UNIVERSIDADE FEDERAL DO PARÁ
CURSO DE SISTEMAS DE INFORMAÇÃO
Campus Marabá

Segurança em redes locais sem fio: um estudo de caso em Marabá

Nádria Marques Ferreira
Paula de Souza Faustino

Trabalho de Conclusão de Curso, apresentado à Universidade Federal do Pará, como parte dos requisitos necessários para obtenção do Título de Bacharel em Sistemas de Informação.

Orientadora: *Prof. Jasmine Araújo, Msc.*

Co-orientadora: *Prof. Joelma Almeida, Esp.*

MARABÁ

2007

Ficha Catalográfica

FAUSTINO, Paula de Souza e FERREIRA, Nádria Marques. Segurança em redes locais sem fio: um estudo de caso em Marabá. Marabá: UFPA, 2007. 41p. (Trabalho de Conclusão de Curso apresentado como parte dos requisitos necessários para obtenção do Título de Bacharel em Sistemas de Informação da Universidade Federal do Pará).

<u>Palavras-Chaves</u>:Redes locais sem fio,Vulnerabilidade, Segurança.

AGRADECIMENTOS

Paula de Souza Faustino;

Agradeço a Deus por estar sempre abençoando a minha vida. A minha mãe Geuslene pelo grande esforço e amor por mim. A minha irmã Bruna pelo amor e apoio. A meu namorado Jadson pelo carinho e companheirismo. A minha tia Lúcia pelo apoio. Aos meus amigos Esmeraldo e Helena pelo apoio. Ao Prof. Ivaldo Ohana pelo empenho em trazer o curso de Sistemas de Informação para Marabá. A minha orientadora Profª. Jasmine Araujo pela dedicação e grande apoio na realização deste trabalho. A minha amiga e colega de TCC Nádria pela dedicação na realização deste trabalho e outros os quais fizemos juntas durante o curso. Em memória da minha amiga de infância Kamila e da minha avó Maria.

AGRADECIMENTOS

Nádria Marques Ferreira;

Agradeço ao meu Deus e Pai, pois minha vida vem d'Ele, tudo o que tenho, tudo o que sou e o que vier a ser é para Ele. Aos meus pais Neuza e Dionel, pelo esforço, amor e dedicação, ao meu namorado Adervan pelo apoio e companheirismo, aos meus irmãos Nara, Ádria, Nadriane e Dionel Jr., a minha orientadora Profª. Jasmine Araújo pelo empenho na realização deste trabalho, ao Prof. Ivaldo Ohana pelo esforço em manter o curso de Sistemas de Informação em Marabá, aos meus amigos Janaina e Fernando, Halene, Luciene e Nathália por todo apoio e a minha amiga e parceira de TCC Paula por toda dedicação e apoio durante os quatro anos de curso.

SUMÁRIO

Agradecimentos.....3
Sumário.....5
Resumo.....7
Abstract.....8
1. *INTRODUÇÃO*.....9
   1.1. *Objetivo*.....9
   1.2. *Motivação*.....9
   1.3. *Organização do Trabalho*.....10
2. *PROTOCOLOS DE REDES SEM FIO*.....11
   2.1. *Introdução as Redes Sem Fio20*.....11
   2.2. *Elementos da Rede Sem Fio*.....12
   2.2.1 *Ponto de Acesso (Access Point)*.....12
   2.2.2 *Antenas*.....13
   2.2.3 *Adaptador de Rede*.....13
   2.2.4 *Placa de Rede Wi-Fi*.....14
   2.2.5 *Portal*.....14
   2.3. *Modos de Operação*.....14
   2.3.1 *Modo Ad-Hoc*.....14
   2.3.2 *Modo Infra-Estrutura*.....14
   2.4. *Camadas*.....15
   2.4.1 *Camada Física*.....15
   2.4.2 *Camada de Enlace*.....15
   2.4.3 *Camada de Rede*.....16
   2.4.4 *Camada de Transporte*.....16
   2.5. *Padrões da Indústria*.....16
   2.5.1 *IEEE 802.11a*.....16
   2.5.2 *IEEE 802.11b*.....16
   2.5.3 *IEEE 802.11g*.....17
   2.5.4 *IEEE 802.11d*.....17
   2.5.5 *IEEE 802.11e*.....17
   2.5.6 *IEEE 802.11f*.....17
   2.5.7 *IEEE 802.11h*.....18
   2.6 *Conclusão*.....18
3. *SEGURANÇA EM REDES SEM FIO 802.11*.....19
   3.1. *Ataques às Redes Sem Fio*.....20
   3.1.1 *Associação Maliciosa*.....21
   3.1.2 *ARP Poisoning*.....22
   3.1.3 *MAC Spoofing*.....23
   3.1.4 *Negação de Serviço*.....23
   3.1.5 *Smurf*.....24
   3.1.6 *Wardriving*.....25
   3.1.7 *Warchalking*.....25
   3.2. *Mecanismos de Segurança*.....26
   3.2.1 *WEP (Wired Equivalence Privacy)*.....26
   3.2.2 *Controle do Endereço MAC*.....29
   3.2.3 *802.1X*.....30
   3.2.4 *802.11i*.....32
   3.2.5 *WPA (Wi-Fi Protected Access)*.....33

3.2.6 Firewall..... 34
3.2.7 VPN..... 35
3.2.8 Site-Survey..... 36
3.2.9 SSID (Service Set Identifier)..... 36
3.3 Conclusão..... 37
4. ESTUDO DE CASO..... 38
4.1. Procedimento de Pesquisa de Campo..... 38
4.1.1 Inspeção e Sondagem..... 38
4.1.2 Sondagem Ativa e Passiva..... 39
4.2. Região Pesquisada e Metodologia Aplicada..... 39
4.3 Ambiente da Pesquisa de Campo..... 40
4.4 Resultados..... 41
4.5 Conclusão..... 42
5. CONCLUSÃO..... 43
REFERÊNCIAS BIBLIOGRÁFICAS..... 44

Resumo

Este trabalho apresenta o conceito de redes sem fio, seus protocolos, os elementos que compõe essas redes, modos de operação, camadas e padrões da indústria. É feito um estudo sobre segurança em redes sem fio 802.11, onde são abordadas suas vulnerabilidades, apresentando tipos de ataques e seus mecanismos de segurança. Finalmente, um estudo de caso na cidade de Marabá é realizado, evidenciando a necessidade da melhoria e obtenção de meios de segurança em redes locais sem fio.

Palavras-chave: ***Redes locais sem fio, Vulnerabilidade, Segurança.***

Abstract

This work presents the concept of Wireless Lan Networks (WLANs). The protocols, including its components elements, operation modes, layers and industry's standards. The main focus is wireless security in 802.11, where their vulnerabilities are approached, presenting types of attacks and their security mechanisms. Finally, a case study in the Marabá city is accomplished, evidencing the need of the improvement and obtaining of security solutions in WLANs.

Keywords: ***Wireless Local Network, Vulnerability, Security.***

CAPÍTULO I

1. INTRODUÇÃO

1.1 Objetivo

As redes de computadores *wireless* são redes sem fio. Elas permitem que diversas estações se comuniquem sem a necessidade de cabos, através de ondas eletromagnéticas. Esta tecnologia vem crescendo amplamente devido a facilidade de configuração, redução de custo, mobilidade, maior produtividade dos usuários e boa conectividade, dentre outros benefícios.

Como em toda rede de computadores, em *wireless* também é importante zelar pela segurança das informações em maior ou menor nível de acordo com a necessidade de cada usuário. Por exemplo, em instituições governamentais que trabalham com documentos importantes e sigilosos precisam de total segurança na transferência destes por meio da rede.

O objetivo deste trabalho é analisar os mecanismos de segurança das redes locais sem fio, conhecidas também como WLAN (*Wireless Local Area Network*), identificando as vulnerabilidades. Serão apresentados os protocolos de segurança WPA (*Wi-Fi Protected Access*), WEP (*Wireless Equivalence Privacy*) assim como as diversas técnicas que podem ser utilizadas para aumentar a segurança e em especial, o padrão IEEE 802.11i, cuja a proposta é nova.

Busca-se, também, fazer um estudo de caso para identificar as falhas de segurança e o grau de comprometimento atingido por cada uma delas dentro da infra-estrutura das redes identificadas no estudo de caso.

1.2 Motivação

As redes *wireless* apresentam problemas quanto a vulnerabilidades e riscos de segurança, isso se deve principalmente por utilizarem sinais de rádio com um conjunto de características bem definidas, de maneira que possibilita a monitoração destes sinais e a leitura de dados neles contidos.

O uso de redes sem fio vem crescendo e à medida desse crescimento as invasões às redes. Em recente pesquisa divulgada pela consultoria mi2g *Intelligence

Unit, o Brasil é responsável por sete dos dez mais ativos grupos responsáveis pos invasão a sites, além de possuir oito entre dez hackers considerados mais perigosos em todo o mundo. Em conseqüência, procedimentos devem ser adotados a fim de solucionar os problemas decorrentes dos ataques às redes.

O IEEE (Institute of Eletrical and Eletronic Engineers) criado em 1884, nos Estados Unidos, é uma sociedade técnico-profissional internacional, dedicada ao avanço da teoria e prática da engenharia nos campos da eletricidade, eletrônica e computação (www.ieee.org).

Com o objetivo de elaborar padrões para redes locais de computadores, foi criado o projeto IEEE 802 que ficou a cargo de um comitê instituído em fevereiro de 1980.

Para elaborar um padrão para redes sem fio (wireless LANs), em 1997 o IEEE constituiu o "Wireless Local- Area Networks Standard Working Group, IEEE Project 802.11". O objetivo desse projeto é definir um nível físico para redes onde as transmissões são realizadas na freqüência de rádio ou infravermelho, e um protocolo de controle de acesso ao meio, o DFW MAC (Distributed Foundation Wireless MAC) (SOARES,1995).

O comitê de padrões IEEE 802.11 passou a discutir a questão da segurança devido os ataques bem sucedidos às redes wireless, definindo assim um novo padrão capaz de lidar com problemas de segurança, denominado 802.11i.

1.3 Organização do Trabalho

Este trabalho está organizado da seguinte forma: o primeiro capítulo faz uma breve introdução às redes sem fio e o objetivo deste trabalho; o segundo capítulo descreve o conceito de redes wireless e seus protocolos, um breve histórico, modos de operação e elementos da rede sem fio e os padrões da indústria; o terceiro capítulo apresenta os principais tipos de ataques às redes sem fio e mecanismos de segurança; no quarto capítulo é descrito um estudo de caso em um trecho da cidade de Marabá, onde foram identificadas redes locais sem fio e finalmente, no quinto capítulo, apresentamos as conclusões.

CAPÍTULO II

2. PROTOCOLOS DE REDES SEM FIO

2.1 Introdução as Redes Sem Fio

O uso de rede de computadores tem como finalidade possibilitar a comunicação entre máquinas localizadas em lugares distintos, podendo ser realizada com o uso de cabos, wired, ou sem, neste caso wireless. Existem várias tecnologias que permitem esta comunicação, porém a que mais tem tido destaque nos últimos anos é a Wi-Fi (Wireless Fidelity), denominação comercial dada a um conjunto de padrões de rede wireless, desenvolvidos pelo comitê 802.11 do IEEE. Atualmente, os computadores portáteis já vêm equipados com esta tecnologia.

As redes locais sem fio, ou WLAN's (Wireless Local Área Network) tiveram seu desenvolvimento proporcionado pelo uso de tecnologias como infravermelho e rádio spread spectrum (espectro de dispersão). No início dos anos 90, algumas empresas passaram a oferecer redes sem fio utilizando espectro de dispersão.

Assim, as primeiras WLAN's eram lentas, caras, utilizavam tecnologias proprietárias, além dos diversos tipos de interferências e alguns problemas que também podem ser encontrados atualmente, como os sinais de rádio que podem ser refletidos; o computador pode perder o sinal se o ponto de acesso for muito afastado; incompatibilidade e gerenciamento do espectro de freqüência, dentre outros.

Em 1997, o IEEE divulgou um padrão específico para WLAN's, chamado 802.11, o que acarretou em grande melhoria da tecnologia, viabilizando a interoperabilidade entre os diversos fabricantes que passaram a adotá-lo. Durante o processo de aperfeiçoamento, houve uma divisão de opiniões, que culminou no prosseguimento de dois padrões independentes: o 802.11a e o 802.11b.

Hoje, as dificuldades técnicas de incompatibilidade e mobilidade vêm sendo resolvidas através de cartões e adaptadores de rede nas placas mães dos notebooks. Por outro lado, existem as dificuldades relacionadas à segurança que o IEEE está respondendo com novos padrões que lidam com problemas de segurança chamados de 802.11i (ROSS, 2003).

2.2 Elementos da Rede Sem Fio

2.2.1 Ponto de Acesso (Access Point)

O ponto de acesso, ou simplesmente AP, pode ser considerado o dispositivo de maior funcionalidade em uma rede sem fio. Ele é responsável pela distribuição de sinais e centralização da rede e assim, as conexões de uma WLAN dependem da potência do sinal gerado por este dispositivo.

O AP também serve de ponte entre uma rede cabeada e uma rede sem fio, pois pode transformar o tráfego da rede cabeada em sinal de rádio, além de prover as funções de um roteador. Os pontos de acesso podem ser classificados em AP *indoor* e AP *outdoor*.

O AP *indoor* é apropriado para lugares fechados ou situações que não precisem de muita potência de sinal, pois o raio de alcance do sinal em ambientes com campo de visada é cerca de 100m e em ambientes com obstáculos de aproximadamente 30m. No entanto, alguns AP *indoor* suportam duas antenas possibilitando uma maior potência de sinal que normalmente vai de 16dBm a 18dBm.

O AP *outdoor* caracteriza-se por ter maior potência de sinal que o AP *indoor*, vai de 19dBm a 28dBm, tendo um alcance de até 20 km com uma antena direcional e 5 km com uma antena do tipo *omni* para o padrão *wi-fi* 802.11b. Para o 802.11g o alcance é cerca de 60% menor, sendo que seus dispositivos podem vir configurados para detectar automaticamente o padrão que devem trabalhar, 802.11b ou 802.11g.

Para o padrão 802.11a, que atua com freqüência de 5GHz, os APs tem *menos* chances de sofrer interferência do aqueles que usam a faixa de 2,4GHz. Dessa forma, proporcionam melhor qualidade de sinal, porém são mais caros.

Encontra-se, no mercado, com maior facilidade e com preços mais baixos o APs do tipo *indoor*, por isso, muitas empresas o utilizam para comunicação entre prédios usando antenas direcionais para aumentar a potência de sinal, no entanto, esta prática não é recomendável porque apresenta maior vulnerabilidade a problemas, como instabilidade do sinal e menor velocidade na transmissão dos dados.

2.2.2 Antenas

São elementos passivos, que transmitem e recebem os sinais, além de poder aumentar a potência de um gerador de sinal. Dessa forma, uma antena de qualidade pode proporcionar menos custos ao permitir que um número reduzido de APs atendam a uma mesma área.

A antena deve ser posicionada em um local distante de materiais sólidos que dificultam a propagação do sinal e de preferência em lugares altos, em posições que permitam o campo de visada e não apresentem entre si aparelhos eletrônicos causadores de ruídos, por exemplo, fornos.

Existem dois tipos, antenas omni e antenas direcionais. As antenas omni são recomendadas para ambientes indoor e em sua utilização não é necessária muita atenção quanto à direção em que estão os dispositivos, pois transmitem sinais em um ângulo de 360° na horizontal e 3° a 30° na vertical. Em locais fechados este tipo de antena proporciona ganho de sinal, podendo estar ligadas a APs e a placas PCI Wi-Fi.

As antenas direcionais são mais usadas em ambientes outdoor, para a ligação de pontos distantes. São apropriadas para situações em que se pretende transmitir dados a uma região específica ao alcance de uma angulação entre 30° e 180° na horizontal e 3° a 30° na vertical (MATOS, 2005).

2.2.3 Adaptador de Rede

Este dispositivo contém um transmissor de rádio que transmite dados do computador ou do ponto de acesso para rede e um receptor que recebe dados da rede contidos nos sinais de rádio e os envia ao destinatário.

Os adaptadores de rede convertem os dados digitais para sinais de rádio que são enviados a outros dispositivos na rede, e convertem os sinais de rádio recebidos dos outros elementos da rede em dados digitais (ROSS, 2003).

São, geralmente, PC Card (Personal Computer Memory Card International Association) com antena integrada desenhada para ocupar um slot de expansão do equipamento.

2.2.4 Placa de Rede Wi-Fi

A placa de rede Wi-Fi é indispensável a todo dispositivo que pretenda se conectar a uma rede Wi-Fi. Podendo ser uma placa interna de barramento PCI, uma placa externa ESB, um cartão PCMCIA wireless, um dispositivo wireless já acoplado na placa-mãe ou até um AP que opere como uma placa de rede wireless.

2.2.5 Portal

Portal é um elemento que torna possível a conexão entre redes do tipo 802.11x e outras redes 802, pois ele traduz os quadros de informações das redes sem fio para quadros de informações específicos para outras redes e quadros no formato de outras redes para o padrão 802.11.

2.3 Modos de Operação

Os modos de operação descrevem como é feita a comunicação na arquitetura 802.11x que integra os padrões 802.11b, 802.11a, 802.11g, podendo ser realizados de duas maneiras descritos a seguir.

2.3.1 Modo Ad-Hoc

Neste modo, a comunicação é feita sem a utilização de um AP e para isso, as placas das máquinas devem estar configuradas para operar no modo Ad-Hoc e devem estar dentro da zona de alcance do sinal uma da outra de acordo com IBSS (Independent Basic Service Set).

As placas de rede sem fio são menos potentes que as antenas dos Pontos de Acesso, embora tenham a mesma velocidade de transmissão. Por este motivo o modo Ad-hoc é mais apropriado para ambientes domésticos que tenham no máximo cinco computadores interconectados.

2.3.2 Modo Infra-Estrutura

O modo infra-estrutura utiliza pontos de acesso para comunicação entre os dispositivos wireless. A área de cobertura de um ponto de acesso chama-se BSS (Basic Service Set). Vários BSSs constituem um ESS (Extend Service Set). Os

dispositivos que se comunicam por um ou mais BSSs dentro de uma BSA (Basic Service Area) são denominados STA (Wireless LAN Stations).

Para haver a comunicação dentro de um ESS, os STAs devem estar configurados com o identificador ESSID ou SSID (Identificador ESS). Geralmente, os pontos de acesso se conectam através de um cabo UTP[1]. Para uma conexão sem fios entre os pontos de acesso, pode-se utilizar o sistema WDS (Wireless Distribution System).

2.4 Camadas

Todas as atividades especificadas pelo padrão 802.11 acontecem nas camadas física (PHY) e de enlace (na subcamada MAC, especificamente), pois as camadas superiores controlam aspectos como endereçamento e roteamento, integridade de dados, sintaxe e formato dos dados contidos dentro de cada pacote, não fazendo diferença se elas estão transportando pacotes através de fios, de fibra óptica ou de sinais de rádio.

2.4.1 Camada Física

Esta camada é responsável pelo envio dos quadros de dados pelo meio de transmissão e pelas especificações mecânicas e elétricas.

O padrão IEEE 802.11 determina três técnicas de transmissão para as redes sem fio: o IrDA (Infrared - infravermelho), o FHSS (Frequency Hopping Spread Spectrum) e o DSSS (Direct Sequence Spread Spectrum). Em 1999, foram apresentadas duas novas técnicas para alcançar maior largura de banda: o OFDM (Orthogonal Frequency Division Multiplexing) e o HR-DSSS (High RateDirect Sequence Spread Spectrum).

2.4.2 Camada de Enlace

Esta camada é responsável por entregar as unidades de dados (grupos de bits) de uma estação até a outra sem erros, recebendo dados da camada de rede e adicionando os cabeçalhos necessários para que o frame possa ser enviado para o próximo dispositivo do trajeto entre emissor e receptor (DUARTE, 2003).

[1] *UTP: Cabo de par trançado não-blindado que tem por padrão quatro pares de fios.*

O protocolo 802.11x define duas subcamadas para camada de enlace: LLC (Logical Link Control) e MAC (Media Access Control). A subcamada MAC define a forma de como o canal é alocado, isto é, quem terá a oportunidade de transmitir em seguida, compatível com o padrão Ethernet.

2.4.3 Camada de Rede

Esta camada é responsável pela entrega de datagramas através de vários links da rede, garantindo que cada datagrama saia de seu host de origem para o seu host de destino de forma eficiente.

2.4.4 Camada de Transporte

Esta camada tem o encargo de entregar a mensagem completa de um host de origem a um host de destino, além de ser responsável pelo estabelecimento, gerenciamento e sincronismo das conexões entre host origem e host destino.

2.5 Padrões da Indústria

2.5.1 IEEE 802.11a

O padrão IEEE 802.11a atua com uma banda de freqüência de 5 GHz e utiliza o método de modulação OFDM (Orthogonal Frequency Division Multiplexing). O 802.11a é cinco vezes mais rápido do que o padrão 802.11b, opera com alto desempenho, sendo a taxa máxima de transferência de 54 Mbps. No entanto, esse padrão não apresenta compatibilidade com o padrão 802.11b.

2.5.2 IEEE 802.11b

O padrão IEEE 802.11b é tecnologicamente e financeiramente o mais viável para pequenas empresas, hospitais e chão de fábrica, portanto o mais popular. Também aplicado nas universidades para proporcionar conectividade em salas de conferências, áreas de trabalhos e ambientes inconvenientes ou perigosos para se instalar cabos ou que tenha a necessidade de mobilidade.

O 802.11b opera com uma banda de 2,4 GHz e utiliza taxas de transferência de até 11 Mbps. Os canais de rádio freqüência usam a modulação DSSS (Direct Sequence Spread Spectrum), permitido altas taxas de velocidade em distâncias de até 50 metros em escritórios.

2.5.3 IEEE 802.11g

O padrão IEEE 802.11g prevê a especificação da subcamada MAC ((Media Access Control) e da camada física. A camada física é uma extensão do IEEE 802.11b, com uma taxa de transmissão de 54 Mbps. Apesar de utilizar a banda de 2.4 GHz, semelhante ao padrão 802.11a, utiliza a modulação OFDM. Sua especificação é compatível com a 802.11b. Através de um protocolo estendido, o 802.11g aceita o uso misto da rede, permitindo que equipamentos que usam o 802.11b, operando em 11 Mbps, possam compartilhar a mesma rede com os novos equipamentos operando a 54 Mbps, o que admite tanto a interoperabilidade entre os dois padrões quanto a migração das redes de 11 para 54 Mbps.

2.5.4 IEEE 802.11d

O padrão IEEE 802.11d possui um frame estendido que inclui campos com informações, parâmetros de freqüência e tabelas com parâmetros de cada país. O 802.11d foi desenvolvido para áreas fora dos chamados cinco grandes domínios (EUA, Canadá, Europa, Japão e Austrália).

2.5.5 IEEE 802.11e

O Task Group, criado para desenvolver o padrão IEEE 802.11e, primeiramente tinha como meta desenvolver os aspectos de segurança e QoS para a subcamada MAC. No entanto, as questões de segurança foram atribuídas ao Task Group 802.11i e o 802.11e ficou encarregado por desenvolver os aspectos de QoS, o qual deverá ser adicionado às redes sem fio para o suporte de voz, vídeo e dados.

2.5.6 IEEE 802.11f

O padrão IEEE 802.11f determina os princípios básicos da arquitetura da rede, especifica a subcamada MAC e a camada física para as redes sem fio, incluindo os conceitos de pontos de acesso e de sistemas distribuídos. O 802.11f define recomendações que descrevem os serviços dos pontos de acesso, as primitivas, o conjunto de funções e os protocolos que deverão ser compartilhados pelos múltiplos fornecedores para operarem em rede.

2.5.7 IEEE 802.11h

O padrão 802.11h acrescenta uma função de seleção dinâmica de freqüência DFS (Dynamic Frequency Selection) e um controle de potência de transmissão TPC (Transmit Power Control) para o padrão 802.11a. Esse padrão, assim como o 802.11a, utiliza uma banda de 5 GHz, empregada na Europa em radares e satélites. Entretanto, esta medida evita interferências com radares e satélites, protegendo as redes militares e de satélites que compartilham esta banda.

2.6 Conclusão

Este capítulo apresentou uma breve introdução aos principais conceitos de redes sem fio, os elementos que as compõem, os conceitos de camadas de rede e as principais características dos padrões da indústria lançados IEEE 802.11.

Estes conceitos são importantes para a compreensão dos próximos capítulos, pois formam a base para o entendimento das formas de ataques, mecanismos de segurança e por fim do estudo de caso realizado.

CAPÍTULO III

3. SEGURANÇA EM REDES SEM FIO 802.11

As redes sem fio tornam-se cada vez mais comuns, por oferecerem praticidade na instalação, mobilidade, boa conectividade, dentre outras vantagens. Por outro lado, o uso crescente das redes sem fio vem enfrentando problemas referentes à segurança das informações e da infra-estrutura das redes, pois as invasões são cada vez mais freqüentes. Nesse sentido, os serviços básicos de segurança para redes wireless são os seguintes:

***Autenticação** – Esta primeira característica tenta assegurar que somente clientes pertencentes à rede poderão acessar a mesma, ou seja, ela verifica a identidade do cliente e avalia se esta estação cliente poderá ou não acessar a rede.*

***Privacidade** – Este serviço pretende assegurar a privacidade dos dados disponíveis na rede, isto é, ele avalia se os dados poderão ser vistos por clientes que tiverem autorização.*

***Integridade** – Um outro quesito presente no protocolo WEP promete garantir que os dados que sejam transmitidos não sejam modificados no caminho de ida e volta entre os clientes e os APs.*

***Disponibilidade e controle de acesso** – Este aspecto permite que a comunicação possa ser feita sem que intrusos impossibilitem que a infra-estrutura seja utilizada por usuários legítimos. A noção de controle de acesso refere-se a realização dos acessos de maneira bem definida aos usuários apropriados.*

Além da comunicação, a segurança em rede também envolve a detecção de falhas em comunicações seguras e ataques à infra-estrutura e reação a esses ataques. Assim, a segurança na rede é conseguida através de um ciclo contínuo de proteção, detecção e reação.

Um intruso passivo pode monitorar – ouvir e gravar mensagens e dados no canal - e modificar, inserir ou eliminar o conteúdo de mensagens, tais capacidades permitem a um invasor montar uma variedade de ataques à segurança.

Assegurar que os pacotes de invasores não entrem na rede é uma forma de garantir que estes não causem danos a rede. Um firewall é um servidor de proxy que filtra todos os dados que passam através dele, em ambos os sentidos, com base em um

conjunto de regras estabelecidas por um gerente da rede, ou seja, regula quais pacotes podem passar para dentro e para fora da rede.

A utilização de criptografia provê confidencialidade, autenticação, integridade de mensagens, não-repudiação de controle de acesso, o que a torna essencial para a segurança na rede.

No entanto, os padrões e as soluções atuais não oferecem o nível desejado de segurança, para exemplificar, um catálogo inteiro de ferramentas para violação de criptografia WEP está disponível na internet. Porém, é possível atenuar a vulnerabilidade utilizando protocolos de segurança específicos para os tipos de invasão mais conhecidos.

3.1 Ataques às Redes Sem Fio

As redes wireless utilizam sinais de rádio com um conjunto de características bem definido, de maneira que um invasor poderá interceptar e ler os dados contidos neles, além disso, os limites da abrangência das redes são definidos pelos dispositivos de ponto de acesso AP, podendo variar entre dezenas a centenas de metros. Esses limites são dependentes da potência do dispositivo AP das antenas utilizadas pelas estações que desejam acesso.

O controle de acesso nas redes sem fio se torna mais complexo que em redes cabeadas. Em uma rede sem fio, é impossível a utilização de dispositivos de controle do meio como, por exemplo, comutadores (switches). Em uma rede com fios, é possível excluir uma determinada sala, simplesmente não fornecendo nenhum ponto para acesso à rede, facilitando a inserção de pacotes de pessoas desautorizadas da rede e o conseqüente comprometimento da infra-estrutura da rede e da segurança da informação.

Os tipos de invasão podem ser classificados em passivos e ativos, os quais se subdividem em:

***Invasão Passiva** – o invasor obtém acesso a uma rede, mas não altera o conteúdo dos dados, podendo ser apenas a análise do tráfego da rede.Os exemplos de invasão passiva mostrados neste trabalho são Wardriving e Warchalking. Existem dois tipos de invasão passiva, são eles:*

- Escuta: o invasor monitora a transmissão para obter o conteúdo do que está sendo transmitido.

- Análise do Tráfego: analisa a transmissão para entender os padrões de comunicação.

***Invasão Ativa** – o invasor obtém acesso à rede e altera o conteúdo da mensagem que está sendo transmitida, este tipo de invasão pode ser detectado, mas nem sempre impedido. Uma invasão desta forma necessita que o invasor utilize algum dos recursos (ou a combinação deles) como:*

- Disfarce: o invasor personifica um usuário e com isso obtém alguns recursos sem autorização da rede.

- Repetição: o invasor intercepta a transmissão e envia uma mensagem como se fosse o usuário legítimo.

- Modificação de Mensagem: o invasor altera uma mensagem legítima.

- Negação de Serviço: o invasor dificulta o uso normal ou o gerenciamento dos dispositivos da rede.

Os exemplos de invasão ativa apresentados neste trabalho são Associação Maliciosa, ARP Poisoning, Mac Spoofing, Negação de Serviço e Smurf.

Estes tipos de invasões acarretam riscos contra as WLANs 802.11. As maiores conseqüências incluem: perdas de informações e serviços da rede.

Os principais ataques às redes sem fio são descritos a seguir.

3.1.1 Associação Maliciosa

A associação maliciosa ocorre quando um atacante aparenta ser um ponto de acesso, iludindo outro sistema de forma que este acredite estar se conectando em uma rede sem fio real. Através de um software, como o HostAP, o atacante é capaz de enganar um sistema, mostrando um dispositivo de rede padrão como um ponto de acesso.

A associação maliciosa, é composta de duas máquinas com dispositivos para redes sem fio e segue as seguintes etapas:

1. A vítima envia pacotes, frames de requisição de informações, à procura de ponto de acesso para conexão;

2. O atacante com o auxílio de programas capazes de transformar um dispositivo de rede padrão em um ponto de acesso - softAP - responde a conexão;

3. A vítima requisita a associação e se associa ao atacante;

4. O atacante responde com as informações de rede necessárias como endereço IP;

5. O atacante envia uma requisição de NET USE;

6. A vítima responde com LOGIN;

7. Qualquer vulnerabilidade de qualquer serviço do cliente pode ser agora explorada.

Há uma pequena diferença entre fazer a associação maliciosa utilizando um softAP ou através de redes Ad Hoc. Esta diferença está na propagação dos riscos em se manter um dispositivo configurado para operar em Ad Hoc. Dessa forma vários usuários e até mesmo sistemas operacionais coíbem este tipo de conexão, permitindo apenas conexões em sistemas de infra-estrutura básica ou sistemas infra-estruturados.

3.1.2 ARP Poisoning

O ataque ao protocolo de resolução de endereços (ARP- Address Resolution Protocol) é um ataque de camada de enlace de dados que só pode ser disparado quando um atacante está conectado na mesma rede local que a vítima, restringindo este ataque às redes que se encontram conectadas por hubs, switches e bridges, pois estes trabalham na camada de rede, excluindo as redes conectadas por roteadores e gateways.

Este tipo de ataque utiliza-se de pacotes de ARP reply para fazer o cache poisoning. Um exemplo seria um atacante que envia um pacote de ARP reply para um determinado host X dizendo que o IP de Y aponta para o endereço MAC de X, semelhantemente envia um pacote de ARP reply para Y dizendo que o IP de Z aponta para o endereço MAC de X.

Como o protocolo ARP não guarda os estados, os hosts X e Y assumem que enviaram um pacote de ARP request pedindo estas informações e assumem os pacotes como verdadeiros. Todos os pacotes trocados entre os hosts Y e Z necessariamente passam pelo host X que se encarregam de reenviar os pacotes para os devidos destinos após capturá-los.

3.1.3 MAC Spoofing[2]

Os dispositivos para redes sem fio possuem a característica de consentir a troca do endereço físico. O que possibilita atacantes capturar por meio de técnicas de Eavesdrooping & Espionage um endereço MAC válido de um cliente, trocar seu endereço pelo do cliente e usar a rede.

Um exemplo de ataque utilizando esta técnica foi descrito em (SILVA, 2005). O software Airsnort quebra a chave WEP, o software Netstambler localiza os APs e a captura do MAC feita pelo software Airopeek que coleta tráfego na rede, em modo espião mesmo antes do processo de associação da rede sem fio. Outro software chamado MAC Make foi utilizado para a troca de endereço MAC.

Uma vez associado a obtenção de um endereço IP válido, caso a rede não seja DHCP (Dynamic Host Configuration Protocol) pode ser obtido utilizando um sniffer como Windump ou Ethereal, ambos podem coletar tráfego na rede, revelando as faixas de endereços utilizados, bem como roteadores.

3.1.4 Negação de Serviço

Conhecido como D.o.S. (Denial of Service), essa forma de ataque torna indisponível algum recurso ou serviço da rede. Um invasor pode disparar um ataque de negação de serviço de diversas formas dentro da área de cobertura da rede sem fio.

Os ataques de negativa de serviço são facilitados com a inserção de ruídos emitidos por diversos aparelhos, como por exemplo fornos microondas e telefones sem fio que utilizam a mesma freqüência, 2.4 GHz, das redes do padrão 802.11b/g.

Outra forma de ataque, seria um invasor se passando por um ponto de acesso com o mesmo SSID (Service Set Identifier) e endereço MAC de um outro ponto de acesso válido contagiando a rede com pedidos de dissociação. Estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se reassociarem, enviando as requisições de dissociação em períodos curtos de tempo e, como os clientes não conseguem permanecer conectados por muito tempo, o D.o.S. é efetivado.

---

[2] *Spoofing - É a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema. Esta técnica não é um ataque e sim parte de um, visando dificultar o rastreamento do agressor.*

Outra forma de realizar um ataque de negativa de serviço é inundar a rede com tráfego aleatório.

3.1.5 Smurf

Este tipo de ataque se beneficia do sistema de endereços broadcast de uma rede, através de negação de serviço - Denial of Service. Apesar de ser simples, o efeito de um ataque smurf pode impressionar.

Este ataque tem a intenção de parar uma rede inteira, e não apenas um computador. É efetivado emitindo contínuas cadeias de pacote ICMP alteradas para a rede alvo. Os procedimentos são os seguintes:

1. Uma lista de endereços broadcast de rede é criada por um invasor.

2. Pacotes "spoofados" são enviados com o IP da vítima para cada um desses endereços.

3. Os computadores das redes que receberam os pacotes respondem, enviando mais pacotes para a vítima e não para o computador do atacante.

Posteriormente a divulgação do código do smurf, surgiram novos tipos de smurf, tais como o papasmurf, fraggle e o smurf4. O fraggle é um smurf baseado em UDP.

O invasor envia pacotes UDP "spoofados" e não ICMP para os endereços de broadcast. Os computadores da rede, ao receberem o pacote UDP, respondem à vítima, que envia mais uma resposta, provocando um aumento de tráfego na rede. O smurf4 é apenas uma revisão do smurf.

Conhecido como smurf5, o papasmurf é uma junção dos ataques de broadcast, smurf e fraggle, num só programa.

Essa forma de invasão é utilizada para interromper vários Provedores de Acesso à Internet e seus usuários. Defender-se de um ataque de broadcast é de fato complexo.

Nem sempre firewalls são eficientes para impedir os ataques. Porém, os administradores de rede podem impedir que suas redes sejam empregadas como amplificadores, pois firewalls podem ser utilizados para bloquear a entrada de pacotes ICMP/UDP que tenham destino o endereço de broadcast. Cuidados como desativar serviços que não estão sendo utilizados pelos computadores de rede também pode auxiliar o combate a invasão.

Nos últimos meses, as redes brasileiras cuja configuração de roteadores permitem este tipo de ataque têm sido utilizadas com intensidade cada vez maior, criando prejuízos tanto para as vítimas quanto para as redes amplificadoras (BOFF, 2003).

3.1.6 Wardriving

Sua denominação refere-se à prática de dirigir um automóvel com um computador, uma placa ethernet configurada no modo "promíscuo" e um tipo de antena em busca de redes wireless disponíveis. Portanto, é uma técnica de ataque de vigilância, a qual tem como meta localizar fisicamente os dispositivos de redes sem fio efetuando a interceptação e leitura dos pacotes de comunicação.

Algumas ferramentas encontradas na Internet são empregadas para localizar redes sem fio que estão desprotegidas. Em seguida, pode-se fazer o logon ou conectar-se através dessa rede à Internet, controlando o tráfego da rede e violando suas chaves de criptografia WEP.

3.1.7 Warchalking

Esse método de ataque detecta locais nas vias públicas de onde se pode invadir redes Wi-Fi privadas. Surgiu em Londres quando marcações feitas a giz apareceram pelas ruas da cidade indicando onde era possível conectar-se em redes privadas wireless. Com o auxílio de técnicas de wardriving, o atacante localiza os sinais de redes acessíveis e identifica através da pichação de muros e calçadas com símbolos próprios para mantê-las em segredo. A simbologia, comumente utilizada no warchalking pode ser observada na figura 1:

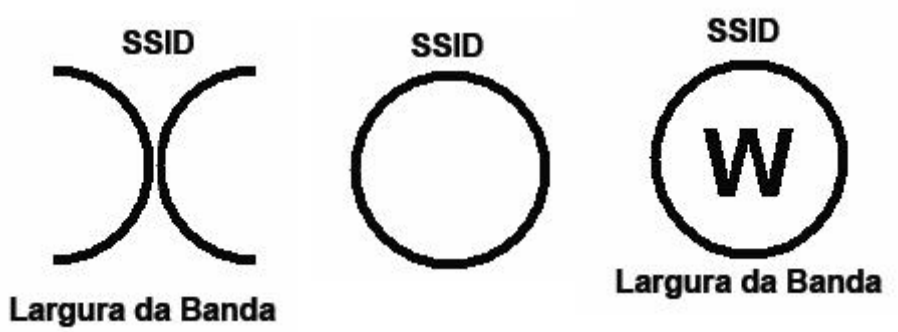

Figura 1: Simbologia utilizada no Warchalking
FONTE: ARAÚJO, 2006

Um par de semi-círculos opostos formando um x significa nó aberto ou link aberto.

Um círculo fechado significa nó fechado.

Um círculo com "W" no centro significa que a conexão está protegida por chave WEP, geralmente indicada no canto superior direito do símbolo.

Abaixo do símbolo deve estar a velocidade do nó e acima o nome do SSID/Hotspot.

O grupo Warchalking BR possui um site descrevendo suas experiências na cidade de São Paulo.

3.2 Mecanismos de Segurança

Por utilizar sinais de rádio como meio de transmissão, as redes wireless apresentam maior vulnerabilidade que as redes cabeadas, de forma que alguém que se dedique poderá interceptar, ler e até mesmo alterar os dados nelas contidos. Portanto, a utilização de mecanismos de segurança em uma rede local sem fio é essencial para garantir a proteção lógica e física dos recursos computacionais e das informações presentes nos computadores ligados à rede.

A questão da segurança em redes wireless vem sendo muito divulgada, portanto a maior parte das redes já utiliza algum tipo de proteção, seja ativando o WEP ou WPA, seja bloqueando os micros que podem se conectar ao ponto de acesso com base no endereço MAC. A seguir serão descritos os principais mecanismos de segurança que podem ser adotados para proteger as redes wireless.

3.2.1 WEP (Wired Equivalence Privacy)

É utilizado para criptografar os pacotes de dados que trafegam nas redes wireless. É fundamentado no algoritmo RC4 desenvolvido por Ronald Rivest em 1987 e publicado na Internet em 2001, o qual criptografa os dados à medida que eles são enviados, é portanto um algoritmo de fluxo.

A criptografia WEP consiste na escolha de uma chave secreta compartilhada entre o ponto de acesso e cada estação da rede na camada de enlace, sendo que a distribuição dessa chave é realizada manualmente por não haver um padrão específico.

A chave de acesso (ou chave secreta) é acoplada ou concatenada a um vetor de inicialização, cujo resultado é utilizado como entrada para o algoritmo gerador de números pseudo-aleatórios, o PRNG (Pseudo Random Number Generator), definido pelo RC4. O PRNG cria uma seqüência de bits do mesmo tamanho que a mensagem a ser criptografada chamada, ou seja, o frame MAC. Em seguida é feito um XOR (OU exclusivo) entre a seqüência de bits e o frame o qual é transmitido com o vetor para que o receptor possa decodificar. Um esquema desse protocolo pode ser melhor analisado na Figura 2.

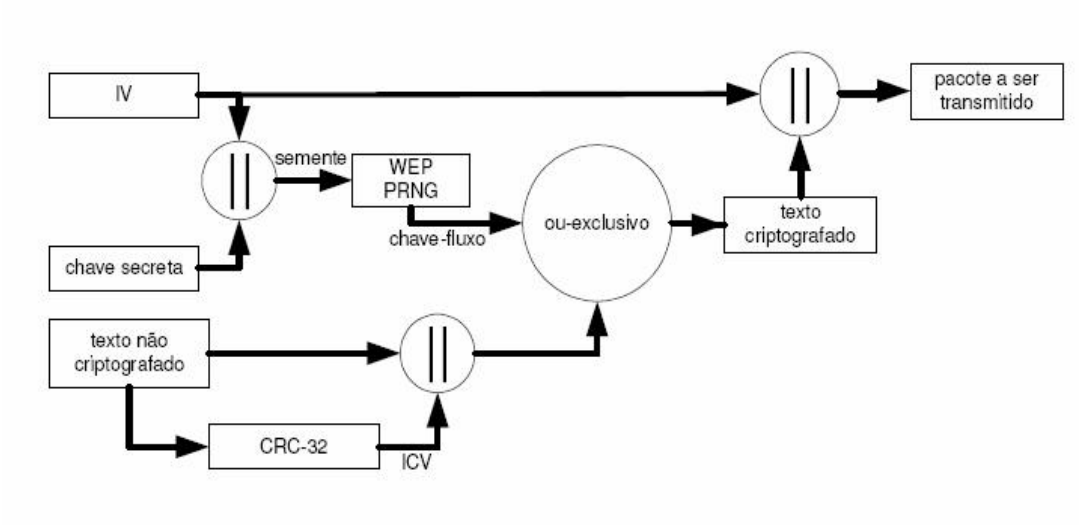

Figura 2: Esquema de Protocolo WEP
FONTE: SILVA, 2005

O receptor, além do texto criptografado, receberá o vetor de inicialização que trafega de forma não criptografada pela rede e desta forma, basta realizar o processo inverso para decriptografia e verificação dos dados recebidos, este processo é ilustrado na Figura 3. (SILVA, 2005).

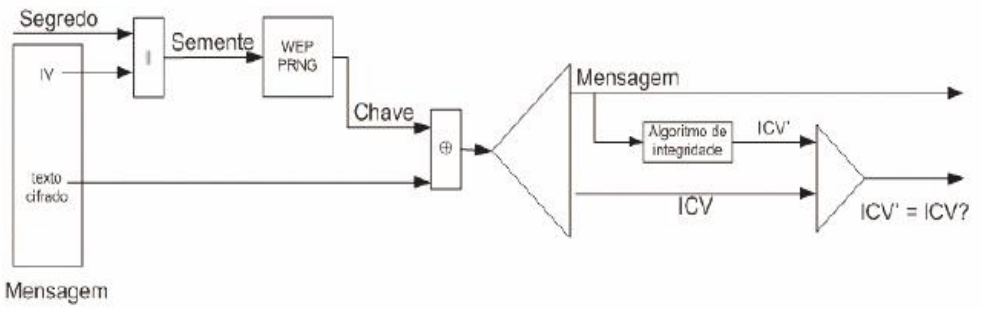

Figura 3: Decifragem
FONTE: PERES; WEBER, 2005

Para proteger a chave secreta utilizada no processo de criptografia, o WEP usa um vetor de 24 bits o qual é gerado e concatenado à chave secreta sempre que um

frame é transmitido, o que resulta na formação de uma nova chave a cada frame enviado. No entanto, o processo de criptografia será mais seguro quanto maior o tamanho da chave criptográfica.

Dessa forma o WEP atende aos seguintes requisitos básicos de segurança em redes:

a) Integridade

A integridade tem como finalidade assegurar que a mensagem enviada não sofra nenhum tipo de alteração durante a transmissão. Para isso, o padrão IEEE 802.11b utiliza a técnica do CRC (Cyclic Redundancy Check) ou seqüência de checagem de quadro, que consiste em um cálculo realizado sobre cada quadro enviado e inserido no final de cada pacote. Ao ser recebida, a mensagem é decriptografada e o CRC é então recalculado e comparado ao CRC da mensagem original. Se os CRCs calculados forem diferentes, significa que a mensagem foi violada e o receptor irá descartá-la.

b) Autenticidade

A autenticidade refere-se a identificação de quem está acessando a rede e pode ser realizada basicamente por três formas: Sistema aberto, Sistema Fechado e o método de Chave Compartilhada.

O Sistema Aberto de autenticação não utiliza criptografia e funciona da seguinte maneira: consiste somente em identificar cada ponto de acesso por meio de seu SSID e um usuário pode ser autenticado mesmo que responda com uma string vazia para o SSID (NULL Authentication), o que representa um ponto vulnerável. O Sistema Fechado de autenticação se difere por exigir que o cliente responda com o SSID válido.

O método de Chave Compartilhada faz uso de chaves WEP pré-compartilhadas para a autenticação. Baseando-se na técnica de challenge-response, o ponto de acesso gera um número aleatório (challenge) e transmite a estação cliente que, através de sua chave WEP, deverá enviá-lo devidamente criptografado (response).

c) Privacidade

Este requisito protege as informações de usuários desautorizados. Para isto esta técnica de criptografia WEP cria uma pseudo-seqüência de números aleatória impedindo a descoberta dos mesmos durante a transmissão. O WEP é empregado em todo o tráfego da rede para proteger o TCP/IP (Transmission Control Protocol /

Internet Protocol), IPX (*Internet Packet Exchange*), HTTP (*Hyper Text Transfer Protocol*).

d) Vulnerabilidades

O WEP é muito utilizado para garantir a proteção de redes sem fio, porém seu método de criptografia não é totalmente seguro. Um de seus principais pontos vulneráveis refere-se à reutilização do vetor de inicialização (IV). Geralmente o vetor inicia com o valor zero e é aumentado em um sempre que um pacote é transmitido. São percebidas duas falhas neste mecanismo: a primeira é que, em um determinado instante, o IV repetirá um valor; a segunda está no fato de que os usuários, freqüentemente, removem e reinserem os adaptadores de redes sem fio em seus computadores, o que faz o vetor de inicialização receber novamente o valor 0, acarretando em pacotes com IV de valores baixos.

A utilização do algoritmo CRC-32 para garantir a integridade dos pacotes também representa um aspecto vulnerável. Por ser linear ele possibilita que alterações sejam feitas sem serem detectadas, bastando conhecer a string de valores pseudo-aleatórias.

O gerenciamento das chaves de criptografia deve ser realizado constantemente, pois as chaves WEP que dificilmente são alteradas, possuem o valor padrão ou são chaves fracas, baseadas em valor trivial como, por exemplo, apenas zeros ou uns representam pontos vulneráveis em uma WLAN. Há, porém, a dificuldade de trocar a chave WEP periodicamente em ambientes grandes, pois dependendo da quantidade de APs torna-se um processo complicado de realizar.

Pesquisadores da AT & T e Rice University (SILVA, 2005) juntamente com os desenvolvedores do AirSnort implementaram o algoritmo que consegue decifrar a chave após a coleta de pacotes. Assim surgiu o AirSnort. Baseado no mesmo algoritmo, tempos depois, foi desenvolvida outra ferramenta com o mesmo objetivo: o WEPCRACK.

3.2.2 Controle do Endereço MAC

O endereço MAC é muito utilizado para garantir a autenticação dos usuários, identificando de forma exclusiva uma placa de rede e desse modo, evita que dispositivos que não possuam o endereço na listagem, que contem todos os endereços MAC válidos nos pontos de acesso, se associem ao ponto de acesso. Essa forma de associação recebe o nome de Sistema Aberto.

a) Vulnerabilidades

No entanto, o controle do endereço MAC não garante a completa segurança nas redes Wireless, uma vez que um invasor que observar o tráfego da rede e encontrar um usuário válido é capaz de adulterar o endereço MAC das placas de redes e clonar o endereço MAC. O fato de não ser escalável é outro fator que dificulta esse tipo de estrutura de autenticação, estabelecendo que a cada novo ou antigo usuário que acesse a rede e que altere sua placa de rede, o administrador terá que manter sua lista atualizada e completa dos endereços MAC desses usuários.

3.2.3 802.1X

O grupo do IEEE 802.11i especificou o 802.1X para autenticação de dispositivos e/ou usuários através da utilização de variações do protocolo EAP - Extensible Authentication Protocol e controle de acesso e gerência da distribuição de chaves criptográficas empregadas na proteção do tráfego tanto em redes locais com fio como sem fio. O acesso a uma rede para os dispositivos autorizados é restringido devido uma técnica conhecida como Robust Security Network (RSN) aplicada em redes wireless 802.11 juntamente com um framework do 802.11X.

O RADIUS (Remote Authentication Dial-In User Service) é um Servidor de Autenticação muito utilizado pelas redes sem fio. Tem a finalidade de validar as credenciais dos usuários e autorizar os usuários válidos e oferecer suporte a autenticações do tipo EAP que utiliza senhas, certificados digitais e outras formas de validação. O protocolo EAP gera uma única chave de criptografia para cada usuário, impedindo os ataques de quebra do WEP.

O servidor RADIUS pode ser utilizado para gerar novas chaves de criptografia dinamicamente para o WEP, permitindo que os algoritmos de criptografia sejam empregados com maior segurança. No entanto, a necessidade de um Servidor de Autenticação dificulta a implementação do padrão 802.1X, por não encontrar na maioria das vezes disponibilidade em ambientes menores.

O EAP é um protocolo de autenticação conectável, localizado nas camadas superiores, além do mais não existe nenhum tipo de EAP específico para o padrão 802.11x. De acordo com as circunstâncias e necessidade da rede, pode-se aplicar bem o EAP. Os protocolos mais utilizados nas redes wireless são: TLS, PEAP, TTLS e LEAP.

a) TLS (Transport Layer Security)

O TLS é um padrão do IETF, desenvolvido pela Microsoft, que apresenta autenticação através da utilização de certificados digitais. É estabelecida uma sessão de TLS criptografada entre esses certificados que são configurados em cada usuário da rede sem fio e no servidor de autenticação. O TLS também permite geração de chaves criptográficas.

b) PEAP (Protected Extensible Authentication Protocol)

O PEAP é um método de autenticação que a executa em dois momentos. No primeiro, uma sessão TLS é estabelecida para o servidor, permitindo que o cliente autentique o servidor usando o certificado digital do servidor. Em seguida, um segundo método EAP é encapsulado na sessão PEAP para autenticar o cliente ao servidor, pois o PEAP não oferece certificados nos clientes.

c) TTLS (Tunneled Transport Layer Security)

De forma semelhante ao PEAP, o TTLS é um protocolo realizado em duas etapas, utilizando uma sessão TLS para proteger determinada autenticação de cliente encapsulado. Além dos métodos de encapsulamento EAP, o TTLS pode usar versões não EAP para protocolos de autenticação.

d) LEAP (Lightweight EAP)

O LEAP é um método EAP proprietário desenvolvido pela Cisco System que usa senhas para autenticar apenas o usuário à WLAN, não ao computador. Por não haver essa autenticação ocasiona alguns problemas, como a execução incorreta das diretivas de grupo da máquina, falhas de configurações de instalação de softwares, perfis móveis e scripts de logon além dos usuários não poderem alterar suas senhas que foram expiradas. O LEAP também possui algumas vulnerabilidades de segurança, como a sensibilidade a ataques por intercepção e a ataques de dicionário off-line, permitindo que invasores consigam senhas de usuários válidos. Além do mais, o LEAP está relacionado à interoperabilidade, já que ele só funciona em hardwares e softwares da Cisco e de alguns outros fornecedores.

e) Vulnerabilidades

Apesar do protocolo 802.1X especificar diversas formas de autenticação entre a estação e o ponto de acesso, não prevê como será realizada a autenticação de uma estação que se movimenta de um ponto de acesso para outro. Neste padrão não é descrita a forma de relação de autenticação, pois o padrão 802.1X foi inicialmente projetado para redes cabeadas.

3.2.4 802.11i

O padrão IEEE 802.11i foi desenvolvido para solucionar problemas do WEP em relação à criptografia e do 802.1X em relação à autenticação de uma estação que se move entre um ponto de acesso e outro.

Os principais aspectos que o IEEE 802.11i pretende melhorar são: autenticação, gerenciamento de chave e transferência de dados. Eles provêem uma nova camada de segurança dentro de 802.11 WLANs (BROWN, 2003).

O 802.11i oferece um sistema de autenticação significativamente mais robusto que os oferecidos pelo padrão 802.11 anteriores, pois além de incluir a necessidade de um servidor de autenticação, também implementa um método de autenticação de dois sentidos. Para isto, foram introduzidas novas chaves: a chave mestra (MK), sendo esta privada e facilita a autenticação entre o hospedeiro e o servidor; e a chave mestra de pairwise (PMK) que é privada e simétrica sendo utilizada pelo hospedeiro e o ponto de acesso para controlar acesso à rede.

O processo de autenticação pode ser dividido em dois caminhos: o primeiro refere-se a comunicação do hospedeiro ao ponto de acesso, sendo controlado pelo protocolo de autenticação extensível revisado (EAP - Extensible Authentication Protocol); e o segundo é a comunicação do ponto de acesso com o servidor de autenticação sendo controlado pelo protocolo RADIUS[3] (Remote Authentication Dial-In User Service).

Para melhorar o gerenciamento de chaves, o 802.11i emprega, além das chaves MK e PMK, a chave temporária PTK, a chave de criptografia de chave KEK, o grupo de chave temporária GTK e, por fim, a chave temporal TK. Para prover um gerenciamento de chaves seguro são realizados os seguintes procedimentos: o primeiro utiliza o RADIUS para passar o PMK do servidor de autenticação para o ponto de acesso; o segundo procedimento é utilizar o PMK e um processo conhecido como 4-way handshake para derivar e verificar o PTK; o terceiro passo é usar o procedimento chamado group key handshake para enviar o GTK do ponto de acesso para o hospedeiro (BROWN, 2003).

O terceiro aspecto que o 802.11i quer aperfeiçoar é a transferência de dados e, com este intuito, são empregados dois mecanismos de criptografia, são eles: o

---

[3] RADIUS: tem como função autenticar as credenciais dos usuários e autorizar os usuários válidos, além de dar suporte a autenticações do tipo EAP que utiliza senhas, certificados digitais ou outros tipos de credencial.

CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) e o TKIP (Temporal Key Integrity Protocol).

a) TKIP

O protocolo TKIP permite que mudanças de chaves ocorram de frame em frame e sejam sincronizadas automaticamente entre o ponto de acesso e o usuário, o que soluciona os problemas de autenticação e integridade apresentado pelo WEP.

Enquanto o TKIP determina que chaves de encriptação serão usadas e se responsabiliza em mudar a chave de cada frame, o chaveamento global trabalha divulgando as novas chaves aos usuários. Conhecido como Michael, o MIC (Message Integrity Check) garante a integridade das mensagens transmitidas. O MIC é um dos campos do frame do 802.11i e é calculado a partir de informações encontradas no próprio frame, como os endereços MAC, tanto de origem quanto de destino.

A segurança deste método é baseada no fato de que o invasor desconhece o valor do MIC criptografado. O TKIP, também implementa um campo denominado SEQ, que é um campo de seqüência, adicionado a cada frame enviado, sendo que os frames que se encontram fora da ordem são descartados.

b) CCMP

Para fornecer uma criptografia simétrica ainda mais segura, o protocolo CCMP (Counter Mode CBC MAC Protocol) emprega um padrão de criptografia avançada, chamada de AES (Advanced Encryption Standard), o qual trabalha com diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado.

Os modos de operação de AES têm a finalidade de prevenir que uma mesma mensagem, quando criptografada, gere o mesmo texto cifrado.

3.2.5 WPA (Wifi Protected Access)

O padrão WPA foi desenvolvido para resolver algumas das vulnerabilidades tanto do método de criptografia WEP, quanto do IEEE 802.11i, sem a necessidade dos usuários mudarem de hardware. Dois modos de operação são especificados no WPA: o WPA-PSK (Chave pré-compartilhada) para uso doméstico e SOHO (Small Office Home Office) para uso comercial. Nesse modo, a autenticação é feita por um servidor de autenticação 802.1x, gerando um excelente controle e segurança no tráfego de usuários da rede sem fio.

Utilizando um excelente esquema de criptografia baseado no protocolo TKIP (Temporal Key Integrity Protocol), o WPA permite uma criptografia de dados mais complexa entre os computadores, auxiliado pelo MIC (Message Integrity Check) que tem como função evitar ataques do tipo bit-flipping facilmente aplicados ao WEP.

O processo de criptografia WAP, além de utilizar o campo MIC, o TKIP implementa um campo de seqüência (SEQ) no frame, para evitar ataques do tipo replay. O número de seqüência é inserido em cada frame enviado, sendo que o ponto de acesso irá eliminar frames que estejam fora da ordem enviados pelo mesmo cliente.

O WPA apresenta algumas vantagens sobre o WEP:

- Autenticação mútua do ponto de acesso e do cliente por meio de uma sincronização com quatro direções, verificando se ambos compartilham a mesma chave pré-compartilhada sem enviar o PSK antecipadamente.

- Criptografia reforçada, utilizando o TKIP (Temporal Key Integrity Protocol) e pares de chaves de sessão temporárias que são derivadas do PSK durante a sincronização com quatro direções.

- O MIC (Message Integrity Check), uma forte função matemática na qual o destinatário e o remetente calculam e comparam individualmente o MIC. Os MIC's incompatíveis indicam que terceiros tentaram adulterar os dados para invadir o sistema.

Como o WPA foi desenvolvido para ser executado com os mesmos equipamentos empregados no WEP, toda a base de interfaces de rede que permite o upgrade de firmware será aproveitada.

3.2.6 FIREWALL

Um firewall é uma combinação de hardware e software que filtra os pacotes que trafegam na rede, permitindo controle de acesso aos recursos da rede e gerenciamento do fluxo de tráfego.

A filtragem de pacotes é um mecanismo que analisa os cabeçalhos de datagrama e aplica as regras especificadas pelo administrador as quais determinam se o datagrama será descartado ou enviado. As regras de filtragem geralmente se baseiam em endereço IP de origem e de destino; porta TCP ou UDP de origem e destino; tipo de mensagem ICMP; datagrama de conexão usando bits TCP SYN ou ACK (KUROSE,2006).

Para assegurar um nível mais refinado de segurança, os firewalls têm de combinar filtros de pacotes com gateways de aplicação, através do qual todos os dados da aplicação que entram e que saem devem passar após examinar os cabeçalhos IP/TCP/UDP e tomar decisões com base em dados da aplicação.

O emprego de um firewall bem configurado pode aumentar consideravelmente o nível de segurança da rede. Porém, se esta rede sem fio for mal configurada, atrás deste firewall, é como se existisse um backdoor devidamente instalado.

3.2.7 VPN

Uma VPN[4] (Virtual Private Network) é uma conexão que utiliza a técnica de tunelamento em que os pacotes de dados são transmitidos por uma rota de rede pública, como a Internet, em um túnel privado que simula uma conexão ponto-a-ponto.

A VPN é um serviço extremo-a-extremo, não importando se está usando um link wireless, um cabo Ethernet, uma linha telefônica convencional ou alguma combinação desses e outros meios e suas funções ocorrem na camada de rede (ROSS, 2003).

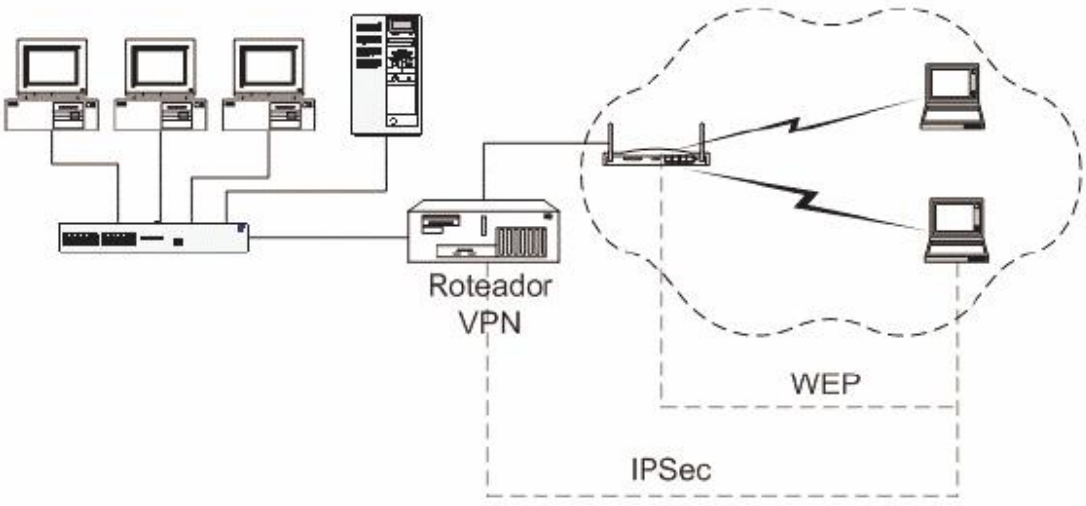

Figura 4: Rede WLAN com VPN/IP Séc

FONTE: PERES; WEBER, 2005

Dessa forma a sua principal característica é criar "túneis virtuais" de comunicação entre dois pontos, de modo que os dados trafeguem criptografados, aumentando a segurança na transmissão e recepção dos dados. Para isso, utiliza-se

[4] *VPN: Rede Privada Virtual.*

autenticação de login e senha restringindo o acesso a usuários autorizados; criptografam os dados para torná-los incompreensíveis para os invasores que interceptem os dados; e utilizam a autenticação de dados para preservar a integridade de cada pacote de dados e para assegurar que todos os dados foram originados em clientes de rede legítimos (ROSS, 2003).

3.2.8 SITE-SURVEY

Site-survey trata-se de uma medição da intensidade do sinal em diversos pontos do local onde a rede será instalada. Para evitar que o sinal esteja muito forte em áreas que não se deseja dar cobertura é necessário algum ajuste no equipamento, diminuindo assim a intensidade de propagação do sinal.

Paredes e portas não são suficientes para barrar o sinal wireless, um AP instalado dentro de um escritório pode transmitir um sinal em um raio de 300m. Normalmente num raio de 100m é suficiente para deixar o sinal fora do escritório. Intrusos podem utilizar desta maneira o wardriving e warchalking para se conectarem a redes wireless.

A maior parte dos APs permite que se configure a potência do sinal, reduzindo ao máximo os sinais que ultrapassam os limites físicos da rede/ambiente, impedindo que eles estejam ao alcance do intruso.

A antena deve ser selecionada corretamente, o sinal diminuído o máximo possível, os vidros exteriores devem ser isolados com tratamento metálico (ex.: insufilm espelhado). Acrescentando a isso a pintura com tintas metálicas nas paredes (ARAÚJO, 2004).

3.2.9 SSID (SERVICE SET IDENTIFIER)

É o nome de identificação da rede wireless. Uma vulnerabilidade muito comum entre os usuários é que eles não modificam o SSID e a senha padrão do fabricante do ponto de acesso. O nome do SSID deve ser modificado antes mesmo de conectar qualquer outro equipamento a rede.

Em redes sem visitantes (apenas computadores que raramente mudam) é possível desligar o envio do SSID pelo sinal, informando manualmente esse nome aos dispositivos autorizados a conectar-se ao ponto de acesso.

3.3 CONCLUSÃO

Embora padrões emergentes como o IEEE 802.11i possam potencialmente melhorar os serviços de segurança nas redes sem fio IEEE 802.11, é necessário desenvolver mais segurança em um ambiente WLAN.

Outro fator a se considerar é que WEP, WPA e 802.11i somente provêem segurança na camada de enlace da arquitetura de rede. Isso significa que a criptografia somente se aplica aos pacotes de dados que trafegam no meio aéreo entre o dispositivo móvel e o ponto de acesso. Uma vez que os pacotes atingem o ponto de acesso, eles são enviados decriptografados sobre a infra-estrutura cabeada. Outras formas de segurança devem ser implementadas como VPN. Assim, a segurança deve ser baseada nos componentes: proteção, detecção e reação.

A proteção pode ser realizada através de uma política de segurança para redes *wireless* e das seguintes medidas:

- ***Empregar filtros de endereço MAC;***
- ***Modificar o valor padrão do SSID e, se possível, desabilitar seu *broadcasting;***
- ***Utilizar criptografia além do WEP;***
- ***Utilizar IP's estáticos ao invés de DHCP para um melhor controle;***
- ***Fazer uso de softwares adicionais de segurança, como VPN e IDS;***
- ***Instalar os últimos *patches* de segurança e atualizações de *firmware* nos equipamentos *wireless.***

As medidas que podem ser adotadas para o processo de detecção incluem a instalação de IDS *(Intrusion Detection Servers)*, identificar a área de alcance do sinal, além de fazer um escaneamento da rede periodicamente para identificar pontos de acesso e conferir os logs dos produtos de segurança.

Para reagir a um ataque é necessário ter um plano de resposta a emergência no caso de atividades maliciosas, manter os *logs* atualizados e ativos a fim de rastrear e auxiliar na acusação a um usuário malicioso, e ainda ter habilidade para controlar e reconfigurar o AP em um momento de emergência, quando um ataque for identificado.

CAPÍTULO IV

4. ESTUDO DE CASO

A utilização de redes sem fio tem aumentado em ambientes diversificados. A priorização da usabilidade e acessibilidade em detrimento da preocupação com a segurança, aliada a má configuração dos dispositivos, tornam esses sistemas extremamente vulneráveis a ataques. Este trabalho aborda um estudo de caso baseado em análise de risco das redes sem fio, quanto às configurações utilizadas, instaladas em um centro comercial de Marabá.

Um dos principais objetivos é mostrar que configurações ineficientes estão colocando em risco as redes sem fio e, conseqüentemente, as redes guiadas[5]. Outra conseqüência é a possibilidade de quebra de confidencialidade através da captura de dados e informações trafegadas no meio aberto conforme técnicas de ataque já citadas.

4.1 PROCEDIMENTO DE PESQUISA DE CAMPO

A principal motivação do trabalho proposto é conhecer os tipos de ataque e modos de garantir segurança para redes sem fio. Desta maneira, uma análise para compreender a real situação de risco de segurança em que se encontram as redes de um centro comercial em Marabá foi utilizado como objeto da pesquisa de modo que este estudo possa ser utilizado para orientação da adoção de medidas de proteção adequadas. Foi feita uma leitura passiva das informações difundidas publicamente, através das redes sem fio dispersas na região pesquisada. O levantamento foi feito em busca de redes desprotegidas, configuração, o nível de exposição e entender a quais ataques elas estão mais suscetíveis.

4.1.1 INSPEÇÃO E SONDAGEM

Esta pesquisa utiliza procedimentos de inspeção e sondagem de redes sem fio, conhecidos como *wardriving*, que consiste em fazer uma varredura em uma área geográfica, em busca de redes sem fio. Em geral, tal procedimento não se caracteriza como um ataque à rede em questão, pois apenas costuma capturar informações que

[5] ***Redes guiadas: são redes que utilizam cabeamento.***

estão sendo divulgadas através do meio compartilhado usado pelas ondas de rádio das redes sem fio.

Existem várias ferramentas de software gratuitas disponíveis na internet, para busca e sondagem de redes sem fio. Estas ferramentas, quando utilizadas de forma apropriada, fornecem diversas informações importantes, como por exemplo, Identificador da rede SSID, endereço MAC, criptografia WEP, canal em uso e potência do sinal.

4.1.2 SONDAGEM ATIVA E PASSIVA

Existem duas técnicas que podem ser empregadas para realizar a sondagem: a sondagem ativa e passiva.

Uma das ferramentas mais utilizadas e completas para inspeção e sondagem é o Network Stumbler que realiza monitoramento ativo e o Kismet que realiza monitoramento passivo pois não troca informações com o emissor.

Na sondagem ativa é feita troca de informações entre o cliente e o concentrador de acesso sob sondagem, podendo inclusive haver possível violação de políticas de segurança ou até mesmo acionar eventuais detectores de intrusão ou outros sistemas de segurança.

O monitoramento passivo, conforme já citado, apenas captura os sinais de rádio-frequência nos canais onde o cliente é configurado para escutar. A interface de rede sem fio é colocada no modo monitor, capturando apenas o tráfego de difusão pública, sendo incapaz de enviar quaisquer frames. Este método torna extremamente difícil a descoberta de intrusos.

Neste trabalho foi usada a sondagem ativa mas sem violação de políticas de segurança.

4.2 REGIÃO PESQUISADA E METODOLOGIA APLICADA

A coleta de dados desta pesquisa foi realizada na cidade de Marabá do estado do Pará, através da técnica de Wardriving. Optou-se por analisar uma área específica com grande concentração de empresas de negócios e serviços, bancos, escritórios de representação, clínicas e estabelecimentos comerciais diversos, além de outros tipos variados de instituições. A área pesquisada na cidade de Marabá foi a VP-

8 no bairro Nova Marabá. Foram realizadas uma leitura e coleta de dados no dia 07 de fevereiro de 2007, entre 9h30min e 10h30min. O percurso total pesquisado para leitura foi de aproximadamente 6Km.

4.3 AMBIENTE DA PESQUISA DE CAMPO

Para realização deste trabalho de campo, foram necessários dispositivos, softwares e configurações especiais. O equipamento básico principal utilizado neste trabalho consiste de um computador portátil, tipo notebook, marca Toshiba com processador Pentium 4, 1.8 GHz, 256 MB de memória RAM, com o sistema operacional Windows XP e um adaptador D-LINK AIRPLUS™ G DWL – G122 802.11g(2.4GHz) Wireless USB 2.0 de rede sem fio.

O software básico de monitoramento utilizado foi o Network Stumbler, cuja tela principal pode ser observada na Figura 5.

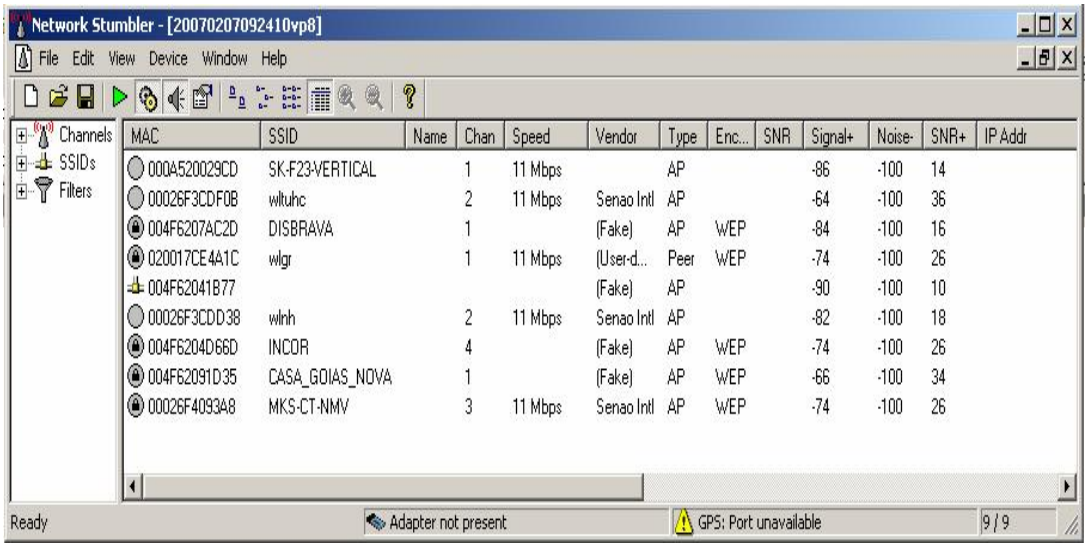

Figura 5: Tela do software Network Stumbler após a conclusão do percurso realizado na cidade de Marabá.

Possui características como potência do sinal, SSID da rede e suporte a GPS. Pode ser utilizado para ações maliciosas ou pelo administrador para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição.

4.4 RESULTADOS

Percebeu-se que uma parte das redes sem fio encontra-se vulnerável, pois não possuem o mecanismo de segurança básico WEP, ou seja um simples wireless sniffer pode comprometer a instituição, os clientes conectados a esses pontos de acesso abertos, devem acessar a Internet, expor senhas e etc. Caso não haja firewall, a instituição inteira estará vulnerável.

Da mesma forma as redes que empregavam WEP poderiam ou não estar utilizando outros mecanismos de proteção, pois apenas a ativação do protocolo WEP não significa que a rede está invulnerável à ataques. Porém é um nível a mais de segurança, e tornam as redes menos atrativas aos atacantes, visto que é necessário quebrar tal criptografia para escutar o tráfego.

Dentro de toda a área pesquisada da cidade foram encontradas oito redes wireless das quais cinco utilizavam WEP e apenas três não utilizavam criptografia. A figura 6 adaptada do Google Earth mostra a localização aproximada (para não comprometê-las) das redes encontradas, em que os pontos vermelhos indicam as redes que utilizam criptografia WEP e as redes indicadas com ponto azul não utilizam criptografia.

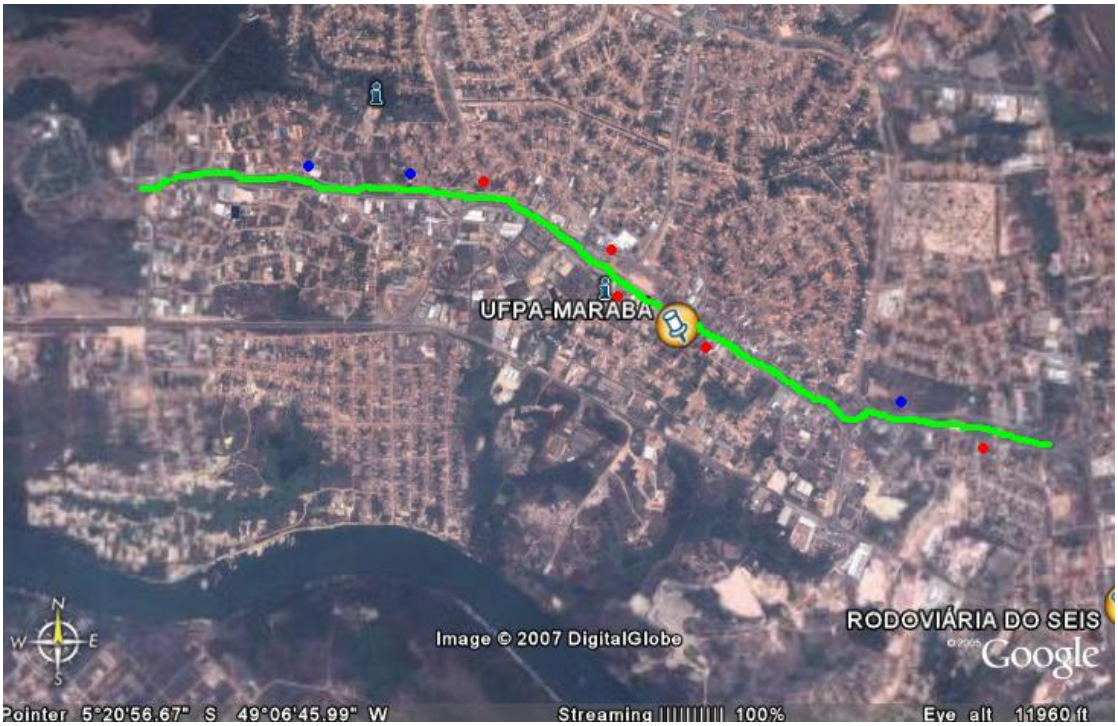

Figura 6: Percurso realizado para identificação das redes wireless na cidade de Marabá.

FONTE: Adaptado do Google Earth

Outra informação obtida é que metade dessas redes estão usando o canal 1, duas o canal 2 e outra o canal 3 e a última a ser citada no canal 4. Estas redes podem estar interferindo umas nas outras caso estejam muito próximas ou por estar utilizando a mesma freqüência ou por estar utilizando freqüência adjacente.

4.5 CONCLUSÃO

Através deste estudo caso realizado em Marabá, percebeu-se a necessidade da adoção de uma política de segurança às redes que não possuem uma criptografia básica e reforçar a segurança nas redes que utilizam apenas WEP.

Este estudo serve como um alerta para adequação dos sistemas existentes, quanto ao aprimoramento acompanhando a evolução tecnológica que eventualmente se torne disponível e no treinamento dos administradores de redes para lidarem com a questão da segurança.

CAPÍTULO V

5. CONCLUSÃO

Este trabalho abordou os principais conceitos de redes sem fio, seus elementos, modos de operação, padrões da indústria, demonstrando aspectos vulneráveis através dos tipos de ataques mais comuns e mecanismos de segurança.

Apesar das redes *wireless* oferecerem vantagens em relação às redes cabeadas quanto a mobilidade, facilidade de configuração dos dispositivos dentre outros, apresentam maior vulnerabilidade principalmente por não haver um controle total da abrangência do sinal, o que facilita ataques a rede.

Através do estudo realizado na cidade de Marabá, verificou-se a necessidade de implantar ferramentas de proteção às redes que não possuem sequer uma criptografia básica e reforçar a segurança nas redes que utilizam apenas WEP. Dessa forma, o emprego de mecanismos de segurança é indispensável para segurança dos dados que trafegam na rede e dos recursos disponíveis.

Este trabalho serve também como um alerta para adequação dos sistemas existentes, seja no sentido do aprimoramento e evolução tecnológica que eventualmente se torne disponível, seja no treinamento dos administradores de redes para lidarem com este problema.

Uma infinidade de ataques, citados neste trabalho podem se evitados com a configuração correta dos dispositivos sem fio, mas devemos ressaltar que esta é a primeira camada de segurança de muitas outras, as quais podem ser implantadas, de acordo com a política de segurança da instituição.

A busca por alternativas que diminua as vulnerabilidades e os ataques às redes *wireless* através de investigação de uma das redes identificadas abertas no estudo de caso, indicando outros mecanismos possíveis além do WEP para garantir a segurança da rede pode ser citado como trabalho futuro.

Outra sugestão para trabalho futuro seria a implementação de um software que permita verificar o tráfego de pacotes no ponto de acesso na rede.

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, B. M; MAESTRELLI, M. ***Segurança em Redes Wireless 802.11.*** *Rio de Janeiro, Jan. 2006 Disponível em: http://cbpfindex.cbpf.br/publication_pdfs/nt00204.2006_01_30_22_51_07.pdf. Acesso em 21/12/2006.*

ANDRADE, L. P. ***Análise das vulnerabilidades de segurança existentes nas redes locais sem fio: um estudo de caso do projeto Wlaca.*** *Belém, Ago. 2004. Disponível em: http://www.lprad.ufpa.br/~margalho/wdeec/wlaca.pdf. Acesso em: 28/10/2006.*

ARAÚJO, A. ***Meios de Transmissão. Meios de Transmissão IV: Transmissão Sem fio (Wireless).*** *Conselheiro Lafaiete, Abr. 2004. Disponível em: http://www.fasar.com.br/p/andre/x12_Wireless_B/img1.html . Acesso em 28/10/2006.*

BOFF, C. ***Técnicas do Hackerismo.*** *Paraná, Abr. 2003. Disponível em http://www.pr.gov.br/batebyte/edicoes/2003/bb130/estagiario.shtml. Acesso em 07/01/2007.*

BROWN, B. ***802.11: The security difference between b and i.*** *Out. 2003. Disponível em: http://ieeexplore.ieee.org/iel5/45/27781/01238689.pdf. Acesso em: 17/01/2007*

CANSIAN, A. M.; GRÉGIO, A. R. A.; PALHARES, C. T. et all; ***Falhas em políticas de configuração: Uma análise do risco para as redes sem fio na cidade de São Paulo. São Paulo.*** *Nov. 2004. Disponível em: http://www.acmesecurity.org/publicacoes/artigos/acme-artigo-ssi-2004-wlan.pdf/view. Acesso em 28/10/2006.*

CUNHA, S. ***Redes 802.11: Segurança, vulnerabilidades e ataques.*** *Belém, Mar. 2003. Disponível em: http:// sergiocunha.com/files/livre/802.11.pdf . Acesso em 17/01/2007.*

DUARTE, L. O. ***Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x.*** *São José do Rio Preto, Dez. 2003. Disponível em http://www.acmesecurity.org/publicacoes/monografias/monog. Acesso em 17/01/2006.*

KUROSE, J. F.; ROSS, K. W., 2006, ***Redes de Computadores e a Internet.*** *3 ed. São Paulo, 2006. Pearson Addison-Wesley.*

MATOS, L., ***Guia Profissional de Redes Wireless.*** *1 ed. São Paulo. Digerati Books.*

PERES, A; WEBER, R. F. ***Considerações sobre segurança em redes sem fio.*** *Natal, Out. 2005. Disponível em: http://www.ppgia.pucpr.br/~maziero/pesquisa/ceseg/wseg03/. Acesso em 23/09/2006.*

ROSS, J. ***O Livro de WI-FI: Instale, Configure e Use Redes Wireless (Sem Fio).*** *1 ed. Rio de Janeiro, 2003. Alta Books.*

SOARES, L. F., 1995, ***Redes de Computadores das LANs, MANs às redes ATM****. 2 ed. Rio de Janeiro, 1995. Campus.*

SILVA, G. M. ***Segurança em redes locais sem fio****. Dissertação de Mestrado. UFU, 2005. Uberlândia, MG, Brasil.*