g mista pode tornar mais lenta a velocidade de envio em qualquer momento.

Uma das grandes vantagens do 802.11g em relação ao 802.11b é que ele trata mais apropriadamente a inevitável reflexão de sinal. O 802.11g (como o 802.11a) divide o espectro de maneira que permita aos receptores tratarem essas reflexões de uma forma mais simples, mas, mais efetiva que o 802.11b.

Como ocorre com o 802.11a, configurar clientes e pontos de acesso 802.11g é exatamente o mesmo que configurar dispositivos 802.11b.

2.1.4 Padrão 802.11i

Homologado em junho de 2004, este padrão diz respeito a mecanismos de autenticação e privacidade e pode ser implementado em vários de seus aspectos aos protocolos existentes. O principal protocolo de rede definido neste padrão é chamado RSN (*Robust Security Network*), que permite meios de comunicação mais seguros que os difundidos atualmente. Está inserido neste padrão também o protocolo WPA, que foi desenhado para prover soluções de segurança mais robustas, em relação ao padrão WEP, além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES (*Advanced Encryption Standard*).

2.1.5 Padrão 802.11n

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

2.2 AUTENTICAÇÃO DE USUÁRIOS COM O 802.1X

Como cita RUFINO (2005, p. 29), o protocolo IEEE 802.1X permite autenticação baseada em métodos já consolidados, como RADIUS (*Remote Authentication Dial-in User Service - Serviço de autenticação remota de usuários discados*), de forma escalável e expansível. Desta maneira é possível promover um único padrão de autenticação, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas e discadas etc.), e manter a base de usuários em um repositório único, quer seja em banco de dados convencional, LDAP (*Lightweight Directory Access Protocol - protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP*) ou qualquer outro reconhecido pelo servidor de autenticação.

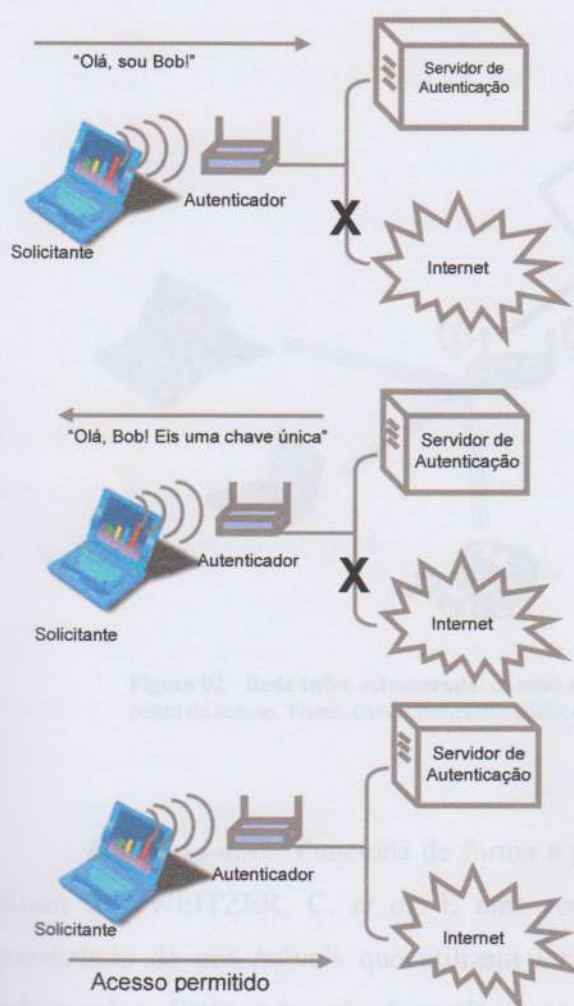
É importante notar que para esta infra-estrutura funcionar, basta que os componentes – concentrador, servidor RADIUS e outros opcionais, como LDAP, *Active Directory*, banco de dados convencionais etc. – estejam interligados por meio de uma rede. A localização física de cada elemento tem pouca importância.

Este padrão pressupõe a presença de elemento autenticador, tipicamente um servidor RADIUS, e um requerente, ou seja, o elemento que requer autenticação, no caso o equipamento cliente. Essa autenticação é feita antes de qualquer outro serviço de rede estar disponível ao usuário requerente. Este primeiramente, solicita autenticação ao autenticador, que verifica em sua base de dados as credenciais apresentadas pelo cliente, e conforme a validade ou não dessas credenciais (normalmente o binômio usuário/senha), permite ou não o acesso a estas. Uma autenticação bem sucedida irá deflagrar todos os outros processos para permitir ao usuário acesso aos recursos da rede, o que pode incluir receber um endereço via DHCP ou outro protocolo de

atribuição de endereços IP, com informações de roteamentos, servidores DNS, liberar roteamento na porta do *switch* etc.

É fácil visualizar o uso deste padrão para coibir o uso não autorizado de pontos de rede, pois em geral pontos de rede desocupados estão ativos e operacionais. Para isso, basta conectar um equipamento de rede para ter acesso total ou parcial aos serviços da rede da organização ou mesmo acesso à Internet.

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



1. Primeiro, um solicitante, tendo se associado a um ponto de acesso, envia suas credenciais de login (como um nome de usuário e senha) para o autenticador, que vai passá-las adiante ao servidor de autenticação. O ponto de acesso não dá ao solicitante acesso à Internet de modo algum.

2. Em seguida, o servidor de autenticação confirma a identidade do solicitante e, então, responde novamente por meio do autenticador, fornecendo ao solicitante uma chave de criptografia única para utilizar a rede local.

3. Por fim, com a chave de criptografia em mãos e suas credenciais confirmadas, o solicitante pode passar tráfego pelo autenticador para a Internet (ou rede local, conforme caso).

Figura 01 - "Os papéis no 802.1X" – ENGST E FLEISHMAN (2005, p.248)

2.3 TIPOS DE REDES SEM FIO

Redes Infra-Estruturadas: O concentrador é o equipamento central de uma rede que se utiliza dessa topologia. Assim, um ponto único de comunicação é rodeado de vários clientes, fazendo com que todas as configurações de segurança fiquem concentradas em um só ponto. Tal fato permite controlar todos os itens (autorização, autenticação, controle de banda, filtros de pacote, criptografia etc.) em um único ponto. Outra vantagem deste modelo é facilitar a interligação com redes cabeadas e/ou com a Internet, já que em geral o concentrador também desempenha o papel de *gateway* ou ponte. Toda a comunicação é feita via este Ponto de Acesso, sendo o seu funcionamento semelhante ao da telefonia celular, onde toda a comunicação deve passar por esse ponto central.

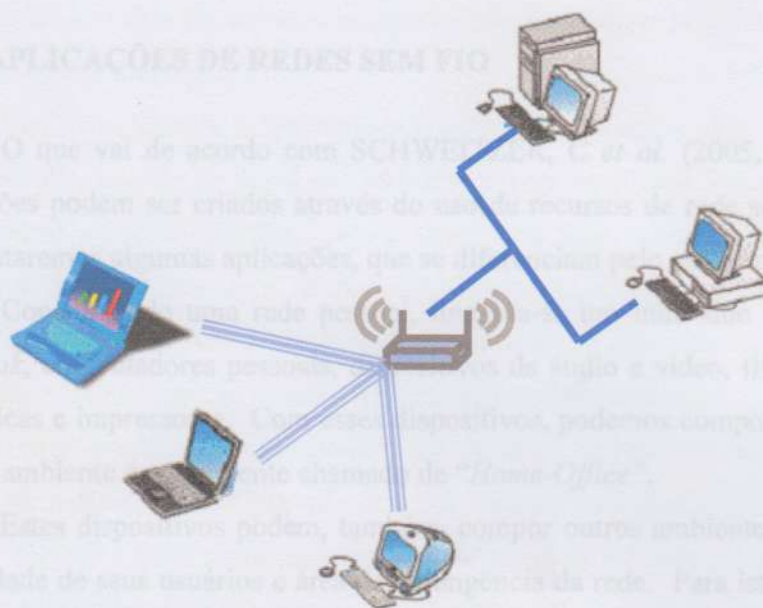


Figura 02 - Rede Infra-estruturada: clientes se associam com um ponto de acesso. Fonte: (www.projetoderedes.com.br)

Redes Ad-doc: Funciona de forma a prescindir de um ponto central de conexão. Como dizem SCHWEITZER, C. et al: É uma rede formada sem qualquer administração central, consistindo de nós móveis que utilizam uma interface de rede sem fio para envio de suas informações. Estas redes são formadas espontaneamente e seus dispositivos são móveis, sua

configuração deve ser feita com a mínima intervenção possível do usuário e os seus nós/membros devem ser capazes de trocar informações ou até mesmo prover serviços entre si.



Figura 03 - Rede Ad-Hoc: Sem necessidade de um ponto de acesso centralizado. Fonte: (www.projetoderedes.com.br)

2.4 APLICAÇÕES DE REDES SEM FIO

O que vai de acordo com SCHWEITZER, C *et al.* (2005, p.5), diversos ambientes de aplicações podem ser criados através do uso de recursos de rede sem fio. Dentro do contexto, apresentaremos algumas aplicações, que se diferenciam pelo ambiente e área de abrangência.

Considerando uma rede pessoal, imagina-se um indivíduo com seus dispositivos como *notebook*, computadores pessoais, dispositivos de áudio e vídeo, filmadoras, webcams, agendas eletrônicas e impressoras. Com esses dispositivos, podemos compor um ambiente pessoal. Este tipo de ambiente é comumente chamado de “*Home-Office*”.

Estes dispositivos podem, também, compor outros ambientes de redes, de acordo com a mobilidade de seus usuários e área de abrangência da rede. Para isto, recursos de redes sem fio, como pontos de acessos e roteadores, são necessários a fim de garantir a mobilidade desses usuários. Neste caso, cenários de redes, públicas ou corporativas, podem ser definidos em diferentes escalas.

Inicialmente podemos tomar, como exemplo, as redes locais sem fio, usadas em museus, que funcionam, muitas vezes, em prédios tombados, onde quase sempre se proíbe a realização de obras civis para passagem de dutos e instalação de cabeamento. Outros cenários de redes locais bastante comuns são os chamados *hot spots*, que consistem na formação de redes sem fio, fazendo uso de pontos de acesso, serviços de rede e Internet providos em áreas públicas como

cafeterias (*cyber cafés*), salas de conferencias, aeroportos, hotéis, estações de trem ou ainda, em áreas públicas de campus universitários ou até mesmo de organizações privadas.

Se aumentarmos a área de abrangência destas redes, passamos a ter as redes metropolitanas sem fio. Assim, ao invés das redes locais, anteriormente citadas, estarem conectadas a uma rede tradicional cabeada, podem estar conectadas a redes sem fio de banda larga, as redes metropolitanas sem fio. Cenários de aplicação para as redes metropolitanas sem fio têm sido testados, por serem tecnologias inovadoras, que podem ser usadas na interligação de prédios (ponto-multiponto) com sub-redes locais e na provisão de banda larga em lugares remotos ou de pouco acesso, com ambientes rurais ou ilhas remotas.

Uma rede sem fio pode ter acesso público ou privado, dependendo de sua aplicabilidade e serviços, disponibilidade rápida e fácil acesso. Considerando, os diversos cenários discutidos anteriormente, que incluem ambientes estruturados em definitivo, ambientes de caráter temporário, serviços inovadores ou extensões de serviços já existentes, podem-se citar alguns exemplos de aplicações:

Aplicações com jogos e utilitários: muitas vezes estas aplicações não necessitam de serviço de comunicação, mas se os jogos são interativos com múltiplos jogadores, comunicações *peer-to-peer* podem ser consideradas. Neste caso, uma rede *ad-hoc* é criada temporariamente – no momento da interação com os demais jogadores, devendo a disponibilidade do serviço de comunicação ser mantida o tempo todo, bem como, o desempenho da aplicação, no dispositivo em questão ser satisfatório durante a interação entre os jogadores.-;

Softwares pessoais, como processadores de texto, apresentações e agendas: essas aplicações podem ser usadas em múltiplas plataformas, podendo um usuário possuir uma versão do *software* em seu *laptop* e uma outra mais atualizada ou mais robusta em seu *desktop*. Os documentos gerados no *software* de um dispositivo devem ser compatíveis com os documentos gerados no outro dispositivo, pois um usuário pode trabalhar em um ambiente, ou em outro, sincronizando múltiplas versões. Soluções proprietárias de controle de versões de documentos existem e são razoavelmente eficientes, no entanto, não consideram um ambiente de rede com comunicação ubíqua, requisitando aplicações cliente-servidor que permitem acesso remoto aos documentos na presença de enlaces de comunicação baseados em tecnologia de rede sem fio (ambientes móveis);

Aplicações para redes ad-hoc e groupware: as aplicações são implementadas em casos como reuniões e conferencias, onde se reúnem diversos usuários que pretendem trocar informações

entre si. Neste caso, não existe grande mobilidade, mas estes usuários podem usufruir a facilidade de se conectarem sem a necessidade de uma infra-estrutura de rede cabeada, criando-se uma rede sem fio temporária e segura. Estes usuários podem, por exemplo, estabelecer uma rede *ad-hoc* para trocar documentos ou executar aplicações de *groupware* para atualizar seus planos de trabalho;

Aplicações sensíveis à localização como guias interativos: este tipo de aplicação é bem interessante, pois explora o fato de o usuário ser móvel. Um usuário pode estar andando por diversos ambientes como lugares turísticos, praças de alimentação, centro de compras, tendo a possibilidade de se conectar a rede como uma entidade visitante e ter disponível em seu dispositivo móvel: apresentações (multimídia), sobre o ambiente em que se encontra; dados históricos (texto e/ou vídeo); cardápios dos diversos restaurantes que ali se encontra, no caso de uma praça de alimentação; e a relação das lojas, produtos e serviços disponíveis no centro de compras. Nestes ambientes, são necessárias soluções para descoberta dos serviços, permissão do uso do ambiente de rede, bem como adaptação das aplicações para os diversos dispositivos que irão surgir e requisitar serviços ao longo do tempo.

2.5 OUTROS ASPECTOS DAS REDES SEM FIO

A tecnologia Wi-Fi ainda não é madura e, portanto, muitos dos seus padrões ainda estão evoluindo e possuem falhas. É muito importante conhecer os padrões existentes hoje, suas potenciais vulnerabilidades e como isso pode afetar cada rede. Com conhecimento mais claro desse cenário, torna-se mais fácil entender as particularidades de cada solução e como as tecnologias podem ser complementadas para aumentar sua eficiência. Tudo isso é fundamental, também, para que o administrador tenha uma noção mais precisa dos riscos e possa avaliar claramente quais são aceitáveis, em função dos benefícios, e quais não são.

Redes sem fio contam com os mesmos princípios que guiam telefones sem fio e todos esses outros dispositivos sem fio. Um transceptor (uma combinação de transmissor e receptor) envia sinais fazendo vibrar ondas de radiação eletromagnética que se propagam a partir de uma antena; a mesma antena recebe sinais sofrendo uma vibração apropriada mediante a passagem de sinais nas frequências corretas.

Passando Sinais através de Paredes

Segundo ENGST e FLEISHMAN (2005, p.06) a parte mágica das redes sem fio é como elas funcionam não apenas sem cabos, mas também quando nem mesmo se pode ver o ponto de acesso ao qual está se conectando. Embora esse caminho obstruído seja óbvio, isso nem sempre é verdade.

As primeiras redes sem fio utilizavam frequências de radiação eletromagnética justamente abaixo do espectro visível, ou seja, o infravermelho. A rede de infravermelho tinha (e ainda tem) uma limitação enorme: precisa de uma perfeita linha de visão entre um transceptor de infravermelho e outro. Em grandes escritórios com várias salas, é difícil posicionar os transceptores em um ponto suficientemente alto para que o sinal passe pelas repartições e é igualmente difícil assegurar que as pessoas que estão paradas conversando no local não bloqueiem o sinal de rede.

Redes sem fio superaram o problema da linha de visão pulando para uma parte diferente do espectro eletromagnético. As redes sem fio modernas, em geral, funcionam a 2,4 GHz ou 5 GHz, bem abaixo do espectro da luz visível. Nessas frequências, o comprimento de onda de cada transmissão é tão pequeno que os sinais podem atravessar objetos aparentemente sólidos.

Apesar de as redes sem fio modernas oferecerem um alcance mais longo quando têm uma linha de visão, elas também funcionam a distancias curtas em espaços internos. Entretanto, alguns obstáculos internos podem reduzir a qualidade do sinal e tornar necessário o ajuste do layout da rede. Por exemplo, paredes de tijolos podem conter uma grande quantidade de água e essa água pode bloquear a energia das frequências a 2,4 GHz em que as redes funcionam. Algumas casas e escritórios têm metal na parte interna, como tela de arame que sustenta o gesso ou a tubulação, e esses metais também podem interferir nos sinais de rede.

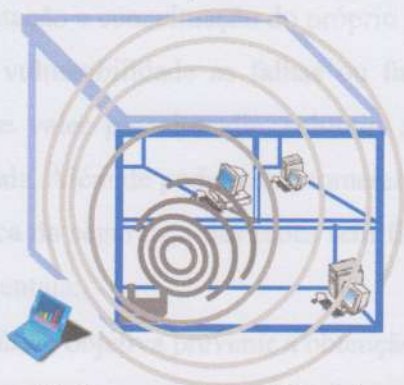


Figura 04 - Como as ondas de rádio viajam pelo espaço.

Fonte: ENGST e FLEISHMAN (2005, p.06)

2.6 SISTEMAS DE SEGURANÇA

Os sistemas de segurança têm, como objetivo, proteger um ambiente contra vulnerabilidades e ameaças. Isso é feito fazendo-se uso dos serviços de segurança.

De uma forma geral, embora todos os serviços de segurança sejam importantes aplicações terão diferentes requisitos de segurança e demandarão que diferentes serviços de segurança sejam priorizados. Na maioria das vezes, estas aplicações estão vinculadas a ambientes específicos de utilização que ditarão seus requisitos. Como exemplo, pode-se citar uma aplicação bancária, onde o serviço de integridade seguido dos serviços de confidencialidade e disponibilidade são os mais importantes.

Cada tecnologia de rede sem fio ou mesmo cabeada, implementa nativamente alguns mecanismos e serviços de segurança. Como essas redes vão ser usadas, em que tipo de ambiente e quais as aplicações suportadas irão determinar a necessidade de se implementar serviços e mecanismos de segurança adicionais objetivando assegurar a robustez do sistema de segurança como o todo e o nível de proteção exigido pelo ambiente considerado.

Para se determinar quais os serviços e mecanismos de segurança dever implementados por um dado sistema de segurança, devem-se então, ter claros as vulnerabilidades, as ameaças e os riscos toleráveis vinculados aos bens e recursos que se deseja proteger.

2.6.1 Falhas de segurança

Segundo DUARTE (2003, p. 26), as redes sem fio tornaram-se alvo de exaustivos estudos e muitos ataques foram desenvolvidos e/ou adaptados para poderem explorar das fraquezas presentes nestas redes. Além disso, estas redes apresentam falhas graves de segurança e problemas na implementação e conceituação do próprio protocolo.

Entende-se por vulnerabilidade as falhas ou falta de segurança das quais pessoas mal intencionadas podem se valer para invadir, subtrair, acessar ilegalmente, adulterar e destruir informações confidenciais. Além de poder comprometer, corromper e inutilizar o sistema.

A pesquisa acerca da segurança das redes sem fio de computadores leva em consideração alguns aspectos fundamentais:

- *Confidencialidade*: objetiva prevenir a obtenção de informação sem autorização;
- *Disponibilidade*: objetiva prevenir que recursos ou informações fiquem indisponíveis;

- **Integridade:** garantir que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor;
- **Usabilidade:** objetiva prevenir que um serviço tenha sua utilidade deteriorada devido à segurança.

Estas características devem ser balanceadas para que o sistema não fique tão seguro a ponto de usuários legítimos não consigam utiliza-lo eficientemente, e que este sistema também não seja inseguro a ponto de permitir a ação de usuários não autorizados.

Existem peculiaridades nos ataques inerentes à redes sem fio. Uma destas é o fato da utilização de equipamento próprio por parte do atacante. Ou seja, há a necessidade de que o atacante esteja dentro da área de cobertura da rede em questão e que esteja utilizando seu próprio equipamento.

As análises baseiam-se no protocolo das redes sem fio e nas possíveis configurações dos dispositivos. As redes Wi-Fi estão, em princípio, expostas a dois perigos principais. O primeiro é um intruso conseguir-se conectar ao ponto de acesso, isto lhe permitiria utilizar alguns dos recursos da rede, como por exemplo: a conexão à Internet e até mesmo impressoras compartilhadas. O segundo é que o invasor consegue de fato acessar a rede interna, seja via doméstica ou corporativa, o que lhe permitiria roubar dados, e-mails, nomes de conta e arquivos de trabalho.

Frete à primeira ameaça, a proteção mais utilizada é algum sistema de autenticação que obriga cada usuário a demonstrar sua identidade no momento de conexão. Isso pode ser feito por meio de uma senha de acesso ou pela validação de um dispositivo específico, como o computador. A identificação do PC é um dos mecanismos de controle de acesso mais simples disponíveis. Para isso, se realiza uma análise do cartão de conexão que foi instalado no PC que deseja se conectar. Esta análise consiste na identificação do endereço MAC (Media Access Control – endereço único atribuído a cada adaptador de rede) do cartão. No entanto, este mecanismo de filtragem pode ser burlado com grande facilidade por um hacker.

Frete à segunda ameaça, a proteção mais indicada é a criptografia da informação que circula pela rede Wi-Fi. O primeiro mecanismo de segurança utilizado foi o denominado WEP – *Wired Equivalent Privacy* – que se baseia no algoritmo de criptografia RC4; pode empregar chaves de criptografia de 64 a 256 bits. No entanto, já faz tempo que a criptografia WEP foi

3 ANÁLISE DAS VULNERABILIDADES

No desenvolvimento são tratados os ataques, e as vulnerabilidades existentes no protocolo 802.11.

Serão analisados os riscos inerentes das redes sem fio, sendo que estes são classificados em riscos externos e riscos internos. Estes riscos também são vulnerabilidades que podem ser exploradas através do uso de ferramentas específicas que também serão analisadas.

Tem-se por objetivo, portanto, ilustrar as vulnerabilidades encontradas através dos estudos realizados, mostrando como estas podem introduzir riscos à segurança e como estas podem ser de fato exploradas.

3.1 VULNERABILIDADES

As análises baseiam-se no protocolo das redes sem fio e nas possíveis configurações dos dispositivos. As redes Wi-Fi estão, em princípio, expostas a dois perigos principais. O primeiro é um intruso conseguir se conectar ao ponto de acesso. Isto lhe permitiria utilizar alguns dos recursos da rede, como por exemplo: a conexões à Internet e até mesmo impressoras compartilhadas. O segundo é que o invasor consiga de fato acessar a rede interna, seja ela doméstica ou corporativa, o que lhe permitiria roubar dados, senhas, nomes de conta e arquivos de trabalho.

Frente à primeira ameaça, a proteção mais utilizada é algum sistema de autenticação que obrigue todo usuário a demonstrar sua identidade no momento da conexão. Isto pode ser feito por meio de uma senha de acesso ou pela validação de um dispositivo específico, como o computador. A identificação do PC é um dos mecanismos de controle de acesso mais simples disponíveis. Para isso, se realiza uma análise do cartão de conexão sem fio instalado no PC que deseja se conectar. Esta análise consiste na identificação do endereço MAC (*Media Access Control* – endereço único atribuído a cada adaptador de rede) do cartão. No entanto, este mecanismo de filtragem pode ser burlado sem grande dificuldade por um hacker.

Frente à segunda ameaça, a proteção mais indicada é a codificação da informação que circula pela rede Wi-Fi. O primeiro mecanismo de segurança utilizado foi o denominado WEP – *Wired Equivalent Privacy* – que se baseia no algoritmo de criptografia RC4 e pode empregar chaves de criptografia de 64 a 256 bits. No entanto, já faz tempo que a criptografia WEP foi

rompida, portanto qualquer hacker que tenha acesso à rede sem fio e que capture alguns megas de informação criptografada poderá romper a chave em poucos minutos.

Há algum tempo está disponível outro padrão, o WPA – *Wi-Fi Protected Access*, que melhorou a proteção proporcionada pelo WEP, e depois, foi criado o padrão 802.11i, também conhecido como WPA2, com mecanismos ainda mais fortes de autenticação e criptografia do tráfego.

A classificação quanto aos riscos é realizada para o entendimento dos ataques e como estes podem ser identificados e minimizados.

Como cita SCHWEITZER, C. *et al.* (2005, p.2), as vulnerabilidades são pontos nos quais o sistema é suscetível a ataques e ameaças de segurança. Existem os seguintes tipos básicos de vulnerabilidades de segurança:

- **Físicas:** os prédios e salas que mantêm sistemas computacionais, são vulneráveis podendo ser invadidos, por exemplo, através de arrombamento;
- **Naturais:** incluem desastres de ordem **natural** e **as ameaças ambientais**. Como exemplos de desastres, podem-se citar: incêndios, inundações, terremotos e perda de energia. As ameaças ambientais, por sua vez, podem advir de poeira, umidade ou condições de temperatura inadequada para instalações computacionais;
- **Hardware e Software:** **Falhas de hardware e software** podem comprometer toda a segurança de um sistema, abrindo **buracos** ou **portas no sistema**, ou ainda, fazê-lo comportar-se de forma imprevista. Como exemplo de falha de hardware, pode-se citar a queda de um enlace ou mesmo do sistema de contingência. No caso de software, a configuração errônea de um roteador de uma rede, por exemplo, pode impedir o tráfego correto de informação entre os sistemas;
- **Mídia:** mídias diversas como discos, fitas e material impresso podem ser facilmente **roubados** ou **danificados**;
- **Emanação:** Os sinais emitidos por computadores. Equipamentos de rede e monitores podem ser captados e decifrados permitindo a **obtenção das informações** contidas no sistema ou a **inferência sobre seu conteúdo**;
- **Comunicação:** mensagens em transito podem ser **interceptadas**, **desviadas** ou **forjadas**. Linhas de comunicação podem ser escutadas ou interrompidas;

- **Humanas:** As **pessoas** que **administram** e **usam** o sistema representam sua maior vulnerabilidade. Os **usuários**, **operadores** ou **administradores** do sistema podem cometer **erros** que comprometem o sistema ou ainda, podem ser subornados ou coagidos a cometer **atos danosos**.

Analisando todas essas vulnerabilidades, pode-se constatar que a grande maioria é comum às redes sem fio e cabeadas, com exceção das vulnerabilidades referentes à *Emissão* do sinal e comunicação.

3.2 MECANISMOS DE SEGURANÇA

Os mecanismos de segurança são concebidos para detectar, prevenir e recuperar de um ataque de segurança. Como exemplo de mecanismos de segurança, pode-se citar a criptografia.

Este tópico objetiva-se conceituar e descrever os mecanismos utilizados, assim como suas características e funcionalidades.

3.2.1 Endereçamento MAC

Para o bom funcionamento de uma rede padrão *Ethernet* ou Wi-Fi, cada dispositivo dela deve ter um número único, definido pelo fabricante e controlado pelo *Institute of Electrical and Electronics Engineers* (IEEE). Esse número (não confundir com número IP) permitiria, teoricamente, identificar de forma inequívoca um equipamento em relação a qualquer outro fabricado mundialmente, do mesmo ou de outro fornecedor. No entanto, alguns modelos de placas bem antigas vinham com um mesmo número, sendo necessário usar um programa fornecido pelo fabricante para cadastrar um MAC único, de uma lista que acompanhava o pacote de placas. Há, ainda, técnicas e ferramentas para se apropriar de um endereço MAC de outra placa ou simplesmente fazer uso de outro que não o original de fábrica.

Uma das formas encontradas para restringir o acesso a uma determinada rede sem fio é mediante o cadastramento prévio dos dispositivos participantes. Como o endereço MAC identifica de forma única cada interface de rede, apenas os dispositivos cadastrados de antemão terão acesso permitido. Esse mecanismo exigirá sempre alguma manutenção, que será maior ou menor, de acordo com o fluxo de usuários e interfaces que entra e sai do cadastro, porém não deixa de ser uma boa solução para pequenas redes e ambientes com poucas mudanças. Mas é importante

lembrar que esse tipo de autenticação pode, no melhor dos casos, identificar o equipamento e não o usuário.

Por outro lado, essa mesma técnica pode ser utilizada por clientes para conectarem-se com o concentrador correto. Alguns programas para acesso permitem especificar o endereço MAC (entre outras opções) do concentrador, ou seja, a configuração neste caso é invertida, em vez de o concentrador selecionar de quais equipamentos aceita conexão. Com base no endereço MAC, o cliente é quem configura o endereço MAC do concentrador. Desta maneira, poderá razoavelmente ter certeza de que estará conectando-se com o concentrador desejado, e não com clone plantado por um atacante ou, por engano, em outro com maior potencia.

3.2.2 *Wired Equivalent Privacy (WEP)*

Diferentemente das redes cabeadas, em que o acesso às informações requer comunicação física ou remota a um componente da rede, em redes sem fio basta ter um meio de receber o sinal, ou seja, a captura da informação pode ser feita de forma completamente passiva. Por essa razão, o protocolo 802.11 oferece possibilidades de cifragem dos dados. O protocolo sugerido para resolver esse problema foi, inicialmente, o WEP, que está totalmente disseminado e presente em todos os produtos que estão em conformidade com o padrão Wi-Fi.

Segundo RUFINO (2005, p.36), “WEP é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas”.

A segurança do WEP é composta de dois elementos básicos: uma chave estática, que deve ser a mesma em todos os equipamentos da rede, e um componente dinâmico que, juntos, irão formar a chave usada para cifrar o tráfego. O protocolo não define de que forma essa chave deve ser distribuída, portanto a solução convencional é também a mais trabalhosa, em que a chave é cadastrada manualmente em todos os equipamentos.

Em um segundo momento, após o estabelecimento de conexão, essa chave estática sofre uma operação matemática para gerar quatro novas chaves: uma destas será escolhida para cifrar as informações em trânsito. Essa chave será fixa e somente trocada se a chave estática original mudar. Portanto, essa nova chave gerada, que é fixa, e susceptível a ataque de dicionário e força bruta. Pode ter tamanho de 40 a 104 bits, no entanto, existem várias implementações com valores maiores.

Para tentar evitar esses tipos de ataque, adiciona-se um segundo elemento que consiste em um conjunto de 24 bits gerados por uma função pseudo-aleatória que será concatenada às chaves fixas (40 ou 104) vendidas, respectivamente, como 64 ou 128 bits. Entretanto, os 24 bits passam em claro pela rede, já que esta foi a forma encontrada para dar conhecimento desse valor, possibilitando que os elementos da rede estabeleçam a comunicação cifrada. Normalmente, esse procedimento é realizado pelo concentrador que, então, distribui a informação para os elementos participantes da rede.

É importante notar que esta noção de equivalência (*Wired Equivalent Privacy*) faz supor que, como não existe proteção ao conteúdo em redes cabeadas (toda proteção deve ser feita por software ou firmware), se pensou em um mecanismo que tivesse dificuldade de quebra compatível a um acesso físico. Porém, após terem sido expostas várias fragilidades do WEP, esse conceito de equivalência não se sustenta. Mas a despeito disso, o WEP ainda provê segurança adequada da vários tipos de cenários.

3.2.3 *Wi-Fi Protected Access (WPA)*

Tendo em vista os problemas de segurança divulgados para WEP, o *Wi-Fi Alliance* adiantou a parte de autenticação e cifração do trabalho que estava sendo feito para o fechamento do padrão 802.11i e liberou o protocolo WPA. Várias mudanças e avanços foram incorporados a esse protocolo, porém a maior parte deles exige a inclusão de outros elementos à infra-estrutura e ainda deve trabalhar combinados com outros protocolos, como o 802.11x. No WPA (versão 1), diferentemente do WEP, não está disponível suporte para conexões Ad-hoc. Portanto, essa modalidade de rede sem uso de concentrador não se beneficia dos mecanismos de proteção introduzidos no protocolo WPA na sua primeira versão.

Atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário utiliza, para isso, padrões 802.11x e EAP (*Extensible Authentication Protocol*).

3.2.3.1 Criptografia

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

3.3 RISCOS E AMEAÇAS

Segundo CARVALHO FILHO (2005, p. 49), as redes sem fio vêm facilitando a vida de muitos usuários e que o número de pessoas que a utilizam cresce constantemente, as redes sem fio tornaram-se alvo de estudos e muitos ataques foram desenvolvidos e/ou adaptados. Além disso, as redes sem fios apresentam falhas graves de segurança.

Um fator importante relacionado à segurança de redes sem fio é o fato de que a maioria dos ataques nestas redes são realizados dentro do mesmo domínio de colisão, ou seja, o suposto invasor se comunica com o mesmo concentrador de tráfego do sistema.

Surge então a necessidade de se realizar uma análise de risco, que é o processo de identificar os riscos de segurança aos quais a organização pode estar exposta.

É importante, portanto, documentar os riscos já descobertos, bem como as providências tomadas para que futuramente possa ser constatado que todas as medidas foram tomadas.

3.3.1 Riscos Internos

Os riscos internos são aqueles que ocorrem devido à má configuração de dispositivos, configurações inseguras, entre outras. Neste tipo de risco não há ação direta do suposto invasor para expor a vulnerabilidade.

3.3.1.1 Rogue WLANs

As Rogue WLANs ou WLANs grampeáveis, são as redes sem fio que, geralmente, foram instaladas por pessoas sem capacidade técnica que configuram os dispositivos de maneira falha, fazendo com que a rede fique exposta a ataques.

3.3.1.2 Configurações Inseguras

Muitos administradores tentam aumentar o nível de segurança de suas WLANs com a utilização de VPNs (*Virtual Private Network* - Rede Privada Virtual) e deixam de lado as configurações de segurança dos dispositivos da rede sem fio.

No entanto, um *hacker* experiente vai, ao invés de tentar quebrar a VPN, atacar os dispositivos de redes sem fio como o *Access Point*, por exemplo.

3.3.1.3 Associações Acidentais

Devido à falta de conhecimento de muitos administradores na forma de configuração dos dispositivos para redes sem fios, há uma grande possibilidade deste dispositivo mal configurado se associar a outro dispositivo, sem consentimento ou mesmo conhecimento do usuário.

A forma de evitar este problema seria configurar os dispositivos para redes sem fios manualmente ou, ao menos, não permitir a atuação em modo Ad Hoc do dispositivo.

3.3.1.4 Problemas de segurança física

Geralmente os que administram as redes não dão a devida importância à segurança física, o que, em geral, é um grande erro, pois um bom programa de segurança física deve ser o primeiro passo para defender uma organização, protegendo suas informações de acessos indevidos.

Temos três pontos a considerar em segurança física:

- *Segurança de Hardware*: Embora, hoje em dia as falhas de hardware sejam mais raras, não há como prever o comportamento dos equipamentos, pois podem ocorrer variações no desempenho em decorrência de eventos físicos. A maior parte dos incidentes ocorre nos periféricos. E em casos mais extremos é requerida disponibilidade de equipamentos como um

sistema reserva para ser usado se ocorrer falhas no sistema principal, uma atualização dos dados em discos, permitindo a imediata disponibilidade dos dados em casos de falha de um dos dispositivos e até uma tecnologia onde dois processadores conectados, estando um deles pronto para assumir as funções do primeiro, se apresentar falha.

- *Segurança física das redes:* O administrador deve sempre se preocupar com a segurança dos dados, atualizando-se em relação a programas que efetuem um controle e segurança mais eficaz. Deve sempre verificar problemas com equipamentos ativos de rede (Hubs, Switches, *Access Point* entre outros), problemas na placa de rede, etc.

Além disso, há vários outros cuidados que fisicamente podem ser tomados para evitar riscos de invasão como, por exemplo, observar a potencia da antena do *Access Point* para evitar que a rede abranja uma área maior que a do local de utilização, evitando assim que a rede seja utilizada, e seus dados sejam capturados por vizinhos ou pessoas que estejam nas proximidades do local. É importante também verificar a posição da antena do *Access Point* e procurar sempre desliga-lo quando não estiver utilizando a rede.

- *Segurança dados:* O *backup* é um ponto importante, pois permite que cópias de arquivos e dados sejam armazenados em locais seguros, criando uma fonte de recuperação dos dados, em caso de perda no seu local de origem. É importante definir as informações que serão armazenadas para que apenas as informações extremamente importantes sejam salvas.

3.3.2 Riscos Externos

Os riscos externos já possuem ação direta do suposto invasor. Muitos ataques a redes sem fio devem aos riscos que serão apresentados.

3.3.2.1 *Eavesdropping & Espionage*

Conseguem capturar todo o tráfego que passa pela rede e utilizam os dados obtidos pra gerar possíveis ataques ou roubos de informações e senhas.

Entretanto, para que o objetivo seja alcançado, é necessário que o suposto invasor esteja dentro do mesmo domínio da rede a ser invadida.

No entanto, nas redes sem fio o *eavesdropping & espionage* são relativamente fáceis de serem realizados já que o sistema do suposto invasor não precisa estar fisicamente ligado, complicando, assim, a identificação do ataque.

A forma de tentar minimizar a ação deste tipo de ataque é utilizando VPN, dificultando a escuta do canal.

3.3.2.2 Roubo de Identidade

O roubo de identidade quando o suposto invasor descobre informações necessárias para poder passar por um cliente autenticado da rede sem fio.

O modo encontrado para tentar minimizar a ação desse tipo de ataque é fazendo a filtragem por endereços MAC. Dessa forma, mesmo que o suposto invasor conheça o ESSID (*Extended Service Set Identifier* – “nome da rede”, para redes com dois ou mais pontos de acesso) da rede e saiba que é aberto à autenticação ele não consegue se associar à rede. Portanto, para que o atacante possa usufruir da rede é necessário que ele obtenha o endereço MAC válido, assim como, o endereço IP também válido.

3.3.2.3 Negação de serviço

Entende-se que na negação de serviço ou DoS (*Denial of Service*), um usuário utiliza um computador para tirar de operação um serviço ou outro computador conectado à Internet, gerando uma grande sobrecarga no processamento de dados, ou grande tráfego de dados para uma rede, ocupando toda a banda disponível.

De acordo com RUFINO (2005, p.49), “Trata-se de um tipo de ataque que não necessita de acesso ou invasão à rede-alvo, mas pode acarretar sérios transtornos dependendo da criticidade do ambiente envolvido”.

Um grande ataque de negação de serviço distribuído para tirar de operação um ou mais serviços ou computadores pessoais contados a rede é chamado de DdoS (*Distributed Denial of Service*).

Esse tipo de ataque tem o intuito apenas de indisponibilizar as máquinas e não de invadir a rede.

3.3.3 Vulnerabilidades nos protocolos

O protocolo 802.11 em si é bem conciso e apresenta inúmeras novidades. Por ser um protocolo muito estudado, não existe um grande número de vulnerabilidades. Entretanto, as poucas que possui podem trazer grandes problemas à rede como um todo.

3.3.3.1 Vulnerabilidades no protocolo WEP

Uma das vulnerabilidades do WEP está no vetor de inicialização (IV). Como as chaves de encriptação são utilizadas por longo período de tempo, recomenda-se que o vetor de inicialização seja alterado a cada quadro enviado. No geral, este vetor inicia em 0 e vai sendo acrescido em 1 a cada nova utilização.

Dois problemas podem ser verificados nesse sistema: Um deles reside no fato de que em algum momento o vetor de inicialização (IV) se repetirá e sendo uma cadeia cíclica, o tráfego poderá ser facilmente monitorado. O outro problema está na freqüente remoção e reinscrição dos dispositivos de rede sem fio, retornando a contagem do vetor de inicialização a 0, fazendo com que os quadros com valores baixos de IV sejam comuns.

Outra grande vulnerabilidade é quanto ao método de criptografia que ele utiliza, o RC4. A criptografia RC4 é simétrica, ou seja, a mesma chave utilizada para a criptografia também é utilizada para decifração. O RC4 é um algoritmo de criptografia de fluxo e não é considerado um dos melhores sistemas criptográficos pelos adeptos da criptografia. De uma forma geral, o algoritmo consiste em utilizar um *array* que a cada utilização tem os seus valores permutados, e misturados com a chave, o que provoca certa dependência desta. Esta chave, utilizada na inicialização do *array*, pode ter até 256 bytes (2048 bits), embora o algoritmo seja mais eficiente quando é menor, pois a aleatoriedade induzida no *array* é superior.

3.3.3.2 Vulnerabilidades no protocolo WPA

Mesmo tendo sido criado para eliminar as vulnerabilidades do protocolo WEP, o WPA também apresenta algumas falhas que devem ser conhecidas para evitar possíveis problemas.

No mais, a maior vulnerabilidade, que não é específica a este protocolo, é o uso de senhas pequenas ou de fácil adivinhação. Porém, esta falha pode deixar a rede sujeita a ataques, onde o suposto invasor testa seqüências de senhas e/ou palavras comuns. Senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque.

Segundo RUFINO (2005, p. 69), “Não há até o momento muitas ferramentas publicamente disponíveis que promovam ataques de força bruta e/ou dicionário para ataques ao WPA. A KisMAC, utilizada em plataforma MacOS X, a partir da versão 0.11a passou a incorporar essa funcionalidade.”

Para plataforma Linux, também já existem algumas ferramentas, como a WPA Crack, que, de posse de um tráfego já capturado, permite ataques combinados usando um dicionário e técnicas de força bruta. Atualmente o uso é pouco intuitivo, pois exige que sejam informadas várias características do tráfego, quais sejam: SSID (*Service Set Identifier* – nome da rede), endereço MAC do cliente e do concentrador, ANONCE (autenticador), SNONCE (suplicante) e o pacote de negociação inteiro no formato hexadecimal.

Kismac - <http://binaervarianz.de/projekte/programmieren/kismac>

3.3.3.3 Vulnerabilidades nas formas de autenticação

O grande problema na autenticação é permitir que o *Access Point* aceite autenticação aberta, permitindo que qualquer dispositivo que saiba qual o ESSID da rede possa se associar.

A autenticação aberta apesar de facilitar a conexão entre um cliente e o *Access Point*, ela pode ser uma grave falha para um suposto invasor, já que basta saber o ESSID para se ter acesso a rede.

3.3.3.4 Outras vulnerabilidades

Ainda há outras armadilhas que podem afetar a propagação do sinal e conseqüentemente, deixar a rede vulnerável:

- Telefones sem fios: apesar da maioria dos telefones sem fios operarem na frequência de 900 Mhz, há modelos que trabalham na de 2,4 Ghz, a mesma utilizada pelos equipamentos 802.11b e 802.11g.

- Microondas: usam frequência de 2,4 Ghz. Recomenda-se que tanto os fornos microondas quanto os telefones sem fios fiquem isolados do ambiente onde se encontra a rede para evitar interferências.
- Água: grandes recipientes com água são inimigos da boa propagação do sinal da rede sem fio, como aquários e bebedouros.
- Vidro: o vidro é outro material que pode influenciar no sinal.

3.4 TÉCNICAS E FERRAMENTAS DE ATAQUE

Como diz CARVALHO FILHO (2005, p. 72), uma rede Wi-Fi desprotegida é um verdadeiro convite aos *hackers* e outras pessoas não autorizadas a acessar seus dados.

As técnicas usadas em ataques às redes sem fio não são novas. Pelo contrário, geralmente elas ocorrem da mesma maneira que nas redes cabeadas. Porém, a cada dia novas técnicas são desenvolvidas ou aperfeiçoadas.

Os intrusos podem comprometer a integridade ou a confiabilidade dos dados de quatro diferentes maneiras. São elas:

- Interrupção: os dados que partem da origem são interrompidos para que não cheguem ao destino.

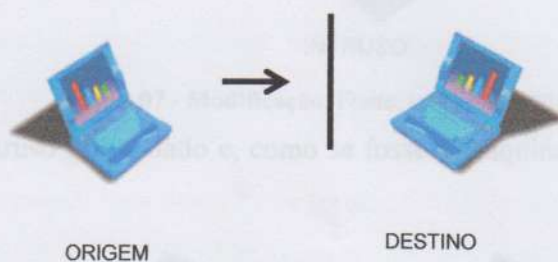


Figura 05 – Interrupção. Fonte: CARVALHO FILHO (2005, p. 73)

- Intersecção: o intruso tem por objetivo capturar o tráfego transmitido na rede.

3.4.1 Ataques mais comuns sem fio

3.4.1.1 MAC Spoofing

Este ataque teria a intenção de permitir acesso apenas a dados de estações com MAC válidos.

Os dispositivos utilizados em WLANs tem a particularidade de permitir a troca de endereço físico. Dessa forma, um atacante mal intencionado pode capturar através de técnicas de *Eavesdropping* e *Exploitation*, por exemplo, um endereço MAC válido de um cliente, alterando o seu endereço e estando apto a participar novamente da rede.

Figura 06 - Intersecção. Fonte: CARVALHO FILHO (2005, p. 73)

- **Modificação:** O intruso além de capturar as informações trafegadas na rede, modifica os dados e os envia ao destino.

O ataque de negação de serviço (*Denial of Service*) tem como objetivo indisponibilizar recursos ou serviços oferecidos pela rede.

Nos padrões 802.11b e 802.11g, que utilizam a frequência de 2,4 GHz, os produtos podem facilitar os ataques de *Denial of Service* a frequência da mesma das ondas microondas, telefones sem fio, aparelho de monitoramento de crises (bela eletrônica). Os ataques de DoS, nesse caso, ocorrem através da inserção de ruído no ar devido a presença desses aparelhos nas proximidades das redes sem fio.

Entretanto, ataques podem realizar ataques sofisticados, passando-se por um *Access Point* com o mesmo endereço MAC de um *Access Point* legítimo, assim, a rede

Figura 07 - Modificação. Fonte: CARVALHO FILHO (2005, p. 73)

- **Fabricação:** O intruso cria o dado e, como se fosse a máquina de origem, envia o dado à máquina destino.

No entanto, ataques de DoS podem ocorrer também quando há alguma relação maliciosa com redes vizinhas, isto é, quando um atacante utiliza o mesmo canal default para os seus equipamentos. Assim, uma rede pode interferir na outra, mesmo de forma não intencional.

A melhor forma de evitar ataques DoS é a autenticação intencional ou não é criando uma barreira física no *Access Point* procurando reduzir o nível de ruído externo.

Figura 08 - Fabricação. Fonte: CARVALHO FILHO (2005, p. 73)

3.4.1 Ataques mais comuns nas redes sem fio

3.4.1.1 MAC Spoofing

Este ataque burla sistemas que permitem acesso apenas a hosts dotados de endereços MAC válidos.

Os dispositivos utilizados em WLANs têm a particularidade de permitir a troca do endereço físico. Dessa forma, um atacante mal intencionado pode capturar através de técnicas de *Eavesdropping* e *Espionage*, por exemplo, um endereço MAC válido de um cliente, alterando o seu endereço e estando apto a participar ativamente da rede.

3.4.1.2 DoS

O ataque de negação de serviço (*Dos* – *Denial of Service*) tem como objetivo indisponibilizar recursos ou serviços providos pela rede.

Nos padrões 802.11b e 802.11g, que utilizam a frequência de 2,4 GHz, os produtos podem facilitar os ataques de DoS já que a frequência é a mesma de fornos microondas, telefones sem fio, aparelho de monitoramento de crianças (babá eletrônica). Os ataques de DoS, nesses casos, ocorrem através de inserção de ruídos a partir de presença destes aparelhos nas proximidades das redes sem fio.

Entretanto, atacantes podem realizar ataques mais sofisticados, passando-se por um *Access Point* com o mesmo ESSID e MAC de um outro *Access Point*, inundando assim, a rede com pedidos de dissociação.

Outra maneira de causar uma negação de serviço é inundar a rede com tráfego aleatório.

No entanto, ataques de DoS podem ocorrer também sem que haja nenhuma intenção maliciosa com redes vizinhas, já que geralmente, cada fabricante utiliza o mesmo canal *default* para os seus equipamentos. Assim, uma rede pode interferir na outra, mesmo de forma não intencional.

A melhor forma de evitar ataques DoS sejam eles intencionais ou não é criando uma barreira física no *Access Point* procurando reduzir os riscos de ruídos externos.

3.4.1.3 Associação Maliciosa

Um ataque de associação maliciosa cria uma espécie de ilusão para o sistema. Nele, o atacante simula a existência de um *Access Point* a fim de que um usuário se conecte a ele. Através de programas apropriados, como o *FakeAp* e *AirJack*, é possível forjar um dispositivo qualquer da rede como um *Access Point*.

3.4.1.4 WLAN Scanners

Os equipamentos que trabalharem na mesma frequência da rede estarão aptos a captar os sinais em transmissão, dando margem à atuação dos *scanners*.

Mesmo que o envio de pacotes em *Broadcast* pelo *Access Point* seja desabilitado pelo administrador, os equipamentos dotados de softwares como o Netstambler, conseguem detectar a rede, já que o próprio programa envia pacotes em todos os canais possíveis para verificar em qual deles o *Access Point* responde.

3.4.1.5 WLAN Sniffers

Este software funciona basicamente da mesma maneira que o *WLAN Scanners*, tendo um detalhe a mais: durante o rastreo da rede, um software *sniffer* permite armazenar os dados obtidos para analisá-lo mais tarde com uma ferramenta para quebra de criptografia WEP.

Exemplos de softwares *sniffers* são o *Kismet* (Linux) e o *Ethereal* (Linux, Windows).

3.4.1.6 Pontos de acesso não autorizado

Este problema se deve ao fato de constante redução de custos dos equipamentos necessários para implementar uma WLAN, tomando cada vez mais fácil que qualquer um possa instalar um *Access Point*.

Dessa forma, um usuário pode configurar o *Access Point* com um sinal mais forte que os outros, tendo prioridade na conexão e tornando-se uma rede de captura de senhas, ESSID ou qualquer outra informação para posterior decifração.

3.4.1.7 Wardriving

É uma técnica onde o invasor anda em um carro com o *laptop* e com uma antena, dentro ou fora do carro, tentando detectar WLANs.

O objetivo desta técnica é o de “vigiar” uma área, para encontrar fisicamente os elementos que compõem a rede sem fio e, futuramente, invadi-las. Isso é alcançado pelo mapeamento dos APs encontrados, com o auxílio de um GPS (*Global Positioning System - Sistema de Posicionamento Global, por satélite*).

Em geral, esta técnica não é danosa em si, já que muitos buscam apenas descobrir uma rede sem fio desprotegida. No entanto, outros usuários já efetuam *login* e fazem uso dos recursos daquelas redes.

3.4.1.8 Warchalking

Após encontrar redes vulneráveis, usando a técnica de *wardriving*, o atacante divulga as mesmas com pichações em muros e calçadas, com símbolos específicos que indiquem a outros atacantes quais as características dessas redes.

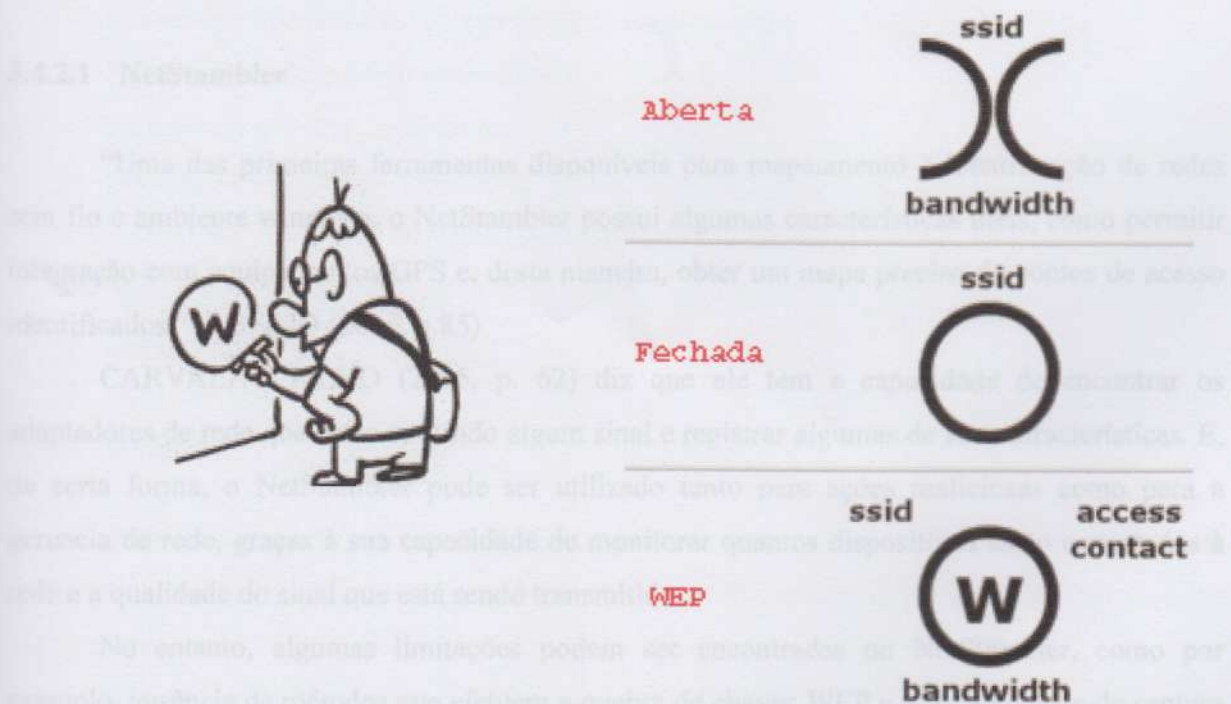


Figura 09 – Warchalking. Fonte: DUARTE (2003, p. 43)

O principal argumento dos praticantes de *warchalking* para a defesa de sua legalidade é a garantia de liberdade de utilização de ondas de rádios presentes no espaço aéreo.

3.4.1.9 Novos Ataques

Novos métodos de ataques as redes sem fio estão surgindo a cada dia. Em meados de 2005, uma empresa divulgou um alerta aos usuários de *hotspots* sobre um novo ataque, onde hackers criam páginas falsas semelhantes aos formulários de autenticação de *hotspots*. Assim, os invasores têm acesso a informações dos usuários que se autenticam a estes sites.

3.4.2 Ferramentas para redes sem fio

RUFINO (2005, p.73) cita que: “A maioria dos ataques pode ser efetuada utilizando ferramentas específicas, porém o arsenal acumulado e já disponível para redes convencionais não pode ser desprezado, sob pena de conceder vantagem significativa a um possível atacante.”

Algumas ferramentas que estão disponíveis tanto para defesa quanto para ataques serão mostradas aqui.

3.4.2.1 NetStambler

“Uma das primeiras ferramentas disponíveis para mapeamento e identificação de redes sem fio e ambiente windows, o NetStambler possui algumas características úteis, como permitir integração com equipamentos GPS e, desta maneira, obter um mapa preciso de pontos de acesso identificados.” RUFINO (2005, p.85)

CARVALHO FILHO (2005, p. 62) diz que ele tem a capacidade de encontrar os adaptadores de rede que estão emitindo algum sinal e registrar algumas de suas características. E, de certa forma, o NetStambler pode ser utilizado tanto para ações maliciosas como para a gerencia de rede, graças à sua capacidade de monitorar quantos dispositivos estão conectados à rede e a qualidade do sinal que está sendo transmitido.

No entanto, algumas limitações podem ser encontradas no NetStambler, como por exemplo, ausência de métodos que efetuem a quebra de chaves WEP e a incapacidade de captura de tráfego. A sua grande vantagem é a integração com dispositivos GPS (*Global Positioning*

System – Sistema de Posicionamento Global) quando se trata de identificar a localização de redes sem fio e a possibilidade de continuar uma análise salva anteriormente.

URL: <http://www.netstumbler.org>

3.4.2.2 Kismet

Esta ferramenta pode ser utilizada para vários fins, todos relacionados a redes sem fio. O Kismet além de funcionar como sniffer, ou seja, um programa que consegue capturar todo tráfego de rede, ainda gera dados relacionados à localização aproximada do dispositivo que está sendo monitorado. Sua vantagem principal é que ele possui uma grande velocidade de atualização e adição de novas funcionalidades.

Outro ponto favorável em relação a outras ferramentas é que o mesmo salva automaticamente todas as redes identificadas. Além disso, ele é uma ferramenta *opensource* muito útil na captura de informações tais como:

- Número de WLANs conectadas;
- Ausência ou não de criptografia WEP;
- Número de quadros com o vetor de inicialização fraco;
- Número total de quadros capturados por WLAN;
- Número de quadros descartados;
- Endereço MAC dos participantes;
- Padrão que está sendo utilizado (802.11a/b/g);
- Identifica o tipo de dispositivo monitorado;
- O canal utilizado;
- Nível de sinal;
- O ESSID.

Todo o tráfego analisado pelo Kismet é gravado em arquivos do tipo log com a extensão .dump. É possível também ver esse tráfego em tempo de captura, o que pode ser útil para um suposto invasor.

Além disso, o Kismet pode ser ligado a um GPS para fazer o mapeamento topológico das redes e registrar a posição em que encontrou cada rede, a potência do sinal entre outros. Esta

integração ocorre por meio do GPSD (*gps daemon*) que é um outro programa que realiza a comunicação do Kismet com o dispositivo. Todos os valores de localização referentes às redes analisadas são armazenados em um arquivo padrão XML.

Uma deficiência desta ferramenta é que diferentemente do NetStambler, os arquivos gerados não são carregados, ou seja, não é possível uma análise posterior já que uma sessão salva não pode ser remontada.

URL: <http://www.kismetwireless.net>

3.4.2.3 Wellenreiter

Esta ferramenta foi desenvolvida para o descobrimento e auditoria das redes sem fios, mas é rudimentar e insere poucas funcionalidades adicionais. No entanto, as suas funcionalidades básicas são suficientes para identificar redes, identificar clientes conectados, confirmar o uso ou não do WEP e, se existir um dispositivo GPS, associar a rede encontrada com sua respectiva coordenada.

Devido as suas limitações, o Wellenreiter esta disponível também em C++ (Wellenreiter II) aceitando muito mais opções de interface de rede que o anterior.

URL: <http://www.wellenreiter.net>

3.4.2.4 Ethereal

Esta ferramenta pode ser utilizada tanto para o ataque como para a segurança. Ela permite a observação dos dados capturados da rede em tempo real ou previamente capturados e armazenados para manipulação posterior. Foi uma das primeiras ferramentas a tratar tráfegos específicos de redes sem fio.

Uma grande vantagem do *Ethereal* é a facilidade de evolução e capacidade de incorporar novas funcionalidades.

URL: <http://www.ethereal.net>

3.4.2.5 WEPCrack

Esta ferramenta foi a primeira publicamente disponível para quebra da chave WEP e que atua nas vulnerabilidades encontradas no WEP.

3.4.2.5 É escrita em *Perl* que supostamente funcionaria em qualquer sistema que suporta esta linguagem como UNIX/Linux, Windows ou mesmo MAC. No entanto, esta ferramenta só é totalmente funcional em sistemas UNIX.

Os atacantes geralmente usam o WEPCrack para obter informações de rede como o ESSID para efetuar ataques posteriores.

URL: <http://wepcrack.sourceforge.net/>

3.4.2.6 AirSnort

O AirSnort é uma ferramenta que, igualmente ao WEPCrack, quebra chaves WEP atuando nas vulnerabilidades.

A diferença do AirCrack para o WEPCrack é que o primeiro consegue quebrar qualquer chave. Esta quebra só ocorre após a obtenção de três a cinco milhões de quadros trocados, portanto quanto maior o volume do tráfego, maiores as chances da chave ser quebrada.

A limitação do AirSnort é que ele não consegue obter informações sobre as redes identificadas, tornando seu uso apenas para quebra de chave.

URL: <http://sourceforge.net/projects/airsnort/>

3.4.2.7 HostAP

Esta não é uma ferramenta de ataque nem de defesa propriamente dita. É um módulo capaz de transformar um dispositivo de rede sem padrão em *Access Point*, ou seja, máquinas convencionais podem funcionar como AP.

No entanto, muitos atacantes geram ataques de associação maliciosa, e outros utilizam as características providas por este módulo.

URL: http://hostap.epitest.fi/wpa_supplicant/

3.4.2.8 AirTraf

O AirTraf é uma ferramenta Linux que procura por *Access Point* 802.11b e exibe estatística de tráfego. Além disso, ele permite coletar algumas informações sobre as redes identificadas, como clientes conectados e os serviços utilizados, tudo em tempo real.

URL: <http://airtraf.sourceforge.net>

3.4.2.9 BSD AirTools

É um conjunto de ferramentas completo que inclui ferramentas de auditoria sem fio para quebrar chaves WEP, detectar pontos de acesso etc.

O programa dstumbler é a ferramenta no pacote que permite a descoberta de pontos de acesso e representação gráfica da razão entre sinal e ruído. E pode ajudar a familiarizar-se com a ativação do ponto de acesso.

Para testar a segurança da rede sem fio, pode-se escolher usar “dweputils” (dwepcrack, dwepdump e dwekeygen) para ajudar a determinar se WEP é a solução adequada para as necessidades de segurança sem fio.

URL: <http://www.dachb0den.com/projects/bsd-airtools.html>

3.4.2.10 FakeAP

É uma ferramenta em Perl que só roda em Linux e facilita interpor o atacante entre o cliente e o concentrador legítimo com o objetivo de capturar informações e senhas. Também facilita que o suposto invasor se passe por um concentrador para obter informações levando o usuário realmente a pensar que está conectado ao concentrador.

Esta ferramenta vai criar *beacons* falsos com ESSID, endereço MAC aleatórios em vários canais, fazendo com que programas como o *NetStumbler* e *Kismet* identifiquem milhares de pontos de acessos. Logo, o FakeAP pode ser usado também na segurança da rede, fazendo simulação de *pontos de acesso* para facilitar a identificação do *ponto de acesso* legítimo.

URL: <http://www.blackalchemy.to/project/fakeap>

3.4.2.11 AirJack

O AirJack é outra ferramenta que, igualmente ao FakeAP, irá simular um *ponto de acesso* tentando se passar por um dele. Com o objetivo de obter informações dos clientes que venham a se conectar a ele.

Além do AirJack e do FakeAP existe também o AirSnarf que segue a mesma idéia de simulação de Pontos de Acesso para obter informações e senhas.

URL: <http://sourceforge.net/projects/airjack>

3.5 MÉTODOS DE DEFESA

É citado por CARVALHO FILHO (2005, p. 81) que as redes sem fios, já algum tempo, se tornaram o foco de estudo de muitos *hackers*. Com isso, diversos métodos foram desenvolvidos ou adaptados para atacá-las diretamente.

Por essa razão foi necessário um desenvolvimento e evolução dos métodos de segurança para, assim, prover um serviço seguro ao usuário.

3.5.1 ESSID

O ESSID é a primeira linha de defesa de uma rede sem fio. É o ESSID que identifica os *hosts* e *Access Points* que a compõem a rede.

Cada equipamento vem com um ESSID configurado de fábrica e, portanto, a primeira coisa que se deve fazer é alterar esse valor, pois ele é padrão.

Um dos problemas é que o ESSID não é criptografado pelo WEP, ou seja, torna-se fácil para que o invasor obtenha informações suficientes para alcançar ser objetivo. Com a opção de difusão do envio habilitada é permitido que o código ESSID seja enviado periodicamente em broadcast, facilitando o acesso à rede por um suposto invasor. E com a opção desabilitada, apenas os clientes com conhecimento prévio de dados como o código e canal poderão estabelecer uma conexão.

Outro grande cuidado é quanto aos clientes que enviam ESSID igual a "ANY". Eles o fazem durante a busca de um concentrador disponível. Portanto, recomenda-se ignorar clientes que fazem tais atitudes, pois mesmo que não sejam atacantes, esta característica pode ocasionar uma conexão de um cliente com um concentrador não desejado, o que pode causar alguns problemas.

3.5.2 Substituição do endereço MAC

Devido à possibilidade de capturar um endereço MAC válido através das técnicas de monitoramento do tráfego e cloná-lo, recomenda-se substituir sempre o endereço MAC.

No entanto, tanto a modificação do endereço MAC quanto outros métodos de ocultamento de informações não são seguros se forem utilizados isoladamente. Para obter um sistema com uma segurança adequada todos mecanismos devem ser implementados em conjunto.

3.5.3 Autenticação

Um dos principais problemas no acesso a redes sem fios é a falta de autenticação. Nas redes sem fios, a autenticação pode ser configurada de três maneiras:

- Autenticação Aberta (*Open Authentication*): neste tipo, qualquer dispositivo pode se associar ao ponto de acesso e se integrar à rede;
- Autenticação Compartilhada (*Shared Authentication*): nesta opção, chaves WEP são previamente compartilhadas, sendo necessárias para autenticação do cliente junto ao *Access Point*;
- Rede – EAP (*Network EAP*): utiliza vários protocolos EAP (*Extensible Authentication*) para dar suporte a autenticação através de servidores RADIUS (*Remote Authentication Dial-In User Service*).

3.5.4 PSPF

O PSPF (*Publicly Secure Packet Forwarding*), ou *Privacy Separator* é um mecanismo que bloqueia a comunicação entre os clientes, evitando um ataque de um usuário contra outro quando ambos estiverem ligados ao mesmo ponto de acesso.

A deficiência do PSPF é que este mecanismo não evita a captura de pacotes, portanto não garante a privacidade se for implementado de forma isolada.

3.5.5 Utilização do 802.1x e RADIUS

O Protocolo 802.1x provê um sistema de autenticação composto por:

- Um ponto de acesso para acesso à rede (*gateway*);
- Um servidor de autenticação que pode utilizar esquema de *login* e senha ou certificados de clientes e que separa, também, a autenticação do usuário e a do computador.

Já o RADIUS é o servidor de autenticação mais utilizado para autenticar os usuários e autorizar o acesso aos mesmos. Ele permite o uso de EAP.

A grande falha do 802.1x é em relação a autenticação das estações que se movem de um ponto de acesso a outro. Esse tipo de autenticação não é possível nesse padrão, tendo em vista que ele foi desenvolvido, inicialmente, para as redes cabeadas.

3.5.6 WEP

Para garantir o sigilo das informações, a maioria das soluções disponíveis no mercado utiliza o protocolo de criptografia WEP. A criptografia no WEP é implementada através do protocolo RC4.

Apesar do WEP não ser garantia de segurança dos dados transmitidos, deve-se sempre habilitá-lo, pois não deixa de ser um método de defesa.

3.5.7 Utilização do 802.11i

Esse padrão de segurança veio para solucionar as falhas de WEP em relação as vulnerabilidades na criptografia e do 802.1x em relação a autenticação de uma estação que se movimenta entre dois pontos de acesso.

Quanto a criptografia, o 802.11i utiliza dois mecanismos que podem funcionar simultaneamente na rede: o TKIP (*Temporal Key Integrity Protocol*) e o CCMP (*Counter Mode CBC MAC Protocol*).

O TKIP é responsável por solucionar problemas de integridade do WEP, através de mudanças das chaves quadro a quadro, que são sincronizadas automaticamente entre pontos de acesso e estações.

O CCMP utiliza um padrão de criptografia chamado AES (*Advanced Encryption Standard*) que fornece criptografia simétrica mais segura.

3.5.8 WPA

O *Wi-Fi Protected Access* (WPA) foi implementado para melhorar os padrões WEP e 802.11i, podendo trabalhar de forma integrada a outras tecnologias como 802.1x e certificados digitais oferecendo uma segurança mais robusta.

No entanto, dependendo do ambiente em que for implementado, o WPA também pode ser usado apenas com recursos de segurança nativos. Isto acontece por meio de chaves compartilhadas, estabelecendo uma conexão entre o cliente e o Ponto de Acesso.

Uma evolução do WPA é o WPA2. Porém, nesse caso, é necessária uma mudança de hardware para sua utilização. Essa segunda versão do acesso protegido Wi-Fi utiliza técnica de criptografia AES, que pode gerar chaves criptografadas de 128, 192 e 256 bits.

3.5.9 Uso de Criptografia

É a arte de escrever de forma codificada através de técnicas matemáticas, o que permite tornar incompreensível um texto ou informação. A criptografia dificulta o ato de indivíduos maliciosos capturarem o tráfego, embaralhando as informações.

A criptografia, desde que foi aplicada à informática sofreu grande evolução, inclusive no que diz respeito à sua aplicação.

Atualmente, a criptografia é usada para prover quatro tipos de serviços distintos:

- **Sigilo:** garantir que pessoas desautorizadas não possam ter acesso a informações trafegadas;
- **Integridade:** garantir que a informação não seja alterada durante a transmissão;
- **Autenticação:** garantir o não acesso a rede por pessoas desautorizadas;
- **Certificação:** gera um certificado de que a informação foi recebida com sucesso, na íntegra e da fonte correta.

A criptografia pode ser classificada pelo número de chaves podendo ser Simétrica ou Assimétrica.

➤ A *criptografia Simétrica*, conhecida também como “Criptografia Convencional”, é um método de chave única, onde uma mesma chave é utilizada para encriptar e desencriptar os dados. Levando em conta o tempo de processamento, é um método bastante eficiente. No entanto, o método de chave única não é aconselhado para a troca de informação confidencial ou vital ao funcionamento de uma empresa caso não haja um meio de transmissão seguro, mas é muito eficiente para conexões seguras na Internet, onde processos computacionais trocam senhas temporárias para algumas transmissões críticas.

➤ A *Criptografia Assimétrica* utiliza duas chaves no processo, sendo uma chave usada apenas para criptografar às informações que serão transmitidas ao destino. Essa chave é

denominada chave pública, pois é divulgada a todos. Além da chave pública, há também a privada, conhecida apenas pelo destino da informação e que será mantida em segredo. A idéia é que a criptografia seja feita utilizando a chave pública e a decryptografia com a chave privada. Esse método possui um desempenho consideravelmente inferior à criptografia convencional, porém tem como a principal vantagem não necessitar de um meio de transmissão confiável.

3.5.10 Certificados digitais

É um dos métodos de autenticação mais seguros, que permite verificar se uma pessoa conectada à rede é quem ela diz ser.

Entretanto, o uso de certificados digitais contribui muito para aumentar a segurança da rede sem fio não somente na autenticação, visto que, em um certificado digital várias informações pessoais são armazenadas, mas a principal é a chave utilizada na encriptação.

Além da criptografia, o certificado digital auxilia na criação de uma assinatura digital, que funciona como um “reconhecimento de firma” digital. Ela é a criação de um código, através de uma chave privada de modo que o destino recebe junto à mensagem um código que permite verificar se o emissor é realmente quem diz ser e confirmar a não alteração do conteúdo da mensagem.

3.5.11 Monitoramento do ambiente

O monitoramento dos padrões que estão sendo utilizados na rede sem fio pode impedir a detecção de invasões que se valem exatamente de algum padrão não existente na rede. Por exemplo: o ambiente utiliza o 802.11g e todo monitoramento realizado é baseado nesse padrão, mas nada impede que invasores utilizem o 802.11a para configurar um Ponto de Acesso ou mesmo estabelecer uma conexão. A solução deste problema é ter interfaces que trabalhem com 802.11a [CARVALHO FILHO, 2005].

Há várias ferramentas especializadas pra realizar o monitoramento do ambiente. Entre eles temos:

- Widz: ferramenta que realiza monitoramento de problemas com tráfego e ataques específicos a concentradores;
- wIDS: detecta qualquer suspeita que aconteça na rede sem fio, como repetidas requisições de associação com um determinado concentrador;

- Garuda: ferramenta robusta com um desenho que facilita a criação e mudança das assinaturas dos pacotes suspeitos e analisados; [RUFINO, 2005 – p. 180]
- AirIDS: ferramenta que detecta nas redes sem fio qualquer tráfego suspeito;
- Snort-Wirelles: ferramenta que, além de detectar o tráfego suspeito, também identifica possíveis ataques baseados em assinaturas e quadros mal formados.

Além dessas ferramentas, ainda temos o Kismet e o NetStambler, que já foram citados anteriormente, e o uso dos concentradores que também podem ser úteis para monitorar o tráfego.

3.5.12 Mantendo a rede sem fio segura

Algumas dicas serão apresentadas para melhor segurança de uma rede sem fio:

1. Habilitar WEP;
2. Alterar o ESSID;
3. Não colocar o ESSID com nomes de fácil identificação;
4. Desabilitar a opção *broadcast* ESSID;
5. Trocar a senha *default* dos Pontos de Acesso e roteadores;
6. Verificar a posição dos Pontos de Acesso para evitar que o sinal dos mesmos vá além do necessário;
7. Realizar sempre um novo monitoramento do ambiente (fazer uso das ferramentas de monitoramento);
8. Sempre verificar os endereços MAC que têm acesso ao Ponto de Acesso;
9. Não comprar Ponto de Acesso ou dispositivos móveis que utilizem WEP com chave de 40 bits, visto que já está ultrapassado;
- 10. Procurar comprar Ponto de Acesso com memória flash. Esta memória auxilia em um possível upgrade de software no futuro;
- 11. Desabilitar DHCP: dessa forma, os invasores terão maiores dificuldades, pois será necessário decifrar o IP, a máscara de rede e outros parâmetros TCP/IP exigidos.

4 CONCLUSÃO

Esta monografia abordou o que, atualmente, é uma grande preocupação dos usuários das redes sem fio: a segurança.

Verificou-se que, apesar das redes sem fio não terem sido criadas para substituir as redes cabeadas, a mobilidade e produtividade gerada pelas redes sem fio são o ponto fundamental para a superação das redes cabeadas que vem acontecendo.

Em vista a todos os riscos e vulnerabilidades que foram apresentados é que, ainda hoje, as questões relativas à segurança merecem estudos e aprimoramentos constantes. As vulnerabilidades são originadas a partir de alguns pontos básicos:

- Falhas nas especificações dos padrões;
- Limitações dos equipamentos utilizados;
- Falha na configuração das redes.

Foi possível perceber também que, o padrão mais utilizado nas redes sem fio, o 802.11b, não é capaz de proporcionar uma boa segurança. Isto se deve ao fato de que, seu principal protocolo de segurança, o WEP, apresenta diversas falhas. E é em cima dessas falhas, que ele está sendo substituído por outros padrões mais eficientes com o TKIP e WPA.

Além disso, os métodos de ataque que foram comentados são os utilizados com mais frequência por usuários maliciosos que procuram, de qualquer forma, explorar as fragilidades das redes sem fio.

Mesmo com o despreparo de muitos usuários, até por desconhecer o risco ou por receio da perda de velocidade na transmissão dos dados, é possível tornar a rede sem fio a mais segura possível. Mas é necessário, pelo menos:

- Os usuários se conscientizem dos riscos e das vulnerabilidades;
- Um protocolo de criptografia seja utilizado, que atualmente é o WPA;
- Seja respeitada a precaução básica de quem se conecta à Internet utilizando antivírus e firewall atualizados;
- Haja cuidado na configuração dos equipamentos utilizados;
- Sejam criados mecanismos que dificultem a operação dos atacantes, limitando os equipamentos que podem acessar a rede;
- Sejam utilizados equipamentos específicos e de grande eficiência na confidencialidade dos dados, caso necessário, como o VPN.

REFERÊNCIAS BIBLIOGRÁFICAS

ENGST, Adam; FLEISHMAN, Glenn. **Kit do iniciante em redes sem fio**. 2.ed. São Paulo: Pearson Makron Books, 2005.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**. 2.Ed. São Paulo: Novatec, 2005.

AURÉLIO, Marco. **Ataque passivo em rede wireless**.

Disponível em: http://www.malima.com.br/article_read.asp?id=224. Acessado em: janeiro de 2006.

AURÉLIO, Marco. **WEP – O que é? Como funciona? É Seguro?**.

Disponível em: http://www.malima.com.br/article_read.asp?id=196. Acessado em: janeiro de 2006.

PINHEIRO, José Maurício dos Santos. **Aspectos para a Construção de uma Rede Wireless Segura**.

Disponível em: http://www.projetoderedes.com.br/tutoriais/tutorial_redes_wireless_segura_01.php. Acessado em Dezembro de 2005.

Decisão sobre uma Estratégia de Rede sem Fio Protegida. Disponível em:

<http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx>. Acessado em: fevereiro de 2006.

SCHWEITZER, C; SAKURAGUI, Rony R.; CARVALHO, T.; VENTURINI, Y.: **Tecnologias de Redes Sem Fio: Wpans, Wlans E Wmans - Desafios De Segurança, Vulnerabilidades E Soluções**. 2005

Disponível em: <http://www.linorg.cirp.usp.br/SSI/SSI2005/Microcursos/MC04.pdf>. Acessado em: fevereiro de 2006.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão de Curso. São José do Rio Preto: UNESP

Disponível em:

<http://www.apostilando.com/download.php?cod=230&categoria=Redes>. Acessado em: fevereiro de 2006.

CARVALHO FILHO, João Rogério lima de. **Um estudo de Protocolos Empregados na Segurança de Dados em Redes Sem Fio – Padrão 802.11**. Trabalho de Conclusão de Curso. Centro Universitário de João Pessoa – UNIPÊ. 2005

Disponível em:

<http://www.unipe.br/graduacao/computacao/projetos/tcc20052/UM%20ESTUDO%20DE%20PROTOCOLOS%20EMPREGADOS%20NA%20SEGURAN%C7A%20DE%20DADOS%20%20EM.pdf>. Acessado em: Janeiro de 2006.