UCL - FACULDADE DO CENTRO LESTE

EDSON BOF

SEGURANÇA EM REDES WIRELESS

SERRA
2010

EDSON BOF

SEGURANÇA EM REDES WIRELESS

Monografia apresentada ao Curso de Pós-graduação **MBA - Gestão da Segurança da Informação**, da Faculdade do Centro Leste, como requisito parcial para obtenção de título de Especialista em Gestão da Segurança da Informação.

Orientador Prof: Marcelo Campos Antunes, Esp.

SERRA
2010

RESUMO

Em se tratando de redes wireless que é a nova tendência em comunicação com menos necessidade de uso de cabeamento. Muitas organizações têm ou pretendem ter algum dia para prover mobilidade e acesso a rede para seus usuários. A facilidade de instalação de uma rede sem fio, aliada ao fácil acesso a essa tecnologia, geram algumas implicações para a segurança. Muitas redes sem fio são instaladas sem nenhuma preocupação com segurança ou por pessoas sem o conhecimento básico necessário, este trabalho faz uma abordagem geral do que vem, a ser a segurança da informação e a gestão de risco. Em seguida analisa os tipos de redes, fazendo uma classificação delas e os padrões de comunicação emitidos por cada qual. Analisa ainda a segurança dessas redes, mostrando detalhadamente as formas de se conseguir obter esta segurança e, por fim, faz uma avaliação dos mecanismos de segurança e prevenção no que diz respeito a invasão dessas redes. O estudo foi feito a partir de uma análise bibliográfica em materiais dispostos na internet e livros. Percebeu-se, portanto, que é necessário investir em soluções que reduzem de forma significativa a possibilidade de ataques em redes wireless.

Palavras-chave: redes wireless, segurança da informação, gestão de risco.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

IEEE Internet Engineering *Task Force*

WPA Wi-fi Protected Access

RADIUS Remote Authentication Dial-In User Servic

AES Advanced Encription Standard

TKIP Temporal Key Integrity Protocol

DES Data Encryption Standard

IDEA International Data Encryption Algorithm

RC Ron's Code ou Rivest Cipher

RSA Ronald, Rivest, Shamir

RSADSI - RSA Data Security Incorporated

WEP Wired Equivalent Privacy Wep

ICV Integrity Check Value

MAC Filtering Filtragem por meio de endereço único de caracteres

FMS Fluhrer Mantin Shamir

TKIP Temporal Key Integrity Protocol

WEP Wired Equivalent Privacy Wep "checksum"

MAC Address Resolution Protocol

FMS Fluhrer, Mantin e Shamir

WPA Wi-Fi Protected Access

WPA-Personal Wi-Fi Protected Access Personal

WPA-PSK - WPA-Pre Shared Key

AP Access Pointer

CRC-32 Verificação de redundância cíclica

ICV Integrity Check Value

EAP Extensible Authentication Protocol

MSK Master Session Key

EAPO Extensible Authentication Protocol over LAN

OSI Open Systems Interconnection

SSID Service Set Identifier

GPS Global Positioning System

ARP Address Resolution Protocol

VPN Virtual Private Network

LAN Local Área Network

WAN Wide Área Network

SUMÁRIO

1 INTRODUÇÃO

Possuir um sistema de informação seguro atualmente é de extrema importância para as organizações se mantenham competitivas e estáveis. As informações que circulam dentro dessas organizações são consideradas como um instrumento de trabalho.

Por isso é necessário que estas informações tenham agilidade no processo de comunicação, sejam confiáveis e úteis para que os usuários as utilizem para a tomada de decisões.

A utilização de redes sem fio seja para uso corporativo ou doméstico está cada vez mais difundida. As redes sem fio podem alcançar distâncias cada vez maiores, embora ainda não superem o desempenho e segurança de uma rede cabeada, e normalmente, são utilizadas em redes internas devido a sua melhor taxa de desempenho e qualidade no sinal.

Nos dias atuais, mais empresas interligam seus computadores à internet, com o objetivo de se obter mais clientes, menor custo de comunicação, oferecer mais serviços, realizar pagamentos, entre outros. Entretanto são poucas as empresas que se preocupam realmente com a segurança e integridade de suas informações, que podem ser extraviadas por indivíduos que querem obter informações sigilosas para cometer crimes digitais, os chamados (*hackers*).

As empresas que não se preocupam com segurança da informação, cultivam falhas na sua infraestrutura de rede degradando a confidencialidade, integridade e disponibilidade dos seus sistemas, arquivos e servidores facilitando assim o risco de sofrer um simples ataque até uma total indisponibilidade de seus sistemas gerenciais.

1.1 JUSTIFICATIVA

O processo de evolução dos Sistemas de Informação - SI caminhou paralelamente com as tecnologias de informática e telecomunicações. A evolução da tecnologia colaborou para surgimento das redes de computadores e o melhoramento de sua capacidade de processamento, com o surgimento de novos sistemas que possibilitam maior integração das áreas empresariais.

Essa tecnologia proporciona mobilidade, agilidade e liberdade em sua utilização. Ao invés de cabos, *modem* e outros meios físicos para de se obter acesso à Internet e redes compartilhadas com outros dispositivos, a rede sem fio só necessita de uma placa de rede sem fio instalada no

equipamento e um sinal aberto para utilização livre como é o caso em aeroportos, *shopping*, entre outros (RUFINO, 2005).

Toda essa evolução possibilitou a integração de sistemas através de redes de computadores e servidores com grande capacidade de processamento de informações que se tornou popular entre pessoas e empresas, pois atualmente é praticamente impossível pensar em conectividade sem a existência de redes de computadores. Com isso o mercado está concentrado em uma das novas e revolucionárias tendências tecnológicas: a comunicação por redes sem fio (*Wireless Networks*).

Portanto, diante da relevância do tema, as redes sem fio devem ser seguras e confiáveis aos usuários através implementações de criptografias e firewalls deixando ser um alvo fácil para pessoas más intencionadas como os *hackers*.

1.2 O PROBLEMA

Assim, o problema gerado neste estudo é: **De que forma pode-se realizar uma segurança nas redes sem fio?** Verificando e entendo como é possível implementar soluções de segurança em redes *wireless* para reduzir drasticamente as vulnerabilidades das informações.

1.3 OBJETIVO

O presente estudo propõe os seguintes objetivos, divididos em geral e específicos:

1.3.1 Objetivo Geral

Este trabalho tem por objetivo estudar as principais funcionalidades das redes *wireless*, focando nas falhas de segurança e possíveis soluções para se obter um ambiente de rede mais seguro.

1.3.2 Objetivo Específicos

- Expor sobre a importância da segurança da informação juntamente com a gestão de risco;
- Expor os principais níveis de vulnerabilidade em redes *wireless;*

- Expor as principais características das redes *wireless*;
- Analisar as principais soluções para um ambiente mais seguro e estável através de exemplos práticos e teóricos;

1.4 RELEVÂNCIA

A proposta é viabilizar as possíveis soluções de segurança nas redes *wireless*, através de equipamentos, criptografia e entendimento das vulnerabilidades dos padrões de comunicação da tecnologia *wireless*.

1.5 METODOLOGIA

Para alcançar tais objetivos, buscou-se constituir a trajetória do trabalho através da contextualização ancorada em uma pesquisa bibliográfica, por meio de fontes secundárias como livros, dissertações, revistas, pesquisas de instituições, *sites* de internet, materiais eletrônicos como CD'S e DVD'S. Além disso, o conhecimento do autor da pesquisa, que trabalha neste ramo, conta de forma relevante para o enriquecimento deste trabalho.

1.6 ESTRUTURA DO TRABALHO

Esta monografia está estruturada em 7 partes, organizadas na seguinte composição:

A Introdução apresenta uma contextualização do tema, a forma como o trabalho foi construído, desde o problema de pesquisa, passando pelos objetivos, metodologia de pesquisa, justificativa, delimitação do estudo, até a relevância do assunto para os meios acadêmico e empresarial.

No primeiro capítulo será abordado a importância da segurança da informação para que seja possível entender e utilizar a prevenção como uma ferramenta juntamente com conjuntos de medidas para reduzir possíveis falhas. Será abordado brevemente os requisitos necessários para entender o que vem a ser gestão de risco.

No segundo capítulo será realizado um breve estudo sobre redes TCP/IP dando uma breve introdução sobre os conceitos de redes TCP/IP e suas classificações de redes internas e externas, abordando também os principais padrões de comunicação de redes wireless exemplificando seus tipos de funcionamento disponíveis.

No terceiro capítulo será destacado as principais tipos de criptografias utilizados pela tecnologia *wireless*.

No quarto capítulo será abordado as principais técnicas de invasão em redes wireless citando algumas ferramentas utilizadas para tais procedimentos.

No quinto capítulo será abordado as principais formas de se proteger as redes *wireless*, através de técnicas e softwares para bloqueio e proteção contra intrusos.

No sexto capítulo será apresentada a conclusão do trabalho com os pontos mais significativos para se obter uma rede sem fio mais segura.

No sétimo capítulo será abordado um estudo de caso para enriquecer os conceitos deste trabalho acadêmico.

2.1 SEGURANÇA DA INFORMAÇÃO (SI)

Entende-se por segurança da informação o conjunto de medidas de controles e política de segurança, que objetivam a proteção das informações, quer sejam dos clientes ou empresas, controlando o risco de revelação ou alteração por pessoas não autorizadas.

Conforme afirma Torres (2001, p. 415):

> Os sistemas ativos de segurança visam evitar que investidas estruturadas sejam feitas contra uma rede ou um sistema específico. Eles independem que pessoas mal-intencionadas consigam explorar brechas e vulnerabilidade com o objetivo de penetrar no sistema com objetivos escusos.

De acordo com a NBR ISO/IEC 17799 (2005) define SI como: é a política de proteção existente sobre as informações de uma determinada organização de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades do negócio. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

De acordo com a norma citada, é necessário estabelecer critérios para a definição do nível de segurança que se pretende, com análise periódica, possibilitando avanços ou retrocessos no cenário de SI na organização.

Para Wadlow (2000, p. 4), a segurança é um processo, podendo aplicá-lo simultaneamente a rede de telecomunicações e a organização que a detém. Desta maneira, é necessário melhorar a segurança dos sistemas e implementar os processos delineados como forma de prevenir as novas ameaças e técnicas que possam surgir.

Melhorar um sistema de segurança da informação não está baseado apenas em aplicar em um conjunto de computadores antivírus ou barreiras de proteção (*firewalls*) interligada na rede de computadores de uma organização. Para se obter um sistema de segurança da informação é necessário entender os princípios de segurança para que possa se gerir políticas e soluções cabíveis para atender as necessidades de cada organização.

Para preencher os requisitos da segurança da informação, de acordo com (LEITÃO, 2005), as necessidades requeridas são a confiabilidade, integridade e disponibilidade das informações utilizadas nos sistemas de informação das organizações, Elas demandam a implantação de

medidas de políticas de segurança para que seja possível garantir a autenticidade e não a negação completa dos serviços que são disponibilizados nas redes das organizações.

É relevante entender os princípios de segurança da informação para assim conseguir implementá-los. No processo de implantação é necessário conseguir verificar ferramentas que auxiliem o usuário antes que alguma falha ocorra. Esse processo de prevenção pode ser classificado em duas grandes categorias indispensáveis: a prevenção e a proteção dos sistemas de informação.

O objetivo de utilizar à prevenção é ter um conjunto de medidas para reduzir o risco de possíveis falhas existentes. O resultado desse conceito é tentar abolir uma ameaça quando se transforma em um ataque ou desastre. Já a proteção, tem por objetivo de implantar políticas de segurança para inibir, detectar e proteger qualquer tentativa de ataque ao sistema de informação da organização (LEITÃO, 2005).

De acordo com Silva (2003), os principais pontos para implantação da segurança da informação devem seguir os cinco princípios básicos*:*

1. **A relação custo e benefício:** garantir investimentos para a implementação e a manutenção favoráveis, e o retorno que proporciona a prevenção e a proteção do sistema de informação. Tal situação só é lembrado pelos proprietários quando um grande desastre ou ataque ocorre e o custo de restauração das informações das bases de dados muitas vezes, é maior do que se tivesse investido meses em um sistema de segurança da informação seguro e estável.
2. **O princípio da concentração:** proporciona à possibilidade de se administrar as medidas necessárias de segurança da informação para atender necessidades de melhoramento de proteção de diferentes bases de dados sensíveis a alterações.
3. **O princípio da proteção em profundidade:** proporciona medidas de proteção de segurança (físicas ou lógicas) como câmeras de vigilância, biometria e reconhecimento de voz. A utilização deste princípio evita um conjunto de medidas de proteção distintas e avulsas para não se tornar uma soma ineficiente e lenta de obstáculos para um ambiente mais seguro.
4. **O princípio da consistência:** determina que as medidas de proteção do SI possuam um nível de sensibilidade intercambiável para que reduzam as falhas do programas de segurança das organizações. Sua utilização atinge a todos os níveis acessos do sistema de informação tanto como físico ou lógico, por exemplo, impedir que um filho de um

sócio da organização instale jogos, acesse páginas indevidas com o servidor da empresa ou permitir pessoas não autorizadas ter acesso aos computadores da organização.

5. **O princípio da redundância:** determina a importância de se adotar mais do que uma forma de proteção dos SI. Caso ocorra a falha do processo A de segurança será executado o processo B para que o sistema de informação continue em pleno funcionamento Ex: possuir servidores de contingência em locais diferentes replicando as informações entre as filiais efetuando *backups* automáticos diariamente com sistemas de espelhamentos de *hard disk*.

Estes princípios são responsáveis pela segurança da informação que deverá ser articulada de forma que venha definir princípios para um ambiente mais seguro. Para uma implementação satisfatória, deve ser bastante aprofundada para se obter o conhecimento, implicações e interação com a equipe responsável de segurança da informação e gestores, resultando melhores resultados dos esforços necessários para um ambiente mais seguro.

Tanto a segurança da informação e a gestão de risco devem trabalhar em conjunto para que, desta forma, seja possível elaborar um plano de contingência de segurança com o intuito de solucionar problemas e prever riscos para melhoria continua da segurança da informação.

Para entendermos melhor, no próximo tópico será apresentado o conceito de gestão de risco, mostrando-a como parte da segurança da informação.

2.1 GESTÃO DE RISCO

A gestão de risco é um processo fundamental de suporte à tomada de decisão para tecnologia da informação (TI) e dos negócios, uma vez que na medida em que os negócios da organização crescem, cresce também a necessidade de sua dependência em relação à internet e aos sistemas de TI. Com isso os riscos de infra-estrutura tornam-se mais visíveis e significantes, pois violações ou falhas em sistemas de informação causam sérias crises de negócio.

Para Campos (2007, p. 50), analisar riscos de incidentes de segurança da informação é essencial para gestão da informação, mantendo os princípios da confidencialidade, da integridade e da disponibilidade.

Pereira (2004, p. 3) diz que:

> É evidente que a gestão da segurança deve se juntar às operações permanentes interagindo e às vezes concorrendo por um mesmo recurso, mas com o objetivo único de garantir a credibilidade e imagem da organização. É importante visualizar que a gestão da segurança existe dentro de um processo permanente dentro da organização, e esta é a meta!

A gestão da segurança da informação se torna relevante por ter o objetivo de evitar danos à reputação causados por roubo de identidade, vazamento de informações confidenciais, em função de falhas de sistemas e de restrições regulatórias para controlar conformidade das informações.

De acordo com Silva (2003) a gestão de risco é um conjunto de medidas adotadas pelas organizações para obter um nível de segurança desejável. Quando se inicia o processo de integração do programa de segurança da informação, automaticamente teremos que envolver uma seqüência de etapas.

Através do conjunto de medidas são determinados e classificados os riscos que a organização pode sofrer. Somente após esta verificação, é possível desenvolver medidas de segurança com uso de controles que proporcionarem a redução ou até mesmo a eliminação dos riscos detectados.

Para que se obtenha um processo de gestão de risco saudável nas organizações, é necessário, segundo Silva (2003), seguir três passos:

1. **Identificar os riscos:** inicia-se com o levantamento de todos os pontos de risco que a empresa possui no seu sistema, para que depois possa intervir com soluções que possuem objetivo de se adotar um sistema de segurança da informação para comportar as necessidades da organização.
2. **Implantar a análise de risco na organização:** utilização de toda informação existente dos processos de infraestrutura de comunicação na organização de forma sistemática, para se originar o grau de exposição da organização as diversas ameaças que tanto internamente ou externamente (Internet) possui. Essa fase é necessária para constituir a base de processo de medidas necessárias para redução de falhas de segurança.
3. **Implantar soluções de segurança:** processo ao qual o departamento da área de negócio se uni com o departamento técnico de Tecnologia da Informação (TI), para discutir e implementar melhores formas de correção de falhas de segurança. Essa é fase de construção de um sistema de segurança no sistema de informação, na qual

> todos podem colocar suas idéias e soluções em prática, sempre avaliando os possíveis impactos nos usuários finais.

O valor da informação atualmente para as empresas possui um custo muito alto, pois estão envolvidos investimentos com a parte tecnológica, funcionários e pessoas envolvidas em geral. Visualizando dessa forma podemos saber realmente se deve investir em um sistema de segurança da informação (SSI) seguindo as três etapas mencionadas acima: Identificar os riscos, Implantar a Análise de risco na organização e Implantar soluções de segurança.

Atualmente não existe sistema totalmente seguro, devido ao constante surgimento de novas vulnerabilidades. Estas causam diretamente uma certa desvantagem para quem pensa que basta investir apenas uma vez em um processo de implantação do sistema de segurança da informação solucionará o problema de sua organização.

Um sistema seguro e estável é aquele que possui investimentos diários e manutenções periódicas para evitar constrangimentos futuros. Mas os benefícios obtidos são muito grandes e trazem grandes vantagens para organizações e confiança para seus clientes (PEREIRA, 2004).

O investimento em sistema de segurança da informação contra desastres diversos proporciona para organização uma grade de confiabilidade, uma vez que dificilmente haverá paradas no sistema de informação por motivos de falhas de segurança, oferecendo maior economia e rentabilidade para organização e as pessoas que estão envolvidas no ciclo produtivo.

Mesmo com tantas notícias sobre pragas virtuais, vírus, *worws* entre outros, muitas empresas ainda não possuem a visão de se preocupar com a segurança da informação. Boa parte delas utiliza softwares piratas o que aumenta muito a probabilidade de ataques. Essa falta de preocupação com a segurança da informação causa grandes prejuízos financeiros e com grandes chances de não serem indenizadas pelo uso desses *softwares* piratas (LONGO, 2005).

Para implementar um sistema de segurança da informação conjuntamente com a gestão de risco, deve-se analisar quais as reais necessidades e prioridades da organização.

3 REDES TCP/IP E REDES SEM FIO *(WIRELESS)*

Nesse capítulo serão abordados conceitos sobre redes TCP/IP, classificações de redes internas e externas, principais padrões de comunicação de redes *wireless* exemplificando seus tipos de funcionamento infra-estrutura e *Ad-Hoc*.

3.1 CONCEITOS DE REDES TCP/IP

O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede (também chamado de pilha de protocolos TCP/IP). Seu nome vem de dois protocolos: o TCP (*Transmission Control Protocol* – Protocolo de Controle de Transmissão) e o IP (*Internet Protocol* – Protocolo de Interconexão).

De acordo com o site Wikipédia (2009) diz que:

> O conjunto de protocolos pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão logicamente mais perto do usuário (chamada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração.

Para o Protocolo de Controle de Transmissão de Internet (TCP/IP) executar sua tarefa deve obedecer a um conjunto de regras.

Conforme afirma Queiroz (2002, p. 34):

> O protocolo é um conjunto de regras para o envio de informações em uma rede, essas regras regem o conteúdo, formato, duração, seqüência e o controle de erro de mensagens trocadas nos dispositivos de rede. Atualmente o TCP/IP (Protocolo de Controle de transmissão de Internet) é o protocolo mais usado em redes locais. Isso se deve basicamente a popularização da Internet, a rede mundial de computadores, já que esse protocolo foi criado para ser usado na Internet.

E este conjunto de regras é o modelo para solução prática para problemas de transmissão de dados, onde nas camadas mais próximas do topo estão mais perto do usuário, enquanto aquelas mais baixo estão mais perto da transmissão física do dado.

O TCP/IP é muito utilizado em redes e para entendermos melhor sobre elas será apresentada sua classificação e sua definição.

3.2 CLASSIFICAÇÕES DE REDES DE COMPUTADORES

Uma rede de computadores consiste de dois ou mais computadores e outros dispositivos conectados entre si de modo a poderem compartilhar seus serviços, que podem ser: dados, impressoras, mensagens (e-mails), etc. A Internet é um amplo sistema de comunicação que conecta muitas redes de computadores. Existem várias formas e recursos de vários equipamentos que podem ser interligados e compartilhados, mediante meios de acesso, protocolos e requisitos de segurança.

Em se tratando de redes TCP/IP, estas podem ser classificadas de várias formas, devidos a seu tamanho e topologia, entretanto as mais comuns são: *Local Área Network* (LAN), *Wide Are Network* (WAN).

Essas duas topologias possuem as seguintes características, segundo Torres (2001), que são:

- ***LAN:*** *Local Área Network* (LAN) são redes locais que se comunicam através servidores, estações e outros. É um tipo de rede capaz de transmitir dados em grande escala e velocidade e com qualidade de transmissão utilizando o protocolo TCP/IP. A figura demonstra uma pequena estrutura de um LAN interligada por computadores, servidores, *hubs* e um *access point* conforme a figura 1:

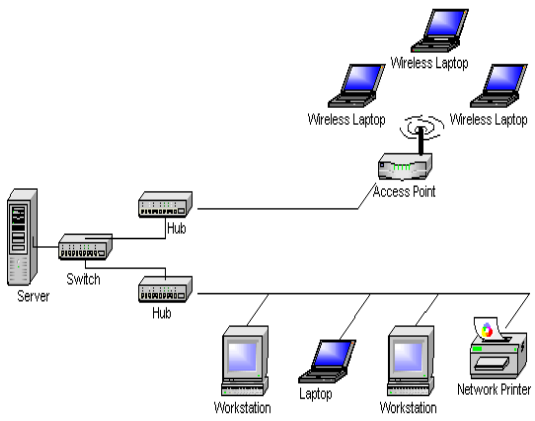

Figura 1: Rede local com compartilhamento de impressora Fonte: CD curso de redes de computadores (digerati)

- ***WAN:*** *Wide Área Network* (WAN) são redes geograficamente distribuídas sendo formada pela ligação de sistemas de computadores diferentes que utilizam meios físicos junto com o protocolo TCP/IP. Normalmente a transmissão de dados entre os computadores diferentes são oferecidas pelas companhias de telecomunicação, conforme o exemplo da figura 2.

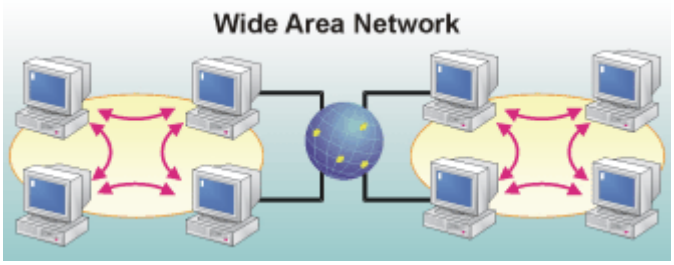

Figura 2: Exemplo de Rede tipo WAN Fonte: http://www.cinelformacao.com/tda/files/ud5/wan.gif

A figura 2 demonstra a comunicação externa para outros computadores e dispositivos de rede localizada em locais geograficamente diferentes, o que caracteriza uma WAN.

Outro tipo de rede é a rede sem fio como é apresentada no próximo capítulo.

3.3 REDES SEM FIO *(WIRELESS NETWORK)*

Uma rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos. A ligação é feita por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho.

O uso desta tecnologia vai desde transceptores de rádio até satélites no espaço. Seu uso mais comum é em redes de computadores, servindo como meio de acesso a Internet, através de locais remotos como um escritório, um restaurante ou até mesmo em casa.

De acordo com Rufino (2005); as redes sem fio possuem dois tipos de funcionamento: Infra-estrutura e *Ad-Hoc*. O funcionamento do modo infraestrutura possui um concentrador que é um equipamento central de uma rede que possibilita, para essa topologia, uma melhor administração e concentração de todos os dispositivos clientes em um só ponto

Tal funcionalidade permite controlar todos os dispositivos e políticas de segurança como autorização, autenticação, controle de banda, filtros de pacote, criptografias em um único ponto. Também possibilita a interligação com redes cabeadas ou com a Internet, já que em geral, os concentradores também desempenham o papel de *gateway* ou ponte de acesso. A figura 3 apresenta uma forma de infraestrutura:

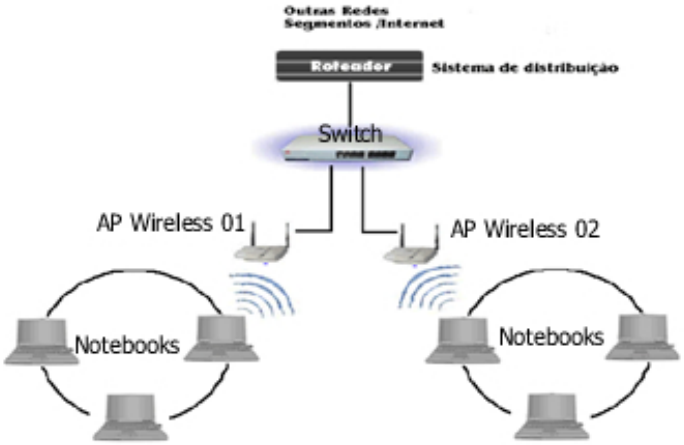

Figura 3: Exemplo do modo de infra-estrutura de redes sem fio

Fonte: CD curso de redes de computadores (digerati)

Ao configurar uma rede *wireless* figura 3 envolvem mais passos do que uma rede cabeada e um número muito maior de escolhas, incluindo o tipo de antenas e o sistema de encriptação a utilizar, sem falar no grande volume de opções para otimizar a conexão presentes na interface de administração do ponto de acesso.

Já o modo de operação *Ad-Hoc*, o funcionamento é baseado em redes ponto-a-ponto nas quais os computadores e dispositivos sem fio conversam diretamente entre si sem a necessidade de um pondo de acesso. Esse tipo de modo de operação possui vantagens de simplificação na troca de arquivos sem necessidade de mão de obra especializada, porém disponibiliza um elevado índice de falta de segurança na comunicação entre os dispositivos sem fio (RUFINO, 2005).

Conforme a figura 4, o modo de operação *Ad-hoc* é uma rede mais simples para uso em pequenos escritórios.

Figura 4: Exemplo do modo de operação *Ad-Hoc*Fonte: CD curso de redes de computadores (digerati)

Para que essas redes possam se comunicar, elas utilizam além do protocolo TCP/IP, padrões de comunicação que possibilitam a comunicação entre dispositivos diferentes sem fio que serão apresentados em outro capítulo.

A grande motivação para a utilização de uma rede sem fio é a facilidade de instalação devido à eliminação da necessidade e do trabalho de passar cabos por paredes, pisos, etc. Além dessa vantagem, há várias outras que motivam a utilização de redes sem fio, como de acordo com Marques (2001):

- Flexibilidade: devido a não utilização de cabos, a rede sem fio permite atingir locais onde não seria possível chegar usando cabeamento;
- Permite o uso em ambientes internos e externos;
- Mobilidade: sistemas de redes sem fio permitem aos usuários acesso à informação em qualquer local e em tempo real.

A principal desvantagem das redes sem fio está no fator segurança. Além dessa, existem outras desvantagens como, por exemplo: as características do meio podem variar muito no tempo influenciando na propagação do sinal e restrições. Marques (2001) cita algumas características que podem influir nas restrições:

- Devido a imposições de órgãos regulamentadores a largura de banda é limitada;
- O meio é de domínio público e, por isso, está sujeito a interferências;
- Alto consumo de energia dos equipamentos portáteis.

Para uma boa implantação de uma rede *wireless* é necessário avaliar as necessidades reais de sua utilização, visando sempre a segurança de perímetro e políticas de segurança adotada pela organização que pretende utilizar essa tecnologia de comunicação. Para a implementação de uma rede é necessário seguir alguns padrões de comunicação como será apresentado.

3.4 PADRÕES DE COMUNICAÇÃO

O objetivo da padronização da comunicação é possibilitar a compatibilidade entre dispositivos de diferentes fabricantes.

De acordo com Franciscatti (2005); as redes *wireless* utilizam freqüências de rádio para se comunicar havendo necessidade de uma padronização dos equipamentos sem fio por existir vários fabricantes. Não havia uma padronização dessa tecnologia causando, assim, a

impossibilidade de comunicação de dispositivos de redes sem fio de outros fabricantes. Assim o *Institute of Electrial and Electronics* (IEEE) formou um grupo de trabalho com o objetivo de definir os padrões de uso em redes sem fio ,denominado 802.11.

Desde a criação das redes sem fio sugiram vários modelos de comunicação que possibilitam o aprimoramento dessa tecnologia baseando-se em nível de velocidade e distância máxima de comunicação. Com essas evoluções sugiram os seguintes padrões da família de redes sem fio, segundo Franciscatti (2005, p. 19). Normalmente são representados pelo padrão 802.11, embora cada padrão possuir suas características que será abordado nesse capítulo:

Padrão 802.11a: foi definido após os padrões 802.11 e 802.11b para tentar resolver os problemas existentes. 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. Vale ressaltar que a operação desse padrão executa na faixa de 5 GHz, uma faixa com poucos concorrentes, porém com menor área de alcance. Oferece também aumento significativo na quantidade de clientes conectados, 64 clientes simultaneamente.

A faixa dos 5 GHz é uma faixa de freqüência muito mais “limpa”, pois existem muito menos dispositivos que utilizam esta faixa de freqüência que os 2.4 GHz e existem muito menos redes 802.11a em uso, o que faz com que as redes 802.11ª, sejam em geral, mais estáveis e susceptíveis a interferências. Muitos pontos de acesso de fabricados recentemente são capazes de operar simultaneamente nas duas faixas de freqüência, atendendo tanto clientes com placas 801.11b ou 802.11g quanto clientes 802.11a. Este recurso é interessante, pois permite que você crie uma rede mista, que permita o uso da faixa dos 5 GHz, mais limpa, sem deixar de fora clientes que suportam apenas os padrões B e G.

Para oferecer este recurso, o ponto de acesso precisa incluir dois transmissores independentes, o que encarece o produto. Um exemplo de equipamento compatível é o *Linksys* WRT600N, onde você encontra a opção “*Network Mode*” dentro da seção “*Wireless*”. Usando o valor “*Mixed*” para as duas seções, você faz com que ele opere simultaneamente nas duas faixas de freqüência conforme a figura 5:

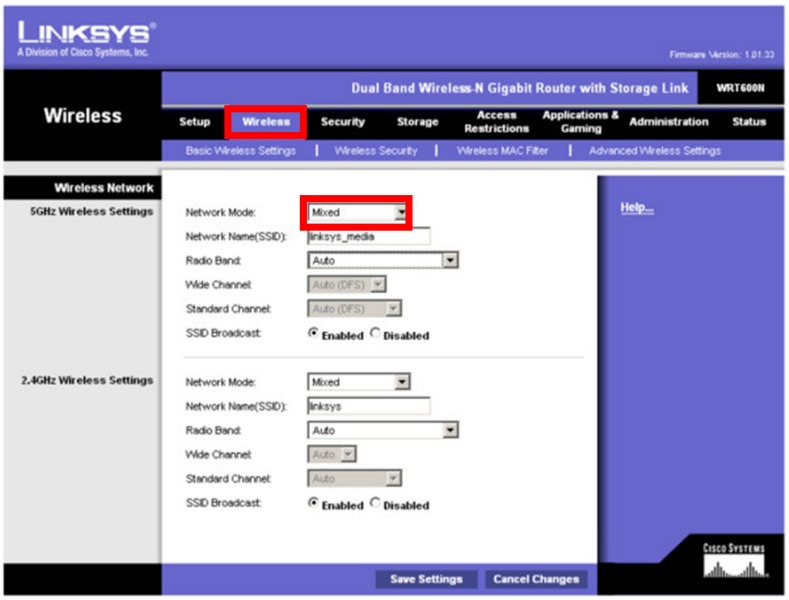

Figura 5: Roteador *wireless Linksys* WRT600N

Fonte: http://images.guiadohardware.net/imagens/img-58e92f49.jpg

Padrão 802.11b: foi o primeiro padrão de comunicação a ser definido pelo *Institute Electrial and Electronics* (IEEE) que permite 11 Mbps de velocidade de transmissão máxima. Entretanto pode comunicar-se a velocidades mais baixas como 5.5, 2 ou até mesmo 1 Mbps. A freqüência de operação é de 2,4 GHz especificada pelo (IEEE). No modo de operação inicial quando surgiram às redes sem fio, ela permite um número máximo de 32 clientes conectado ao mesmo tempo.

Padrão 802.11i (WPA2): é um conjunto de padrões e especificações para redes *Wireless*. Foi criado como uma evolução ao protocolo WEP, sendo uma alternativa ao WPA que necessita de um servidor RADIUS. Esse padrão tem como objetivo tornar redes sem fio tão seguras quanto redes com fio. O WPA2 permite a implementação de um sistema completo e seguro, mantendo compatibilidade com sistemas anteriores.

Padrão 802.11g: Utiliza a mesma faixa de freqüência do 802.11b, 2.4 GHz. Isso permite que os dois padrões sejam inter compatíveis, possibilitando adicionar placas e pontos de acesso 802.11g a uma rede 802.11b já existente. Apesar disso, a velocidade de transmissão no 802.11g é de 54 megabits, como nas redes 802.11a. Ou seja, o 802.11g junta o melhor dos dois mundos. Note que para que a rede efetivamente trabalhe a 54 megabits, é necessário que o ponto de acesso e todas as placas sejam 802.11g. Ao incluir uma única placa 802.11b na rede, toda rede passa a operar a 11 megabits.

Padrão 802.11n: Opera nas faixas de 2,4Ghz e 5Ghz, o que proporciona melhor distribuição de mídia, oferecendo, através do *Multiple Input*, *Multiple Output* (MIMO), taxas mais altas de

transmissão (até 300 Mbps), maior eficiência na propagação do sinal e ampla compatibilidade reversa com demais protocolos. O 802.11n atende tanto as necessidades de transmissão sem fio para o padrão HDTV, como de um ambiente altamente compartilhado, empresarial ou não. Graças ao uso do MIMO, os pontos de acesso 802.11n podem utilizar dois ou quatro fluxos simultâneos, o que dobra ou quadruplica a taxa de transmissão, atingindo respectivamente 144.4 a 300 megabits. A figura 6 demonstra o processo de reflexão de sinais utilizado pela tecnologia MIMO.

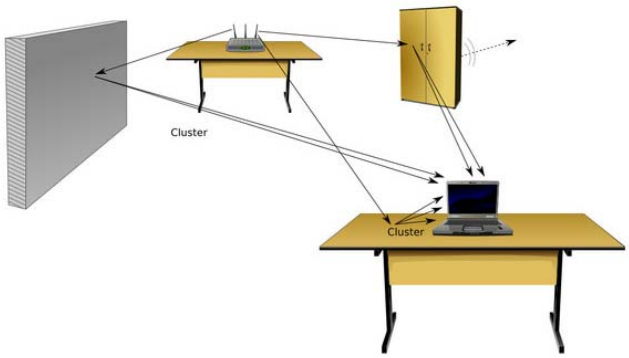

Figura 6: Reflexão dos sinais do padrão 802.n
Fonte : http://www.guiadohardware.net/artigos/802-11n/

A tecnologia MIMO tira proveito da reflexão do sinal transmitindo por antenas diferentes, os sinais efetuam percursos diferentes até o receptor, ricocheteando em paredes conforme no exemplo da figura 06, e entre outros obstáculos, o que faz com que não cheguem exatamente ao mesmo tempo, possibilitando maior desempenho de transmissão de dados.

Existem vários padrões de comunicação em redes *wireless*, eles foram criados devido a necessidade de melhorias nos aspectos de segurança e velocidade de transmissão de dados.

Com a necessidade de melhor segurança e taxas de transmissão mais altas foram surgindo novos padrões em redes *wireless* que serão abordados no próximo capítulo.

4 CRIPTOGRAFIA EM REDES SEM FIO *WIRELESS*

Nos dias atuais, onde grande parte dos dados é digital, sendo representados por bits, o processo de criptografia é basicamente feito por algoritmos que fazem o embaralhamento dos bits desses dados a partir de uma determinada chave ou par de chaves, dependendo do sistema criptográfico escolhido.

A criptografia é utilizada nas redes *wirelees* para não permitir acesso não autorizado, quando adquirimos equipamentos wireless devemos entender quais são principais meios de criptogrfia para redes wireless disponiveis que proporcione maior segurança será abordado os principais tipos de criptografia disponiveis para redes *wireless* adiante:

4.1 CRIPTOGRAFIA DE DADOS

A criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Dessa forma apenas o receptor da mensagem pode ler a informação com facilidade.

> A criptografia forte pode resistir com sucesso a ataques que lhe são direcionados até certo ponto onde se torna mais fácil obter, de alguma outra maneira, a informação que ele protege. Um sistema criptográfico, não importa quão seguro, não irá impedir que alguém vasculhe seu lixo. Mas pode perfeitamente prevenir ataques de colheita de dados. (SCHNEIER 2006)

A facilidade em obter ferramentas de ataques para quebra de criptografia em redes *wireless* está tem se tornando uma atividade simples e rotineira. Por outro lado as empresas estão buscando mecanismos para impedir que ataques sejam bem sucedidos. Para que seja possível reduzir a possibilidade de um ataque com sucesso é necessário entender quais são os principais tipos de criptografias utilizados nos equipamentos de redes *wireless*.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação, conforme mostra o exemplo da figura 7.

Figura 7: Processo de criptografia

Fonte: http://www.infowester.com/criptografia.php

Existem dois tipos de chaves criptográficas: chaves simétricas e chaves assimétricas.

A criptografia de chave privada (simétrica) é um método conhecido também como criptografia tradicional que funciona de forma eficiente em aplicações de uso limitado, onde tanto o receptor quanto o transmissor se preparam antecipadamente para o uso da chave, para o correto funcionamento deste método, todos os indivíduos envolvidos na transmissão da informação precisam estar cientes da chave utilizada. Ao enviar uma mensagem, o emissor deve criptografá-la utilizando um algoritmo de criptografia em conjunto com a chave privada. Quando a mensagem cifrada chega ao seu destino, o receptor deve saber a chave de criptografia para poder decifrá-la. Quando utilizado sobre conexões seguras à criptografia simétrica se torna bastante eficiente.

Vários algoritmos de criptografia foram desenvolvidos a partir de chaves simétricas. Dentre os mais comuns estão o DES, o IDEA e o RC.

DES (*Data Encryption Standard*): criado pela IBM em 1977, usa chaves de 56 bits, permitindo até 72 quatrilhões de combinações. Apesar disso, foi ‘quebrado’ ou desvendado utilizando-se as chamadas técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet.

IDEA (*International Data Encryption Algorithm*): criado em 1991 por James Massey e Xuejia Lai é um algoritmo que usa chaves de 128 bits e tem estrutura semelhante ao DES.

RC (*Ron's Code* ou *Rivest Cipher*): criado por Ron Rivest na empresa RSA Data Security é muito utilizado em e-mails e usa chaves de 8 a 1024 bits. Há várias versões: RC2, RC4, RC5 e RC6. Cada uma delas difere da outra por trabalhar com chaves de maior complexidade.

É relevante ressaltar que a utilização das chaves simétricas implica em algumas desvantagens, fazendo com que sua utilização não seja adequada em situações onde a informação é muito valiosa. Possui a necessidade de usar uma grande quantidade de chaves caso exista necessidade de várias pessoas ou entidades estejam envolvidas. Ainda, há o fato de que tanto

o emissor quanto o receptor precisam conhecer a mesma chave. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em mãos erradas através de *softwares* de análise de pacotes. Para entender melhor o processo de encriptação vejamos a figura 8 utilizando criptografia simétrica.

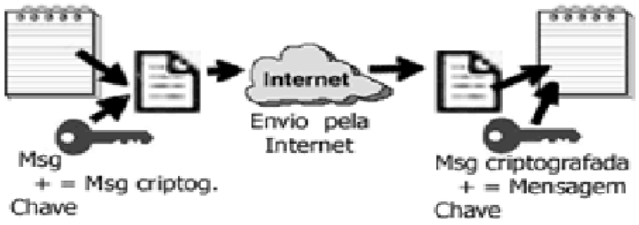

Figura 8: Exemplo de criptografia de simétrica

Fonte:http://www.modulo.com.br/media/TA_MarcioEdmar_SegurancaRedesVPN-SSL.pdf

A criptografia de chave pública (assimétrica) é uma criptografia de chave pública foi desenvolvida em 1976 por Diffie e Hellman. Possui uma chave para criptografar uma mensagem, e outra chave para descriptografar. Nesse sistema, cada participante deve possuir duas chaves distintas. Uma denominada pública, que será divulgada aos demais indivíduos da rede, e outra chave privada que será mantida em segredo. O algoritmo utilizado e que se mantém até hoje é o (*Ronald, Rivest, Shamir)* RSA, que é patenteado pela (*Data Security Incorporated*) RSADSI. Entendermos sobre o funcionamento deste método, observe a figura 9.

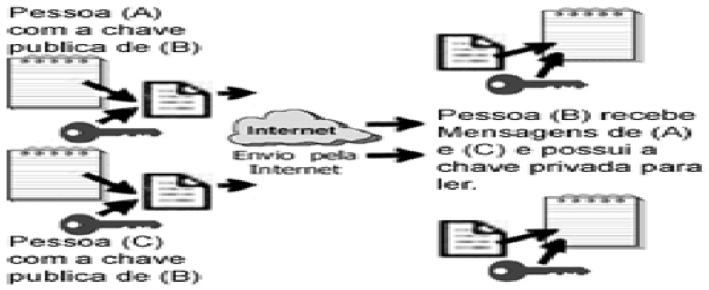

Figura 9: Processo de criptografia por chave assimétrica

Fonte:http://www.modulo.com.br/media/TA_MarcioEdmar_SegurancaRedesVPN-SSL.pdf

No exemplo da figura 9 (A) e (C), escrevem mensagens utilizando a chave pública de (B). A partir desse momento, apenas (B) poderá ler as mensagens. Ao receber a mensagem, (B) utiliza a sua chave privada para descriptografá-la. Caso (B) precise responder aos indivíduos (A) e (C), deverá utilizar a chave pública de cada um deles para enviar a mensagem criptografada.

A grande vantagem deste sistema é permitir que qualquer um possa enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la, não havendo a necessidade do compartilhamento de uma mesma chave nem de um pré-acordo entre as partes interessadas. Com isso o nível de segurança é maior. (SCHNEIER, 1996). Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como é feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura.

Ambas as chaves são necessárias para bloquear e desbloquear os dados, podendo uma delas se tornar pública sem colocar a segurança em perigo. Essa chave é conhecida como Chave Pública, e sua contraparte é chamada de chave privada. Para criptografar os dados é utilizada a chave pública, e para decriptografá-los é utilizada a chave privada. (BURNETT e PAINE, 2002).

Qualquer uma dessas chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida secreta, enquanto a chave pública disponível a todos.

4.1.1 *Wired Equivalent Privacy* (WEP)

Ao longo dos últimos anos, observa-se um grande aumento no número de redes sem fios utilizadas por usuários domésticos, instituições, universidades e empresas. Essa crescente utilização e popularização trouxe consigo mobilidade e praticidade para seus usuários mas também trouxe uma preocupação com a segurança destas redes. É exatamente por essa preocupação que os protocolos de segurança são criados, desenvolvidos e atualizados com uma velocidade cada vez maior.

Foi *Wired Equivalent Privacy Wep* (WPE) o primeiro protocolo de segurança adotado em redes *wireless.* Este protocolo foi muito utilizado por passar certa imagem de segurança no inicio da difusão da tecnologia *wireless* e até hoje é utilizado por alguns usuários que não se preocupam com segurança de seus dados. O WEP utiliza o algoritmo RC4 para criptografar os pacotes que serão trocados numa rede sem fios a para tentar garantir confidencialidade aos dados do usuário.

Mas segundo Rufino (2005); existem problemas administrativos e técnicos em relação ao protocolo WEP. Em relação ao padrão original, os principais relacionam-se ao fato de usar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes de uma determinada rede. Portanto, caso seja necessária a troca da chave, o processo pode ser trabalhoso e, em alguns casos, inviável. Outro problema vincula-se ao fato de que, na época em que o padrão foi definido (1997), havia restrição dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits. E finalmente, foram revelados outros problemas técnicos, que permitem ataques ao próprio algoritmo.

O WEP também utiliza a verificação de redundância cíclica (CRC-32) que é uma função que detecta erros ao fazer o "*checksum*" de uma mensagem enviada. Ela gera um *Integrity Check Value* (ICV) que deve ser conferido pelo receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida ou alterada no meio do caminho. No entanto, após vários estudos e testes realizados com este protocolo, foram achadas algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade, devido aos seguintes fatores:

Tamanho da Chave: Originalmente quando o WEP foi lançado, a chave estática WEP era de apenas 40 bits. Chaves com este tamanho podem ser quebradas por “força bruta” usando-se máquinas atuais. Para solucionar este problema, fabricantes de produtos *Wi-Fi* lançaram o WEP2 com chave estática de 104 e 232 bits, mantendo o vetor de inicialização de 24 bits. Com isto tornou-se praticamente impossível quebrar, em tempo factível, a chave por meio de força bruta.

Reuso de Chaves: Os 24 bits do vetor de inicialização permitem pouco mais de 16,7 milhões de vetores diferentes. Este número de possibilidades é relativamente pequeno. Dependendo do volume de tráfego da rede os vetores de inicialização se repetirão de tempos em tempos e, portanto, as chaves usadas pelo RC4 também se repetirão. A repetição de chaves fere a natureza do RC4 que assim não garante mais a confidencialidade dos dados. Se os vetores de inicialização forem escolhidos aleatoriamente, a freqüência de repetições pode aumentar significativamente. Como por exemplo, tem-se o paradoxo do aniversário. De acordo com o paradoxo, após 4823 pacotes há uma probabilidade de 50% de ocorrer uma repetição de vetores de inicialização. Como o vetor é a parte inicial da chave, passa-se em claro uma parte da chave que codificou o pacote. Devido a esta falha, são explorados ataques poderosos contra redes *wireless* que ainda utilizam a criptografia WEP.

Gerenciamento de Chaves: O WEP não possui um protocolo para gerenciamento de chaves, portanto a chave utilizada pelos dispositivos não pode ser trocada dinamicamente. Isso dificulta a manutenção das redes, principalmente as de grande porte como, por exemplo, as redes corporativas.

Protocolo de autenticação Ineficiente: No modo de autenticação por Chave Compartilhada o atacante pode através de uma simples escuta de tráfego ter acesso a um pacote em claro (pacote texto-desafio) e a sua respectiva cifra (pacote codificado). Com estes dados é possível achar os *keystreams* (seqüência chave) e usá-los para criar uma resposta válida para qualquer texto-desafio. O atacante poderá autenticar-se sem conhecer a chave WEP. O uso de MAC Filtragem por meio de endereço único de caracteres (*Filtering)* não garante nenhuma segurança ao processo de autenticação, pois existem ataques de MAC *Spoofing* (falsificação de endereço MAC) que facilmente podem se realizados. Um atacante pode rapidamente descobrir um endereço MAC válido, através da escuta de tráfego, e usar o endereço descoberto para burlar o MAC *Filtering*.

Problemas do RC4: o algoritmo KSA do RC4 apresenta uma fraqueza muito grave e por isso, até hoje esse tipo de ataque é realizado a redes sem fio que utilizam WEP como meio de proteção utilizando um ataque estatístico que revela a chave WEP estática. Este ataque ficou conhecido como *Fluhrer, Mantin e Shamir* (FMS). Sendo que a técnica KoreK8, otimizou este ataque, aumentando a probabilidade de acerto da chave com um menor número de chaves, diminuindo, assim, o tempo necessário para a quebra da chave. Um bom exemplo são softwares como *AirSnort*9, *WEPCrack*10 e *Aircrack* que tem como objetivo implementar estes ataques de forma simplificada, como obter acesso a redes sem fios de terceiros em menos de meia, através da quebra da chave estática do WEP.

Re-injeção de Pacotes: Redes protegidas pelo WEP são passíveis de ataques de re-injeção de tráfego. Este tipo de ataque sozinho, não afeta diretamente a segurança da rede. Porém pode ser usado para aumentar o tráfego na rede e assim diminuir o tempo necessário para que ataques como o *Fluhrer, Mantin e Shamir* (FMS) que se baseia na idéia de que o atacante recebe passivamente as mensagens enviadas por alguma rede, salvando esses pacotes criptografados com os vetores de inicialização usados por eles. Isso porque os primeiros bytes do corpo da maioria dos pacotes são facilmente previsíveis e o atacante pode conseguir com pouca matemática e analisando uma grande quantidade de pacotes, descobrir a senha de criptografia da rede.

Com todas essas brechas de segurança no padrão WEP não é recomendável utilizar esse tipo de criptografia para redes *wireless* que desejam integridade e segurança em suas informações trafegadas, principalmente em ambientes corporativos.

4.1.2 *Wi-Fi Protected Acess* (WPA)

O *Wi-Fi Protected Access* (WPA) é um protocolo de comunicação via rádio. É um protocolo WEP melhorado. Também chamado de WEP2, ou *Temporal Key Integrity Protocol* (TKIP), essa primeira versão do WPA surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

Conforme afirma Rufino (2006, p. 68); “A respeito do WPA possuir características de segurança superiores ao WEP, ainda assim ele apresenta algumas vulnerabilidades já reportadas e que devem ser conhecidas para que seu impacto possa ser minimizado.”

Essa substituição do WEP pelo WPA teve como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária *Temporal Key Integrity Protocol* (TKIP) que possibilita a criação de chaves por pacotes automaticamente, além de possuir função de detecção de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

A chave de criptografia dinâmica é uma das principais diferenças do WPA em relação ao WEP, que utiliza a mesma chave repetidamente. Esta característica do WPA também é conveniente, porque não exige que se alterem manualmente as chaves de criptografia, ao contrário do WEP. O WPA introduziu diversos mecanismos para resolver os problemas de existentes de segurança associados ao WEP**,** que foi estendido para 48 bits em relação aos 24 bits de Chaves utilizado pelo WEP que permitiam pouco mais de 16 milhões de chaves diferentes, facilitando repetições em um curto espaço de tempo. O WPA introduziu chaves estendidas de 48 bits. Assim, proporcionando mais de 280 trilhões (248) de Chaves diferentes, o que eleva o nível de segurança.

Mesmo com tantas melhorias foi descoberto existência de falhas no padrão WPA foi necessário então um novo lançamento para efetuar a correção destas falhas de segurança. Assim surgiu o WPA 2 - *Personal* que será abordado a seguir.

4.1.3 *Wi-Fi Protected Access – Personal*

O *Wi-Fi Protected Access* é um programa de certificação criada para indicar a conformidade com o protocolo de segurança de redes de computadores sem fio. Este protocolo foi criado em resposta a tinha graves deficiências encontradas no sistema anterior, *Wired Equivalent Privacy* (WEP).

Com a necessidade de solucionar os problemas de segurança das redes *wireless* domésticas foi necessário criar um modo de criptografia forte e intuitiva para sua implantação pois um usuário comum não seria capaz de instalar e fazer a manutenção de um servidor de autenticação. Por esse motivo criou-se o WPA-PSK (*WPA-Pre Shared Key*) que é uma *passphrase*, previamente compartilhada entre o *acess poiter* e os clientes.

Neste caso, autenticação é feita pelo *acess pointer*. A chave é configurada manualmente em cada equipamento pertencente à rede e pode variar de 8 a 63 caracteres ASCII, mas com uma segurança muito mais elevada se comparado ao WEP e com bastante facilidade para implantação conforme a figura 10 que demonstra como selecionar a opção WPA Personal.

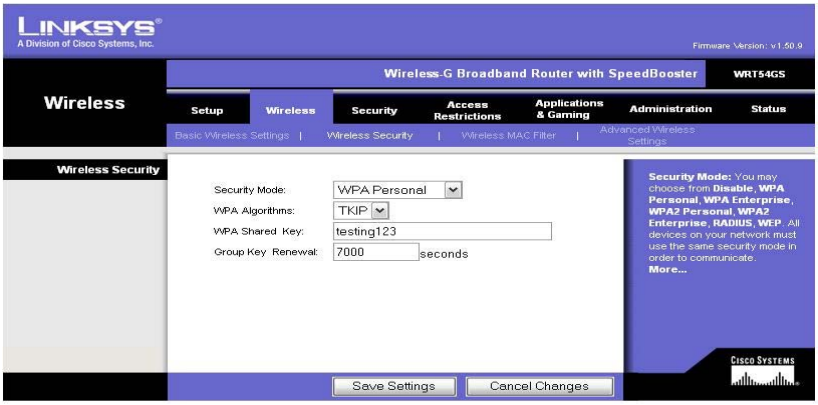

Figura 10: Configurando WPA Personal
Fonte: http://img127.imageshack.us/i/router2cc4.jpg/

Conforme a figura 10, o uso do WPA 2 *Personal* é bastante indicado para utilização em ambientes domésticos ou que não possuam um servidor de autenticação para administrar acesso dos usuários da rede. Em casos de ambientes corporativos em redes com mais de 80 usuários é recomendável o uso do WPA 2 enterprise que será abordado a seguir.

4.1.4 *Wi-fi Protected Acess* (WPA) *Enterprise*

O WPA tem como foco não permitir que o *access point* seja responsável por nenhuma autenticação. Tanto a autenticação do usuário quanto do dispositivo é feita por um servidor de autenticação. É utilizada uma infra-estrutura complementar formada por um servidor que usa

o protocolo de autenticação 802.1x em conjunto do *Extensible Authentication Protocol* (EAP).

O 802.1x é um protocolo de comunicação utilizado entre o roteador *wireless* e o servidor de autenticação. Este protocolo já era largamente utilizado em redes cabeadas e se mostrou também adequado quando integrado às redes sem fio.

O seu funcionamento é o seguinte: quando um cliente solicita uma autenticação, o servidor de autenticação verifica em sua base de dados se as credenciais apresentadas pelo solicitante são válidas. Em caso positivo o cliente é autenticado e uma chave chamada *Master Session Key* (MSK) que é enviada ao mesmo.

Normalmente, utiliza-se como servidor de autenticação RADIUS, contudo não é obrigatório sendo possível utilizar outras soluções pagas ou não que utilizam os mesmos meios autenticação, como é ilustrado na figura 11.

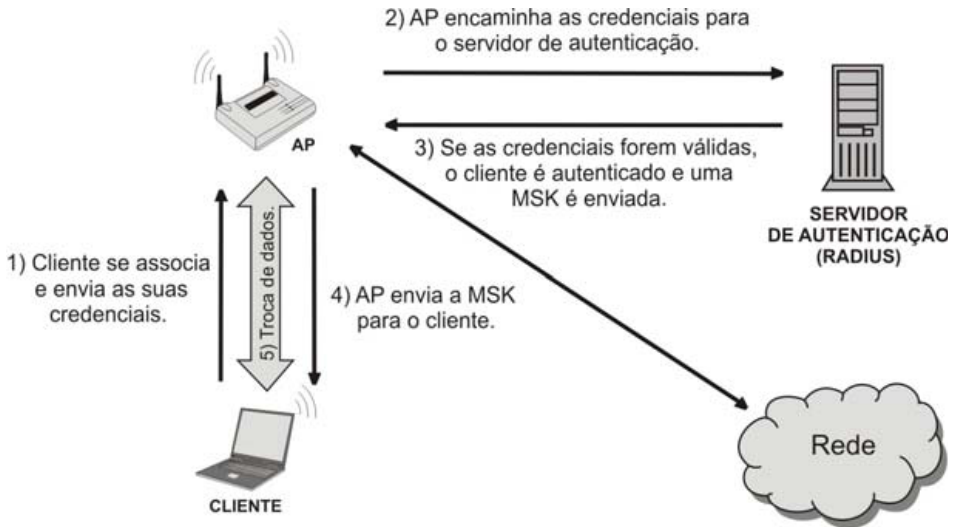

Figura 11: Processo de autenticação com servidor Radius

Fonte: http://www.unibratec.com.br/jornadacientifica/diretorio/UFPEAGL.pdf

O Protocolo de Autenticação Extensível (EAP) faz a parte de levar o cliente até o servidor radius para que seja feita a autenticação. Em seguida ele libera o acesso ou não caso o usuário não faça parte da rede como será apresentado.

4.1.5 Protocolo de Autenticação Extensível (EAP)

O protocolo de autenticação extensível (EAP) possui a responsabilidade de criar um canal lógico de comunicação seguro entre o cliente (*supplicant*) e o servidor de autenticação, por onde as credenciais irão trafegar. Fisicamente, o cliente se comunica com o *Access Point* (AP) através do protocolo *Extensible Authentication Protocol over LAN (EAPOL).* O AP, por sua vez, se comunica com o servidor de autenticação através do protocolo 802.1x, conforme ilustrado na Figura 12:

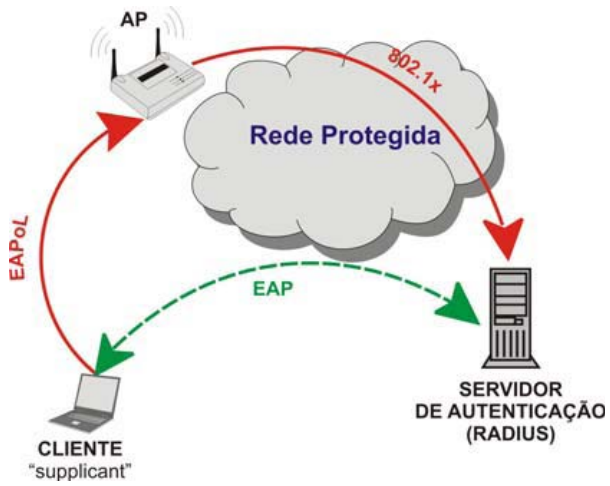

Figura 12: Processo de autenticação com EAP

Fonte: http://www.unibratec.com.br/jornadacientifica/diretorio/UFPEAGL.pdf

Existem vários acessórios para trabalhar junto com a autenticação do Servidor *Radius*. Dentre eles, *smart cards*, certificados digitais, biometria, entre outras formas que elevam o nível de segurança. Em resumo o *WPA2-enterprise*, oferece maior garantia de segurança e autenticação para os usuários de redes *wireless* corporativas.

5 TIPOS DE ATAQUES EM REDES *WIRELESS*

Nesse capítulo pode-se observar que atualmente redes sem fio possuem grandes gargalos e brechas de segurança que qualquer pessoa, com apenas com um dispositivo sem fio, poderá ter acesso à rede dependendo do nível de segurança adotado, para que isso não ocorra, é necessário entender quais técnicas são utilizadas para violar segurança nos equipamentos sem fio. Para que seja possível reduzir e dificultar os ataques às organizações que utilizam redes sem fio tem-se que entender o funcionamento da tecnologia de comunicação de redes sem fio de computadores e suas falhas e possíveis soluções que possibilitem um nível maior de segurança. Isso é possível através do entendimento das técnicas utilizadas pelos invasores que será abordado nos seguintes subitens desse capítulo.

5.1 TÉCNICAS DE INVASÃO

Devido a facilidade de acesso que os dispositivos de redes sem fio proporcionam muitos usuários e algumas empresas da tecnologia *wireless* não se preocupam com a segurança de sua própria rede e acabam dando mais atenção ao seu desempenho. Muitos não adotam uma configuração necessária de segurança e criptografia para se obter uma confiabilidade maior de segurança de transmissão de dados em redes sem fio.

Através da falta de preocupação com a segurança nas redes sem fio, muitos indivíduos podem obter acesso não autorizado a ela, pelo fato de muitos usuários e empresas utilizarem equipamentos com configuração de fábrica (*Default*). Isso ocorre pela falta de informação que em algumas vezes não são passadas para o consumidor final (RUFINO, 2005).

Com tantas possibilidades de invasão facilitada através de *softwares* ou até mesmo sem nenhum conhecimento, muitos indivíduos obtêm acessos à rede sem fio sem autorização, comprometendo assim a confiabilidade e a integridade das informações que circulam pela rede sem fio. Indo mais a fundo o *hacker* pode ter quatro comportamentos estratégicos diferentes em relação ao processo de invasão de redes sem fio, de acordo com (RUFINO, 2005).:

- **Interrupção:** Nesse procedimento o invasor influi em interromper as passagens de dados de um ponto para outro, conforme a figura 13 abaixo:

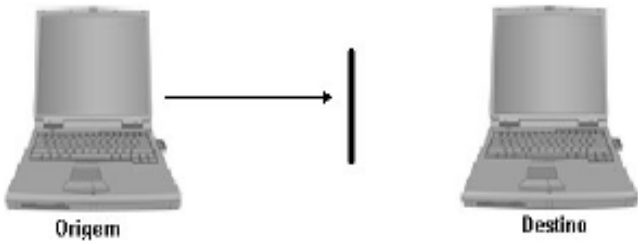

Figura 13: Exemplo de ataque utilizando sinais interferências

Fonte: CD curso de redes de computadores (digerati)

- **Interseção:** Nesse procedimento o invasor realiza coleta de informações para saber o que se passa dentro da rede e por fim ter acesso a ela futuramente, conforme a figura 14 abaixo:

Figura 14: Exemplo de espionagem da rede sem fio Fonte: CD curso de redes de computadores (digerati)

- **Modificação:** Nesse procedimento o invasor não apenas escuta o tráfego da rede, mas também modifica e compromete os dados para depois enviá-los para o dispositivo a que está sendo atacado. O objetivo é que este se torne um dispositivo zumbi e o invasor tenha total controle os dispositivos conforme a figura 15.

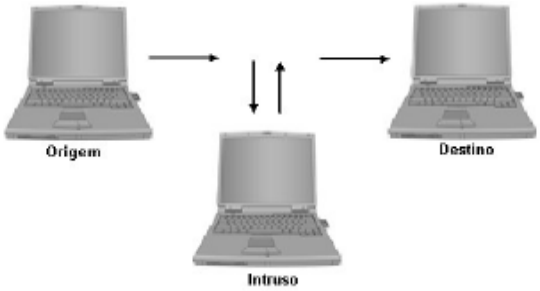

Figura 15: Exemplo de ataque com envio de pacotes de dados maliciosos

Fonte: CD curso de redes de computadores (digerati)

– **Fabricação:** Nesse caso, o invasor desenvolve os dados a serem enviados para um determinado destino com intuito de se obter acesso a rede sem fio, conforme a figura 16 abaixo:

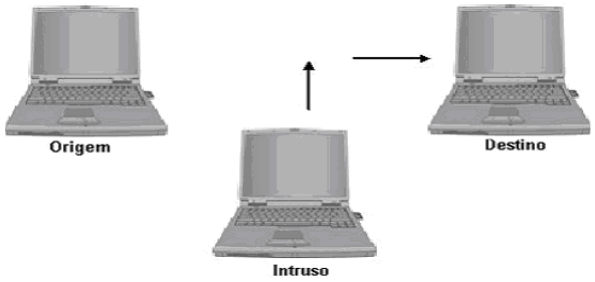

Figura 16: Exemplo de intercessão de pacotes de dados
Fonte: CD curso de redes de computadores (digerati)

Quando um invasor descobre uma rede sem fio completamente mal configurada, ele pode utilizar *softwares* maliciosos (*Scanners)* que capturam os pacotes de dados com o intuito de se obter o SSID e a chave de acesso.

Existe a possibilidade do atacante se passar por um membro da rede sem fio e assim os dispositivos dão a permissão para executar tarefas como se fosse um usuário normal (RUFINO, 2005).

5.1.2 Negação de Serviço – *Denial of Service*

Um ataque de negação de serviço é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Alvos típicos são servidores web. O ataque tenta tornar as páginas hospedadas indisponíveis na www. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Carvalho Filho (2005, p. 57) diz que a negação de serviço em redes sem fio:

> É um tipo de ataque que se baseia em não invadir computadores, mas sim tirar o serviço fora do ar com dispositivos que emitam uma grande carga de freqüência de 2,4 GHz. Assim prejudicando a qualidade do serviço de transporte de informação ou até mesmo interrompendo completamente o funcionamento da rede sem fio.

Também pode ocorrer esse tipo de problema com algum vizinho que tenha algum rádio amador que trabalhe na mesma frequência, ocasionando paradas e quedas na rede sem fio. O objetivo deste ataque é impedir o acesso aos recursos de uma rede. Normalmente, o atacante inunda (*flood*) a rede com pacotes defeituosos fazendo com que esta não consiga responder. No caso das redes sem fio estão mais suscetíveis a esse tipo de ataque devido à comunicação

entre as camadas do modelo *Open Systems Interconnection* (OSI). A camada física de uma rede sem fio é mais fácil de ser atacada do que a camada física de uma rede cabeada, devido ao meio de ondas de radio. O invasor não precisa obter acesso à rede como em redes cabeadas, e ele pode disparar inserir um simples ruído na faixa de transmissão para criar um DoS na camada física . A função do telefone na figura 17 é meramente ilustrativa para demonstrar a criação de ruídos.

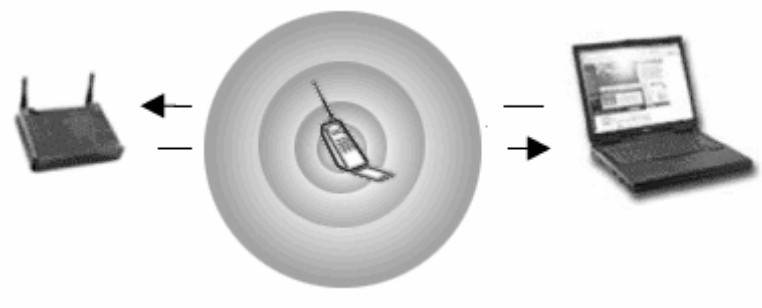

Figura 17: Ruído de um telefone para um DoS na camada física
Fonte: http://www2.dc.uel.br/nourau/document/?view=317

É possível através da clonagem do endereço MAC disparar o ataque de DoS na camada de enlace de dados da pilha de protocolo do modelo OSI. Caso aconteça a clonagem a primeira estação que se autenticar no AP obtém acesso à rede. No exemplo da figura 18, o endereço MAC de A foi clonado em B. Desta forma o AP não envia e nem recebe dados de A. Mesmo o protocolo WEP não auxiliaria neste tipo de ataque.

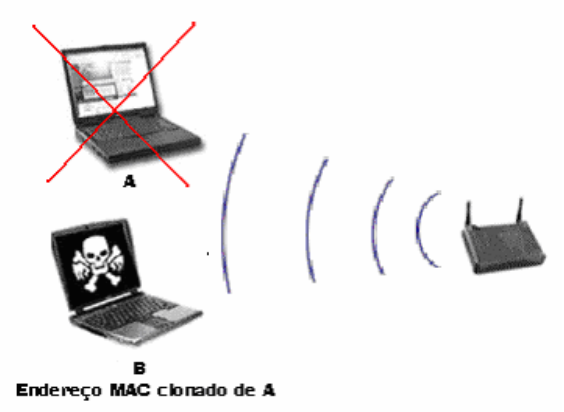

Figura 18: Negação de serviço através de clonagem de MAC
Fonte: http://www2.dc.uel.br/nourau/document/?view=317

Outra forma de se atacar via DoS na camada de enlace é através do envio em x do SSID. Usualmente, uma estação é configurada para se conectar com o sinal mais forte de um determinado local, portanto, bastaria ao invasor se passar por um AP e enviar o SSID para as estações de trabalho que estão procurando acesso, conforme ilustrado na figura 19. Bastaria um pouco de tempo para que o atacante conseguisse a chave WEP que autentica e codifica uma determinada rede.

Figura 19: Invasor se passar por AP e envia em broadcast o SSID do AP
Fonte: http://www2.dc.uel.br/nourau/document/?view=317

Para se considerar um ataque Dos, basta um invasor simplesmente inundar todo o tráfego com comandos de requisição como um *ping* na camada rede ou então, se associar a um AP, inundar as estações com requisições de associação ou desassociação, fazendo com que a comunicação entre as estações e os equipamentos de redes fiquem intransitável.

5.1.3 Mapeamento do Ambiente

Este tipo de procedimento realizado pelo atacante tem o objetivo de verificar o maior número de redes disponíveis, permitindo conhecer quais tipos de criptografia estão sendo utilizandos, permitindo definir quais redes devem ser atacadas de forma mais precisa e com menos risco de ser identificado (CARVALHO FILHO, 2005). Esse procedimento pode ter maior ou menor grau de êxito dependendo dos mecanismos de proteção existentes no alvo. Uma boa ferramenta para essa atividade é o *Network Stumbler* conforme na figura 20:

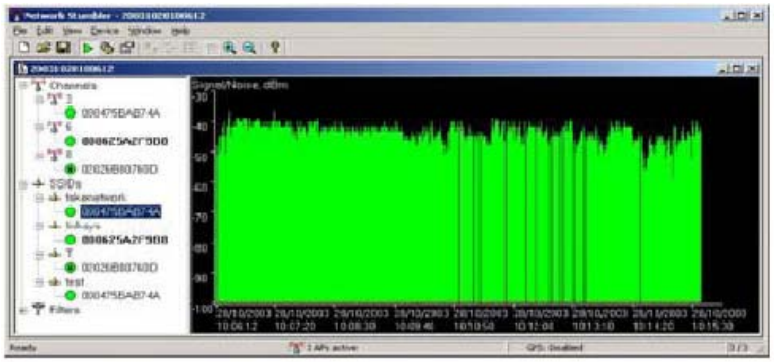

Figura 20: Exemplo de capturas de dados efetuado pelo Software Network Stumbler®.

Fonte: http://www.freewarebox.com/images/screenshot/netstumbler_19692.png

Na figura 20 é demonstrada a interface do software *Network Stumbler* que além de localizar redes wireless e informar quais tipos de criptografia estão sendo utilizados, permite a integração com um *Global Positioning System* (GPS) que cria mapas de redes disponíveis em um perímetro para que seja usado em futuros ataques.

5.1.4 Arp Spoofing

É uma técnica relativamente antiga, simples e eficaz de ataque. Consiste em passar um mac-address (endereço mac) falso para o sistema alvo de forma que este redirecione o tráfego para outro destino que não o legítimo conforme o exemplo na figura 21 que demonstra este tipo de ataque.

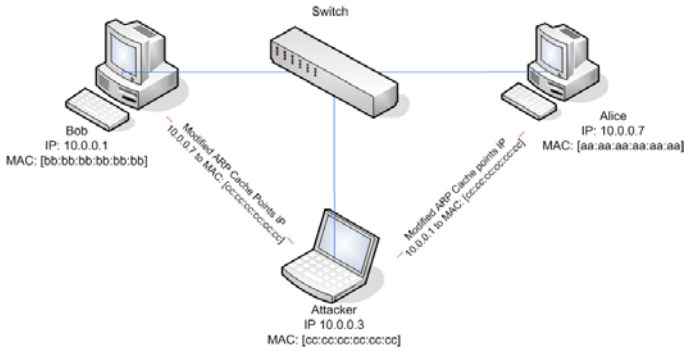

Figura:21 Efetuando arp spoofing

Fonte: http://securitymusings.com/article/tag/arp-spoofing

Santos (2003, p. 56) diz que:

> Cada dispositivo fabricado de rede possuem um *MAC Address* único, cada placa dispositivo de rede possui uma numeração única, ou seja, com essa numeração é possível que o administrador de rede utiliza esse conjunto de letras e números para obter uma forma mais segura de autenticação.

Existem duas formas simples de se modificar o mac: a primeira utilizando o sistema operacional Linux com o comando *#ifconfig atho* e a segunda no próprio Windows através da propriedade dos dispositivos de rede.

5.1.5 Sniffers

É um tipo de *Scanner* utilizado para capturar dados para logo após tentar quebrar a criptografia. E caso não esteja criptografados será facilmente possível visualizar as informações que estão sendo transmitidas. Para esse procedimento o invasor utiliza um famosa ferramenta que possibilita esse tipo de ataque chamada de *Kismet* que também não deixa de ser um *Scanner* (SANTOS, 2005). A figura 22 demonstra o funcionamento *kismet* em funcionamento.

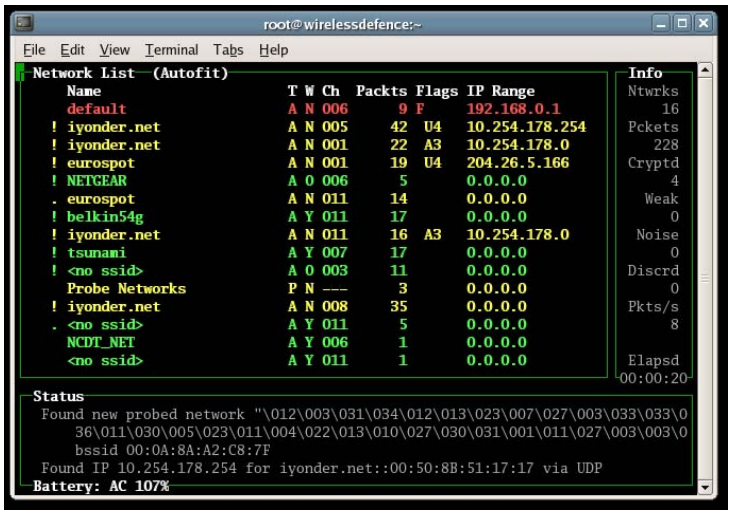

Figura 22: Kismet capturando dados de redes wireless

Fonte: http://linuxkismet.files.wordpress.com/2008/08/kismet1.png

Na figura 22, o Kismet possui a função de ser uma ferramenta passiva, colocando a placa wireless em modo de monitoramento *(rfmon)* e passando a escutar todos os sinais que cheguem até sua antena. Mesmo pontos de acesso configurados para não divulgar o SSID ou com encriptação ativa são detectados para que esses dados capturados sejam utilizados para um futuro ataque.

5.1.6 Associação Maliciosa (Access Point Spoofing)

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

“É o processo em que o invasor realiza uma simulação do ponto de acesso utilizando um software chamado de softAP. Esse tipo de ataque engana o usuário fazendo com que ele pense que ele está conectado a uma rede real mas, na verdade o usuário está sendo atacado pelo invasor (SANTOS, 2005)”

Através de ferramentas amplamente disponíveis, um usuário mal intencionado pode forçar uma estação autenticada se conectar a outra rede, ou então alterar as configurações da estação para esta operar em modo *ad-hoc*. No caso de uma estação ser forçada, o ataque inicia quando o usuário converte a estação para um access pointer funcional através de um softAP forçado a mandar em *broadcast* um *Probe Request* a procura de APs disponíveis, desta forma o usuário responde à requisição para uma associação e inicia a conexão entre eles . A partir deste momento, o usuário pode explorar todas as vulnerabilidades da estação. A figura 23 ilustra este ataque via softAP.

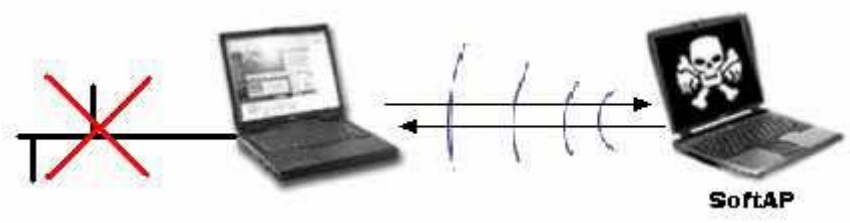

Figura 23: Associação maliciosa via softAP

Fonte: http://www2.dc.uel.br/nourau/document/?view=317

Devido o grande risco de uma estação operar em modo *ad-hoc*, os próprios usuários ou mesmo o próprio sistema operacional desabilita esta função, diminuindo assim o número de ataques deste tipo em redes *ad-hoc*. A associação maliciosa é um ataque que prova a falha sobre os métodos de autenticação, Por uma estação não saber em qual rede (modo *ad-hoc*) ou em qual AP (modo infraestruturado) ela está conectada. Vale ressaltar que mesmo uma STA(estação) que esteja localizada em uma VPN continua sujeita a este tipo de ataque, pois o mesmo não ataca o ‘túnel’, mas sim a própria STA através de uma segurança fraca que esta possa ter. Uma forma de evitar associações maliciosas é a prevenção das conexões de certo local, isto é, formas de monitoramento, fazendo com que as estações se conectem apenas em

APs *(access pointers)* e redes autorizadas. Monitorando a rede é o único meio de conhecer onde as estações estão se conectando corretamente aos APs da rede corporativa.

5.1.7 *Man-In-The-Middle* (Homem-No-Meio)

O ataque *Man-in-the-middle* é um ataque sofisticado e usualmente praticado em redes sem fio, pois não há a necessidade do atacante estar conectado a uma rede cabeada, diferente de ataques como o ARP *Poisoning*. Este tipo de ataque pode quebrar a segurança de uma VPN (rede virtual privada) através da inserção de uma associação maliciosa entre uma estação e um AP, onde o atacante finge ser um AP autenticado para uma estação e finge ser uma estação autorizada para um AP.

O *Man-in-the-middle* é similar à associação maliciosa e ao *Denial of Service* (Negação de Serviço), contudo como o próprio nome diz, o invasor fica entre o AP e uma estação. A viabilidade deste tipo de ataque em relação à associação maliciosa é de, ao invés do invasor ter que se conectar com todas as estações que ele deseja invadir, todas as estações passam por ele antes dos dados chegarem ao AP, assim como no ARP *Poisoning*. A diferença entre o ARP *Poisoning* e o *Man-in-the-middle* é a forma de aquisição do acesso. No primeiro é utilizada a autenticação pelo endereço MAC e no segundo pelo *Challenge Handshake Authentication Protocol* (CHAP). As diferenças entre os ataques e o ataque *Man-in-the-middle* passo-a-passo, conforme, são ilustrados na figura 24.

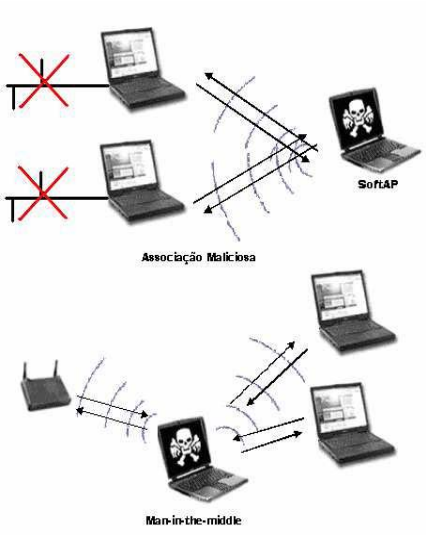

Figura 24: Diferença entre uma associação maliciosa e man-in-the-middle

Fonte: http://www2.dc.uel.br/nourau/document/?view=317

O ataque *Man-in-the-middle* se baseia no CHAP (*Challenge-Handshake Authentication Protocol*), onde o invasor faz com que a estação se *reautentique* com o *access pointer*, respondendo devidamente as requisições para o invasor obter as informações necessárias e por fim o *access point* responder com sucesso a *reautenticação* da estação. Este processo é ilustrado em 4 fases distintas a seguir:

Fase 1:

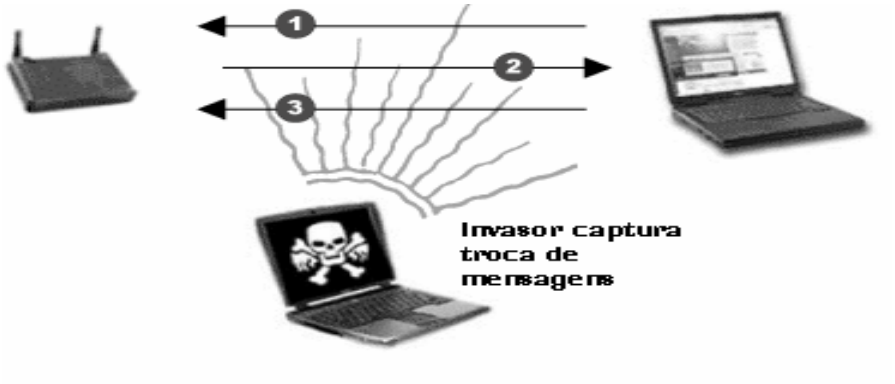

Figura 25: Man-in-the-middle fase 1

Fonte: http://www2.dc.uel.br/nourau/document/?view=317

1. A estação começa processo de conexão com o AP;

2. AP responde a estação com outra requisição;

3. A estação responde ao AP;

Preparando o ataque: Invasor manda uma requisição para o AP como se fosse a requisição feita pela estação autenticada e escuta as informações de requisição

e resposta.

Fase 2:

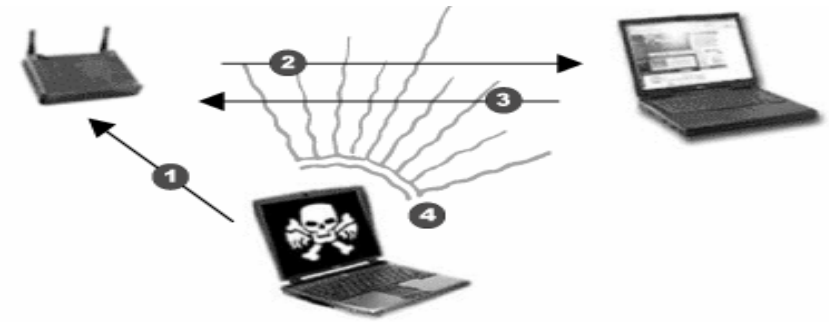

Figura 26: Man-in-the-middle -

Fase 2 Fonte: http://www2.dc.uel.br/nourau/document/?view=317

1. Invasor manda uma requisição ao AP forçando uma outra requisição AP-ESTAÇÃO;

2. AP manda requisição AP-ESTAÇÃO para a ESTAÇÃO já autenticada;

3. A estação computa e manda a resposta;

4. Invasor captura a resposta válida;

Ganhando o meio: Invasor faz o papel inverso, como se fosse o AP e escuta as informações necessárias.

Fase 3:

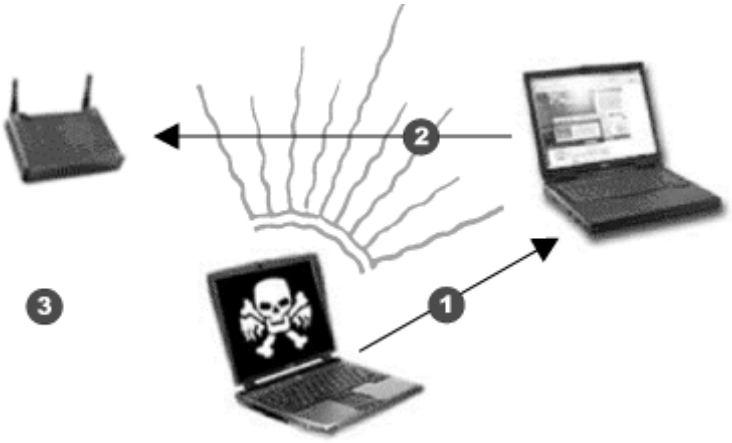

Figura 27: Man-in-the-middle - Fase 3
Fonte: http://www2.dc.uel.br/nourau/document/?view=317

Fase 4:

1. Invasor manda uma requisição AP-ESTAÇÃO falsa para a STA autenticada;

2. A estação manda a resposta para o AP;

3. Invasor captura a informação para se autenticar;

Entrando na rede: Invasor força a caída da estação para na reautenticação conseguir o acesso a rede

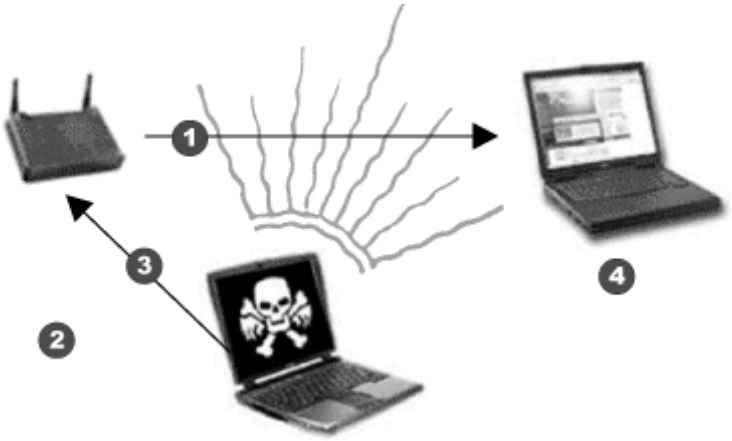

Figura 28: Man-in-the-middle - Fase 4 Fonte: http://www2.dc.uel.br/nourau/document/?view=317

1. AP envia o pacote que indica sucesso na conexão entre a ESTAÇÃO e o AP;

2. Invasor captura o pacote de sucesso;

3. Invasor manda uma resposta adequada e obtém acesso a rede;

4. STA antes autenticada é impedida de se reautenticar a rede;

Nesse tipo de ataque há requisitos a serem cumpridos para o seu sucesso: a estação deve responder às requisições do access pointer (CHAR RFC), o *protocolo Point-to-Point Protocol* (PPP) desconhece os endereços IPs e o AP deve mandar a ultima resposta de sucesso para a ESTAÇÃO com o pacote de sucesso (CHAR RFC).

5.1.8 *Wardriving*

O *Wardriving* é a prática de procurar por redes sem fio dirigindo um automóvel. Para isto, usa-se um carro ou uma caminhonete e um computador equipado para redes sem fio, como um *laptop* ou um PDA, para detectar a rede.

Martini (2000, p. 46) diz que *Wardriving*

> É um tipo de ataque aonde o invasor sai em busca de redes sem fio em cidades com seu carro acompanhado com seu *Notebook* equipado com uma placa de rede sem fio interligada a uma antena construída por ele mesmo para aumentar a captura dos sinais das redes sem fio. O principal objetivo de tipo de ataque é definir as localizações das redes sem fio e determinar o nível de segurança e verificar se ela se encontra aberta ou fechada para seguir com o ataque final a rede.

O invasor logo após de obtido sucesso ou fracasso para invasão da rede sem fio, ele classifica da forma apresentada na figura 29.

SSID 	Esse símbolo define que a rede sem fio se encontra aberta, ou seja o SSID está disponível.
SSID 	Esse símbolo define que a rede sem fio se encontra fechada com seu SSID.
SSID 	Este símbolo define que a rede sem fio está protegida com protocolo de criptografia WEP, e também seu SSID não pode ser revelado.

Figura 29: Exemplo de pichações realizadas por *Wardriving* em grandes cidades

Fonte: http://www.wardriving.com

Um dado importante é que todos esses tipos de invasão e ferramentas para quebra de criptografia *wireless* foram iniciadas após a descoberta e publicação de falhas de segurança na Internet por Walke *(*2000*),* que era funcionário da Intel na época aonde ele provou que os algoritmos de criptografia utilizados nas redes sem fio possuíam muitas falhas no processo de funcionamento e autenticação.

Logo após dessa descoberta uma pesquisadora chamada Borisov (2001*)* da Rússia fez a façanha de quebrar o sistema em apenas 4 horas utilizando super computadores interligados em rede. Atualmente a ferramenta mais famosa para esse tipo de ataque para tentar quebrar as chaves Isolamento Equivalente telegrafado (WEP) é chamada de *AirSnort.*

6 MECANISMOS DE SEGURANÇA E PREVENÇÃO

Com as necessidades atuais do mercado corporativo, exige-se das grandes organizações um sistema mais seguro e estável e com menos acessos indevidos, sobretudo para se evitar espionagem empresarial. Enquanto muitos dispositivos ainda utilizam protocolos de segurança fracos como o WEP, que pode comprometer a integridade e confiabilidade no tráfego das informações. Mas para tudo tem uma solução, ou, pelo menos, uma proteção necessária para implementar controles aos equipamentos externos. Implementar uma configuração adequada, por exemplo, criptografias de acesso maiores e estáveis, monitoração dos acessos da rede sem fio entre outras formas, pode possibilitar às organizações um ambiente mais seguro e estável nas redes sem fio. Este capítulo trata separadamente dos principais mecanismos de segurança disponíveis em redes sem fio e seus mecanismos utilizados para se obter um ambiente mais seguro e estável.

6.1 Service Set ID (SSID)

O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar à uma rede sem fio se puder fornecer o SSID correto.

Engst e Fleishman (2005) dizem que a principal função do SSID (*Service Set Identification*) é identificar o nome da rede que o dispositivo cliente está se conectando. O SSID e basicamente uma forma de nomear uma rede *wireless* conforme a figura 30 que demonstra um computador conectado a uma rede *wireless*.

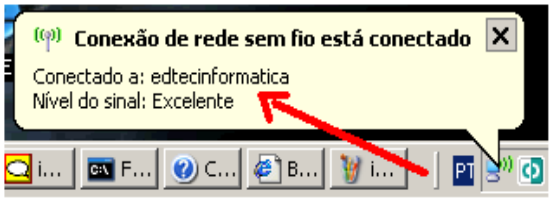

Figura 30: Exemplo de um SID em funcionamento

Fonte: Windows Server 2003.

Outra vantagem que o SSID proporciona é a utilização dele como uma senha para usuários não autorizados tenham acesso à rede. Pois só é possível ter acesso à rede se tiver realmente o nome exato da mesma e as chaves de criptografia para efetuar com sucesso o processo de autenticação (ENGST e FLEISHMAN, 2005).

6.2 Endereçamento *Media Access Control* (MAC)

O endereçamento MAC é um conjunto de 12 números e letras que identificam os dispositivos conectados à rede. Esses conjuntos de letras e números possibilitam encadear a rede sem fio para que somente os computadores que possuam o endereço MAC tenham acesso à rede (ENGST e FLEISHMAN, 2005).Esses números e letras descrevem que cada dispositivo é único na rede conforme o exemplo na figura 31:

= Servidor

FIGURA 31: Exemplo de um endereço MAC
Fonte: Windows Server 2003.

O endereçamento MAC em redes sem fio possibilita que apenas os computadores que estão registrados com seus endereços de MAC tenham acesso à rede. Essa técnica não disponibiliza um nível aceitável de segurança, porém dificulta um possível ataque por uma pessoa com menos conhecimentos de intrusão e captura de dados (ENGST e FLEISHMAN, 2005).

6.3 Análise do Ambiente

Para que o sinal da rede sem fio não ultrapasse ou não cubra a área da empresa, é necessário analisar o ponto de acesso das antenas para que realmente seja possível saber se a empresa pode sofrer um possível ataque a sua rede sem fio (ENGST e FLEISHMAN, 2005).

Atualmente existem várias ferramentas de análise de sinal e identificação do alcance espalhadas pela Internet como, por exemplo, o *Network Stumbler* que foi mencionado no capítulo anterior. A utilização desse tipo de *software* localizará os pontos de acesso da organização, trará todas informações como freqüência, SSID, MACs, possibilitando demarcar a amplitude do sinal.

6.4 Atraindo Dispositivos Decoy Device

A técnica de *Honeypots*, conhecida popularmente no meio dos administradores de rede, possui o objetivo de iludir e dificultar possíveis invasores. Basicamente essa técnica funciona com a instalação de vários equipamentos que irão enviar varias informações falsas sobre redes sem fio inexistentes como por exemplo vários SSID. Adotando essa técnica, o possível

invasor terá muito mais, trabalho por não saber para onde realmente direcionar o seu ataque e assim se tornando uma tarefa mais complexa. (ENGST e FLEISHMAN, 2005).

6.5 Desabilitando o Service Set Identification (SSID)

Em uma rede sem fio (*Wireless Network*) é necessário ter um SSID para a identificação da rede para oferecer uma facilidade aos clientes para obter acesso. A grande desvantagem é que o SSID não é criptografado pelo WEP, facilitando para o invasor a obtenção de informações para concluir com êxito seu ataque (ENGST e FLEISHMAN, 2005).

Atualmente as empresas que fornecem concentradores como, por exemplo, a *Linksys* já possui a opção de se desabilitar o SSID facilmente em uma interface amigável. É muito importante também colocar nomes no SSID que não tenham referência a organização ou usuário dos concentradores de rede sem fio, o que dificulta uma possível tentativa de invasão.

6.6 Rede Virtual Privada (VPN)

A utilização das redes *Virtual Private Network* (VPN) é usada por muitas organizações que utilizam tecnologia de redes sem fio e também em redes cabeadas para que os dados que circulem pela rede não possam ser interceptados. Essa técnica também é conhecida como tunelamento, pois a sua utilização cria túneis virtuais entre dois dispositivos, evitando que uma rede de uma organização seja grampeada por um possível atacante. Basicamente seu funcionamento é executado desde a saída dos dados do computador ou dispositivo (matriz) acompanhado de um *firewall* até a chegada ao outro dispositivo ou computador com um *firewall* instalando (filial) (ENGST e FLEISHMAN, 2005).

A técnica de tunelamento possibilita que os dados sejam criptografados antes mesmo que sejam transmitidos para que se torne ilegível caso seja interceptado no processo de envio dos dados para o dispositivo interligado na Internet. Após a viagem dos dados pela rede na qual antes do seu envio, passaram pelo processo de criptografia e encapsulamento, até chegar ao destino correto. Logo após são descriptografados e desencapsulados, voltando a serem informações legíveis (ENGST e FLEISHMAN, 2005). A figura 32 demonstra um exemplo de utilização de redes VPNs:

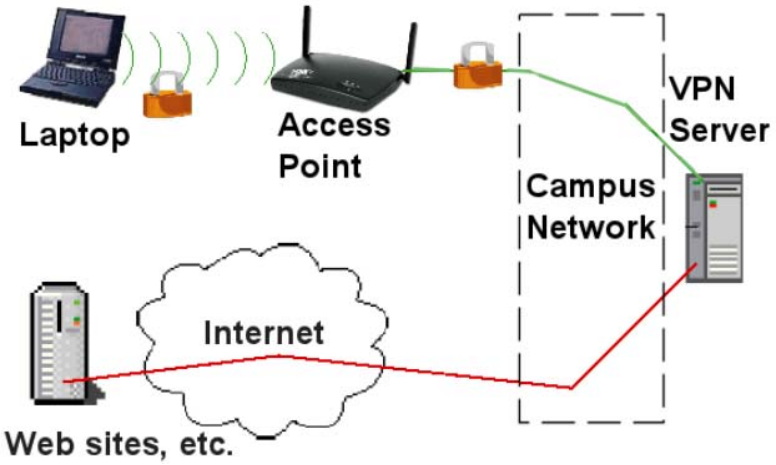

FIGURA 32: Exemplo de uma rede virtual privada

Fonte: http://law.gsu.edu/technology/images/wireless-vpn.gif

Embora as VPNs ofereçam muitas vantagens de segurança e autenticidade sua utilização deve ser muito bem analisado, devido o alto custo e redução da velocidade da rede, pois quanto mais políticas de segurança e criptografias maiores são as possibilidades de ocorrências de gargalos em períodos de pico de utilização da rede (ENGST e FLEISHMAN, 2005).

6.7 Barreiras de Proteção (*Firewalls)*

A principal finalidade de um *firewall* é manter os computadores mais seguros. Basicamente essa ferramenta atua como uma “defesa”, monitorando e controlando ambos os lados através de políticas de segurança e configuração.

Além de oferecer mais segurança aos computadores o *firewall* também pode atuar como um *gateway* entre duas redes, caso uma seja *WI-FI* e outra LAN (Local Área *Network*), possibilitando o bloqueio de atividades suspeitas de ambos lados.

O *firewall* possui duas formas de execução de processos de filtragem de tráfego, segundo Sinkoç (2005):

Filtragem de pacote: Este tipo de filtragem se baseia em trabalhar nas camadas TCP/IP, analisando todo o tráfego por essa camada de rede, permitindo ou não os transportes dos dados na rede. Uma das grandes vantagens desse tipo de filtragem do *firewall* é a função de análise de atividades suspeitas, bloqueando no caso de uma tentativa externa de invasão.

Filtragem de aplicação: Este tipo de filtragem possibilita um ambiente mais seguro, pois todas as aplicações devem passar pelo processo de filtragem. Este tipo de *firewall* tem a função de intermediar todo o processo de comunicação entre dois ou mais dispositivo.

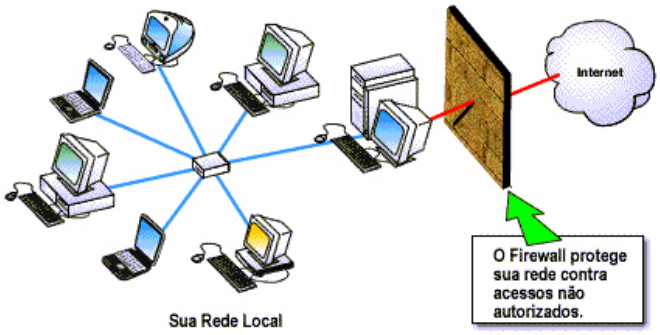

Figura 33: Exemplo do Funcionamento de firewalls

Fonte: http://www.gta.ufrj.br/grad/08_1/firewall/firewall_1.jpg

Essas formas de filtragens de dados que os *firewalls* possuem não impedem que documentos compartilhados sejam acessados por outras pessoas da mesma rede ou que tenham privilégios concedidos ao acesso, tanto como externamente como internamente, desde que sejam previamente configurados.

7.0 ESTUDO DE CASO

Como forma de enriquecimento desta pesquisa, fez-se um estudo de caso visando mostrar de que forma determinada empresa, no caso a FCS TECNOLOGIA, realiza a segurança na rede de um de seus clientes, uma empresa de mármore, na qual não será citado seu nome.

Esta empresa iniciou-se no ramo de mármore há mais de 10 anos, sendo uma empresa de conhecimento de toda população da cidade de Linhares. Além de extrair mármore, ela o exporta e trabalha com ele realizando peças para vendas, atraindo pessoas da região e da própria cidade.

Ela começou com poucos trabalhadores, mas foi ampliando seu espaço no mercado e necessitando estar sempre em contato com clientes e fornecedores de outros países.

Essa empresa procurou a FCS TECNOLOGIA, pois recebia constantemente, clientes do exterior e estes precisavam ter acesso a uma rede sem fio para se comunicarem com seu país de origem. Esses clientes já possuíam uma placa wirelless instalada e, por sua vez, entravam em contato com os arquivos pessoais da empresa.

A empresa, sentindo-se insegura, procurou formas de implementar uma rede sem fios pelos seguintes motivos:

- Atender melhor ao cliente externo;
- Obter facilidade no acesso a essa rede pela própria empresa;
- Aumentar a segurança de seus arquivos pessoais, através de WPA digitando uma senha de acesso a rede;
- Gerar senha apenas para pessoal autorizado;
- Utilizar um rádio transmissor para reduzir o sinal no pátio da empresa.

Essas atitudes fizeram a empresa ter segurança de seus dados, passando-os apenas a quem tivesse acesso a senha gerada para um administrador. Além disso, a redução no sinal do pátio impede que os clientes externos acessem arquivos particulares da empresa.

Para realizar isso foi necessário como equipamentos:

- Roteador link system;
- Ponte de acesso a Internet da empresa;
- Política de segurança no roteador.

As principais vantagens da rede sem fio foram:

- Facilidade em comunicação com empresas no exterior;
- Facilidade de comunicação com os funcionários através de telefonia VOIP;
- Compartilhamento de arquivos;

- Computadores móveis com redes sem fio;
- Bloqueio de pessoas externas no escritório da empresa, reduzindo o risco de fraudes.

No entanto, as desvantagens são:

- Ainda há possibilidade se ataques de hackers;
- Devido à facilidade de acesso ao cliente SSDI vai estará aberto com a identificação da empresa;
- Tendo acesso a rede externa há a possibilidade de acesso á rede interna da empresa.

Mesmo tendo desvantagens, ainda existem formas de melhoria para a referida empresa, que estão sendo estudadas para serem postas em prática. São elas:

- Implementar rede privada VPN que possibilita um túnel criptografado, para que a pessoa tenha acesso livre ela deve ter uma senha;
- Implementar servidor de autenticação LDAP (que faz com que a máquina do domínio possa ter acesso à rede);
- Todos os computadores devem estar com firewalls instalados e anti-vírus licenciados e atualizados, aumentando o nível se segurança.

Dessa forma, pode-se perceber que a empresa teve avanços com a rede sem fio e que suas negociações passaram por uma fase melhor, mesmo notando que ela é uma rede frágil em segurança. Porém, com as medidas de precaução ela é muito bem utilizada, gerando ganhos e avanços tecnológicos.

CONCLUSÃO

A segurança em redes é de suma importância para proteger as informações de uma organização. Desta forma, centrou-se nesta pesquisa, no ponto-chave de que as redes sem fio e redes TCP/IP são mais frágeis e, portanto, devem ter um adicional diante das outras para que seja melhor protegida em termos de qualidade de serviços aos clientes.

Viu-se ainda o que se trata de segurança dos SI, segurança e gestão de segurança, além de pormenorizar as formas com as quais são feitas as redes e seus padrões de comunicação existentes e suas vulnerabilidades encontradas , enfim, analisou-se também os principais detalhes de uma rede sem fio e suas arquiteturas, mostrando a forma de se deixá-la menos vulnerável ao ataque de pessoas más intencionadas.

Por fim, a segurança das redes sem fio e verificando que, apesar de elas não terem sido criadas para substituir totalmente as redes cabeadas, a mobilidade e produtividade gerada pelas redes sem fio é o ponto fundamental para a superação das redes cabeadas que paulatinamente vem acontecendo.

Percebeu-se, neste estudo as questões referentes ao 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, WEP, apresenta diversas falhas. E é em cima dessas falhas encontradas no WEP, que ele não oferece segurança adequada, sendo substituído por outros padrões mais eficientes como o TKIP e WPA e o WPA Enterprise que é mais recomendável para ambientes corporativos devido utilizar o padrão 802.i que exige a utilização de um servidor Radius para autenticação e monitoramento de seus usuários.

Os métodos invasão comentados nesta pesquisa são os mais freqüentemente utilizados por indivíduos maliciosos que procuram, de qualquer forma, explorar as fragilidades das redes sem fio, o que se tenta reverter através de muitos estudos e de práticas condizentes com esta realidade.

Viu-se ainda que existem várias opções de melhoria da segurança em redes wireless desde pequenas mudanças no protocolo de criptografia, utilização de firewalls até a utilização se redes virtuais privadas (VPNs) que trabalham com túneis de informação criptografados e soluções mais robustas como servidores de autenticação.

Assim, pode-se realizar uma segurança nas redes sem fio através de estudos e acompanhamento da rede desde sua idealização até o momento em que a mesma está sendo trabalhada, sempre buscando novas possibilidades de melhorias para elas.

REFERÊNCIAS

BORISOV, N. ***Intercepting móbile communications***: tha insecurity of 802.11. 2001.

CARVALHO FILHO, João Rogério Lima de. **Um estudo de protocolos empregados na segurança de dados em redes sem fio padrão 802.11**. Monografia do curso de Ciências da Computação. João Pessoa: UNIPE, 2005.

ENGST, Adam; FLEISHMAN, Glenn. **Kit do iniciante em redes sem fio**. 2. ed. Rio de Janeiro: Markon Books, 2005.

FERNANDES, Nelson Luiz Leal. **Voz sobre IP**: uma visa geral. Artigo científico. São Paulo: EDUSP, 2002.

FRANCISCATTI, Vagner. **Segurança e redes sem fio**. Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados. Londrina: UEL, 2005.

LAUDON, Kenneth C; LAUDON, Jane P.. **Sistemas de informação gerenciais**: administrando a empresa digital. 5. ed. São Paulo: Prentice Hall, 2004.

LEITÃO, Hugo Ferreira. **Introdução à segurança da informação**. São Paulo: FocoSecurity, 2005.

LONGO, Gustavo D.. **Segurança da informação**. Artigo científico. Bauru: UEP, 2005.

MARQUES, Alexandre Fernandez**. Segurança em rede IP**. Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados. Londrina: ASIT, 2001.

MARTINI, Renato. **Curso de segurança e redes linux**. São Paulo: CIPSGA, 2000.

PAPERT, Seymour. **A máquina das crianças**: repensando a escola na era da informática. Porto Alegre: Artes Médicas, 1994.

PEREIRA, Cristiane. **Atividades de gestão e segurança da informação**. Artigo científico. Brasília: UNB, 2004.

QUEIROZ, Daniel Cruz de. **Voz sobre IP em rede corporativa**. Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados. Londrina: ASIT, 2001.

ROSINI; Alessandro Marco; PALMISANO, Ângelo. **Administração de sistemas de informação e a gestão do conhecimento**. São Paulo: Pioneira, 2003.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio**. 2. ed. São Paulo: Novatec, 2005.

SANTOS, Ricardo Luiz dos. **Segurança em redes sem fio**: wlans. Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados. Londrina: UEL, 2003.

SILVA, Pedro Tavares et all. **Segurança em sistemas de informação**: gestão estratégica da segurança da empresa real. Portugal: Centro Atlântico, 2003.

SINKOÇ, Luiz Henrique. **Segurança em redes sem fio**. Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados. Londrina: UEL, 2005.

TORRES, Gabriel. **Redes de computadores**: curso completo. Rio de Janeiro: Axel Books, 2001.

TAJRA, Sanmya Feitosa. **Informática na educação**: professor na atualidade. São Paulo: Érica, 1998.

Gesbert; H. Bölcskei; D. Gore; A. Paulraj; "MIMO Wireless Channels: Capacity and Performance Prediction", Proceedings Global Telecommunications Conference, 2002

Yu, Kai; Ottersten, Björn; "Models For MIMO Propagation Channels, A Review Summary", Wiely Journal on Wireless Communications and Mobile Computing, July 2002

TERADA, Routo. **Segurança de Dados: Criptografia em Redes de Computador**.

O LIVRO DO WI-FI **- Instale, configure e use redes wireless Cobertura em Windows, Macintosh, Linux, Unix e PDA's, John Ross, Alta Books**

STOHLER, Paulo. **Criptografia: Conceitos Básicos.** Segunda Parte Future, Technologies**,** fevereiro. 2002.