INSTITUTO DE ENSINO SUPERIOR - FACULDADE LABORO
TECNÓLOGO EM REDES DE COMPUTADORES

BRUNO EMANUEL SETUBAL LEARTE
EMANUEL FERNANDES SOUZA

ANÁLISE DE VULNERABILIDADE E AMEAÇAS PRESENTES EM REDES WIFI (IEEE 802.11) EM BAIRROS E CENTRO DE SÃO LUIS-MA UTILIZANDO A TÉCNICA DE MAPEAMENTO WARDRIVING

SÃO LUÍS - MA
2018

BRUNO EMANUEL SETUBAL LEARTE
EMANUEL FERNANDES SOUZA

ANÁLISE DE VULNERABILIDADE E AMEAÇAS PRESENTES EM REDES WIFI (IEEE 802.11) EM BAIRROS E CENTRO DE SÃO LUIS-MA UTILIZANDO A TÉCNICA DE MAPEAMENTO WARDRIVING

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Me. Luan Carlos de Oliveira Moraes

SÃO LUÍS - MA

2018

BRUNO EMANUEL SETUBAL LEARTE

EMANUEL FERNANDES SOUZA

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: **/ /**

Nota :

BANCA EXAMINADORA

_____

Prof. Ms. Luan Carlos de Oliveira Moraes (Orientador)

_____

Prof. Ms. Milson Louseiro Lima

Dedico este trabalho a minha mãe, Maria Setubal e ao meu pai, José Amorim Learte, por todo o amor e dedicação que tiveram comigo, por terem sido pessoas fundamentais para que eu tenha me tornado a pessoa que hoje sou.

Dedico este trabalho a minha mãe, Maria Helena Rodrigues (in memorian), e ao meu pai, Francisco Barbosa (in memorian), por todo o amor e dedicação que tiveram comigo, por terem sido pessoas fundamentais para que eu tenha me tornado a pessoa que hoje sou

AGRADECIMENTOS

A Deus, por ter me dado forças e iluminado meu caminho para que eu pudesse concluir mais uma etapa vitoriosa da minha vida.
A minha mãe, Maria Setubal Learte, por todo amor e dedicação que sempre teve comigo, mulher pela qual tenho maior orgulho em chamar de mãe, meu eterno agradecimento pelos momentos em que esteve ao meu lado, me apoiando, guiando e me fazendo acreditar que nada é impossível para aqueles que lutam. Mãe dedicada, amiga, batalhadora, que acredita na minha capacidade e pessoa que sigo como exemplo.
Ao meu pai, José Amorim Learte, que sempre lutou para que eu chegasse até esta etapa da minha vida.
A minha namorada, Luciana Mello, por todo carinho, amor e atenção que sempre teve comigo, sempre apoiando em todos os momentos que já enfrentamos juntos e pela confiança em mim depositada, meu imenso agradecimento.
Ao meu colega, Emanuel Fernandes, que sempre estivemos juntos em todas as atividades e trabalhos acadêmicos, fica meu agradecimento.
Ao meu orientador, orientador Prof. Luan Carlos de Oliveira Moraes, pelos ensinamentos e dedicação dispensados no auxílio à concretização do TCC;
A todos os professores do curso de Redes de Computadores, pela paciência, dedicação e ensinamentos disponibilizados nas aulas, cada um e de forma especial, que contribuíram para a conclusão desse trabalho e, consequentemente, para minha formação profissional.
Por fim, gostaria de agradecer aos meus amigos e familiares, pelo carinho e pela compreensão nos momentos em que a dedicação aos estudos foi exclusiva e a todos aqueles que contribuíram, direta ou indiretamente, para que este trabalho fosse realizado, meu eterno AGRADECIMENTO.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, que me deu energia e benefícios para concluir todo esse trabalho.
Agradeço aos meus pais Maria Helena Rodrigues Fernandes e Francisco Barbosa Souza que me incentivaram todos os anos que estiveram ao meu lado.
Aos meus colegas de classe que participaram das pesquisas.
Ao meu irmão Bruno Rafael e minha irmã Rosivanda Barbosa, que mesmo longe, me apoiaram e contribuíram para que esse trabalho se realizasse.
Enfim, agradeço a todos as pessoas que fizeram parte dessa etapa decisiva da minha vida.

“Seu trabalho vai preencher uma parte grande da sua vida, e a única maneira de ficar realmente satisfeito é fazer o que você acredita ser um ótimo trabalho. E a única maneira de fazer um excelente trabalho é amar o que você faz”.

Steve Jobs

RESUMO

LEARTE, Bruno; SOUZA, Emanuel. **Análise de vulnerabilidade e ameaças presentes em redes Wifi (IEEE 802.11) em bairros e centro de São Luís-MA utilizando a técnica de mapeamento wardriving.** 2018. 87 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro, São Luís - MA, 2018.

Os avanços tecnológicos ao longo do tempo permitiram a integração e o rápido compartilhamento de informações através das redes de computadores. A crescente necessidade de troca de informação em qualquer lugar e horário trouxeram consigo a necessidade de criação de redes de computadores que se adequem a este novo conceito, dai surgindo as chamadas redes wireless (sem fio). Tal praticidade no uso de equipamentos móveis e integração destes dispositivos trazem consigo uma constante preocupação com a segurança dos dados que trafegam nestas redes. Embora os constantes avanços das tecnologias de segurança, uma rede sem fio não é completamente segura. Mecanismos de segurança são utilizados na tentativa de impedir que algum interceptador possa acessar a uma rede privada ou ler o conteúdo de pacotes que trafegam na mesma. Atualmente protocolos de criptografia WEP, WPA e WPA2 são alguns dos mecanismos de segurança que visam este propósito. Porém, muitos problemas para estes mecanismos são conhecidos e, além disso, há a falta de conhecimento dos administradores de redes com relação a estes, o que torna a segurança em redes sem fio um tanto duvidosa. A facilidade na captação de sinais de redes wireless, utilização da técnica do wardriving, domínio de ferramentas para testes de invasão e aplicação dos conceitos de redes sem fio facilitam o processo de ataque. Sendo assim, o presente trabalho tem por objetivo utilizar a técnica do wardriving para identificar as redes sem fio utilizadas nos bairros de São Luís-MA com os seus respectivos protocolos de criptografia WEP, WPA e WPA2. Analisando suas estruturas, características, funcionamento, apresentando os resultados dos testes de invasão às redes sem fio que utilizam estes tipos de criptografia, posteriormente consolidando os dados do mapeamento quantitativo das redes dos bairros da cidade de São Luís do Maranhão que utilizam estes protocolos e apresentar a sociedade o resultado geral que relate a situação atual em relação à segurança da informação nestes locais.

Palavras-chaves: Segurança da Informação. Wardriving. WEP. WPA2. Ataques.

ABSTRACT

LEARTE, Bruno; SOUZA, Emanuel. **Análise de vulnerabilidade e ameaças presentes em redes Wifi (IEEE 802.11) em bairros e centro de São Luís-MA utilizando a técnica de mapeamento wardriving.** 2018. 87 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2018.

Technology advances over time, allow the integration and the rapid sharing of information through computer networks. The growing need for exchange of information at any place and time, with the requirement to networks of computers that fit this new concept, hence the calls coming wireless networks (wireless). Such practicality in the use of mobile devices and integration of these devices bring with them a constant the safety of data traveling on the networks. Although the constant advances in technology security, a wireless network is not completely secure. Security mechanisms are used in and attempt to prevent any eavesdropper can acess a private network or read the contents of packets traveling the same. Currently encryption protocols WEP, WPA and WPA2 are some of the security mechanisms aimed at this purpose. However, many problems for these mechanisms are known and, moreover, there is a lack of knowledge of network administrators in relation to these, which makes security in wireless networks somewhat dubious. The ease of picking up signals from wireless networks, using the technique of wardriving, domain tools for penetration testing and application of the concepts os wireless networks facilitate the process of attack. Thus, this paper aims to describe the protocols WEP, WPA and WPA2, analyze their structure, characteristics and functioning, presenting the results of the penetration testing of wireless networks neighborhoods in the city of São Luís of Maranhão using these protocols society and present the general result that reports the current situation in relation to information security in the places.

Keywords: Information Security. wardriving, WEP. WPA2. Attacks.

LISTA DE FIGURAS E ILUSTRAÇÕES

LISTA DE TABELA

LISTA DE GRÁFICOS

LISTA DE SIGLAS

AES	Advanced Encryption Standart
Bps	Bits por segundo
CA	Certificate Authority
CBC	Cipher Block Chaining
CBC-CTR	Cipher Block Chaining Counter Mode
CBC-MAC	Cipher Block Chaining Message Authenticity Check
CCMP	Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol
CRC-32	Cyclic Redundancy Check
DES	Data Encryption Standart
DFS	Dynamic Frequency Selection
DoS	Denial of Service
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP–TLS	Extensible Authentication Protocol-Transport Layer Security
EAP–TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
ESSID	Extentended Service Set Identifier
FSK	Frequency Shift Keying
GHz	Gigahertz
GPS	Global Positioning System
HTTP	Hyper Text Transfer Protocol
IAAP	Inter Acess Point Procol
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISA	Internet Security and Acceleration

SUMÁRIO

1 INTRODUÇÃO

1.1 Justificativa

A denominada Sociedade da Informação, na qual vivemos, teve a sua evolução no berço da Segunda Guerra Mundial com o seu apogeu durante a Guerra Fria, com as revoluções técnicas e cientificas que ocorreram durante o período entre 1939 e 1960, houve o advento de novas tecnologias tais como: novos sistemas de comunicação, criação de processadores analógicos de dados (computadores primitivos) e inovação a partir do projeto ARPANET (projeto piloto da internet) (SACEVIC, 1966).

Com o constante avanço das tecnologias para compartilhamento das informações, houve a necessidade de conectividade para acesso aos dados em tempo real, com maior mobilidade, flexibilidade e disponibilidade que levaram ao avanço das tecnologias de comunicação sem fio.

Tais revoluções trazem consigo a constante necessidade da segurança em redes. Tal importância surge pelo fato das informações valiosas estarem sendo transmitidas constantemente pelo ar, sem qualquer tipo de gestão sobre esses dados sensíveis, ficando sujeitos a ataques sem a necessidade da presença física do infrator.

Embora os avanços nas últimas décadas na área da segurança da informação em redes sejam expressivos, uma rede sem fio (wireless) não é completamente segura. Em um universo globalizado e competitivo, as informações são os ativos mais importantes de qualquer setor. Falhas de configurações descuidos, posicionamento inadequado do ponto de acesso à rede sem fio ou falta de conhecimento das ameaças são fatores agravantes para o aumento do risco de invasões e podem gerar prejuízos irrecuperáveis.

1.2 Objetivos da pesquisa

O principal objetivo da pesquisa é avaliar e analisar o grau de vulnerabilidades das redes sem fio em 5 (cinco) grandes bairros da cidade de São Luís do Estado do Maranhão.

Com a facilidade de captação do sinal das redes sem fio e com a

necessidade de proteção dos dados nelas trafegados, questiona-se o real nível de proteção dessas redes e quais as melhores práticas para fortalecimento da segurança da informação em redes.

1.2.1 Objetivo geral

Analisar o grau vulnerabilidades das redes sem fio dos bairros de São Luís do Estado do Maranhão.

1.2.2 Objetivos específicos

Este trabalho esta dividido em 4 (quatro) capítulos, o primeiro é uma introdução ao assunto proposto. O segundo corresponde à fundamentação teórica, apresentando os conceitos para segurança da informação, redes sem fio e a técnica para levantamento de informações de pontos de acesso a rede sem fio, o wardriving. O terceiro aborda o desenvolvimento do estudo de caso, com uma breve descrição dos materiais e métodos utilizados, enfatizando principalmente os resultados obtidos desta pesquisa. Por fim, no quarto capítulo encontram-se as considerações finais.

1.3 Metodologia

Para isso, utilizará a técnica wardriving para levantamento de informações das redes sem fio e algumas ferramentas (software) para quebra de proteção (invasão) dos protocolos de criptografia destas redes.

Para tal, leva-se em consideração a necessidade dos estudos relacionados às tecnologias das redes sem fio, processo de transmissão de dados entre equipamentos, modos de operações, padrões utilizados e métodos de invasões em redes wireless “protegidas”, para assim, chegarmos a resultados que possibilitem mapear a quantidade de pontos de acesso encontrados nestes locais e o nível de proteção dos mesmos.

1.4 Estrutura do trabalho

Este trabalho esta dividido em 4 (quatro) capítulos, o primeiro é uma introdução ao assunto proposto. O segundo corresponde à fundamentação teórica, apresentando os conceitos para segurança da informação, redes sem fio e a técnica para levantamento de informações de pontos de acesso a rede sem fio, o wardriving. O terceiro aborda o desenvolvimento do estudo de caso, com uma breve descrição dos materiais e métodos utilizados, enfatizando principalmente os resultados obtidos desta pesquisa. Por fim, no quarto capítulo encontram-se as considerações finais.

2.1 Segurança da informação

De acordo com Peixoto (2006, p. 37). “O temo segurança da informação pode ser designado como uma área do conhecimento, informático ou não, que salvaguarda os chamados ativos de informação, contra acessos indevidos, modificações, não autorizadas ou até mesmo sua não disponibilidade”.

A Segurança da Informação está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou uma organização. Possui conceitos básicos que devem ser levados sempre em consideração, sendo eles: confidencialidade, integridade e disponibilidade da informação. Por esses e outros motivos, antes de qualquer coisa, todos os usuários devem saber o que é a informação para sua empresa ou vida pessoal, qual a sua importância e por que a segurança da informação é fundamental.

De acordo com as pesquisas mais recentes, aproximadamente 53% das empresas brasileiras apontam os funcionários insatisfeitos como maior ameaça á segurança da informação, 40% delas afirmam ter sido vítimas de algum tipo de invasão, 31% não sabem dizer se sofreram ataques e somente 29% alegam nunca ter sofrido ataques. [...] Em 22% dos casos de ataque, as organizações não conseguiram detectar as causas e em 85% dos casos não souberam quantificar o prejuízo. (BANNWART, 2001 apud PEIXOTO, 2006, p. 36).

O vazamento de dados e informações pessoais e corporativos vem em um crescente constante e causando prejuízos imensuráveis, um simples clique pode abrir portas para um mundo de exploração de malfeitores.

Segundo a Revista época (2011, p.13) “o momento é bastante preocupante, passamos por um momento no Brasil na qual não tivemos iguais, ataques e roubos de informações a órgãos públicos e privados são a moda da época”, além da onda de hacketivismo proposto por um grupo principal, denominado anonymous. A mídia vem tentando desempenhar um papel de alertar a população, principalmente no que se trata do mercado, no entanto, muito pouco tem feito a sociedade para proteger as suas informações.

Complementando o assunto, vejamos algumas noticiais veiculadas nas mídias:

Coca-Cola: secretária é condenada a oito anos por roubo de segredo – a

ex-secretária da Coca-Cola acusada de roubar segredos da gigante dos refrigerantes e tentar vendê-los à rival Pepsi por US$ 1,5 milhão foi condenada a oito anos de prisão. A sentença foi determinada nesta quarta-feira. […] as provas mostra que ela queria ferir a Coca-Cola. Ela achava que estava sendo tratada de forma injusta pela empresa, afirmou o juiz Owen Forrester, da corte federal de Atlanta (PORTAL TERRA, 2007).

Hacker invade e-mail de Dilma e José Dirceu – um “hacker” invadiu o correio eletrônico pessoal da presidente Dilma Rousseff e copiou e-mails que ela recebeu durante sua vitoriosa campanha […] Dirceu disse que seu e-mail pessoal foi invadido por volta das 2h da manhã da última segunda. Segundo ele, sua senha teria sido alterada após telefonema de uma pessoa ao serviço de atendimento ao usuário do UOL. [...] “O que importa é que, verdadeiros ou falsos, esses e-mails são frutos de um ato criminoso”, declarou a ministra da Comunicação Social, Helena Chagas (IMPLICANTE.org, 2011).

A segurança da informação pode ser caracterizada pela preservação e manipulação de três fatores básicos e seus complementares, estes estão demostrados na Figura 1.

Figura 1 - Os pilares da Segurança da Informação

Fonte: Alves e Gustavo (2006).

Os pilares da Segurança da Informação são bordados a seguir:

Confidencialidade: É a garantia de que as informações alcançaram o seu

destino final, sem que dissipem para outro lugar onde não deveria passar. Visando a garantia de que a informação é acessível somente por pessoas na qual lhe respeitem o poder de acesso. Não sendo, portanto, divulgadas a indivíduos, entidades ou processos sem autorização.

Integridade: Propriedade que garante que a informação manipulada mantenha toda as características originais estabelecidas pelo proprietário da informação original, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição) até o usuário final.

- Disponibilidade: Propriedade que garante que a informação esteja sempre disponível para o uso legitima, ou seja, informações ou sistemas informáticos resistentes a falhas. Segundo Peixoto (2006, p. 37), sendo o grande o desafio da disponibilidade da estrutura de transporte de informações de forma confiável e integra sem que haja impossibilidade de captar as informações.

Alguns pesquisadores chegam a incluir mais dois pilares básicos (complementares), que agregam ainda mais valor para segurança da informação:

- Não Repúdio e Autenticidade: Conhecido como responsabilidade final, tem como objetivo verificar a identidade e autenticidade de alguém ou até mesmo de um agente exterior a fim de garantir a integridade de origem.

Os pilares acima se relacionam intimamente aos três aspectos da segurança da informação, conforme descrição a seguir e ilustração contida na Figura 2:

Figura 2 - Aspectos da Segurança da Informação

Fonte: Peixoto (2009, p. 211)

- Pessoas: Orientação, treinamentos e conscientização dos usuários minimizam os riscos a segurança da informação.
- Processos: Regras bem claras para utilização dos recursos tecnológicos, scripts pré-estabelecidos para o manuseio de sistemas, conversas e manipulação de acesso. Além do uso de leis rigorosas, que visam à punição corretiva dos infratores no caso de desvio de informações ou processos.

Tecnologia: Aquisição de equipamentos certificados com selo de garantia da segurança, por empresas que busquem a continua evolução da segurança dos seus equipamentos.

A informação precisa ser protegida, pois:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização ou pessoas, e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR/ISO 27002:2005, p.2).

A segurança da informação é necessária pelos seguintes motivos:

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação pode ser atividades essenciais para assegurar a competividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado. [...] a função da segurança da informação é viabilizar os negócios [...] (ABNT NBR/ISO 27002:2005, p.2).

Como o próprio Comitê Gestor da Internet no Brasil diz:

> Computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços: comunicação, por exemplo, através de e-mails; armazenamento de dados sejam eles pessoais ou comerciais, etc. (TAKASHI, 2000, p.13-24).

- “A informação é um ativo que, como qualquer outro, importante para os negócios, tem um valor para a organização. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos ao negócio e maximizar o retorno dos investimentos e as oportunidades de negócios”. (NBR ISO/IEC 1799:2001, p. 2).
- Compreende-se, portanto, que o vazamento das informações e falta de segurança para a informação são predeterminada por muitas variáveis, a

necessidade do equilíbrio entre segurança e eficácia no uso da tecnologia deve ser estuda e mapeada para o bem da sociedade.

2.1.1 A informação e sua importância

- “O conceito de informação deriva do latim *informatio* (“delinear, conceber ideia”) e significa um processo de comunicação ou algo relacionado com construção e armazenamento de dados e conhecimentos” (Zhang, 1988), mas na realidade existem muitas e variadas definições de informação.
- A informação tornou-se tão importante que Drucker (1993 a, b) defende “[...] o primado da informação como base e a razão para um novo tipo de gestão, em que em curto prazo perspectiva a troca do binômio capital/trabalho pelo binômio informação/conhecimento como fatores determinantes no sucesso individual e principalmente empresarial. Caminha-se para a sociedade do saber onde o valor da informação tende a suplantar a importância do capital”. A informação e o conhecimento são a chave da produtividade e da competitividade.
- A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo critico para continuidade operacional da empresa. (PEIXOTO, 2006, p.37).
- Informação também se define como:
- “Ato ou efeito de informar ou informa-se; comunicação, indagação ou devassa. Conjunto de conhecimentos sobre alguém ou alguma coisa; conhecimentos obtidos por alguém. Fato ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens. Elemento de conhecimento suscetível de ser transmitido e conservado graças a um suporte e um código” (PEIXOTO, 2006, p.4).
- Conforme definição da norma NBR ISO/IEC 27002:2005 que trata do código de prática a Gestão da Segurança da informação, diz o seguinte:
- “A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente”.

2.2 A tecnologia das redes sem fio

Nas últimas décadas a Internet, cresceu de tal forma que se tornou uma ferramenta indispensável no dia a dia das pessoas. É impossível imaginar o mundo atual sem acesso a grande quantidade de dados (big data) com os mais variados assuntos que estão disponíveis na internet.

As grandes difusões das redes de computadores possibilitaram um avanço sem procedentes no compartilhamento de aplicações e informações. A crescente necessidade de acesso à informação em tempo real e em qualquer lugar traz a constante necessidade de avanço tecnológico no acesso a redes sem fio, segundo Felipe Lucchese (ANO, p. 00):

> Redes Wireless (sem fio), em particular as redes Wi-Fi (Wireless Fidelity) tornam-se, sem dúvida, cada dia mais populares e imprescindíveis, sendo inegável a conveniência de sua utilização em lugares como aeroportos, hotéis e cafés. Redes wireless propiciam uma considerável praticidade e mobilidade em ambientes corporativos e/ou domésticos e pode mudar a maneira como as pessoas trabalham e permanecem on-line quando distantes de sua base habitual.

É importante um aprofundamento no conceito de rede sem fio, não é difícil a confusão entre computação móvel com redes sem fio. Apesar do envolvimento, não é a mesma coisa. Computação móvel é a capacidade de acesso à informação a qualquer lugar e a qualquer momento, é tecnicamente a união entre processamento, mobilidade e comunicação sem fio. Já as redes sem fio tem como ideia principal a utilização de outro meio de comunicação de dados ou pacotes que não seja cabeada como, por exemplo, ondas de rádio.

O temo Wireless provém da língua inglesa wire (fio, cabo) e less (sem), ou seja, sem fio. Portanto, wireless é caracterizado pelo tipo de conexão sem utilização de cabos e transmissão de informação através do ar. Dentro deste modelo de comunicação, podemos citar várias tecnologias como: bluetooth, Wi-Fi e infravermelho. Para que o processo de transporte de dados através de uma rede wireless aconteça, é necessário o envolvimento de três elementos: o meio físico de transmissão, o formato dos dados e a estrutura da rede.

> As redes sem fio consistem em redes de comunicações por enlaces sem fio como rádio frequência e infravermelho que permitem mobilidade continua através de sua área de abrangência. As redes sem fio são compostas por sistemas móveis, que têm como principal e mais difundido representante as redes celulares (PEIXOTO, 2004, p.5).

A área de atuação das redes sem fio abrange desde a comunicação entre dispositivos até a comunicação em escala global, tornando assim uma tecnologia atraente e promissora.

Um dos principais fatores que contribuem para a crescente utilização de uma rede sem fio é a facilidade de instalação devida à eliminação da necessidade e do trabalho de passar cabos por paredes, pisos, etc. Além dessa vantagem, há vários outros benefícios que motivam a utilização de redes sem fio, como de acordo Lucchese (2007).

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

A principal desvantagem que envolve as redes sem fio é o fator da segurança, onde a dificuldade de gestão dos dados que trafegam no ar deve ser uma constante para desenvolvimento da proteção. Além dessa, existem outras desvantagens como, por exemplo:

- O ambiente onde o equipamento emissor de sinal esta inserido, dependendo da quantidade de barreiras e interferências, pode dificultar a transmissão do sinal.
- Alto consumo de energia dos equipamentos portáteis;
- Largura da banda é limitada devido a imposições de órgãos regulamentadores.

Para um implantação adequada de uma rede wireless é necessário desenvolver uma visão mais aprofundada do fator segurança da informação. Onde as politicas de segurança da informação devem ser adotadas pela organização de maneira que uma cultura interna seja criada e desenvolvida.

2.2.1 Meios de transmissão em redes sem fio

Todo meio de transmissão de dados disponível atualmente, tem um conjunto de limitações funcionais. Essas limitações devem ser levadas em consideração no momento da estruturação da rede, alguns autores afirmam que a transmissão em rede sem fio pode ser dividido em quatro grandes grupos: laser,

radiofrequência, micro-ondas e infravermelho.

2.2.1.1 Laser

É considerada a nova geração da tecnologia de rede wireless, é capaz de converter pulsos de laser ultrarrápidos em sinais de radiofrequência. Nesta tecnologia as ondas contínuas das transmissões convencionais são substituídas por sinais pulsantes produzidos por um “gerador espectral”, com a duração extremamente curta de cada pulso, o dispositivo torna-se capaz de transmitir dados de forma extremamente rápida, tendo como receptor para processamento uma tecnologia chamada “onda óptica arbitrária”. Assim a rede sem fio a laser é chamada de banda ultra larga.

Segundo Farias (2006), a transmissão laser é unidirecional, ou seja, tem de existir obrigatoriamente uma linha de vista entre o emissor e o receptor para que se venha a ter comunicação. Sendo assim a tecnologia a laser é apropriada a conectar redes LAN's equidistantes geograficamente. Algumas dificuldades desta tecnologia ainda estão sendo estudadas para melhoria, fatores como chuva ou nevoeiros dificultam a penetração do laser no processo de transmissão de dados.

2.2.1.2 Radiofrequência

A radiofrequência em sua grande maioria é omnidirecional, ou seja, não se faz necessário à existência de uma linha de vista entre o emissor e receptor para concretização da comunicação. Segundo Forouzan (2006, p. 00) “essa característica pode ser considerada uma desvantagem pelo fato das ondas transmitidas por uma antena estarem sujeitas as interferências provocadas por outras antenas que estejam transmitindo na mesma frequência”.

O autor afirma ainda que “Quase a banda inteira é regulada pelas autoridades governamentais. Para utilizar qualquer faixa da banda é necessário obter permissão dessas autoridades” (FOROUZAN, 2006 p. 43).

2.2.1.3 Micro-ondas

A transmissão em micro-ondas atua em um nível de frequência que proporciona transmissões de longo alcance, a transmissão em micro-ondas também

é unidirecional, ou seja, necessita da existência de uma linha de vista entre a antena emissora e a antena receptora do sinal para que a comunicação possa fluir. Segundo Forouzan (2006), uma característica das micro-ondas é o fato de não conseguir atravessar obstáculos muito grande e nem penetrar nos edifícios, devido ao fato de usar frequência muito alta.

2.2.1.4 Infravermelho

O infravermelho é caracterizado pelas suas altas taxas de frequência e a transmissão entre os dados tende a ser feita sem a existência de nenhum obstáculo sólido entre o emissor e receptor. De acordo com Fourouzan (2002), as grandes vantagens do infravermelho é o valor custo beneficio e não sofre de interferência eletromagnética e nem da radiofrequência, tornando assim uma tecnologia com um maior grau de segurança. Segundo Zanetti e Gonçalves, existem dois tipos de propagação do infravermelho: a direta e a difusa.

- Direta: necessita que as transmissões do sinal entre o emissor e o receptor sejam feitas sem nenhum impedimento físico.
- Difusa: a propagação da transmissão entre o emissor e receptor é feita utilizando superfície refletiva, já que ela utiliza o teto, as paredes e os pisos para refletir os sinais.

2.2.2 Tipos de redes sem fio (*wlan-wpan-wman*)

Uma rede sem fio (Wireless) é um sistema que interliga vários equipamentos fixos ou móveis utilizando o ar como meio de transmissão e que possuem um ponto de acesso por onde os dados são transmitidos através da rede em todas as direções.

- WLAN: É uma rede de computadores local que se utiliza de ondas de rádio para fazer uma conexão à internet ou a outra rede, também pode ser uma extensão a uma rede local cabeada. Fornecendo maior funcionalidade, flexibilidade e facilidade de acesso a dispositivos móveis em locais com grandes espaços físicos e com alta concentração de usuários. É constituída por transmissores, receptores e um ponto de acesso onde os dados são modulados, permitindo transmissão e recepção dos dados pelo ar.

> As tecnologias de redes sem fio destinadas ao uso em Wireless LAN (Local Area Networks) foram padronizadas pelo IEEE (Institute of Electrical and Electronics Engineers) através do grupo 802.11. O objetivo dessa padronização era definir um nível físico para redes onde a transmissões são realizadas nas frequências de rádio (RF) ou infravermelho (IR), e um protocolo de acesso ao meio. (FRANCESCHINELLI, 2003, p. 00).

- WPAN: É basicamente um tipo de rede onde vários tipos de dispositivos móveis, como celulares e notebooks estão conectados a uma rede sem fio de pequeno alcance. Utiliza-se principalmente da tecnologia Bluetooth para conectar os dispositivos e a rede possui características distintas como: alcance de pequenas distâncias, baixas taxas de transferência e custo.

A rede WPAN é definida pelo padrão 802.15, e nessa categoria as tecnologias Bluetooth são as mais utilizadas. Segundo a visão de Tanenbaum (2003) a tecnologia Bluetooth atinge uma área de cobertura de 10 metros. Diferente da visão de Tanenbaum (2003), Alecrim (2008), afirma que a área de cobertura atingida pela tecnologia Bluetooth varia de acordo com as classes e as potências utilizadas. A tabela 1 informa os alcances e as potências usadas em cada uma das classes.

Classes	Potência Máxima (mV)	Área cobertura (metro)
Classe 1	100	100
Classe 2	2,5	10
Classe 3	1	1

Tabela 1 - Potência e alcance das classes da tecnologia Bluetooth

Fonte: Xxxxx (00000, p. 00)

A comunicação da tecnologia Bluetooth é feita entre os dispositivos através de uma rede denominada de piconet. Esta rede pode suportar até oito dispositivos, sendo 1 mestre e os demais escravos. Esta tecnologia trabalha na frequência de 2,4 Ghz (utiliza padrões 802.11b e g), o que pode acarretar na geração de interferências ás outras tecnologias que trabalham nesta mesma faixa de frequência.

Segundo Alecrim (2008), dentro da rede piconet da tecnologia bluetooth o

mestre é quem controla toda a comunicação na rede, existindo assim comunicação somente entre mestre e escravos. Havendo, portanto, um dispositivo mestre para cada rede, um escravo da mesma rede pode agir como mestre numa outra rede, através da interligação de dois ou mais piconet, formando assim uma scatternet. A scatternet pode suportar no máximo de até oitenta equipamentos, permitindo assim que vários dispositivos possam ser interconectados.

- WMAN: Rede sem fio de área metropolitana (WMAN) e também conhecida por redes sem fio de banda larga. O seu funcionamento é idêntica às redes de celulares, onde existem estruturas (torres) próximas aos usuários que recebem o sinal (na maioria das vezes de satélites), transmitem para estações base e depois fazem um roteamento através de uma conexão Ethernet padrão diretamente ligadas aos usuários.

2.2.3 Modos de operações

Em termos organizacionais, as redes sem fio no padrão 802.11 definem dois modos distintos de operação: Ad-Hoc e infraestrutura.

2.2.3.1 Rede *Ad-hoc* ou *Independent Basica Service Set* (IBBS)

São redes em que os equipamentos conectam-se diretamente uns aos outros ou com propósitos específicos, de maneira mais ou menos análoga as antigas redes coaxiais, onde apenas um cabo interligava vários equipamentos, sendo que os dispositivos sem fio comunicam-se diretamente entre si sem a necessidade de um ponto de acesso. Esta topologia pode ser apropriada para pequenas redes que não precisam de segurança e nenhum dado sigiloso deve ser trafegado, pois, deve-se enfatizar, a ausência do ponto de acesso gera vários problemas de segurança, administração e gerência da rede.

> A rede é formada conforme a necessidade, com os equipamentos utilizados próximo uns dos outros e em locais que não dispõem de infraestrutura de rede. Esta rede pode ser formada por equipamentos portáteis, com o intuito de trocar dados na ausência de pontos de acesso (como por exemplo, em salas de conferencias, aeroportos) (KUROSE; KEITH, 2006).

De acordo com Farias (2006), as redes Ad-Hoc como não possuem uma

infraestrutura física, são geralmente pequenas e não possui uma conexão com a rede com cabo. Contudo, não existe um limite máximo definido para o número de dispositivos que podem fazer parte dessa rede.

Na Figura 3 é mostrado o modelo de operação do Ad-Hoc.

Figura 3 - Rede Ad-Hoc

Fonte: Site : pplware.sapo.pt/tutoriais/rede-sem-fios-how-to/

De acordo com Rufino (2005) e Farias (2006), a ausência de uma infraestrutura física leva as redes Ad-Hoc apresentar as entre suas desvantagens, o problema de segurança, administração e gerência de rede e os problemas de comunicação, devido ao problema do nó escondido.

2.2.3.2 Rede infraestrutura

O concentrador (ponto de acesso) é o equipamento central de uma rede que se utiliza dessa topologia. Sendo assim, um ponto único de comunicação (ponto de acesso) é rodeado de vários clientes, centralizando as configurações de segurança. Com isso há a possibilidade de controle dos itens (autenticação, autorização, criptografia, etc.) em um único ponto. Segundo Rufino (2005), outra vantagem deste modelo é facilitar a interligação com a rede cabeada e/ou com Internet, já quem em geral o concentrador também desempenha o papel de gateway ou ponte. Na Figura 4 é mostrado o funcionamento deste modo de operação:

Figura 4 - Rede Infraestrutura

Fonte: Farias (2010)

2.2.4 Principais padrões

As redes wireless utilizam de padrões técnicos aprovados pelo IEEE (Institute of Electrical and Electronic Engineers), o IEEE é uma associação profissional técnica com mais de trezentos mil membros, cujo objetivo é desenvolver padrões para as áreas de engenharias eletrônicas e computação. Um das suas frentes de trabalho é denominado de 802.11, que segundo Rufino (2005 p. 30), reúne uma serie de especificações que basicamente definem como é feita a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes.

2.2.4.1 Padrão 802.11a

Tentando resolver os problemas existentes nos protocolos anteriores, o 802.11a têm como principal característica o aumento da velocidade para no máximo de 54 Mbps, mas pode também operar em velocidades baixas. Outra grande diferença está na operação na faixa de frequência de 5 GHz, uma faixa com pouca interferência, mas com alcance reduzido. Oferece também aumento no número de clientes conectados, mas precisamente sessenta e quatro totais, e o aumento da chave de criptografia. Não possui compatibilidade com o 802.11b, pois utiliza diferentes faixas de frequência.

2.2.4.2 Padrão 802.11b

O padrão 802.11b surgiu em 1999 e foi aprovado pela IEEE em 2003, possui uma base grande de base instalada. De acordo com Alecrim (2008) e Rufino (2005), este subpadrão da 802.11 opera na faixa da frequência que varia entre 2,4 Ghz a 2,48 Ghz e utiliza a técnica DSSS[3], para transmitir e receber dados nas seguintes velocidades: 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps, possibilitando no máximo 32 clientes conectados. O padrão 802.11b pode alcançar teoricamente aproximadamente 400 metros em lugares abertos e 50 metros em lugares fechados.

2.2.4.3 Padrão 802.11g

O padrão 802.11g surgiu em meados de 2003, sendo considerado o sucessor do padrão 802.11b devido à compatibilidade com o mesmo. Segundo Alecrim (2008), o padrão 802.11g opera na mesma faixa da frequência utilizada pelo padrão 802.11b e pode transmitir a velocidade de 54 Mbps, assim como o padrão 802.11a. O padrão 802.11g utiliza a técnica OFDM para a transmissão dos dados, contudo quando se faz a comunicação com o dispositivo com o padrão 802.11b a técnica utilizada será o DSSS.

O padrão 802.11g pode se tornar um pouco lento, pois segundo Gouveia e Magalhães (2005), pode-se interligar vários componentes com as duas normas como uma placa de rede 802.11g a comunicar com a norma 802.11b. Nesta situação a rede vai comunicar com a velocidade mais baixa.

2.2.4.4 Padrão 802.11H

O padrão 802.11h é considerado uma atualização do padrão 802.11a, onde foram adicionados serviços como DFS (Dynamic Frequency Selection) e o TPC (Transmite Power Control).

O serviço de DFS permite que o sistema alterne e escolha de forma automática o canal para comunicação, diminuindo as interferências com outros sistemas. Já o serviço de TPC permite que a placa de rede do transmissor do sinal ajuste a potência do sinal de acordo com a distância do receptor, proporcionando economia de largura de banda e sinal.

2.2.4.5 Padrão 802.11N

Com o 802.11n, os fabricantes chegaram próximos do que era fisicamente possível transmitir usando uma faixa de frequência de apenas 23 MHz e um único transmissor. Porém, chegaram à conclusão que algumas melhorias deveriam ser feitas. Entre estas melhorias cita-se a combinação de melhorias nos algoritmos de transmissão e do uso do MIMO (multiple-input-multiple-output) para solucionar o problema de se alcançar os 100 megabits de transmissão. Segundo Alecrim (2008, p. 00), "... o MIMO permite que a placa utilize diversos fluxos de transmissão, utilizando vários conjuntos transmissores, receptores e antenas, transmitindo os dados de forma paralela".

2.2.4.6 Padrão 802.11e

O padrão 802.11e tem por objetivo base fortalecer a entrega e transmissão de serviços de multimídia e proporcionar a qualidade de serviço (QoS) à padrão 801.11.

Gouveia e Magalhães (2005) Engst e Fleishman (2004) corroboram que "com este padrão certos tipos de tráfegos possuem prioridade em relação ao outro em uma rede sem fio".

Ainda segundo Gouveia e Magalhães (2005, p. 00), "O QOS (Quality of Service) tem a ver com garantias quanto a transmissão de dados e porcentagens da mesma. Enquanto que o serviço de multimídia permite o funcionamento de componentes como o VOIP (Voice Over IP)."

2.2.4.7 Padrão 802.11i

O padrão IEEE 802.11i, homologado em junho de 2004, foi desenvolvido com o objetivo de prover uma melhor segurança na comunicação, corrigindo as vulnerabilidades que o protocolo WEP apresentava.

Tal padrão refere-se a mecanismos de autenticação e privacidade, podendo ser implementado aos vários protocolos hoje existentes. Tal padrão tem como novo método de criptografia a utilização de um maior poder computacional do NIC (Network Interface Card) durante o processo de codificação/decodificação, impossibilitando, portanto, uma única atualização do firmware.

2.2.4.8 Padrão 802.1X

O IEEE 802.1x é um link padrão de autenticação de camada de controle de acesso baseado em portas. Ele foi originalmente concebido em redes com fio, posteriormente, renovada para atuar em redes de área locais sem fio (WLAN). O 802.1x é utilizado para adicionar autenticações baseados em usuários cadastrados em servidores ou repositórios únicos como RADIUS (Remote Authentication Dial-In User Service) e EAP. O padrão basicamente identifica e autentica os usuários através de uma chave de reconhecimento.

Silva e Duarte (2009,) afirmam que “a sua implementação pode ser feita via software, hardware ou embarcados em dispositivos específicos, oferecendo interoperabilidade e flexibilidade para a integração de componentes e funções”.

Segundo Engst e Fleishman (2004) o modo de funcionamento deste padrão, “consiste em colocar um ponto de acesso para controlar o acesso à rede. Seu trabalho é garantir que só as pessoas autorizadas tenham acesso à rede, e para isso fornece credenciais que podem variar de um simples nome de utilizador e um password ou até, por exemplo, uma autenticação mais robusta usando certificado digital”.

2.3 Mecanismos de Segurança

O conhecimento aprofundado de mecanismos de segurança em rede sem fio são fatores que contribuem para a obtenção de nível de segurança mais elevado. Para alcance deste nível de excelência medidas como: configuração apropriada, criptográfica devidamente implementada, forte autenticação e constante monitoramento das redes sem fio, são fatores que fortificam a segurança da informação.

De acordo com Silva (2005,),

> [...] é necessário ter um conhecimento razoável de todos os padrões disponíveis e o que eles têm a oferecer e, de acordo com sua aplicação, objetivo e politica de segurança, implementar o nível correto. Ser o último padrão desenvolvido e disponível não garante que a segurança será eficiente e que ele será o mais seguro, tudo vai depender da sua configuração. Será preciso fazer uma avaliação de todo o conjunto e decidir

> com base nos equipamentos que irá utilizar e na sua experiência, objetivando o melhor custo".

2.3.1 Endereço MAC

Para que cada dispositivo de rede funcione de forma correta, faz-se necessário a identificação de cada dispositivo, ou seja, para que funcione de forma eficaz e eficiente cada equipamento deve ser controlado com um número de registro das placas de rede. Este número é único para cada equipamento fabricado, permite de forma unívoca identificar um equipamento em relação a qualquer outro fabricado mundialmente (RUFINO, 2005).

De acordo com Shikota (2006), uma das formas para limitar o acesso não legitima na rede sem fio é mediante o registro dos endereços MAC de cada dispositivo cliente no ponto de acesso. Como esse endereço é único para cada dispositivo, apenas os dispositivos registrados no ponto de acesso terão acesso permitido, ignorando os dispositivos não registrados que possam tentar entrar em sua área de atuação.

2.3.2 Criptografia

As técnicas de criptografias se propagam há milhares de anos. O desenvolvimento da criptografia foi acompanhado pelo desenvolvimento das técnicas de comunicação, onde diversos padrões e politicas de criptografia surgiram e evoluíram principalmente nos meios computacionais visando a segurança no processo de transmissão dos dados.

A comunicação sem fio proporcionou grandes danos no processo de transmissão de dados através do ar, onde os dados podem ser facilmente interceptados. Dada à fragilidade, houve a necessidade de desenvolvimento de técnicas de criptografia em redes sem fio, proporcionando uma maior segurança e privacidade durante a utilização das tecnologias que utilizam as redes sem fio.

2.3.2.1 *Wired Equivalent Privacy* (WEP)

O protocolo de segurança WEP foi introduzido no padrão IEEE 802.11 em 1999. Ele provê dois métodos de autenticação de dispositivos, usa o algoritmo de

criptografia RC4 (Ron's Code #4) para prevenir a leitura de dados dos usuários que transitarão na rede e utiliza o CRC-32 (Cyclic Redundancy Cheks) para verificação da integridade de dados. O WEP pode ser utilizado tanto no modo de operação Ad-Hoc quando no modo com infraestrutura.

Para Rufino (2005, p. 00) “WEP é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens tracejadas”.

a) Autenticação: existem dois tipos de autenticação para o protocolo WEP: Chave Compartilhada (Share Key) e Sistema Aberto (Open System).

O processo de autenticação por Chave Compartilhada necessita que o usuário e o ponto de acesso possuam uma mesma chave. Na Figura 5 é mostrado o processo de autenticação por chave compartilhada. O usuário envia uma solicitação de autenticação ao ponto de acesso que em resposta envia um texto-plano sem criptografia, o chamado texto-desafio (challenge text). O usuário por sua vez usa sua chave pré-configurada para criptografar o texto-desafio, retornando o resultado ao ponto de acesso. O Acessa Point (AP) descriptografa com sua própria chave e compara o texto obtido com o texto-desafio anteriormente enviado. Se o texto for o mesmo, o cliente é autenticado, caso contrário o cliente não consegue se associar à rede.

Figura 5 - Autenticação por chave compartilhada.

Fonte: Farias (2006)

O Sistema Aberto permite que qualquer dispositivo se associe à rede. Para isto é necessário informar o Service Set Identifier (SSID) da rede. O SSID pode

ser adquirido através de pacotes do tipo BEACON. Estes pacotes não possuem criptografia padrão e são periodicamente enviados em broadcast pelo Ponto de Acesso. Além do SSID, estes pacotes contem outras informações sobre a rede como, por exemplo, a taxa de transmissão, o canal de transmissão, etc. Na Figura 6 é mostrado o processo de autenticação WEP com sistema aberto. Basicamente o dispositivo envia uma solicitação de autenticação ao ponto de acesso que por sua vez envia uma mensagem informando que o dispositivo foi autenticado. E o cliente associa-se ao ponto de acesso, estabelecendo o processo de comunicação.

Figura 6 - Autenticação por chave aberta
Fonte: Farias (2006)

b) Integridade: para o processo de verificação de integridade dos dados recebidos, o WEP adiciona à mensagem a ser enviada um Integrity Check Value (ICV). O ICV nada mais é que um típico CRC adicionado à mensagem original antes da conclusão da criptografia. Quando um usuário ou ponto de acesso recebem uma mensagem, a decodificação e calculo do CRC-32 da mensagem é realizada, conferindo com o CRC-32 informado no campo ICV. Se forem distintas, a mensagem é descartada.

c) Confidencialidade: o protocolo WEP opera na camada de enlace de dados e para tornar as mensagens confidenciais apenas o ICV e as mensagem são criptografados, o protocolo WEP utiliza o algoritmo de criptográfico *Route Coloniale* 4 (RC4). O mesmo foi projetado por Ronald Rivest em 1987 e foi publicado em 1994, utiliza de um vetor de inicialização (IV – Initialization Vetor) de 24 bits e uma chave secreta compartilhada (secret shared key) de 40 ou 104 bits.

O RC4 é dividido em dois algoritmos: Pseudo-Random Generation Algorithm (PRGA) e Key-Scheduling Algorithm (KSA). O PRGA executa um swap e

gera um byte como saída que será utilizado na operação XOR. O KSA é bem simples, ele inicializa um array de 256 posições com os valores de 0 a 255. Logo após, executa um série de swaps, permutando o array. A permutação é feita de acordo com a chave, chaves diferentes permutam o array de formas diferentes.

Segundo Linhares e Gonçalves (2010, p. 6), “Para a criptografia de cada mensagem com seu respectivo ICV um novo IV deve ser gerado, fazendo portando, o incremento de uma unidade para evitar a repetição de chaves. Uma vez que o RC4 é um algoritmo de criptografia simétrico, a mesma chave deve ser utilizada para o processo de decodificação. Por este motivo, o IV é enviado em claro concatenado à mensagem criptografada conforme é mostrado na Figura 7. Sendo este processo também conhecido como encapsulamento WEP”.

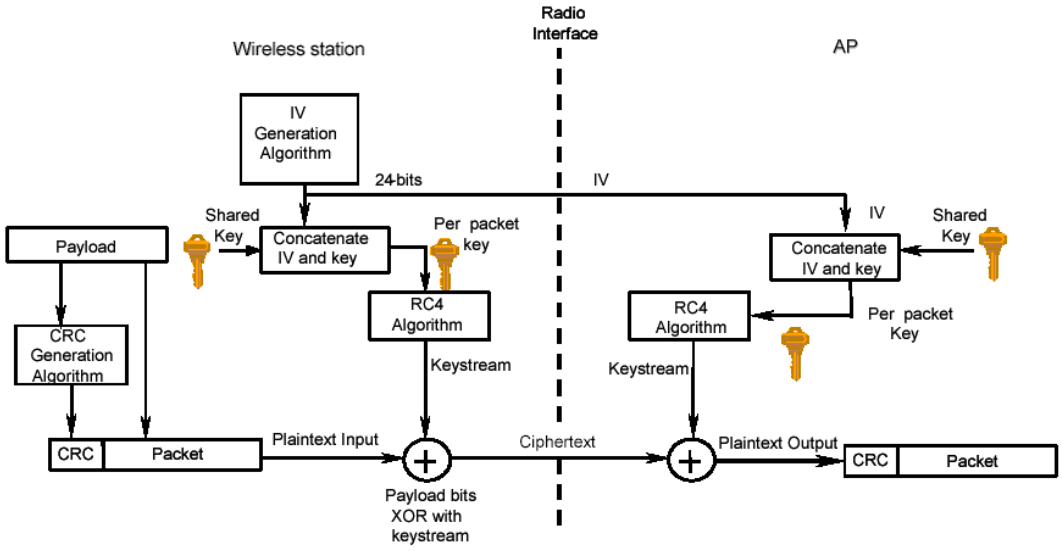

Figura 7 - Confidencialidade do protocolo WEP

FONTE: <http://www.gta.ufrj.br/seminarios/semin2003_1/ncb/02_protocolo_wep>

d) Vulnerabilidades:

Re-injeção de Pacotes: Este tipo de ataque não afeta sozinho a segurança da rede protegida pelo WEP. No entanto, pode ser usado para aumentar o tráfego na rede e assim diminuir o tempo necessário para que ataques como o FMS e o KoreK quebrem a chave WEP.

Problemas do RC4 ou ataque FMS: neste tipo de ataque o algoritmo KSA do RC4 apresenta uma fraqueza. Dada a situação, foi desenvolvido um ataque estatístico que revela a chave WEP estática. KoreK melhorou esta ataque, aumentando a probabilidade de acesto da chave com um número menor de IVs,

permitindo que o tempo de quebra de chave fosse diminuída. O AirSnort, WEPCrack e Aircrack são exemplos de ferramentas que utilizam este tipo de ataque.

Negação de Serviço (DoS – Deny of Service): este tipo de ataque caracteriza por derrubar a comunicação entre o ponto de acesso e os usuários a utilizarem o serviço. Caracteriza-se por forjar pacotes do tipo De-Authetication que invalidam o usuário na rede e enviá-los em broadcast ou diretamente para um usuário especifico usando seu endereço MAC de origem. O void11 e aircrack implementam este tipo de ataque.

Protocolo de autenticação Ineficiente: no modo de autenticação por Chave Compartilhada o atacante durante o processo de escuta de trafego ou também conhecido como ataque sniffing ter acesso a um pacote texto-desafio e sua respectiva decodificação. O atacante poderá autenticar-se sem conhecer a chave WEP.

Gerenciamento de Chaves: o protocolo WEP não possui um gerenciador de chaves, portanto a chave a ser utilizada pelos dispositivos clientes não pode ser trocada dinamicamente.

Tamanho da Chave: quando o protocolo WEP foi lançado a chave estática era de apenas 40 bits. Chaves com tal tamanho, porem facilmente serem quebradas com força bruta.

Reuso de Chaves: os 24 bits do IV permitem pouco mais de 16,7 milhões de vetores distintos. Para o ambiente computacional este número de possibilidades é considerado pequeno, podendo os IVs e as chaves usadas pelo RC4 se repetirem de tempos em tempos.

2.3.2.2 Wi-fi Protected Access (WPA)

Devido ao grande número de vulnerabilidades apresentadas pelo protocolo WEP, um grupo de trabalho do IEEE 802.11 iniciou um estudo com o intuito de desenvolver um novo protocolo que pudesse corrigir as falhas do protocolo WEP. Durante o processo do desenvolvimento, tendo em vista os problemas de segurança do WEP, o Wi-Fi Alliance adiantou o processo de autenticação e criptografia dos dados e em 2003 apresentou um novo protocolo denominado de WPA (Wi-Fi Protected Acess) (RUFINO, 2005; CERIONI, 2009).

Algumas características do WPA são:

- ✓ Não tem suporte a redes do tipo Ad-Hoc de forma diferente ao WEP;
- ✓ Trabalha em dois modos distintos de funcionamento. O primeiro destinado a redes domésticas e o segundo as redes de grandes instituições. Tendo o segundo, a possibilidade de autenticação em um servidor de autenticação centralizado;
- ✓ Trabalha com o conceito de chaves temporais, no qual já uma hierarquia de chaves. Há uma chave principal, chamada de Pairwise Master Key (PMK), de onde são derivadas outras chaves como a chave de integridade e criptografia de dados.

a) Autenticação: Conforme anteriormente citado, existem dois tipos de autenticação para as redes baseadas no protocolo WPA, o WPA Pessoal e WPA Corporativo.

WPA Pessoal: também conhecido como WPA-PSK (WPA-Pre Shared Key), possui sua autenticação feita pelo ponto de acesso. A chave é configurada manualmente em cada equipamento cliente ligado a rede.

WPA Corporativo: ao contrario do WPA Pessoal, neste o ponto de acesso não é responsável por nenhuma autenticação. Neste utiliza-se uma infraestrutura ligada a um servidor externo que utiliza o protocolo de autenticação 802.1x em conjunto com algum tipo de Extensible Authentication Protocol (EAP). Quando um usuário solicita uma autenticação, o servidor de autenticação (geralmente o RADIUS) verifica em sua base de dados se as credenciais apresentadas pelo solicitante são válidas, em caso positivo o cliente é autenticado e uma chave Master Session Key (MSK) é retornada.

As credenciais de acesso podem ser representadas através do smart cards, binômio usuário/senha, certificados digitais, biometrias, etc.

Segundo Linhares e Gonçalves (2010, p. 7), “após a autenticação, inicia-se o processo de derivação da PMK onde as chaves serão estabelecidas, este processo é chamado de 4-Way-Hadshake”. Se a autenticação foi baseada no modo PSK, a chave PMK é a própria PSK. Se não, a PMK é derivada a partir da MSK que foi compartilhada durante o processo de autenticação 802.1x/EAP. A PMK nunca é usada para encriptação ou integridade. Ela é usada para gerar chaves temporárias (Pariwise Transient Key – PTK). A PTK é um conjunto de chaves, entre elas a chave de criptografia de dados (Temporal Encryption Key – TEK ou TK) e a chave de integridade de dados (Temporal MIC Key – TMK). Ao final do 4-Way-Hadshake é

garantido que tanto o cliente quanto o ponto de acesso possuem a mesma PTK, estando prontos para troca de dados. Tal situação esta é mostrada na Figura 8:

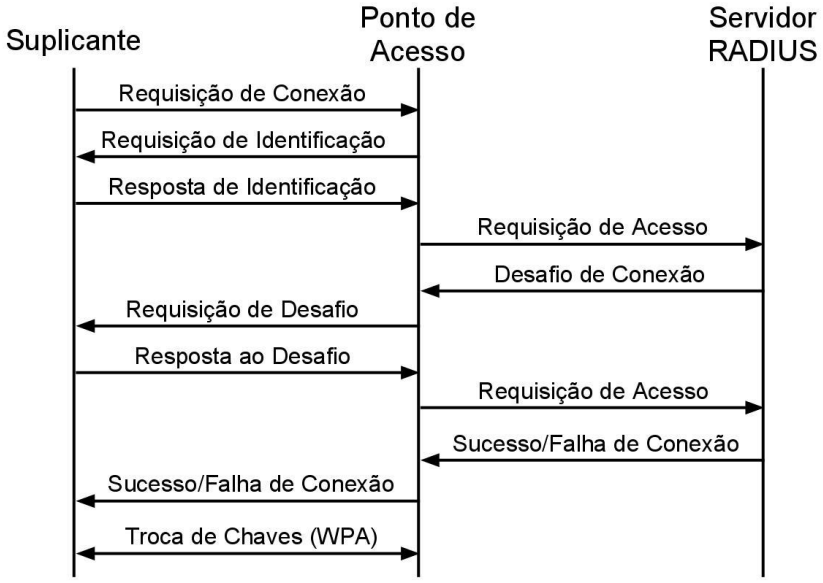

Figura 8 - Autenticação WPA Interprise (802.1x/EAP)

Fonte: Sartora et al (2009,).

b) Integridade: a integridade no WPA é composta basicamente por dois valores. Além da utilização do ICV que foi herdado do protocolo WEP, foi adicionado uma mensagem para verificação de integridade chamada de Message Integrity Check (MIC), sendo o algoritmo que implementa o MIC denominado de Michael.

Segundo André Linhares e Paulo Gonçalves (2010, pag. 11), “O Michael é uma função hash não linear, diferentemente do CRC-32. O endereço de destino, de origem, a prioridade (definida atualmente como zero, mas reservada para objetivos futuros, e.g. 802.11e), os dados e uma chave de integridade são inseridos no Michael para produzir o MIC. A saída corresponde a 8 bytes que juntamente com o ICV formam a integridade do protocolo WPA.

Portanto a integridade é representada por um total de 12 bytes, 8 gerados pelo Michael e 4 pelo CRC-32.

c) Confidencialidade: a implantação do Temporal Key Protocol (TKIP) soluciona boa parte das vulnerabilidades apresentadas pelo protocolo WEP. O TKIP também é baseado no conceito de chaves temporais, onde certa chave é utilizada por um curto espaço de tempo e posteriormente é substituída dinamicamente.

> O TKIP faz com que cada estação da mesma rede utilize uma chave diferente para se comunicar com o ponto de acesso. O problema da colisão de chaves do RC4 é resolvido com a substituição da TK antes que o IV assuma novamente um valor que já assumiu, ou seja, a cada vez que o IV assuma o seu valor inicial, o TK deve assumir um valor distinto." (VERÍSSIMO, 2003).

d) Vulnerabilidades: O WPA corrigiu muitas vulnerabilidades do protocolo WEP. No entanto, falhas em sua implementação o tornaram vulnerável.

- Negação de Serviço: O MIC possui em seu código fonte um mecanismo capaz de evitar ataques de força bruta, porém, essa proteção facilita os ataques de negação de serviço (DoS). Basicamente quando dois erros de MIC são identificados (injeção de pacotes mal formados, por exemplo) em um curto espaço de tempo o ponto de acesso cancela a conexão por 60 segundos e altera a chave de integridade.

- PSK é suscetível a ataques de dicionário: o ataque de dicionário consiste no processo de tentativa de invasão a partir de testes com palavras pertencentes a um dicionário previamente construído. O sucesso deste tipo de ataque ainda é bastante amplo, pois a grande maioria das pessoas tem costume de utilizarem palavras fáceis. Porém, vale a pena ressaltar que quando maior for a chave PSK, maior será a possibilidade de insucesso deste ataque.

2.3.2.3 IEEE 802.11I (WPA2)

O padrão WPA2 foi homologado em junho de 2004. A nova metodologia de criptografia utilizada exige um maior poder computacional do NIC (Network Interface Card) durante o processo de codificação/decodificação. O WPA2 herda a base do WPA, tendo como principais avanços, o desenvolvimento de novos algoritmos de criptografia e de integridade.

a) Autenticação: O WPA2 herdou o dispositivo de autenticação no WPA. Tendo apenas como avanço no processo de autenticação o desenvolvimento do roaming.

De acordo com Rockenbach (2008,),

> Quando um cliente se autentica, uma serie de mensagens são trocadas entre o cliente e o ponto de acesso, e quando um cliente se desloca de um ponto de acesso para outro há um atraso para estabelecer a autenticação. Para minimizar esse atraso durante o processo de autenticação, os

> equipamentos WPA2, podem dar suporte a PMK caching e Preauthentication.

Para Rockenbach (2008,).

> O PMK Caching consiste no AP aguardar os resultados das autenticações dos clientes. Se o cliente voltar a se associar com o AP, estas informações guardadas são utilizadas para diminuir o número de mensagens trocadas na re-autenticação. Já no Preauthentication, enquanto o cliente está conectado a um AP principal, ele faz associações com outros AP's cujo sinal chega até ele. De forma, quando já uma mudança de AP não há perda de tempo com a autenticação.

b) Confidencialidade e Integridade: Segundo Linhares e Gonçalves (2008) apud Rockenbach (2008) a confidencialidade e a integridade do protocolo WPA2 são garantidas pelo protocolo CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol).

Segundo Rockenbach (2008,), “o protocolo CCMP utiliza o padrão de criptografia simétrico AES (Advanced Encryption Standard) para fornecer uma criptografia mais segura”. E de acordo com Rocha (2006, p. 34), “o AES permite a utilização das chaves de 128, 192 ou 256 bits e trabalha com diferentes modos de operação, que alteram a forma como o processo de criptografia é realizado”. Os modos de operação tem o objetivo de prevenir que uma mesma mensagem, quando criptografada, gere o mesmo texto cifrado.

De acordo com Maia (2009, p. 40), “o modo de operação do AES implementado pelo WPA2 e o CCM. O CCM utiliza o modo de operação conhecido com CBC (Cioher Block Chaining)”. Nesse modo de operação, é feita uma operação XOR entre cada novo bloco de texto cifrado. Assim o texto no passo anterior é utilizado como entrada no processo de criptografia subsequente. No primeiro passo, como ainda não existe um texto cifrado, é utilizado o vetor de inicialização.

O processo de operação do CBC é mostrado na Figura 9:

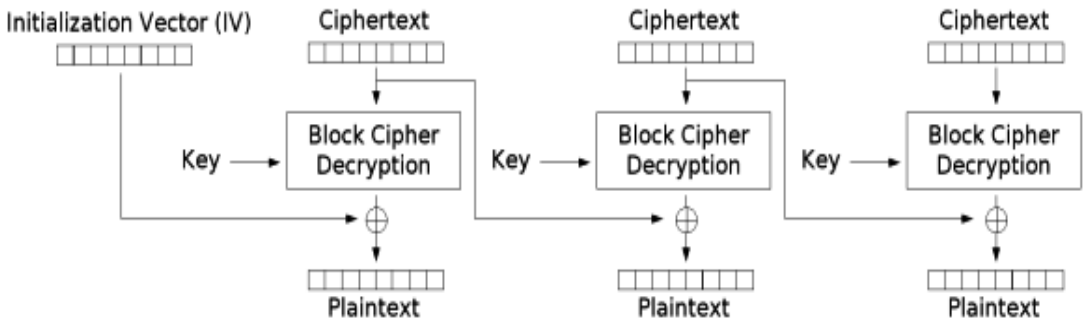

Figura 9 - Processo do CBC

Fonte: Sartora et al (2009,).

d) Vulnerabilidades: de todos os protocolos conhecidos, o WPA2 é o mais seguro atualmente. Algumas vulnerabilidades conhecidas são:

- PSK pequeno: o protocolo WPA2 permite a utilização do PSK por parte do usuário com menos de 20 caracteres, o que torna suscetível a ataques de dicionário por exemplo.
- Negação de Serviço: é possível criar falsos quadros de gerenciamento e controle do tipo *authentication*. O que resulta na negação de acesso por parte do ponto de acesso para o cliente em cerca de 60 segundos. Além disso, existem outros ataques como: RSN *Information ELemente* (RSN IE), *Poisoning* e 4-*Way-Handshake Blocking*.

2.3.3 Firewall

Atualmente o Firewall é uma ferramenta indispensável para garantir a segurança nos ambientes em redes computacionais, pois constitui como uma barreira que fica entre a rede interna e a externa, atuando com a implementação de um conjunto de regras, que permite o controle do tráfego que entra e sai da rede.

> O firewall também pode assumir o papel de gateway entre duas redes, podendo estas redes ser uma Wi-Fi e a outra LAN (Local Area Network), desta forma é possível isolar as duas redes, evitando que pessoas não autorizadas que possuem acesso a uma rede, não tenham o mesmo privilégio em acessar a outra, bloqueando como desejado o tráfego que ocorre do lado Wi-Fi para a LAN e da LAN para Wi-Fi.” (JUNIOR et AL, 2005).

De acordo com Peterson e Davie (2004), os firewalls podem ser classificados em duas categorias: baseado em filtro e baseado em proxy.

a) Baseado em filtro: Os firewalls desse tipo são mais simples e mais utilizados. São configurados como uma tabela de endereços IP e portas de acesso para origem e destino. Este tipo de firewall decide ou não encaminhar um pacote com base em lista de acesso, que é configurado manualmente pelo administrador do sistema (PETERSON; DAVIE, 2004; MONTEIRO; BOAVIDA, 2000).

> A vantagem dos firewalls desse tipo referem-se ao baixo custo e a facilidade de configuração. Como desvantagem há a destacar as implementações em termo de degradação de desempenho de router, a relativa facilidade com que se cometem erros de configuração das listas de acessos e o fato de só atuarem nos níveis protocolares inferiores o que impede filtragens com base nas aplicações e no comportamento dos utilizadores." (MONTEIRO; BOAVIDA, 2000,).

b) Baseado em proxy: Segundo Medeiros (2004), "neste tipo de firewall o controle é executado por aplicações especificas, denominadas proxies, para cada tipo de serviço a ser controlado".

Tal configuração resulta na perda significativa de desempenho, pelo fato da grande quantidade de dados a serem analisados durante o processo de comunicação, porém, aumenta o controle e gestão da segurança.

A desvantagem desse tipo de firewall tem a ver com a complexidade de configuração e manutenção do proxy para cada aplicação, sendo que muitos não trabalham muito bem com proxy constituindo assim pontos únicos de falhas. (Monteiro e Boavida, 2000).

2.4. Riscos, Ameaças e Vulnerabilidades

Toda tecnologia possui a sua limitação, e a rede sem fio não é diferente das demais tecnologias. Portanto, para que se garanta ou alcance a tão desejada segurança da informação se faz necessário à disseminação do conhecimento dos riscos, ameaças e vulnerabilidades que podem ser exploradas pelos possíveis invasores. Levando em conta o pensamento anterior, os principais riscos para as redes sem fio são apresentados a seguir.

2.4.1 Configuração d*efault*

Para Rufino (2005,) é “A segurança das redes sem fio é elaboradas desde a sua concepção, a desde esse momento tem evoluído rapidamente”. Atualmente os mais variados tipos e modelos de equipamentos para montar uma rede sem fio é encontrada no mercado, os mais variados tipos de mecanismos de seguranças já saem com estes dispositivos de fábrica, porém, nem todas as vezes eles vem ativos. Os fabricantes visam em primeiro lugar proporcionar uma instalação simples e amigável para os seus clientes, com isso, os mais variados produtos vem com o seu padrão de configuração das fábricas.

Souza et al (2006) consideram que este fato faz com que as redes sem fio implantadas por administradores com poucas experiências ou com prazos de implementações ultrapassados, deixem a rede extremamente vulnerável. Isso porque na grande maioria das vezes essas redes são implementadas sem qualquer alterações nas configurações dos padrões default ou padrão vindos das fábricas. O mesmo autor aponta como exemplo o password de administração e endereço Internet Protocol (IP) padrão, caso essas configurações não forem alteradas, a rede fica extremamente vulnerável.

> Portanto a primeira medida a ser feita ao instalar uma rede sem fio, é a mudança de todos os valores que saem de fábrica por padrão, como as senhas de acesso a parte administrativa, o endereço IP, as chaves de WEP ou WPA, o SSID, ou seja, tudo que puder ser alterado a fim de não identificar a rede. (MARTINS, 2005,).

2.4.2 Segurança física

De acordo com Rufino (2005, p. 57), “antes de montar uma rede sem fio, se faz necessário efetuar um estudo cuidadoso, que engloba desde o equipamento utilizado, e seus potenciais e a área de abrangência, bem como o mecanismo de segurança usado de modo a não comprometer o bom funcionamento de uma rede, de a não permitir o acesso de utilizadores não autorizados”.

Geralmente a segurança física é tratada com certa indiferença, sendo as ameaças internas consideradas como o risco principal em relação à segurança computacional. De acordo com a ABNT NBR ISO/IEC 27002 (2005), o objetivo de uma área segura é prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

Convém logicamente, que as instalações de processamento da

informação sejam mantidas em locais seguros, protegidas por perímetro de segurança previamente auditado e com barreiras de segurança.

2.4.3 Posicionamento do ponto de acesso

O posicionamento adequado do ponto de acesso pode ajudar a aumentar a segurança da rede sem fio, uma vez que estará em alinhamento com a segurança física do ambiente na qual está inserido. Segundo Rufino (2005), a qualidade e a segurança da rede sem fio esta ligada diretamente ao posicionamento do ponto de acesso. Tal pensamento é baseado na ideia de o sinal do ponto de acesso é enviado para todas as direções, neste caso se faz necessário localizar o ponto de acesso em um lugar estratégico que possibilite o sinal ecoar somente pela área pretendida de cobertura, evitando assim que o sinal saia da sua área de segurança.

Na Figura 10 é mostrado do lado direito (do leitor), o posicionamento incorreto do ponto de acesso, proporcionando a “fuga” de sinal da área de atendimento. E do lado esquerdo, da mesma figura, é demonstrado o comportamento da cobertura quando o ponto de acesso estiver bem posicionado, ou seja, no ponto central da área onde se deseja que o sinal têm a máxima qualidade do sinal.

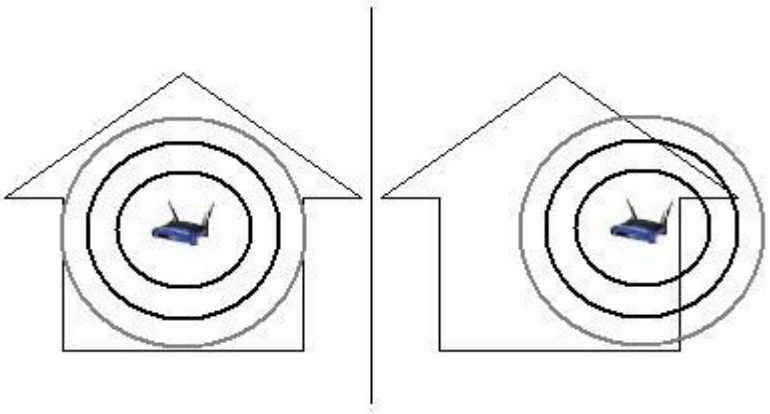

Figura 10 - Posicionamento do ponto de acesso
Fonte: Desconhecido.

2.5 A técnica do *wardriving*

Os sinais das redes sem fio se propagam no ambiente através ar, tendo os dados transmitidos por toda a faixa abrangente, sem o conhecimento do local

físico dos equipamentos clientes que se comunicam com o ponto de acesso.

Portanto, qualquer dispositivo dentro da área de alcance dos sinais emitidos pelo ponto de acesso recebe os dados trafegados e aqueles que não estão autorizados descartam os pacotes que não forem endereçados ao dispositivo em questão. Um dos grandes problemas é a falta de controle sobre a área de cobertura do sinal, podendo um atacante efetuar a captura e analise desses pacotes enviados de forma aleatória e assim conseguir acesso ilegal sem está próximo ao ponto de acesso.

Tal prorrogativa, colaborou para o surgimento da técnica conhecida como Wardriving.

> Wardriving é o ato de mover-se ao redor de uma área especifica e mapear a população de pontos de acesso wireless para um propósito estatístico. Estas estatísticas são então utilizadas para elevar a atenção sobre problemas de segurança associados a estes tipos de rede (tipicamente wireless). (HURLEY; FAIRBAIRN, 2004, p.12).

A definição aceitável para wardriving entre as pessoas que praticam este tipo de atividade conceitua que esta técnica não é obrigatória à utilização de um automóvel. Wardriving é realizado por qualquer um que se mova ao redor de uma determinada área a procura de dados.

Tal técnica foi desenvolvida por Pete Shipley, em abril de 2001. Outros tinham que correr por ai com laptops, lendo e tomando notas (muitas vezes no papel) sobre os pontos de acesso. Mas Peter foi o primeiro a automatizar o processo com software dedicado, e também a primeira a integrar os dados de localização GPS com bancos de dados de pontos de acessos detectados. Tempos depois Marius Milner NetStumbler desenvolveu uma ferramenta mais conhecida para a prática do wardriving, o NetStumbler.

O termo “war” de wardriving não tem nada haver com guerra. O termo é descendência do wardialing, que era a prática de discar números de telefone aleatórios através do computador para ver se poderia encontrar um modem resposta para conexão a internet.

O wardriving proporciona uma oportunidade única par avaliar o crescimento de um segmento de mercado de tecnologia por inspeção direta. Em outros termos, não precisamos ser um vendedor ou empresa de pesquisa de renome para quantificar as redes sem fio de uma determinada área.

O wardriving pode ser considerado um conjunto de métodos que auxiliam

na identificação das redes sem fio, capturam os pacotes e analisam informações que possibilitem o acesso as redes. A técnica pode ter o potencial de sucesso aumentando a partir da utilização de equipamentos e conjuntos de softwares especiais, que facilitam a obtenção de informações.

3. ESTUDO DE CASO

3.1 Materiais e métodos

O principal objetivo deste trabalho é avaliar e analisar o grau de vulnerabilidades das redes sem fio em 5 (cinco) grandes bairros da cidade de São Luís do Estado do Maranhão.

A metodologia adotada foi o levantamento bibliográfico, pois, segundo Martins (2007, p. 35), “se vale de estudo para conhecer as contribuições cientificas sobre determinado assunto”. E se caracteriza como exploratória porque, na concepção de Gil (2008, p. 27), “busca proporcionar visão geral, de tipo aproximativo, acerca de determinado fato”, já que ao longo do estudo o tema será explorado e aplicado de forma a proporcionar um rico conhecimento.

Para o desenvolvimento da proposta inicialmente efetuou-se testes de invasão em redes sem fio que utilizam as criptografias: WEP, WPA e WPA2. A partir dos resultados obtidos, verificaram-se quais tipos de criptografias foram as mais seguras. O segundo passo foi utilizar a técnica do wardriving para chegar ao quantitativo de redes sem fio de cada um dos 5 (cinco) bairros analisados, apresentando as características de cada um dos pontos de acessos identificados.

De dentro de um veiculo automotor foi efetuada a movimentação ao redor e nas proximidades da área física dos bairros analisados. Também foram necessários pontos internos fixos para aquisição de informações que não foram detectadas externamente. Sendo assim possível determinar a quantidade total de pontos de acessos às redes sem fio nestes locais. Após a identificação dos pontos de acessos, foram utilizados alguns softwares para consolidar os resultados das varreduras. A partir deste levantamento foi realizado o cruzamento da quantidade de redes sem fio identificadas com os seus respectivos tipos de tecnologia de criptografia.

3.1.2. Equipamentos utilizados

Para a realização dos testes nos ambientes de redes sem fio, foi utilizado além do automóvel, um notebook DELL INSPIRION. Na Tabela 2 são apresentas as especificações do equipamento utilizado.

.

Sistema Operacional	*KALI LINUX 3.0*
Memória	8 Gb
Adaptador de rede *Wireless*	Atheros Communications Inc. AR9285 *Wireless* Network Adapter (PCI-Express)
Processador	Intel@ Core i7 4500U CPU @ 1.8GHz x4

Tabela 2 - Especificações do equipamento utilizado

Fonte: Autor

3.1.3 Ferramentas utilizadas

As ferramentas utilizadas para identificação e mapeamento das redes locais, são as seguintes:

a) KALI LINUX 3.: O Kali Linux é um sistema operacional Linux baseado no Debian, com mais de 300 ferramentas para estudos e análise, focados em testes de invasões e auditoria de segurança da informação;

b) Gerenciador inSSIDer: É um gerenciador de conexões utilizado durante a prática do wardriving. Com ele é possível efetuar uma varredura de busca das redes sem fio ao alcance da antena da máquina hospedeira, captando a força do sinal em intervalos de tempo definidos e ainda determina durante a varredura todas as especificações lógicas da rede, inclusive o tipo de criptografia utilizada;

c) Kismet: É uma ferramenta para identificar e analisar a segurança de redes wireless.

É capaz de encontrar redes que estão ocultas (ESSID não divulgado);

d) Aircrack: É uma suíte de aplicações poderosa, capaz de efetuar uma análise de tráfego para auditoria em redes sem fio. Através dos pacotes coletados é possível efetuar a quebra da criptografia das redes sem fio (WEP, WPA e “WPA2”);

e) Reaver: Uma ferramenta capaz de comprometer a segurança de redes com criptografia WPA/WPA2, considerada a mais forte atualmente. A quebra de segurança acontece em cima da tecnologia WPS (Wi-fi Protected Setup) utilizada em equipamentos SOHO (Small Office – Home Office) (Figura 11).

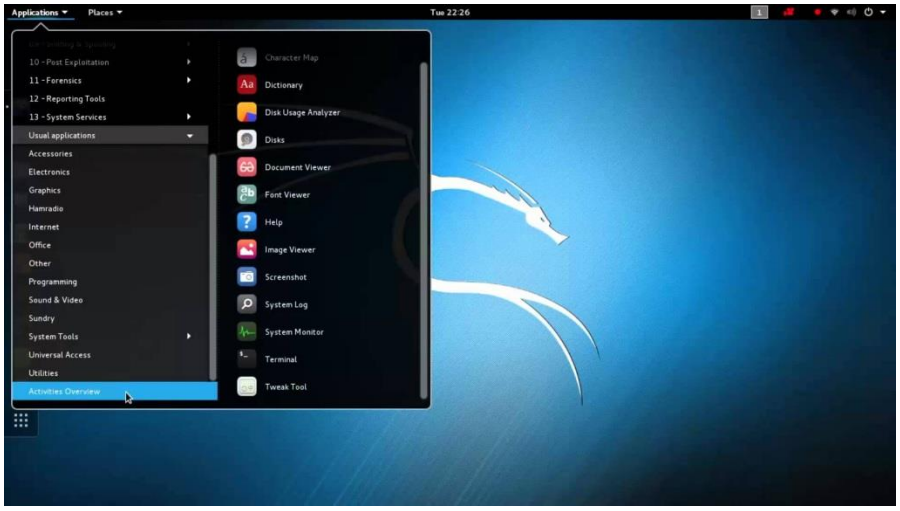

Figura 11 - Tela inicial do Kali Linux 3.0

Fonte: Google web

3.1.3.2 Gerenciador InSSIDer

O gerenciador de conexões utilizado durante a prática do Wardriving foi o inSSIDer. Com ele é possível efetuar uma varredura em busca das redes ao alcance da antena da maquina hospedeira, captando a força do sinal em intervalos de tempo definidos e ainda determina durante a varredura o tipo de criptografia utilizada ou não pelas mesmas.

O programa usa o aplicativo nativo para Wi-fi, monitorando a placa de rede sem a necessidade de utilização de componente extra. Os resultados são apresentados em colunas classificadas por endereço MAC, SSID, canal, etc. Este assinala aleatoriamente uma cor para cada ponto de acesso (PA). Essas cores são usadas para exibir a força do final, podendo também efetuar um comparativo entre as redes em um único gráfico.

3.1.3.3 Kismet

Segundo Marimoto (2006, p. 56),

> O *Kismet* é uma ferramenta poderosa, que pode ser usada tanto para chegar a segurança de sua própria rede wireless quanto para checar a presença de outras redes próximas. Ao ser ativado ele coloca a placa wireless em modo de monitoramento (*rfmon*) e passa a escutar todos os sinais que cheguem até sua antena. Mesmo que o ponto de acesso seja

> configurado para não divulgar o ESSID e a criptografia ativa o mesmo detecta.

Utilizando o kismet é possivel capturar os pacotes que trafegam pelo ar sem a necessidade de associação direta a um ponto de acesso, escutando as transmissões de uma forma praticamente indetectável. A sua principal limitação é que, enquanto a placa estiver sendo utilizada em modo de monitoramento ou o chamado promiscuo, não é possível utilizar a mesma placa para outros fins.

O Kismet é um software livre, ou seja, esta ferramenta possui o seu código-aberto que inclui um grande aparato de ferramentas e opções de filtragem. No Kali linux por padrão o Kismet já vem instalado, para abrir o programa basta seguir os seguintes passos:

1º – Abrir o terminal e executar o seguinte comando como super usuário:

sudo kismet

A intenção desta pesquisa não é analisar o trafego de pacotes, mas para o experimento o kismet servirá como tecnologia de levantamento de informações sobre os pontos de acesso.

3.1.3.4 Aircrack-NG

O aircrack é um suíte de aplicações muito poderosa, capaz de efetuar uma analise de trafego para auditoria em redes sem fio. Basicamente ele implementa a ataque de FMS padrão juntamente com algumas características de otimizações adquiridas do tipo de ataque korek, tornando o ataque muito mais rápido e eficiente comparado as demais ferramentas.

O único problema para este tipo de ataque é que as quantidades de dados coletados implicam diretamente no tempo de quebra da chave. Em uma rede onde o tráfego é baixo, o processo de quebra pode demorar dias ou semanas. Já em ambientes onde o trafego é alto, a quebra pode levar horas ou até mesmo minutos, alguns atacantes também se utilizam de técnicas mais inteligentes que geram grande quantidade de trafego para capturar textos cifrados.

Esta ferramenta já vem inclusa no conjunto das aplicações nativas do sistema operacional Kali Linux, para os demais sistemas operacionais é necessário efetuar o download que pode ser encontrado no endereço <http://freshmeat.net/projects/aircrack/>. Para instalá-lo em outras distribuições do Linux,

basta efetuar o seguinte procedimento:

1º – Abrir o terminal e executar o seguinte comando como super usuário: # sudo apt-get install air crack-ng

Para abri-lo no sistema operacional Kali Linux, basta executar o seguinte comando no terminal: # aircrack-ng

3.1.3.5. Reaver

O reaver é uma ferramenta nova capaz de comprometer a segurança de redes com criptografia WPA/WPA2, considerada a mais forte atualmente. Na verdade, a criptografia não está comprometida, mas sim uma tecnologia que acompanha a grande maioria dos pontos de acessos atuais.

A quebra de segurança acontece em cima da tecnologia WPS utilizada em equipamentos SOHO (Small Office – Home Office). O protocolo WPS (Wi-fi Protected Setup) é vulnerável a ataques de força bruta, permitindo o atacante recuperar um WPS PIN de um ponto de acesso e, posteriormente, a senha WPA/WPA2 dentro de algumas horas.

O Reaver é uma ferramenta desenvolvida pela Tactical Network Solutions que explora uma falha do projeto do protocolo WPS. Tal vulnerabilidade expõe um ataque de side-channel, permitindo a extração da chave pré-compartilhada (PSK) usada para dar segurança da rede. Em média, o Reaver irá recuperar a senha em texto plano do ponto de acesso alvo em 4-10 horas.

Para instalar o Reaver basta digitar o comando a seguir no terminal:

1º – Abrir o terminal e executar o seguinte comando como super usuário: # sudo apt-get install reaver.

3.2 Resultados

3.2.1 Resultados – Vulnerabilidades nos protocolos de criptografia

Nesta etapa foram realizados testes de invasão em algumas das redes sem fio dos bairros, tendo por objetivo obter uma amostragem dos protocolos de criptografia e evidenciar as suas vulnerabilidades. As redes sem fio analisadas como experimento foram: uma rede sem fio com criptografia WEP encontrada no Bairro A,

outra WPA escolhida no Bairro B e uma terceira com criptografia WPA2 escolhida no Bairro C.

3.2.1.1 Tentativa de quebra da chave WEP no Bairro A

Muitos pontos de acesso, principalmente os antigos, utilizam versões do WEP, que são as mais fáceis de quebrar. Nesta etapa, é demonstrado o processo de quebra de criptografia WEP.

O primeiro passo é executar o Kismet para obter informações da rede sem fio como: SSID e BSSID (nome da rede sem fio de serviço), endereço MAC (endereço físico da Interface de comunicação) de alguns clientes do ponto de acesso selecionado, o canal do ponto de acesso e o tipo de encriptação da rede, no caso, o WEP.

O próximo passo é necessário abrir outro terminal. O objetivo agora é falsear o endereço MAC de sua placa de rede com a do ponto de acesso à rede intencionada.

3º – Abrir o terminal do KALI LINUX e executar o seguinte comando: # ifconfig wlan0 down - // ”derrubar” a placa wireless para poder trocar o endereço MAC da placa de rede.

4º – O comando a seguir vai permitir falsear o endereço MAC: # macchanger -m 00:23:e5:1b:df:0d wlan0

5º – Se o Kismet não estiver executando automaticamente a placa de rede em modo de monitoramento (também conhecido como promíscuo), torna-se necessário executar o comando para coloca-la em modo monitor: # airmon-ng start wlan0 - // caso o comando anterior não seja executado, é porque o Kismet já está executando a placa em modo de monitoramento.

6º – Nesta etapa foi executado o comando aireplay somente para gerar uma quantidade suficiente de tráfego na rede, tal comando servirá para gerar pacotes mais rapidamente, diminuindo o tempo para quebra da criptografia: # aireplay-ng -2 -p 512 -c ff:ff:ff:ff:ff:ff -b <BSSID> -h <MAC falseado> wlan0 - // as partes em destaque devem ser substituídas pelas informações obtidas pelo Kismet. Ficando assim: # aireplay-ng -2 -p 512 -c ff:ff:ff:ff:ff:ff -b 00:23:69:fa:9e:d1-h 00:23:e5:1b:df:0d wlan0

7º – Agora se deve criar um arquivo em uma pasta local. Este arquivo armazenará IV's (pacotes), o nome do arquivo foi chamado de test e sua extensão é .ivs. O comando anterior deverá continuar executando, portanto, deve-se abrir outro terminal e executar o comando a seguir: # airodump-ng -channel <Nº canal>-bssid <BSSID>-ivs –write <nomeArquivo> wlan0

8º – Por fim será foi executado o comando aircrack-ng que efetivamente efetuará a tentativa de quebra da criptografia WEP, também deverá ser aberto outro terminal para execução: # aircrack-ng -f 4 -n 128 test.ivs - // Observe-se que o nome do arquivo com os IV's armazenados é chamado.

O resultado só foi possível graças ao armazenamento de um pouco mais de 65.000 pacotes em 4 dias de captura. A senha do ponto de acesso com endereço MAC ligado a ela (C8:3A:35:10:BC:90) é: Beila. Na Figura 12 mostra o exemplo do momento do processo de captura de pacotes IV's:

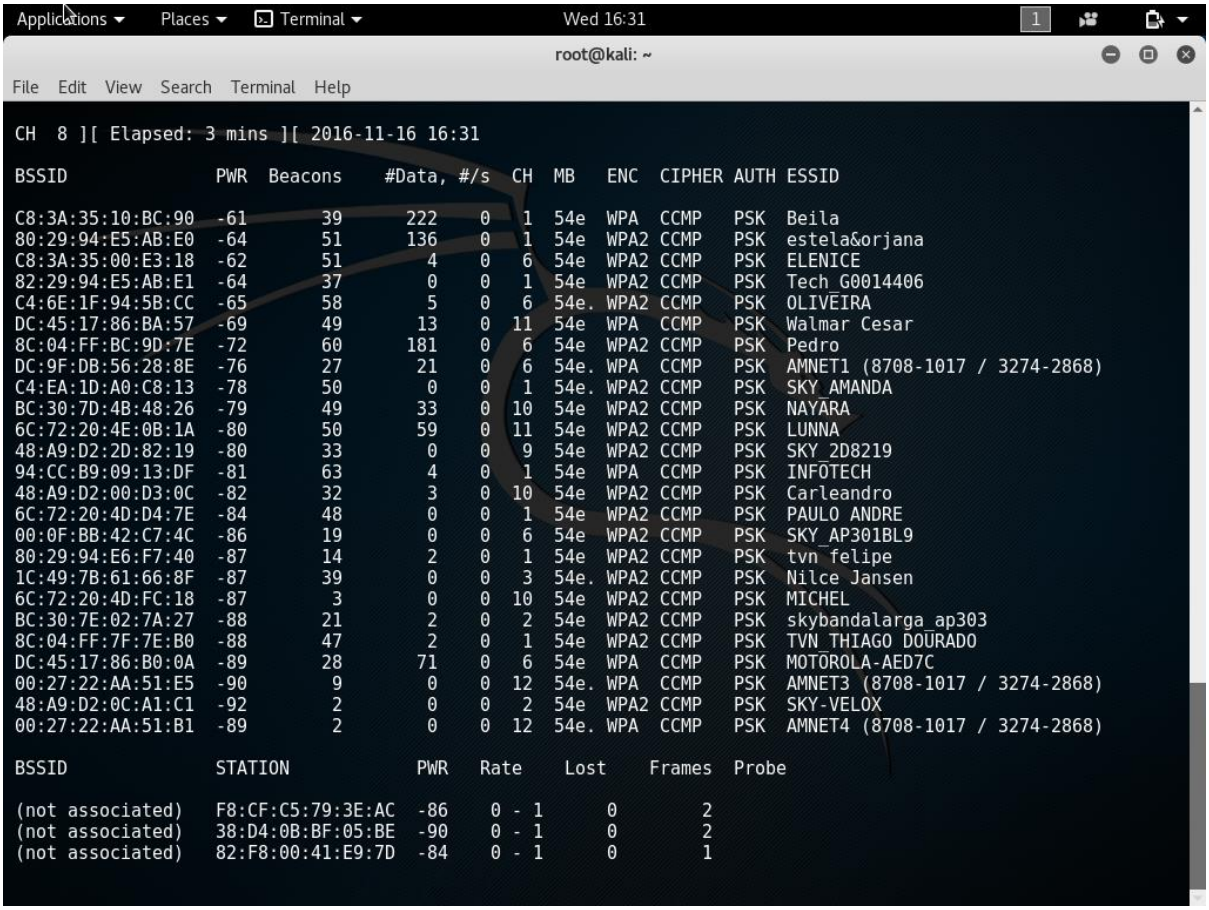

Figura 12 - Processo de captura de pacotes IV's

3.2.1.2 Tentativa de quebra da chave WAP no Bairro B

O processo de quebra da chave WPA é parecido. Porém para a tecnologia de criptografia WPA é mais difícil de ser burlada. Para esta tarefa fez-se será necessário a utilização do ataque de força bruta que visam descobrir passpharase, baseadas em listas de dicionário, que podem ser encontradas fazendo a busca por “wordlists” no Google, também pode ser encontrado no repositório no seguinte endereço <http://www.outpost9.com/files/WordLists.html>. Essas listas são armazenadas no diretório /usr/share/dict/words.

1º – Deverão ser seguidos os passos do tópico anterior para colocar a placa em modo monitor novamente. Isso serve para obter os dados da rede WPA e falsear um novo MAC para a placa wireless da maquina atacante.

2º – Abrir o terminal e executar o executar novamente o comando airodump-ng para capturar as transmissões, em outro terminal deverá rodar o aireplay-ng para desconectar o cliente e o obrigar a se reconectar ao ponto de acesso, de forma que os pacotes sejam capturados.

3º – Esse comando cria um arquivo chamado lost.cap onde serão armazenados os pacotes da rede do canal referenciado com o respectivo ponto de acesso.

airodump-ng -w lost –channel <nº canal> wlan0

4º – O comando a seguir irá simular uma solicitação de desconexão da maquina atacante ao ponto de acesso, desconectando o cliente especifico. O cliente certamente tentará se reconectar, fazendo com que a autenticação seja realizada novamente, neste momento os pacotes são capturados.

aireplay-ng -0 -1 -a <BSSID> -c <MAC falseado> wlan0

5º – Em outro terminal foi executada a tentativa de quebra de chave, usando a lista de palavras do diretório especificado anteriormente. Importa ressaltar que a word list possui mais de 5 Gigas de palavras chaves. Na decima terceira tentativa, houve sucesso.

aircrack-ng -e <SSID> -w /usr/share/dict/words lost.cap

Pode-se observar que esse processo só terá sucesso mediante a robustez da wordlist versus ao nível de senha utilizada pelo ponto de acesso.

3.2.1.3 Tentativa de quebra da chave WPA2 no Bairro C.

O paradigma recente para quebra da criptografia WPA e principalmente o WPA2 diz que é extremamente demorado e difícil para serem quebrados. Entretanto, a recente técnica a ser utilizada para este experimento altera toda a visão sobre este paradigma.

Tudo mudou com o descobrimento de uma falha grosseira no protocolo WPS, que é suportado pela maioria dos roteadores atuais. Basicamente, o WPS oferece uma forma simples de configuração para as redes sem fio. O equipamento de acesso (acess point) inclui um PIN de 8 (oito) dígitos, geralmente informado em uma etiqueta na parte inferior, permitindo a conexão de qualquer cliente onde este PIN seja informado. A ideia do WPS é que seja um padrão de suporte para as redes domésticas.

> Desde o inicio, WPS parecia ser uma brecha esperando para ser explorada, mas a facilidade de configuração foi suficiente para reduzir bastante as chamadas de suporte e devoluções de produtos, o que foi suficiente para convencer quase todos os principais fabricantes a incluírem a tecnologia em seus roteadores domésticos. Eventualmente, a bomba explodiu, dando origem a maior brecha de segurança em redes *Wi-fi* desde o WEP. (MARIMOTO, 2012,).

Ainda segundo Marimoto (2012,):

> [...] a forma como o roteador responde as tentativas mal sucedidas de conexão, enviando um pacote WPA-NACK permite que o atacante descubra se os 4 primeiros dígitos do PIN estão corretos. Para piorar, o último digito do PIN é um *checksum*, que pode ser facilmente calculado uma vez que os 7 primeiros dígitos são conhecidos. Com isso, o atacante precisa de um número de tentativas suficiente para descobrir os 4 primeiros dígitos, gerar uma tabela com as possibilidades possíveis para os 3 últimos dígitos e mais o *checksum* (uma vez que o *checksum* é a soma dos 7 primeiros dígitos) e realizar uma última rodada de tentativas até encontrar o PIN correto. Com isso, o número de possibilidades cai de 1 bilhão para apenas 11.000 tentativas, que podem ser esgotadas em poucas horas.

O grande agravante para esse tipo de ataque é que uma vez que o consegue, em acesso à rede, continuará a conseguir conectar-se, mesmo que o administrador altere a chave de acesso ou mesmo o SSID da rede, seja ela WPA ou WPA2.

Para essa etapa de quebra de criptografia WPA2, foi utilizada a

ferramenta Reaver.

Seguem os passos utilizados:

1º – Para utilizar a ferramenta Reaver foi necessário colocar a placa em modo monitor. Para tal, abriu-se o Kismet. Se o Kismet não estiver executando automaticamente a placa de rede em modo de monitoramento (também conhecido como promíscuo), será faz- se necessário executar o comando para colocá-la em modo monitor: # airmon-ng start wlan0 - // caso o comando anterior não seja executado, é porque o Kismet já está executando a placa em modo de monitoramento.

2º – O próximo passo é necessário foi obter informações sobre o dispositivo de rede e do endereço MAC do roteador alvo; para tal basta retirar as informações fornecidas pelo Kismet.

3º – Depois de descoberto o endereço MAC do ponto de acesso, o Reaver é executado no terminal, associando-o com MAC do ponto de acesso, com o seguinte comando: # reaver -i mon0 -b 97:FD:22:98:11:09 –vv- // onde o reaver = programar, mon0 = interface e 97:FD:22:98:11:09 = endereço MAC.

A partir deste ponto, todo o processo de ataque é realizado automaticamente, o Reaver tenta todas as possibilidades possíveis para o PIN, até encontrar a chave PIN. A partir desta informação é possível ter acesso a rede WPA2. É importante ressaltar que por si só a criptografia WPA2 não é vulnerável.

3.2.2.1 Resultados – Pesquisa nos bairros

Após a verificação e definição do nível de segurança dos protocolos de criptografias, foi aplicada a técnica Wardriving durante o período de 20 a 26 de Outubro de 2017 com o objetivo de mapear as redes sem fio dos 5 grandes Bairros mais o centro da capital de São Luís – MA. Foram realizadas capturas externas de dentro de um carro, porém, como o sinal da antena não foi suficiente para fazer a cobertura de toda a área física dos locais, houve a necessidade da captura a partir das escolhas de pontos fixos internos dos locais.

3.2.2.1.1 Resultados – pesquisa bairro A

O Bairro A foi escolhido para coleta de dados por ser o local onde há um

grande fluxo de lojas e residências e esperava-se encontrar um número significativo de redes sem fio protegidas. Foram identificados os nomes destas redes e os seus respectivos protocolos de criptografia. Como instrumento de trabalho utilizou-se um notebook com sistema operacional Kali Linux e ferramentas para levantamento de informações.

As capturas foram realizadas entre os dias 20 e 21 de Outubro 2017 utilizando a técnica do Wardriving com captura externa dentro do carro e captura interna a partir da escolha de oito pontos fixos . Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física.

A linha em vermelha o compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do bairro) escolhidos para análise no bairro A.

A partir do caminho externo percorrido e dos oito pontos fixos, foi mapeado um total de 93 redes sem fio distintas encontradas pelo programa InSSIDer. Conforme ilustrado no Gráfico 1 a seguir, do total de 93 redes sem fio localizadas, 10 estavam abertas para acesso, sem nenhum tipo de segurança. Sendo que, sua maioria (90) possue algum tipo de protocolo de criptografia de segurança. Cabe ressaltar que 9 redes são possuidoras do protocolo WEP que é 100% vulnerável a ataques. Assim sendo, 12 redes possuem o protocolo WPA e 59 do WPA2 que são detentoras de uma segurança mais avançadas, mas ainda vulnerável (dependendo das variáveis da infraestrutura utilizada em cada rede).

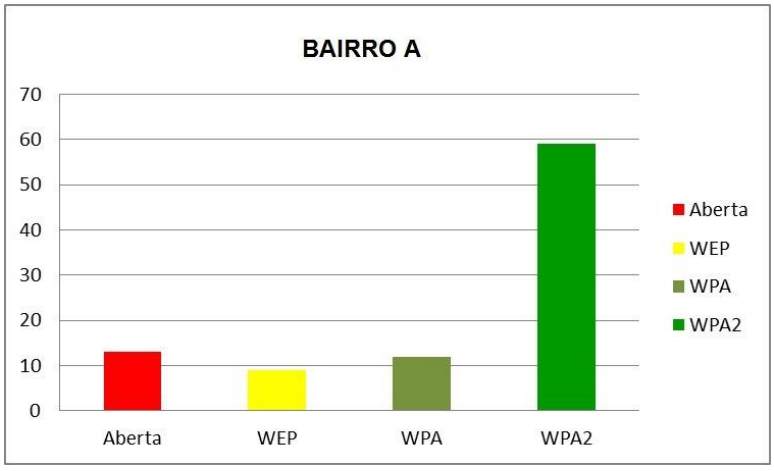

Gráfico 1 - Quantitativo das redes mapeadas no Bairro A

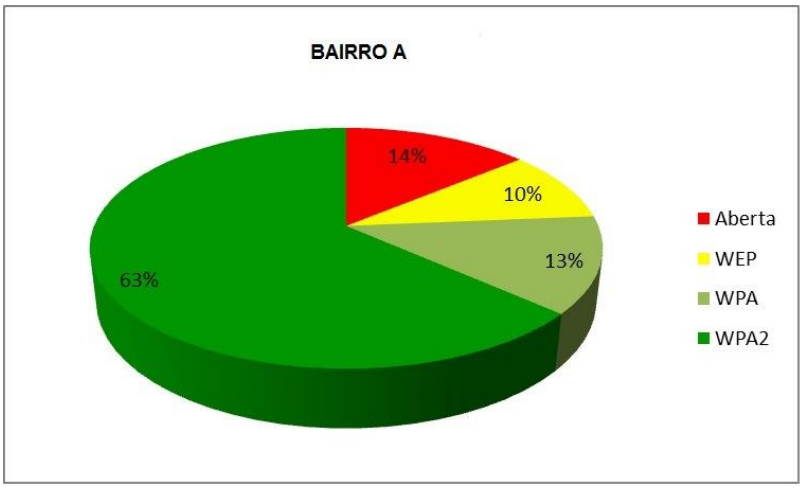

Gráfico 2 - Porcentagem das redes mapeadas no Bairro B

O levantamento destes dados concretizada a partir da técnica do Wardriving foi para verificar o quantitativo das redes sem fio do Bairro A e subdividir esse total em partes menores que compreendem o quantitativo das tecnologias de criptografia existente neste local. Através do Gráfico 2, verificou-se que as redes que utilizam a tecnologia de criptografia WPA2 representam a grande maioria com 63% do total de redes, enquanto que redes com WPA possuem 13%, WEP 10% e redes abertas representam 14%.

3.2.2.1.2 Resultados – pesquisa Bairro B.

O Bairro B foi escolhido para coleta de dados por ser o um dos maiores da capital do Estado do Maranhão e esperava-se um número pequeno de redes sem fio desprotegidas. Foram identificados os nomes destas redes e os seus protocolos de criptografia. As capturas foram realizadas entre os dias 22 e 23 de Outubro utilizando a técnica do Wardriving com captura externa dentro do carro e captura interna a partir da escolha de doze pontos fixos do bairro. Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física do bairro.

A linha em vermelha corresponde ao caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do bairro) escolhidos para análise no bairro B. A

partir do caminho Externo percorrido e dos doze pontos fixos foram identificadas um total de 135 redes sem fio distintas. Destas 135 redes localizadas, 14 estavam abertas, sem nenhum tipo de segurança. Sua maioria (121) possui algum protocolo de criptografia de segurança. Cabe ressaltar que 21 possuidoras do protocolo WEP são vulneráveis a ataques. Assim sendo, 20 redes possuem o protocolo WPA e 78 do WPA2. A seguir o Gráfico 3:

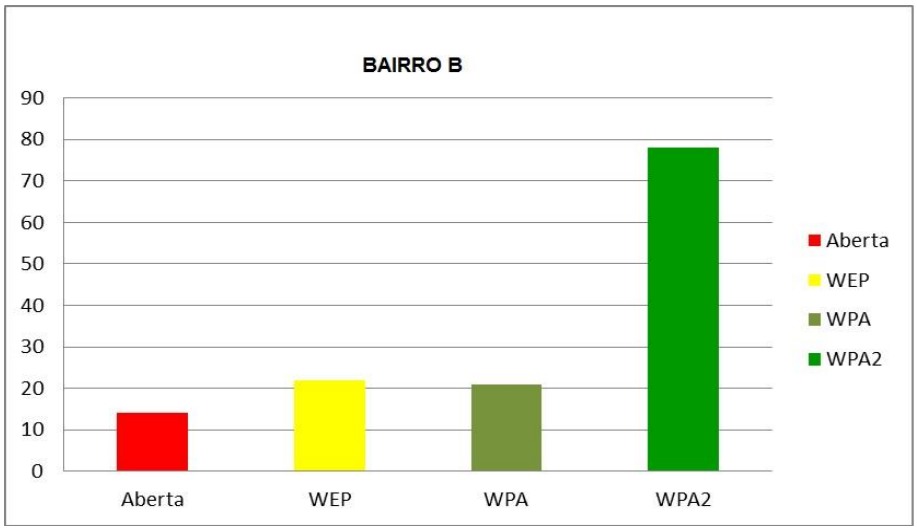

Gráfico 3 – Quantitativo das redes mapeadas no Bairro B

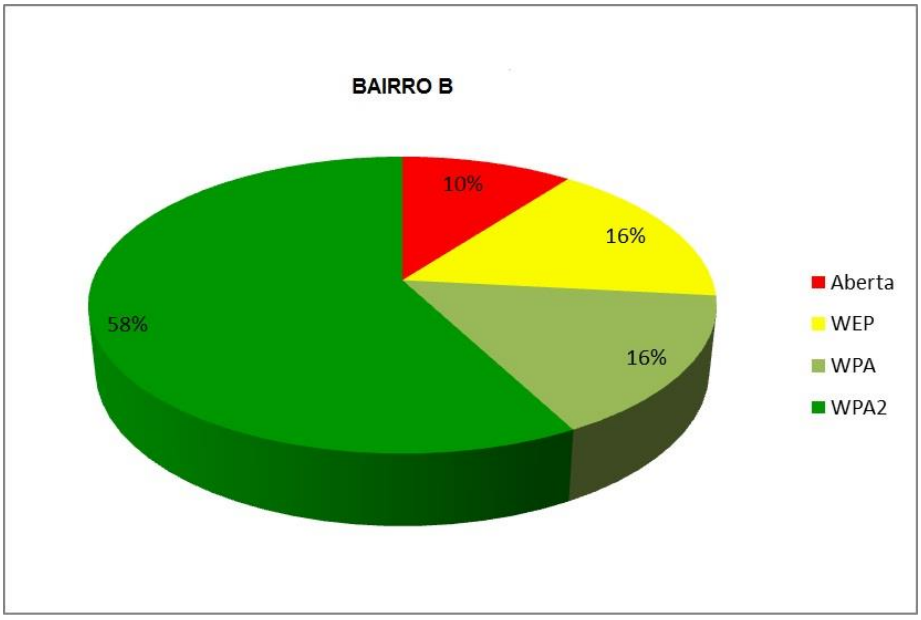

Gráfico 4 – Quantitativo das redes mapeadas no Bairro B

A partir dos dados mostrados no Gráfico 4, foi possível verificar a

porcentagem dos protocolos de criptografia utilizados no bairro B. Verificou-se que as redes que utilizam a tecnologia de criptografia WPA2 representam 58% do total geral de redes, enquanto que redes com criptografia WEP e WPA representam ambas respectivamente 16%, 10% são referentes as redes abertas ou sem nenhum tipo de proteção.

3.2.2.1.3 Resultados – pesquisa bairro C

O Bairro C foi escolhido para coleta de dados por ser o bairro localizado mais próximo da periferia da capital maranhense, tendo um ótimo fluxo de pessoas, porém, com um número de lojas reduzidas. Esperava-se encontrar um número pequeno de redes sem fio. As capturas foram realizadas no dia 26 de maio com captura externa dentro do carro e captura interna a partir da escolha de seis pontos fixos do bairro. Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física do bairro.

A linha em vermelho compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do bairro) escolhidos para análise no bairro C.

A partir do caminho externo percorrido e dos seis pontos fixos foram obtidos um total de 72 redes sem fio distintas encontradas pelo programa de captura de informações, o InSSIDer. Destas 72 redes localizadas, 9 estavam abertas, sem nenhum tipo de segurança. Sendo que, em sua maioria (63 das 72) possuem algum tipo de protocolo de criptografia. Em relação às redes que utilizam o protocolo WEP, 16 foram identificadas com este tipo de criptografia. Assim sendo, 12 redes possuem o protocolo WPA e 35 são do tipo WPA2. Esse quantitativo é apresentado no Gráfico 5.

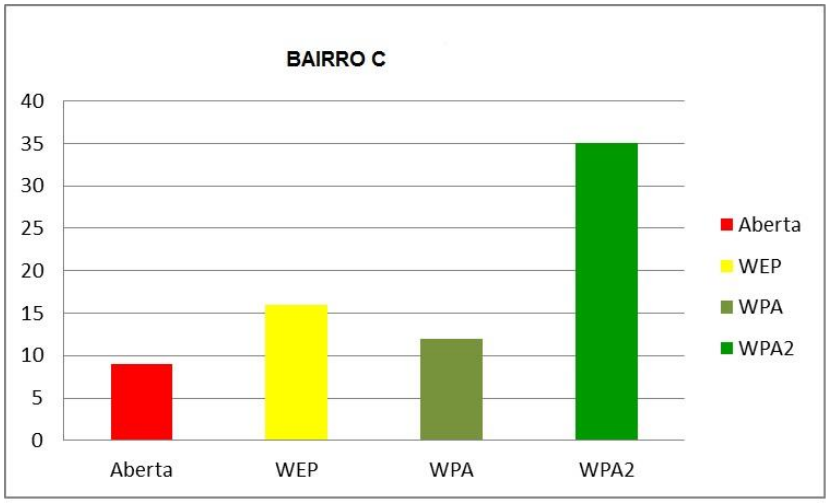

Gráfico 3 - Quantitativo das redes mapeadas no Bairro C

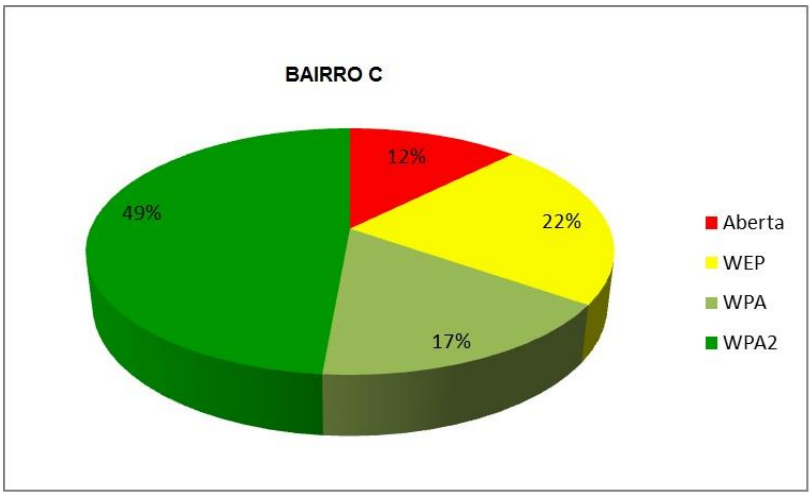

Gráfico 4 - Porcentagem das redes mapeadas no Bairro C

A partir dos dados mostrados no Gráfico 6, foi possível verificar a porcentagem dos protocolos de criptografia utilizados no Bairro C. Verificou-se que as redes que utilizam a tecnologia de criptografia WPA2, possuem menos da metade do quantitativo geral em relação as demais juntas, representando 49% do total de redes. Enquanto que redes com criptografia WPA representam 17%, tendo as redes com tecnologia WEP com 22% e 12% referentes às redes abertas.

3.2.2.1.4 Resultados – pesquisa Bairro D

O Bairro D foi escolhido para coleta de dados por ser um bairro localizado

próximo da área nobre capital maranhense, tendo um grande fluxo de pessoas, com um grande número de lojas. Esperava-se encontrar uma grande quantidade de redes sem fio. Foram identificados os nomes destas redes e os seus protocolos de criptografia.

As capturas foram realizadas entre os dias 25 e 26 de outubro com captura externa dentro do carro e captura interna a partir da escolha de dez pontos fixos. Os locais foram escolhidos por serem pontos importantes para a cobertura de toda a área física do bairro.

A linha em vermelho compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos internos escolhidos para análise no bairro D. A partir do caminho externo percorrido e dos dez pontos fixos foram obtidos um total de 177 redes distintas encontradas pelo programa utilizado para captura de informações. Destas 177 redes, 18 estavam abertas, sem nenhum tipo de segurança. Sendo que, em sua maioria (159 de 177) possuem algum tipo de criptografia. Destas 159 que possuem proteção, 25 são possuidoras do protocolo de criptografia WEP, outras 20 redes possuem o protocolo WPA e 114 são do tipo WPA2.

No Gráfico 7 é apresentado este quantitativo:

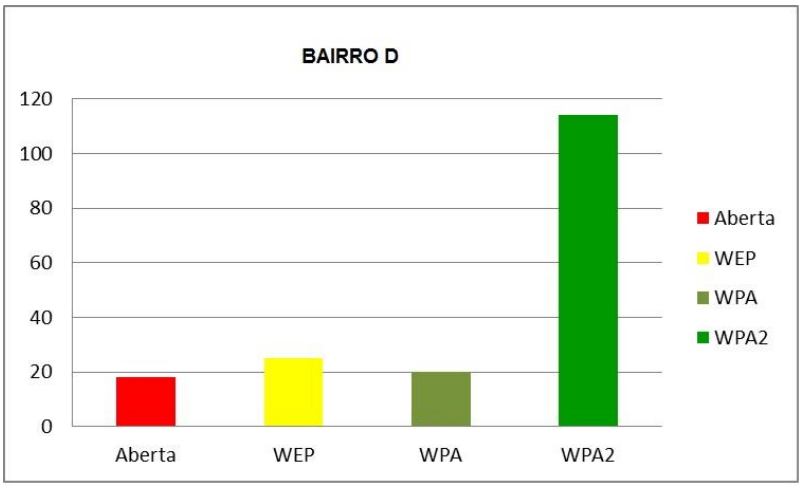

Gráfico 5 - Quantitativo das redes mapeadas no Bairro D

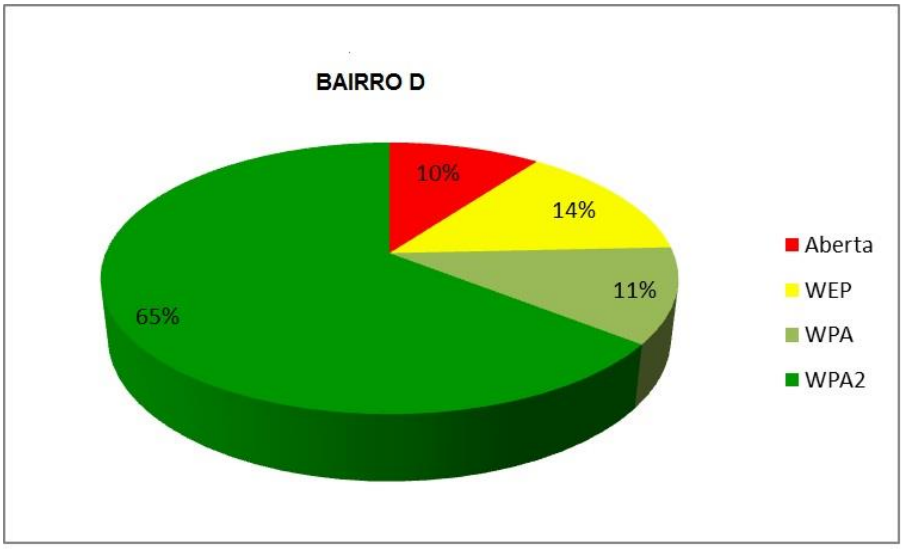

Gráfico 6 - Porcentagem das redes mapeadas no Bairro D

O gráfico 8 apresenta a divisão em porcentagens das redes sem fio e suas respectivas tecnologias de criptografia encontradas no Bairro D. Verificou-se que as redes que utilizam a tecnologia de criptografia WPA2 representam a grande maioria com 65% do total de redes, enquanto que redes com WPA possuem 11%, WEP 14% e as redes abertas representam 10%.

3.2.21.5 Resultados – pesquisa Bairro E.

O Bairro E foi escolhido para coleta de dados por ser o bairro intermediário localizado próximo dos bairros B e D. Esperava-se encontrar um número razoável de redes sem fio. As capturas foram realizadas entre no dia 26 de outubro utilizando a técnica do Wardriving com captura externa dentro do carro e captura interna a partir da escolha de quatro pontos fixos internos do bairro.

A linha em vermelha compreende o caminho de deslocamento do carro para coleta das informações e as marcações em laranja representam os pontos fixos (visto de cima da parte externa do bairro) escolhidos para análise no bairro E.

A partir do caminho externo percorrido e dos quatro pontos fixos, foram obtido um total de 56 redes distintas. Destas 56, apenas 13 estavam abertas, sem nenhum tipo de segurança. Sendo que, sua maioria (43 das 56 encontradas) utilizavam de algum tipo de protocolo de criptografia. Cabe ressaltar que apenas 6

são possuidoras do protocolo WEP. Assim sendo, 10 redes possuem o protocolo WPA e 27 utilizam o protocolo WPA2.

No Gráfico 9 é apresentado estes valores em escala:

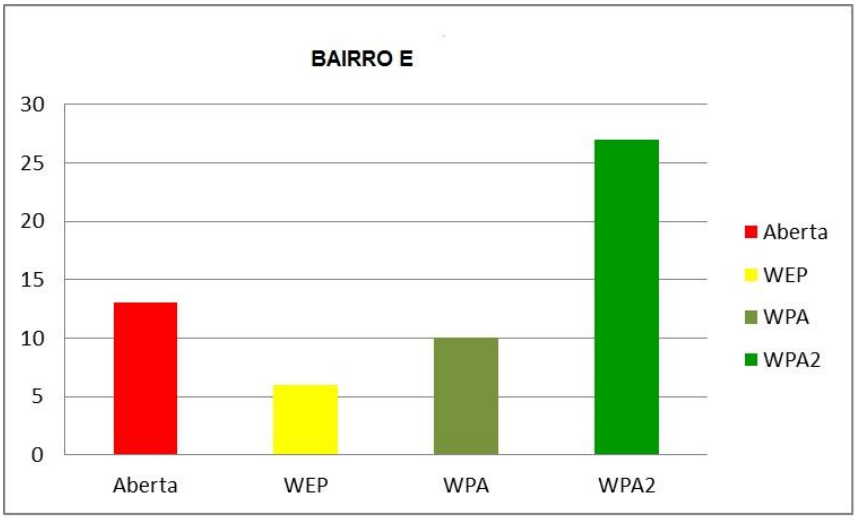

Gráfico 7 - Quantitativo das redes mapeadas no Bairro E

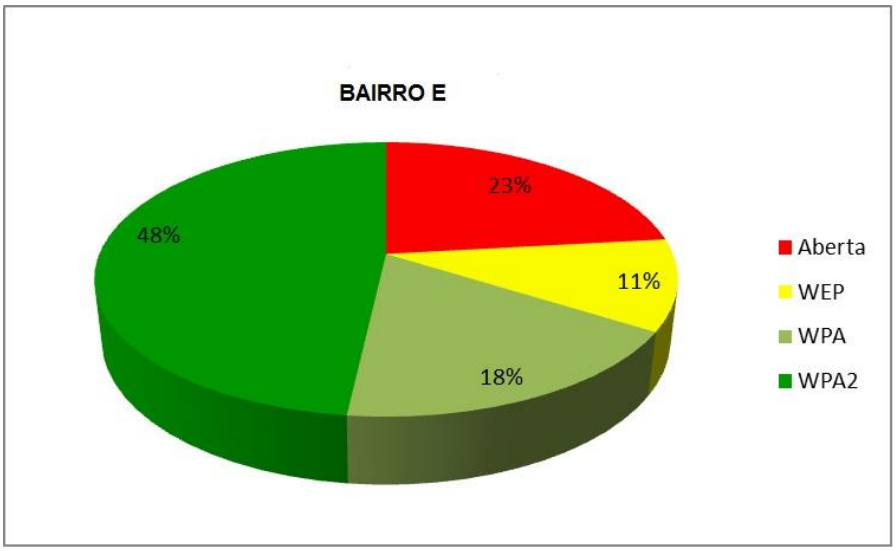

Gráfico 8 - Porcentagens das redes mapeadas no Bairro E

Conforme mostrado no gráfico 10, verificou-se que as redes, que utilizam a tecnologia de criptografia WPA2, representam 48% do total de redes, enquanto que redes com WPA possuem cerca de 18%, a WEP com apenas 11% e as redes abertas representam 23% do total.

3.3 Discussão

Segundo Schineier (2009, p. 83),

> Implementações de novas tecnologias sem fio e sem a prévia análise podem resultar em sérios riscos, podendo gerar impactos negativos que contrapõem e até mesmo anulam os benefícios alcançados, seja por não se incorporarem adequadamente aos sistemas de informações que os suportam, seja por trazerem consigo outras falhas inesperadas, por vezes maiores que as falhas que uma tecnologia possa vir a corrigir.

Efetuando a análise dos dados obtidos, constata-se que existe certa variação na utilização dos diferentes tipos de tecnologias de criptografia. Para fins didáticos são criados dois agrupamentos distintos a fim de consolidar os resultados. O primeiro é constituído pelo quantitativo de redes com criptografia WPA2 e WPA e o segundo com a tecnologia WEP e redes abertas. Tal divisão parte do pressuposto de que as redes utilizam WPA2 e WPA são mais difíceis de serem quebradas do que a WEP que é 100% vulnerável.

Considerando a classificação dos bairros baseando-se na quantidade total das redes encontradas nas mesmas, temos o seguinte ranking: 1º Bairro D (177), 2º Bairro B (135), 3º Bairro A (93), 4º Bairro C (72), 5º Bairro E (56).

No bairro A, a relevância da porcentagem obtida dos protocolos de criptografia WPA2 e WPA, é satisfatória no que se trata de segurança da informação. Pois apresentam juntas cerca de 76% do total das redes que utilizam este tipo de criptografia, que atualmente são as mais seguras.

No bairro B, verifica-se que existe mais da metade de redes com algum tipo de criptografia de dados, essa grande maioria são de pontos de acesso que utilizam WPA2, com 58%. Somadas as redes que utilizam criptografia WPA (16%) os números totais chegam a 73%.

Analisando os dados fornecidos no capitulo anterior, verifica-se no bairro C 34% das redes ou estão abertas para acesso livre ou utilizam criptografia WEP, essa quantidade é considerado como um valor critico de vulnerabilidade. Observa-se também que o quantitativo das redes com WPA2 não chegam a metade do total geral, que para os tempos atuais é um fator critico para um ambiente com alto fluxo de pessoas.

No bairro D, verifica-se que existe mais da metade de redes com algum

tipo de criptografia de dados, essa grande maioria são de pontos de acesso que utilizam WPA2 (64%) e WPA (11%). Somando estes valores o total é de 76% (em números este valor representa 134 redes). Vale a pena ressaltar que dos 5 bairros onde esta pesquisa foi realizada, o bairro D apresentou a maior quantidade de redes protegidas.

Levando-se em consideração os resultados obtidos no Bairro E, neste caso especifico, deve ser levado em consideração o quantitativo de redes abertas e redes que utilizam sistema WEP de criptografia de dados, que representam juntas 34% do total. Então, com base na norma ISO/IEC 27002 podemos dizer que este ambiente possui um nível de segurança lógica ruim, pois possui mais de 30% de vulnerabilidade.

Na Tabela 3, apresenta-se o resultado final obtido através dos estudos realizados:

LOCAL	CRIPTOGRAFIA	QUANTIDADE	PERCENTUAL	TOTAL	NIVEL DE VUNERABILIDADE
RENASCENÇA	WPA2	59	63%	93	Vulnerabilidade Baixa
	WPA	12	13%		
	WEP	9	10%		
	OPEN	13	14%		
JARACATY	WPA2	78	58%	135	Vulnerabilidade Baixa
	WPA	21	16%		
	WEP	22	16%		
	OPEN	14	10%		
CALHAU	WPA2	35	49%	72	Vulnerabilidade Alta
	WPA	12	17%		
	WEP	16	22%		
	OPEN	9	13%		
SÃO FRANCISCO	WPA2	114	63%	177	Vulnerabilidade Baixa
	WPA	20	11%		
	WEP	25	14%		
	OPEN	18	10%		
CENTRO	WPA2	27	48%	57	Vulnerabilidade Alta
	WPA	10	18%		
	WEP	6	11%		
	OPEN	13	23%		

Tabela 3 - Nível de Vulnerabilidade

Para classificação em “Vulnerabilidade Baixa” ou “Vulnerabilidade Alta”, utilizou-se o como base de cálculo a seguinte formula:

= Quantidade de redes com WEP + Quantidade redes Abertas <= 30

Se a soma das redes (WEP e abertas) forem maior ou igual a 30% (valor baseado na norma ISSO/IEC 27002, para classificação de vulnerabilidades) do total geral de redes a classificação será dada como Vulnerabilidade Alta, caso contrário, será classificado como Vulnerabilidade Baixa.

As fraudes crescem rapidamente de forma vertical, devido às dificuldades de controle do trafego de dados na rede, barreiras de jurisdição e falta de profissionais qualificados para atuar na área de investigação afim, são alguns dos fatores que deixam para trás, no que se trata em métodos eficazes de antifraudes e busca dos infratores por parte do Estado.

De acordo com o que foi anteriormente abordado, os riscos na quais as redes públicas ou privadas estão expostas são enormes. A necessidade de implantação de procedimentos que minimizem os ataques são fatores determinantes para a segurança da informação. A sensatez, desconfiança, atenção e percepção são as peças fundamentais para a luta contra os crimes cibernéticos.

Um dos procedimentos que podem agregar valor é a utilização da monitorização da rede sem fio, ou seja, sistemas de detecção de intrusão tornam as redes menos vulneráveis, mitigando e mapeando, por exemplo: pontos falhos da rede, os ataques realizados, etc.

Algumas ferramentas específicas permitem monitorar a rede, como é o exemplo de:

- ***Kismet –*** que monitora e alerta as tentativas de ataque, o *Kismet* permite analisar os tráfegos de dados irregulares e integrar a dispositivos GPS, que ajudam na localização de um possível atacante.
- ***Snort –*** é uma ferramenta capaz de analisar o trafego da rede em tempo real, além de identificar uma variedade de ataques e ponto de acessos não legítimos.

Outra ferramenta que deve ser utilizada é uma ferramenta para filtragem dos endereços MAC que solicitam conexão a rede. Tal medida irá controlar o acesso, de forma que apenas os endereços MAC’s cadastrados no sistema poderão aceder à rede.

Conforme mostrado na Figura 18, à base da segurança da informação são as pessoas. Ou seja, treinamentos de segurança da informação para funcionários e comunicação clara sobre os riscos da utilização rede sem fio para os clientes, ajudam a diminuir os impactos da exposição de dados sensíveis.

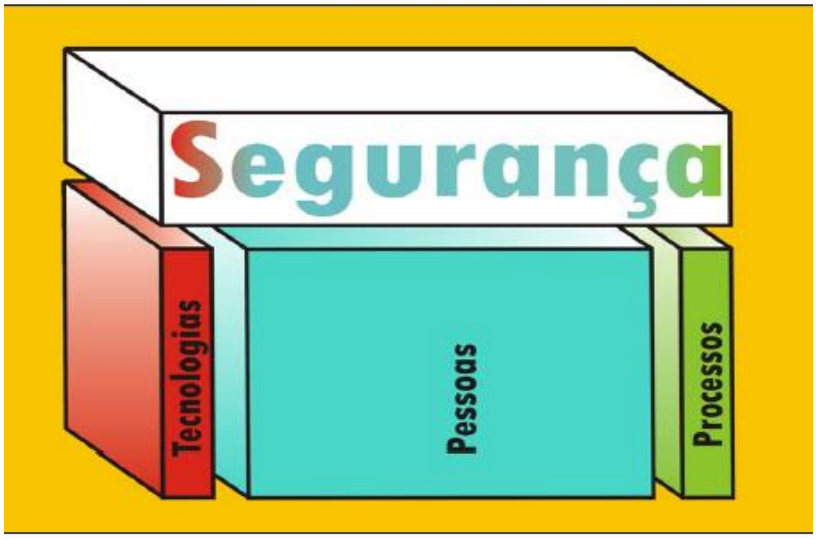

Figura 13 - A Base da Segurança da Informação

FONTE: Desconhecida

Podemos observar na Figura 8, que a base da segurança da informação é composta por:

- 80% Pessoas;
- 10% Tecnologias;
- 10% Processos;

4. CONSIDERAÇÕES FINAIS

Esse trabalho procurou mostrar um cenário onde o fator de vulnerabilidades nas redes sem fio nos ambientes públicos pode ser um fator critico para o aumento do roubo de informações.

O trabalho de pesquisa procurou abordar através da contextualização e pesquisa aplicada, identificar às vulnerabilidades as redes sem fio e suas criptografias de maneira a demonstrar e esclarecer como funciona este modelo de ataque e os seus impactos, além da importância da necessidade de proteção.

Inicialmente através do estudo bibliográfico foram esclarecidos os conceitos da segurança da informação, das redes sem fio e os mecanismos de segurança que envolve as mesmas. Posteriormente, a partir dos resultados obtidos foram apresentadas as facilidades peculiares que propiciam a atuação do atacante no processo de invasão das redes sem fio, que atuam na grande maioria das vezes de forma indireta, sem a necessidade de presença física nos locais alvos. O crescimento descentralizado e constante das redes sem fio esta relacionado aos impactos das exposições de informações dos usuários é uma constante que deve ser estuda, combatida e acompanhada com mais veemência nos campos computacionais.

Foi visto que em São Luís, no total de 533 redes sem fio mapeadas durante a utilização da técnica do wardriving na identificação das redes sem fio nos bairros da capital maranhense, 313 redes utilizam criptografia WPA2. Este número representa 59% do total geral, ou seja, podemos concluir que apesar de 2 bairros serem caracterizados como “Vulnerabilidade Alta”, baseando-se apenas no quantitativo geral das redes com WPA2 (redes mais seguras) o saldo geral no que refere-se a segurança da informação das redes sem fio na capital maranhense é caracterizado como :‘bom’.

Entretanto, percebe-se também, a necessidade de ampliação ou criação do número de equipes capazes de trabalhar com a gestão da Segurança da Informação nas empresas e órgãos públicos, profissionais estes capazes de treinar a sua equipe e ter respostas a incidentes eficazes.

Também foram apresentadas sugestões para uma melhor qualidade do tratamento das informações e construção de uma infraestrutura de rede mais

confiável. Outro aspecto relevante e que merece ser dada a devida atenção é o papel do Estado Brasileiro na divulgação e implantação de politicas profundas que levem em consideração as bases da segurança da informação.

Concluímos, portanto, que através do estudo proposto e pesquisa realizada, verifica-se que os ataques as redes sem fio é um método pouco divulgado, porém, muito eficaz. A partir do mesmo, também se pode iniciar inúmeros ataques que buscam roubo de informações, podendo ser realizado sem a necessidade de altos investimentos financeira.

Vale a pena lembrar, que este estudo tem fins didáticos e não definitivo, que busca apresentar questionamentos e sugestões que ajudem na disseminação desta modalidade de ataque ainda pouco divulgada.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002** – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2005.

ALECRIM, E.**Ataques Dos (*Denial of Service*) e DDoS (*Distributed DoS)***. São Paulo: Nova Era, 2008.

ALVES, G.A. **Segurança da Informação**: uma visão inovadora da gestão. São Paulo: Ifweb, 2010.

DRUCKER, D., **Definitions and Systems Security**, v.1, Alemanha, 2008.

ENGST, A.; FLEISHMAN, G.: **The Wireless Networking Starter Kit Second** Edition: The practical guide to Wi-Fi networks for Windows and Macintosh. 2.ed., 2004.

FARIAS, P. **Redes Básico**. Parte VIII. Disponível em: <http://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico008.asp>. Acesso em: 05 mar. 2018.

FOROUZAN, B. **Comunicação de dados e redes de computadores**. 3. ed.São Paulo: Armed, 2006.

FRANCESCHINELLI, D. **Estudo comparativo dos aspectos de segurança em redes WWAN, WLAN e WPAN**. São Paulo: Nova Era, 2009.

GIL, A.C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2008. 184p.

GOUVEIA, J.; MAGALHÃES, A. **Redes de Computadores.** FCA: Editora de Informática, LTDA, 2005.

Hacker invade e-mail de presidente Dilma e já pode trabalhar com Mercadante, Portal Implicante.org, Jun. 2011. Disponível em: < http://www.implicante.org/noticias/hacker-invade-e-mail-de-dilma-e-ja-pode-trabalhar-com-mercadante/> Acesso em: 03 de Nov. de 2012.

HURLEY, P. M.; FAIRBAIRN, H. W. 1978. **System Networks attacks***.* Geal, Sco. Am. Bull. v.89, n.9, p. 1.335-1340. 2004

KUROSE, F. & Ross, W.: **Redes de computadores e a internet**: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LUCCHESE, F. **Utilizando Wardriving para a detecção de vulnerabilidades em redes locais sem fio na região Farroupilha**. Novo Hamburgo, 2007.

MARTIN, V. **Manual prático de eventos**. 4.reimp. São Paulo: Thomson Learning, 2007.

MARTINS, G.. **Análise de vulnerabilidade e ataques a redes sem fio z02.11**. São Paulo: Editora de Informática, LTDA, 2005.

MONTEIRO, E. & BOAVIDA, F. **Engenharia de Redes de Informáticas.** 7. ed. FCA: Editora de Informática, LTDA, 2000.

PEIXOTO, M.C.P. **KONSULTEX**, Rio de Janeiro: Braspost, 2008.

PERTERSON, L. & Davie, B. (2004). **Redes de Computadores: Uma abordagem de sistema.** Editora: Elsevier, 3º Edição. ISBN: 85-352-1380-5, 2004.
RUFINO, N.: **Segurança em Redes sem Fio.** Editora Novatex, 2.ed. São Paulo/SP, 2005.

PORTAL TERRA. **Coca-Cola**: secretária é condenada a 8 anos por roubo de segredo. Portal Terra, mai. 2007. Disponível em: <http://br.invertia.com/noticias/noticia.aspx?idNoticia=200705231732_RED_35438262&idtel>. Acesso em: 02 nov. 2012.

SACEVIC, T. **Ciência da Informação**: origem, evolução e relações. Belo Horizonte, jun. 1996.

SHIKOTA, R. **Sistema especialista para verificar a vulnerabilidade de rede de computador sem fio**. Disponível em <http://bibdig.poliseducacional.com.br/document/?code=99> Acesso em: 22 abr. 2013.

SILVA, L.; DUARTE, O. (2009). **RADIUS em Redes sem Fio.** Disponível em <http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RADIUS_em_Redes_semFIO.pdf> Acesso em: 22 abr. 2013.

TANENBAUM, A.; ALECRIM P. **Computer Network**. 4.ed. São Paulo: Patti Guerrieri, 2003.

TAKAHASHI, T. Mercado, trabalho e oportunidades. In: _____. (Coord.). **Sociedade da informação no Brasil**: livro verde. Brasília: Socinfo/MCT, Cap. 2, p. 13-24. 2000. Disponível em: <http://www.socinfo.gov.br>. Acesso em: 22 ago. 2000.

ZANETTI, A.; GONÇALVES, L.: **IEEE 801.11 Padrão para Redes Locais sem Fio**. Editora: Abril, v.1. Brasilia, 2009.

ZHANG, Y. **Definitions and Sciences of Information, InformationProcessing &Management.** v.24, n.4, China, 1998.