FACULDADE ANHANGUERA DE RONDONÓPOLIS

Av. Ary Coelho, nº 829 – Cidade Salmen – Rondonópolis MT

CEP 78705-050 – (66) 3411-7600

VALDOMIRO SOARES ROSA – RA: 4442666711

**PROTOCOLO WPA:** Benefícios e Vulnerabilidades.

Rondonópolis- MT

2015

VALDOMIRO SOARES ROSA – RA: 4442666711

**TEMA**

**PROTOCOLO WPA:** Benefícios e Vulnerabilidades.

Trabalho de Conclusão de Curso apresentado ao Departamento de Ciências da Computação da Faculdade Anhanguera de Rondonópolis.

Professor Orientador: Rodolpho Schwingel de Souza

Rondonópolis- MT

2015

AGRADECIMENTOS

Ao Professor Rodolpho, meu orientador, pela paciência, compreensão e todo apoio ao longo desta pesquisa.

Ao colega Douglas que gentilmente me emprestou alguns livros que contribuíram para enriquecer o referencial teórico deste trabalho.

Aos meus familiares e amigos que sempre procuravam motivar-me para não desistir ao longo da caminhada.

**RESUMO**

Hoje em dia com o desenvolvimento tecnológico e a facilidade que as pessoas possuem para acessar a internet faz com que, indiscutivelmente, a rede wireless ou Wi-Fi se torne cada vez mais popular. Essa modalidade de conexão é conveniente porque permite que os usuários estejam sempre conectados, independente, do lugar onde estejam. Embora o Wi-Fi permita que o indivíduo se conecte de forma rápida, neste tipo de conexão o usuário fica exposto aos ataques que acontecem devido às vulnerabilidades dos protocolos de segurança. Com base nisso, este estudo tem por objetivo compreender a importância do Protocolo WPA como componente de segurança para os usuários das redes sem fio no ambiente virtual, mostrando seus benefícios e vulnerabilidades e dando ênfase para as medidas que devem ser tomadas, a fim de proteger seus dados e identidade no universo virtual. Para tanto, foi realizada uma pesquisa bibliográfica e na internet a fim de verificar de que forma esses ataques podem acontecer e como o Protocolo WPA pode ajudar o usuário a se manter seguro no ambiente virtual.

**Palavras Chave**: Usuários, Rede Wi-Fi, Protocolo WPA

**ABSTRACT**

Nowadays with technological development the people have facility to access the internet and this, undoubtedly, the wireless or Wi-Fi become more popular. This connection mode is important because to allow internet users are always connected, independent, of place wherever you are. Although the Wi-Fi to allow that the individual log in quickly, in this mode connection, the internet users get exposed to attacks that happen due to vulnerabilities of security protocols. Based on that, this study has for objective to understand the importance of the WPA Protocol like security component to internet users of wireless, showing yours benefits and vulnerabilities emphasing measures to be taken to protect yours informations and identity in the virtual universe. Were made a bibliographic research and on internet to check in what way these attacks can to happen and how the WPA Protocol can help the internet users to stay safe in the environment virtual.

**Keys Words:** Internet users, Wireless, WPA Protocol

**LISTA DE FIGURAS**

Figura 1 ……………………………………………………………………………………20

Figura 2……………………………………………………………………………………26

Figura 3……………………………………………………………………………………27

Figura 4……………………………………………………………………………………29

**LISTA DE ABREVIAÇÕES E SIGLAS**

AES – Advanced Encryption Standard

AP – Access Point

BSD – Berkeley Software Distribution

CCMP – Counter Mode with CBC-MAC Protocol

DoS – Denial of Service

DSSS - Direct Sequence Spread Spectrum

EAP – Extensible Authentication Protocol

IDS- Intrusion Detection System

IEEE – Institute of Electrical and Electronics Engineers

IV – Initialization Vector

LAN – Local Area Network

MAC – Media Access Control

OFDM - Orthogonal Frequency Division Multiplexing

OSA – Open System Authentication

OSI - Open Systems Interconnectation

PSK – Pre-Shared Key

RF – Rádio Frequência

RADIUS – Remote Authentication Dial-In User Service

RC4 – Ron´s Code 41

RSN – Robust Security Network

SKA – Shared Key – pré-compartilhada

SNMP – Simple Network Management Protocol

TI - Tecnologia de Informação

TKIP – Temporal Key Integrity Protocol

VDI – Virtual Disk Image

WEP – Wired Equivalent Privacy

WI-FI – Wireless Fidelity

WLAN – Redes Locais Sem Fio

WPA – Wi-Fi Protected Access

 WWW – World Wide Web

**SUMÁRIO**

**1 INTRODUÇÃO**.....................................................................................................9

* 1. DELIMITAÇÃO DO TEMA.................................................................................10
	2. PROBLEMA.......................................................................................................10
	3. OBJETIVOS.......................................................................................................11
		1. Objetivo Geral...............................................................................................11
		2. Objetivos Específicos....................................................................................11
	4. JUSTIFICATIVA.................................................................................................12
	5. HIPÓTESE.........................................................................................................13
	6. METODOLOGIA................................................................................................13
1. **REFERENCIAL TEÓRICO**.................................................................................16
	1. A Importância da Internet para o Ser Humano...................................................16
	2. Modalidades de Conexão para Internet..............................................................18
		1. Wi-Fi: uma Rede Sem Fio baseada no Padrão 802.11..................................20
		2. Vantagens e Desvantagens da Rede Wireless..............................................23
	3. Segurança na Rede Wireless..............................................................................24
		1. Vulnerabilidades do Protocolo WPA...............................................................30
		2. Criptografia nas Redes Sem Fio.....................................................................31
		3. Ataque às Redes Sem Fio..............................................................................36
		4. Ferramentas para Ataques nas Redes Sem Fio............................................38
	4. Teste de Invasão do WEP...................................................................................39
	5. Segurança da Informação: Física e Lógica.........................................................43
	6. Computação Forense..........................................................................................44

**3 CONCLUSÃO**........................................................................................................46

REFERÊNCIAS.........................................................................................................48

## GLOSSÁRIO..............................................................................................................53

**1 INTRODUÇÃO**

Vivemos em um mundo globalizado no qual as coisas acontecem rapidamente, as transformações na sociedade deixam o ser humano cada vez mais dependente dos instrumentos tecnológicos que a modernidade proporciona. Neste contexto, destaca-se a internet, que revolucionou a vida do homem.

Dentre os novos meios tecnológicos a Internet é, sem dúvida, o mais revolucionário deles. Sua utilização nos permite, por exemplo, organizar, transformar e processar as informações em velocidade e capacidade cada vez maiores e com custos cada vez mais reduzidos. (SCHIAVONI, 2015). Por meio dela, o indivíduo pode realizar atividades como: pesquisar conteúdos, interagir em redes sociais, trabalhar on line, entre outras coisas. E, tudo se tornou, ainda, mais fácil depois do surgimento das redes sem fio (wireless) que permite que o indivíduo acesse a internet em qualquer local que tenha Wi-Fi disponível, sem necessitar de fio.

Navegar na internet em qualquer lugar e a qualquer momento pode ser ótimo, entretanto, o indivíduo deve tomar cuidado com a segurança no ambiente virtual, uma vez que ficam expostos aos ataques de pessoas mal-intencionadas na rede.

Com o desenvolvimento tecnológico a preocupação dos engenheiros da computação aumentou em relação à criação de novos protocolos para garantir a segurança dos internautas na rede. Ao longo dos anos foram criados diversos protocolos até chegar ao Protocolo WPA (Wi-Fi Protected Access ou Wi-Fi protegido).

Portanto, esta pesquisa tem por finalidade compreender a importância do protocolo WPA como componente de segurança para os usuários das redes sem fio no ambiente virtual, mostrando seus benefícios e vulnerabilidades.

1.1 DELIMITAÇÃO DO TEMA

A segurança dos usuários na internet tem gerado diversos debates, tendo em vista que o índice de crimes que acontecem no ambiente virtual têm se elevado consideravelmente nas últimas décadas. Em razão disso, os engenheiros da computação têm criado vários protocolos de forma a proporcionar aos usuários da rede uma navegação segura.

Portanto esta pesquisa tem como tema “Protocolo WPA: Benefícios e vulnerabilidades” que visa analisar a importância deste protocolo para os usuários do Wi-fi, em uma era na qual a tecnologia está extremamente avançada e que as pessoas têm acesso a todo tipo informação de forma simples e rápida.

* 1. PROBLEMA

O uso de redes sem fio (wireless) vem aumentando substancialmente, resultando em um impacto significante na vida das pessoas, em distâncias médias (WIRELESS LAN, WLAN) ou em curtas distâncias (Bluetooth). As redes sem fio facilitam o dia-a-dia das pessoas, no entanto, trazem consigo novos riscos. (PIZON, 2009)

Com o avanço dos aparelhos tecnológicos, os profissionais da área da computação foram criando protocolos para garantir a segurança dos usuários das redes sem fio e, embora, alguns tenham sido testados, mesmo assim, encontraram falhas neles.

A segurança nas comunicações sem fio ainda é encarada como um requisito passivo a questionamento e, medidas abordadas para garantir a integridade das informações estão sendo gradativamente aplicadas, dentre elas, dá-se uma atenção especial para o protocolo WPA (Wi-Fi Protected Access). (TEXEIRA; GOMES, 2015)

Partindo desse princípio esta pesquisa tem como objetivo analisar a importância deste protocolo para os usuários das redes sem fio, uma vez que hoje as pessoas resolvem tudo on line ficando vulneráveis aos perigos das redes.

A própria natureza de uma rede (Wireless) Wi-Fi já a torna vulnerável a ataques, afinal basta possuir uma antena para detectar seu sinal. Devido a este fato as redes estão, em princípio, expostas a alguns perigos. O primeiro seria um invasor obter acesso a nossa rede. Isto lhe permitiria utilizar alguns recursos, como por exemplo, a conexão à internet. Outro problema seria se esse invasor conseguisse realmente acessar a rede interna, seja ela doméstica ou corporativa isso que lhe permitiria o acesso a dados (informações), senhas, números de contas e arquivos de trabalho. (SILVA, 2010)

Considerando o quanto a rede Wi-fi é relevante para a vida das pessoas na atualidade, surgem os seguintes questionamentos: o que significa o Protocolo WPA? Por que ele é importante para os usuários da rede Wi-fi? O que acontece quando o usuário não tem acesso a esse Protocolo? Quais suas vulnerabilidades?

* 1. OBJETIVOS

1.3.1 Objetivo Geral

* Compreender a importância do protocolo WPA como componente de segurança para os usuários das redes sem fio no ambiente virtual.
	+ 1. Objetivos Específicos
* Conceituar o protocolo WPA e seus benefícios para os usuários das redes sem fio;
* Estabelecer um comparativo entre o protocolo WPA e o WEP evidenciando os pontos positivos;
* Analisar as vulnerabilidades de segurança do protocolo WPA;
* Falar sobre criptografia e ataques à rede;
* Comentar sobre a segurança da informação e computação forense.
	1. JUSTIFICATIVA

Há alguns anos atrás tudo era conectado por fio em se tratando de computadores, porém, na atualidade com o advento dos notebooks, smartphones, Ipods, Ipads dentre outros aparelhos sem fio, foi necessário pesquisar novas formas de conexão para que as pessoas pudessem ficar antenadas sem se incomodarem de carregar e conectar fios em locais pouco apropriados e, em razão disso criou-se as redes sem fio, das quais destaca- se o Wi-Fi. Uma rede sem fio Wi-Fi é uma tecnologia que permite a comunicação entre equipamentos sem a necessidade de utilizar cabos. Os equipamentos enviam e recebem sinais através do ar, utilizando uma faixa de frequência não licenciada e, portanto, não necessitam de permissão para seu uso. A rede sem fio permite uma maior mobilidade e redução de custo em relação às redes tradicionais, porque sua instalação é mais simples e rápida. (CARTILHA REDES SEM FIO, 2010)

 As redes *(*wireless) ou **Wi-Fi** surgiram para eliminar as limitações que os usuários tinham ao usar aparelhos conectados à tomada e, é visível que o uso deste tipo de rede está se tornando cada vez mais comum, não só nos ambientes domésticos e corporativos, mas também em locais públicos como bares, lanchonetes, shoppings, livrarias, aeroportos, contudo, a fim de que sejam acessadas com segurança são necessários alguns protocolos de segurança. Dentre os protocolos, destaca-se o protocolo WPA que é uma versão recente, em se tratando de segurança on line.

 Sendo assim, esta pesquisa é relevante porque vem trazer alguns esclarecimentos sobre este protocolo de segurança tão importante para os usuários da rede.

Espera-se que este trabalho possa ser útil não só aos profissionais da informática, mas a todos quanto interessar, pois, no mundo tecnológico as pessoas ficam cada vez mais vulneráveis aos perigos da internet e o protocolo WPA surge como um grande aliado dos internautas.

* 1. HIPÓTESE

Fala-se muito hoje em dia sobre os riscos que o indivíduo corre ao utilizar a internet. As pessoas vivem atarefadas e muitas não possuem tempo disponível para ficarem se deslocando de um local para outro para resolverem seus problemas, consequentemente, acabam optando por usar a internet para fazer transações bancárias, compras virtuais, sem falar das redes sociais que são utilizadas para compartilhar opiniões, postar fotos, entre outras coisas.

Sendo assim, se por um lado a internet facilita a vida da pessoa, por outro pode representar um perigo e, pensando numa forma de amenizar estas ameaças virtuais os cientistas da computação começaram a criar protocolos de segurança para proteger o usuário da rede até chegar ao WPA.

Estes especialistas têm pesquisado formas de garantir proteção total aos usuários da rede, porém, ainda não alcançaram o objetivo.

No entanto, o protocolo WPA é uma versão de segurança recente e esta pesquisa mostrará a importância deste protocolo para os usuários, bem como comparará essa versão com a WEP enfatizando os aspectos positivos da mesma.

* 1. METODOLOGIA

A Pesquisa científica consiste na realização de um estudo bem planejado, no qual o método usado para abordar o problema vai caracterizar o aspecto científico da investigação. Tem por finalidade descobrir respostas para questões proposta mediante ao método científico.

Considerando que a pesquisa científica visa conhecer cientificamente um ou mais aspectos de determinado assunto, ela deve ser sistemática, metódica, crítica e o seu produto, isto é, o seu resultado deve contribuir para o avanço do conhecimento humano.

Os critérios adotados para classificar o tipo de pesquisa que está sendo realizada variam de acordo com o enfoque, os interesses, o campo, a metodologia, as situações e os objetos ligados a ela. Quanto à forma de abordagem pode-se dizer que esta pesquisa é, fundamentalmente, bibliográfica.

Para a realização deste trabalho será realizado uma pesquisa bibliográfica e exploratória. Segundo Gil (2002, p.44), “a pesquisa bibliográfica obtém os dados a partir de trabalhos publicados por outros autores, como livros, obras de referência, periódicos, teses e dissertações e a pesquisa de levantamento”: Este levantamento será feito com o intuito compreender a importância do protocolo WPA como componente de segurança para os usuários das redes sem fio no ambiente virtual.

Nesta pesquisa há algumas questões que serão respondidas por meio de consulta a autores que já trataram do assunto dando embasamento a este trabalho

Um trabalho que é baseado na pesquisa bibliográfica não pode deixar de conter explanações que sigam um fluxo para facilitar a compreensão e a aplicação.

Portanto, neste estudo, especificamente, serão analisados alguns testes de segurança que se pode fazer por meio do BackTrack, para verificar a consistência da chave de segurança.

Sendo assim, entende-se que na, era globalizada a tecnologia da informação e a inclusão digital aumentam a cada dia. Hoje é possível que uma pessoa, utilizando um computador e possuindo acesso a “internet”, possa usufruir de serviços de sistemas financeiros on line como “netbank”, trocar e-mails, adquirir vários tipos de produtos através do comércio eletrônico etc. (GIAVAROTO, SANTOS, 2013)

Paralelamente, com as facilidades do mundo digital, a fim de manter seguro e proteger os dados que ali estão inseridos e comuns, a maioria das empresas, utilizam tecnologias avanças para a proteção de seus ativos, sejam eles tangíveis ou intangíveis. Soluções que vão desde um simples antivírus a complexos sistemas de firewall ou detecção de intrusos IDS. (GIAVAROTO, SANTOS, 2013)

Neste meio, um inimigo caminha silenciosamente, o invasor chamado “*Blackhat*” que pela mídia é conhecido como *Hacker.* Este indivíduo é dotado de conhecimentos avançados sobre sistemas e redes de computadores, habilidades que permitem ao mesmo tempo o sucesso na interceptação e subtração indevida de informação. (GIAVAROTO, SANTOS, 2013)

Neste contexto, o BackTrack baseado no WHAX, Whoppix e Auditor é uma ferramenta voltada para testes de penetração muito utilizada por auditores, analistas de segurança de redes e sistemas, hackers éticos e etc. Sua primeira versão foi criada em maio de 2006 e a mais recente em 2011. Atualmente possui mais de 300 ferramentas voltadas para teste de penetração. (GIAVAROTO, SANTOS, 2013)

A instalação do BackTrack é relativamente fácil e, o indivíduo poderá instala-lo diretamente em sua máquina, em uma máquina virtual, rodar diretamente de um *live cd* ou até mesmo de um dispositivo pen drive. (GIAVAROTO, SANTOS, 2013)

Para instalar o BackTrack 5 a partir da inicialização da VirtualBox é necessário seguir as seguintes etapas: iniciar o assistente de criação dando um clique no botão novo; abrirá uma página de seja bem-vindo ao assistente e você deve clicar em próximo; na janela seguinte escolha um nome para sua máquina, o sistema operacional Linux e a versão; a seguir selecione a quantidade de memória a ser utilizada, é aconselhável usar 1GB.; na próxima tela habilite a opção de disco boot e criar novo disco rígido, depois habilite a opção VDI (Virtual Disk Image); na sequência selecione a opção dinamicamente alocado; ajuste o tamanho do disco virtual para 8GB. Será mostrado o sumário de configurações e clique na máquina que você criou a mesma estará no modo desligada. A próxima janela a surgir será o assistente de primeira execução, dê um clique em próximo; depois selecione a mídia de instalação, no caso a imagem baixada BR5-KDE-32 iso. A janela seguinte exibirá o sumário de configurações, clique em iniciar, se você seguir todos os passos, a tela de subida do sistema será exibida, selecione o modo *Default Boot Mode*. (GIAVAROTO, SANTOS, 2013)

O Penetration testing (Teste de Penetração) trata-se de um método para testar e descobrir vulnerabilidades em uma rede ou sistemas operacionais. Nesta etapa, são analisadas e exploradas todas as possibilidades de vulnerabilidades. Pentest insere métodos de avaliação de segurança em um sistema de computador ou rede, aplicando simulações de ataques como se fosse um estranho mal-intencionado no intuito de invadir um sistema. Tais Pentest possibilitam verificar a real estrutura do sistema, que é vasculhado em todas as áreas inerentes a estrutura de segurança. (GIAVAROTO, SANTOS, 2013)

1. **REFERENCIAL TEÓRICO**

2.1 A Importância da Internet para o Ser Humano

De acordo com Pinho (2003, p.19) “a internet constitui-se em uma grande rede mundial que inclui desde computadores empresariais até microcomputadores pessoais conectados em países do mundo todo”.

Apesar de ter começado com fins militares, a rede agora possui inúmeras funções, além do compartilhamento de informações. Por meio dela, é possível a expressão de opinião, a interatividade de pessoas de diferentes países, a comunicação entre as empresas e seus consumidores, pesquisas acadêmicas, entre outros. (ROBERTO, 2009)

Para Costa (2003, p.20) “a internet se apresenta como uma extensão da experiência costumeira das pessoas”.

A geração deste milênio ficará marcada, entre outras coisas, pelas mudanças que acontecem em virtude da internet que está explodindo como a mídia aberta e descentralizada mais promissora desde a implantação da televisão. (MORAN, 1997)

A internet é fantástica e, sem dúvida, transcende a todos os demais processos, quebrando barreiras e ao mesmo o tempo, sendo capaz de instigar a capacidade e a inteligência do homem. (CARVALHO, 2005)

 Segundo Terra (2006, p.19) “com a internet e as redes digitais surgem novos modelos de comunicação”.

Graças à introdução das modernas invenções tecnológicas, hoje, pode-se ter acesso a notícias de qualquer parte do mundo, instantaneamente, além de conhecer cidades, museus, fazer negócios, enfim, o universo de informações disponíveis foi rapidamente ampliado. (TERRA, 2006)

A utilização destas novas ferramentas muda a comunicação, tornando-a ágil, instantânea, potencialmente eliminando intermediários entre emissor (CORRÊA, 2008; TERRA, 2009).

A comunicação e as novas tecnologias digitais proporcionam espaços de expressão como *blogs, sites, posts,* mensagens instantâneas, fóruns, *chats*, salas de bate papo, que permitem que qualquer indivíduo com acesso a rede publique ou divulgue opiniões, pensamentos, ideias etc. (TERRA, 2006)

De acordo com Kaplan & Haelein (2010), as Mídias Sociais Digitais são entendidas como aplicativos construídos sobre a base tecnológica Web 2.0, que facilita a criação e a troca de conteúdos gerados por usuários. São consideradas Mídias Sociais Digitais os textos, imagens, áudio e vídeo em blogs, quadro de mensagens*, podcasts*, *wikis,* blogs e afins que permitem a interação entre os usuários (Terra, 2009).

Para Mangold e Faulds (2009), as mídias sociais digitais permitem maior Conversação e diversidade de fluxos de informação entre seus participantes, devem ser incluídas no mix de comunicação, sendo consideradas extensões da tradicional comunicação boca-a-boca. Os autores pontuam que elas diferem significativamente no tocante à velocidade do processo de comunicação e no número de pessoas impactadas, pois, por meio delas o processo de comunicação se intensifica.

As mudanças trazidas pelas tecnologias de informação e comunicação, trouxeram transformações que dizem respeito à linearidade e não linearidade dos fluxos da informação e da comunicação, bem como o papel do emissor e do receptor no processo comunicativo. (TEMP; MULLER, 2015)

Na atualidade passamos de uma sociedade massificada para uma sociedade informacional, inundada por uma imensa quantidade de informações. A expansão e a popularização da Internet e de outras tecnologias de comunicação e informação nos levam a um tempo onde o objetivo é a conexão generalizada, capaz de definir uma nova configuração comunicacional, que não é mais editada por um centro, mas disseminada em todos os sentidos. (TEMP; MULLER, 2015)

O desenvolvimento da Internet e de suas diversas ferramentas tecnológicas rompem com o modelo tradicional de comunicação – concebido como a troca de informações entre um emissor e um receptor – e favorece o aparecimento de outras formas de interação e novas práticas sociais. (TEMP; MULLER, 2015)

O acesso à internet é cada vez mais abrangente, pelo fato de poder facilmente ser utilizada em computadores, celulares, televisores, tablets, além de ter um baixo custo. Esta grande facilidade de acesso permite também que o conteúdo disponibilizado ou recebido pelo usuário esteja cada vez mais inserido no seu cotidiano, e que este interfira positivamente ou negativamente. A liberdade de informação, expressão e conteúdo, então se contrapõe à falta de ética, de autocensura e de respeito aos direitos autorais praticadas por muitos utilizadores (NEVES et al. 2015)

Por meio da Internet você pode encontrar amigos; acessar sites de notícias e de esportes; participar de cursos à distância, pesquisar assuntos interessantes; efetuar serviços bancários; fazer compras em supermercado, lojas de comércio eletrônico, pesquisar preços e verificar a opinião de outras pessoas sobre os produtos ou serviços ofertados por uma determinada loja; acessar sites dedicados a brincadeiras, passatempos, jogos, para as mais diversas faixas etárias; enviar a sua declaração de Imposto de Renda; consultar a programação das salas de cinema, verificar a agenda de espetáculos teatrais, exposições e shows e adquirir seus ingressos antecipadamente; entre outros. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012)

Porém, para usar a internet de forma segura é necessário que o indivíduo tome algumas precauções como não acessar sites com conteúdo impróprios ou ofensivos; evitar o contato com pessoas mal-intencionadas, considerando que existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro. Para ajuda-lo nisto, há diversos mecanismos de segurança que você pode usar como a criação de contas e senhas, criptografias, conhecer os protocolos de segurança como o WPA, entre outros. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012)

2.2 Modalidades de Conexão para Internet

 A conexão define as formas disponíveis no mercado para a internet. Está disponível uma série de formatos através de uma extensa gama de produtos e serviços de conexão, dentre eles, destacam-se: a conexão *Dial Up*, Banda Larga e *Wireless*. (Acervo do IESDE BRASIL, 2015)

As conexões *dial up (*linha discada) são um tipo de conexões à internet disponível fisicamente a partir de qualquer linha telefônica. Para utilizar este serviço deve-se ter uma conta com usuário e senha e um provedor de acesso à internet que fisicamente vai conectar o computador à internet. Neste tipo de conexão utiliza o moldem externo ou uma placa no computador com a mesma finalidade. (Acervo do IESDE BRASIL, 2015)

Uma conta de usuário, também chamada de “nome de usuário”, “nome de login” e username, corresponde à identificação única de um usuário em um computador ou serviço. Por meio das contas de usuário é possível que um mesmo, computador ou serviço seja compartilhado por diversas pessoas, pois, permite, por exemplo, identificar unicamente cada usuário, separar as configurações específicas de cada um e controlar as permissões de acesso. A sua conta de usuário é de conhecimento geral e, é o que permite a sua identificação. Ela é muitas vezes, derivada do seu próprio nome, mas pode ser qualquer sequência de caracteres que permita que a pessoa seja identificada unicamente, como o seu endereço de e-mail. Para garantir que ela seja usada apenas por você, e mais ninguém, existem os mecanismos de autenticação. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012)

Existem três grupos básicos de mecanismos de autenticação, que se utilizam de: aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho), aquilo que apenas você possui (como seu cartão de senhas bancárias e um token gerador de senhas) e, finalmente, aquilo que apenas você sabe (como perguntas de segurança e suas senhas). (CARTILHA DE SEGURANÇA PARA INTERNET, 2012)

Uma senha, ou *password*, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na internet devido, principalmente, a simplicidade que possui. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012)

Por outro lado, qualquer conexão à internet que possuía velocidade superior ao moldem (56Kbps – kilo/mil bits por segundo) é denominada no Brasil como Banda Larga. Ela é a evolução natural tecnológica de transmissão de dados para a crescente exigência da internet com conteúdo de imagens cada vez maiores e mais elaborados com SOS, vídeos e fotos, que exige do usuário uma conexão cada vez mais veloz. Existem várias tecnologias de tráfego de dados em Banda Larga. (Acervo do IESDE BRASIL, 2015)

Já o *Wireless* é uma forma de conexão sob formas de ondas de radiofrequência com velocidade até 11MBps. Para a sua utilização uma rádio antena deve transmitir os dados do computador para o provedor de acesso à internet. A comunicação entre o computador e a rádio- antena é feita por uma placa de rede (Acervo do IESDE BRASIL, 2015)

2.2.1 Wi-Fi: Uma Rede Sem Fio baseada no Padrão 802.11

Uma rede sem fio pode ser compreendida como uma rede de computadores sem a necessidade do uso de cabos, segundo Moraes (2004, p.185) “existem basicamente três tipos de redes sem fio: baseadas em infravermelho; baseadas em radiofrequência: Wi-Fi e Bluetooth; baseadas em laser”.

Distinguem-se habitualmente várias categorias de redes sem fio, de acordo com o perímetro geográfico que oferece uma ligação (chamado zona de cobertura), conforme se pode notar na **Figura 1**:

.

Figura 1. Categorias de Redes Sem fio Fonte: Redes Sem Fio- Wireless Networks, 2014

Atualmente, entende-se que a comunicação de dados nas redes sem fio acontece basicamente por meio da radiofrequência (comunicação via rádio). Para MORAES, 2004, p.186:

Os sistemas baseados em radiofrequência utilizam microondas para transmitir o sinal através do ar. Geralmente elas utilizam faixas de frequência conhecidas como (Industrial Scientific Medical), que são abertas porque não existe a necessidade de autorização para transmitir sinais nessas frequências.

. Este é um esquema preferido dos usuários porque permite ao internauta usar a rede em qualquer ponto dentro dos limites de alcance da transmissão; possibilita a inserção rápida de outros computadores e dispositivos na rede; evita que paredes ou estruturas prediais sejam furadas ou adaptadas para a passagem de fios, enfim, é um sistema rápido e prático que facilita a vida do homem.

Para o autor Alexandre Moraes (2004) as redes wireless são um sistema de comunicação de dados extremamente flexível que pode ser usado como uma extensão, ou uma alternativa a redes locais (LAN cabeadas). É uma tecnologia que combina a conectividade dos dados com mobilidade por meio da radiofrequência (RF).

De acordo com Rufino (2005, p.17) “inúmeras tecnologias estão incluídas na categoria de redes sem fio, mas a ênfase recairá sempre nas relacionadas com o padrão 802.11 (conhecida genericamente como Wi-Fi)”.

O **Wi-Fi** consiste em um conjunto de especificações para redes locais sem fio (WLAN - Wireless Local Área Network) baseada no padrão [IEEE 802.11](http://www.ieee802.org/11/).

Conforme, Ross, (2009, p.21) o IEEE (Instituto de Engenheiros Elétricos e Eletrônicos) produziu um conjunto de padrões e especificações para as redes *wireless* sob o título de IEEE 802.11 que definem formatos e estruturas dos sinais de curto alcance que fornecem o serviço do Wi-Fi.

O IEEE formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio e um desses grupos de trabalho foi denominado 802.11, que reúne uma série de especificações que basicamente definem como deve ser a comunicação de uns dispositivos clientes e um concentrador ou comunicação entre dois dispositivos clientes. Ao longo do tempo foram criadas várias extensões, onde foram incluídas novas características operacionais e técnicas. Ao padrão 802.11original (também conhecido como Wi-Fi). (RUFINO, 2005, p.25)

O IEEE primeiro padrão 802.11 foi criado em 1997 e, a partir de então foram surgindo vários padrões com novas características para deixar a conexão do internauta cada vez melhor. Segundo Ross (2009, p.21) “entre os padrões que foram criados as especificações mais usadas hoje são o 802.11a, 802.11b e 802 g”.

De acordo com Assunção (2013, p.20) “o IEEE 802.11 é um padrão de redes WLAN operando de 1 a 2 Mbps. Esse padrão especifica que transmissões sem fio podem ser feitas de duas formas: através da luz infravermelha ou enviando sinais de rádio”

Apesar de o padrão IEEE 802.11 permitir a transmissão das duas formas citadas acima, a transmissão por meio do rádio é a mais comum nos dias atuais.

 Já o padrão IEEE 802.11b por sua vez segundo Assunção (2013, p. 20) “adicionou duas novas velocidades (5.5 Mbps e 11Mbps). Este padrão usa a faixa de 2,4 Ghz. Neste padrão usa a modulação DSSS e possui um alcance de 100 metros indoor e 300 metros, outdoor, podendo variar de acordo com a antena.)

É válido ressaltar que a modulação DSSS significa (Direct Sequence Spread Spectrum) que é a mesma tecnologia utilizada em sistemas de navegação GPS.

Por outro lado, conforme Marcos Assunção (2013) o IEEE 802.11a trabalha com a modulação OFDM e especifica uma velocidade máxima de 54 Mbps, também suporta transmissões de 6,9, 12, 18, 24, 36 e 48 Mbps utilizando a frequência de 5 Ghz. Ele suporta dispositivos a uma distância média de 60 metros indoor e 100 metros outdoor, podendo vaiar de acordo com a antena. Na sua definição inicial suporta um máximo de 64 clientes conectados.

A modulação OFDM (Orthogonal Frequency Division Multiplexing) consiste em uma tecnologia que divide um canal de comunicação entre um número de “subcanais”. Cada um deles carrega uma parte da informação do usuário.

E, por último. Pode-se destacar o IEEE 802.11g que segundo Assunção (2013, p.20) “é um padrão que combina o melhor dos mundos do 802.11a E 802.11b. Ele adota a modulação OFDM assim como 802.11a e é compatível com 802.11b, operando também com a frequência de 2,4 Ghz.

2.2.2 Vantagens e Desvantagens da Rede Wireless (Wi-Fi)

É evidente o quanto a rede *wireless* é fundamental no cotidiano das pessoas, porém, possui pontos positivos e negativos.

Para Moraes (2004, p.184) as redes *wireless* apresentam uma série de benefícios se comparadas às redes tradicionais, entre elas, a mobilidade, a rápida e simples instalação, a escalabilidade, a redução de custo na instalação, além de ser uma solução completa para grandes, médias e pequenas empresas.

O Wi-Fi permite que as pessoas tenham acesso à internet em qualquer lugar e isto faz com que os usuários ficam conectados por mais tempo.

A computação sem fio traz à vida das pessoas uma mobilidade que ultrapassa fronteiras, pois com o Wi-Fi disponível as pessoas não necessitam ficar no mesmo local, elas podem, por exemplo, se for um Wi-Fi residencial, acessar a internet em qualquer lugar da casa, o que possibilita uma melhor comodidade e mais privacidade para as pessoas daquela residência, da mesma forma acontece em ambientes que possuem o Wi-Fi disponível. (MORAES, 2004)

Outro aspecto que é válido destacar é que quando não há fio o custo praticamente vai embora. Além disso, com o Wi-Fi gratuito disponível em locais públicos permite que muitas pessoas acessem a internet de forma rápida e eficaz. (MORAES, 2004)

Contudo, esta tecnologia também apresenta alguns pontos negativos e a segurança representa uma das grandes desvantagens do Wi-Fi, quando as pessoas acessam a internet por meio do Wi-Fi, principalmente, os gratuitos, podem estar correndo sérios riscos de ter os seus dados pessoais hackeados por pessoas mal-intencionadas na rede, portanto, é necessário ter muito cuidado. (MORAES, 2004)

 Uma rede sem fio pode ser garantida nos escritórios e nas residências, mas nunca se deve conduzir assuntos confidenciais em uma rede de Wi-Fi gratuita. Entretanto, em casa também as pessoas devem tomar cuidado com os roteadores de Wi-Fi, pois, eles têm um alcance relativamente longo e pessoas próximas a sua casa podem capturar seu sinal acessando a internet e dados e arquivos de seu computador, portanto, deve colocar uma senha difícil de ser criptografada. (MORAES, 2004)

Outras desvantagens do Wi-Fi são a interferências que são possíveis acontecer quando as pessoas estão acessando, considerando que o Wi-Fi opera na frequência 2,4 GHz. Além do alcance limitado, especialmente em edifícios, (MORAES, 2004)

* 1. Segurança na Rede Wireless

Com o advento das redes locais sem fio (WLANS – Wireless Local Área Networks) o paradigma de segurança sozinho se mostra inadequado, visto que estas redes se baseiam na comunicação via ondas de rádio e, portanto, qualquer um possuindo um receptor de rádio pode interceptar a comunicação. Em razão disso, foram criados os protocolos WEP, WPA e WPA2 para garantir a segurança na rede, entretanto, frequentemente, é necessário haver mudanças, pois, os hackers encontram maneiras de burlar a segurança destes protocolos. Geralmente, os engenheiros avaliam os protocolos para verificar sua autenticação, integridade e confidência. (LINHARES; GONÇALVES, 2015)

Conforme, Assunção 2013, este é um problema complexo, uma vez que diversas variáveis e problemas podem ocorrer e comprometer a segurança de todo ambiente. Sendo assim, para promover um nível mínimo de segurança em uma rede sem fio devem-se alcançar três objetivos.

O primeiro consiste em manter a integridade dos dados, isto significa cuidar para que os dados estejam intactos quando forem recebidos. Na sequência, o indivíduo deve se preocupar em conservar a privacidade da comunicação, considerando que ao utilizar a internet o usuário tem o desafio de enviar a informação pelo espaço aberto (acessível por todos, amigos ou inimigos) e para solucionar esse problema entra em cena os algoritmos de criptografias e estratégias de derivação dinâmica de chaves criptográficas. E, por último, não deve esquecer-se da autenticação mútua, que garante que ambos - cliente e Access Point – “se reconheçam” de forma a garantir que dispositivo “seja quem diz ser”. (ASSUNÇÃO, 2013)

Normalmente, o AP é o ponto de entrada para os recursos da rede, independentemente do tipo de informações guardadas na rede (fotos, documentos, vídeos. Fórmula supersecreta), o acesso a esses recursos deve ser controlado pela autoridade adequada. (ASSUNÇÃO, 2013)

Outra razão para o AP autenticar é porque um falso AP (fake AP, também chamado de rogue AP) poderia ser inicializado e usado para capturar o tráfico e senhas de usuários *wireless* ou causar recusa de serviço. (ASSUNÇÃO, 2013)

Se as comunicações de rede não forem criptografadas ou se a criptografia usar um algoritmo fraco haverá uma vulnerabilidade que permitirá ao invasor visualizar as comunicações enquanto elas viajam pelo meio de transmissão. A criptografia é utilizada como em qualquer outra tecnologia. Ela faz um trabalho de ocultação para que só as pessoas autorizadas possam visualizar os dados reais. (WRIGHTSON, 2014)

Por isso, que ao criar uma senha para e-mail, redes sociais, ou para qualquer finalidade na internet deve - se criar uma senha forte, isto é, difícil de ser descoberta, porque as ameaças estão na rede o tempo todo e, portanto, a pessoa não deve facilitar.

Para Wrightson, (2014, p. 101) “um cliente sem fio pode ficar vulnerável não só devido à configuração de padrão fracas, mas também devido à funcionalidade básica que um invasor possa atacar de maneiras criativas não consideradas pelos projetistas”.

Assim, entende-se que por mais que as tecnologias evoluam para o bem, há pessoas que utilizam seus conhecimentos de forma negativa roubando informações alheias e, muitas vezes, seus métodos são inovadores que nem mesmo os cientistas eletrônicos responsáveis em criar os protocolos de segurança têm conhecimento.

Há diversos fatores que podem agravar as vulnerabilidades dos dispositivos clientes, isto acontece porque os clientes sem fio estão em toda parte, além disso, sua presença é transmitida o que deixa os internautas mais vulneráveis ainda aos perigos da rede. (WRIGHTSON, 2014)

Só o fato de os clientes sem fio estar em todo lugar torna os dispositivos sem fio um alvo interessante para um invasor. Independentemente de o invasor querer atacar uma empresa específica ou apenas sentar em uma cafeteria e “ver o que pode encontrar”, ele nunca ficará sem dispositivos clientes para definir como alvo. O fato de um invasor pode testar novos ataques contra sistemas reais de maneira quase totalmente anônima sem ter que “encontrar” um alvo em potencial significa que ataques a sistemas sem fio estão em constante desenvolvimento. (WRIGHTSON, 2014)

Neste contexto, apesar de acessar bastante a internet, a maioria das pessoas são leigas em se tratando segurança na rede e acabam cometendo erros que podem expor seus dados confidenciais. A praticidade que a internet e a rede sem fio trouxeram para vida do ser humano é um aspecto que o expõe aos perigos da rede, uma vez que este começou a fazer tudo pela internet, inclusive, transações bancárias e outros assuntos confidenciais. (WRIGHTSON, 2014)

Infelizmente, há pessoas que ficam na rede simplesmente, para roubar informações confidenciais de outras pessoas, dificultando a vida das mesmas. Portanto, os usuários da rede devem ter cuidado, porque segundo Ross (2009, p.213) “se você enviar informações confidenciais a partir de um link wireless, um bisbilhoteiro poderá copiá-las. Número de cartão de crédito, senhas de conta e outras informações pessoais são vulneráveis na internet”

De acordo com Moraes (2004, p.133) “protocolos são regras e procedimentos de comunicação. Os protocolos de rede operam nas camadas físicas, enlace de dados e rede. São responsáveis por informações de endereçamento e rolamento, verificação de erros e requisições de retransmissão”

 A princípio, os IEEE criaram o protocolo de segurança chamado WEP (Wire Equivalent Privacy) o qual era usado para criptografia de dados, o WEP criptografa o tráfego entre o cliente e o access point . A criptografia é realizada na camada enlace, usando o algoritmo criptográfico Rc4 da RSA (40 – bi secret key).



Figura 2 Diagrama de Blocos do Protocolo WEP, Fonte: PAIM, 2014

Este protocolo foi criado e acharam diversas falhas nele e, por isso, o IEEE criou um novo protocolo chamado WPA. (Wi-Fi Proteced Access).

O protocolo WPA (Wi-Fi Proteced Access) atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata de cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário (área coberta efetivamente pelo padrão WEP) utiliza, para isso, padrões 802.1x e EAP (Extensible Authentication Protocol). (RUFINO, 2005)

:

Figura 3 Diagrama de Blocos do Protocolo WPA Fonte: PAIM,2014

Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados. Para solucionar esses problemas, o WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. (RUFINO, 2005)

 O foco do WPA está na combinação algorítmica e na temporalidade da chave que são considerados os pontos mais vulneráveis e então, criou diferentes modelos de protocolo para atender os usuários em ocasiões diferentes, pois, Rufino (2005, p.38) afirma que:

Considerando os dados de diversidade e os ambientes onde uma rede sem fio pode existir( ambientes domésticos, pequenos escritórios, pequenas e grandes empresas etc. pensou-se ser razoável que o WPA tivesse também diferentes modelos de segurança para ter melhor aderência às diferentes necessidades [...] os protocolos usados para cifrar as informações podem ser de dois tipos: um voltado para pequenas redes e de uso doméstico, onde existirá uma chave compartilhada previamente ( Pre shared key, ou WPA- PSK ) conhecida como chave master que será responsável conhecida como equipamento pelo concentrador, e outro é conhecido como infra- estrutura , que exigirá, ao menos, a figura de um servidor de autenticação9 RADIUS), portanto um equipamento adicional.

 No protocolo WPA há o método da chave compartilhada e segundo Rufino (2005, p. 38) “sua principal vantagem é sua simplicidade, pois não necessita de equipamentos extras como servidores de autenticação, sendo de fácil instalação e uso”.

 Uma diferença fundamental em relação ao WEP é que não existem problemas conhecidos (divulgados) nos protocolos usados com WPA – PSK TKIP, dentre eles, é o responsável pela troca dinâmica das chaves usadas em uma determinada comunicação estabelecida.

O protocolo WPA veio cheio de novidades o que deixa navegação dos usuários mais segura.

Dentre as novidades do WPA há o protocolo TKIP (Temporal Key Integrity Protocol) responsável pela gerência de chaves temporárias usadas pelos equipamentos em comunicação, possibilitando a preservação do segredo mediante a troca constante da chave, visto que uma das vulnerabilidades do WEP advém exatamente das chaves utilizadas serem estáticas e as partes que não atravessaram a rede em claro. (RUFINO, 2005)

O protocolo WPA foi criado na intenção de corrigir as vulnerabilidades deixadas pelo protocolo WEP, sendo assim, conforme Rufino (2005, p. 39).

Outra vulnerabilidade do WEP corrigida no WPA é usada no TKIP é o aumento significativo do tamanho do vetor de iniciação (Inicialization Vector) que passou dos originais 24 para 48 bits, permitindo um substancial elevação na quantidade de combinação possíveis, tornando ataques baseados na relativamente rápida repetição dos valores[...] Diferentemente do que ocorria no WEP O TKIP pode ser configurado para substituir o vetor de iniciação e cada pacote, por sessão ou por período (este último compatível com WEP) As vantagens dessa modalidade de troca de vetor são claras: quanto mais rápido essa troca ocorrer, menor será a chance de um atacante conseguir descobrir o valor do vetor de iniciação.

Então, as mudanças no protocolo WPA permitem que os usuários da rede naveguem com mais tranquilidade, porque a maior preocupação destes engenheiros consiste em criar métodos para impedir que invasores entrem na rede particular do usuário. Eles procuram criar um método ao qual nenhum hacker mal-intencionado possa burlar e, para tanto, vão fazendo modificações no protocolo a fim de obter sucesso na criação de um protocolo de segurança que realmente permite que os usuários naveguem na rede com tranquilidade.

Portanto, de acordo com Rufino (2005, p. 39) “um modelo para a autenticação também foi definido no WPA, conhecido como EAP (Entensible Authentication Protocol), que permite integrar soluções de autenticação já conhecidas e testadas”.

O EAP utiliza o padrão 802.11x e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital [...]. Mesmo que nem todos estejam possíveis de uso em conjunto com WPA, vários deste o são, o que torna bastante flexível essa solução porque permite integrar padrões de autenticação tradicionais e já em uso para os usuários discados, por exemplo, como RADIUS, e incorporar novos usos (autenticar rede sem fio (RUFINO, 2005, 39)

Várias soluções tentaram resolver o problema da WEP, no entanto, os problemas só foram realmente solucionados com a definição da especificação IEEE 802.11i, que definiu o WPA e WPA2.

O WPA foi lançado pela Wi-Fi *Alliance* como uma atualização de *firmware* para sistemas baseados em WEP antes mesmo da padronização IEEE 802.11i. A primeira versão WPA (conhecida por WPA1) foi definida na terceira versão do padrão e logo foi seguida pelo WPA2, que foi baseado na versão final. (ASSUNÇÃO, 2013).

A **Figura 4** ilustra a evolução em ordem cronológica dos mecanismos de segurança que protegem redes WLAN da família 802.11



Figura 4. Evolução dos Mecanismos de Segurança 802.11 Fonte:LINHARES; GONÇALVES,2015

Os processos de autenticação são os mesmos no WPA e WPA2, entretanto, os mecanismos para garantir a confidencialidade e a integridade dos dados são diferentes. O WPA também consegue identificar problemas nos dados através do CRC. E uma das características interessantes do WPA2 é que ele possui um modo de detecção de ataques de *Denial* of *Service* (DoS), que é a versão original não completa. (ASSUNÇÃO, 2013).

2.3.1 Vulnerabilidades do Protocolo WPA

O WPA solucionou praticamente todas as vulnerabilidades apresentadas pelo protocolo WEP. Porém, falhas em sua implementação o tornaram vulnerável: por exemplo, a fraqueza no algoritmo de combinação de chave - tendo conhecimento de algumas chaves RC4 (menos de 10 chaves) geradas por IVs, cujos 32 bits mais significativos são os mesmos, um atacante pode achar a chave de criptografia de dados e a chave de integridade [10]. PSK é susceptível a ataques de dicionário - Diferentemente do ataque de força bruta, que tenta todas as possibilidades possíveis exaustivamente, o ataque de dicionário tenta derivações de palavras pertencentes a um dicionário previamente construído. Este tipo de ataque, geralmente é bem sucedido porque as pessoas têm o costume de utilizarem palavras fáceis de lembrar e que normalmente pertencem a sua língua nativa. Além do dicionário, informações capturadas durante o 4-*Way-Handshake* são necessárias para a quebra da PSK. Um detalhe que não é muito sabido é que se a chave PSK for de mais de 20 caracteres este ataque não funciona em tempo factível. (LINHARES; GONÇALVES, 2015)

Negação de Serviço - O MIC possui um mecanismo de proteção para evitar ataques de força bruta, porém esse mecanismo acarreta um ataque de negação de serviço (DoS). Quando dois erros de MIC são detectados em menos de um minuto o AP cancela a conexão por 60 segundos e altera a chave de integridade. Portanto, com uma simples injeção de pacotes mal formados é possível fazer um ataque denegação de serviço. Além disso, o WPA continua sofrendo dos mesmos ataques de negação de serviço que o WEP já sofria, visto que esses ataques são baseados em quadros de gerenciamento. (LINHARES; GONÇALVES, 2015)

2.3.2 Criptografia nas Redes Sem Fio

Criptografia é o processo de obscurecer os dados para que qualquer pessoa não autorizada que os intercepte não consiga entendê-los. Ela seria relativamente irrelevante se não pudéssemos voltar os dados “misturados” à sua forma original. Logo a criptografia é um processo de duas vias. Pegar os dados criptografados e transformá-los novamente em dados legíveis chama-se descriptografia. Há dois sistemas básicos para a criptografia dos dados: criptografia de chave compartilhada e criptografia de chave pública. (WRIGHTSON, 2014).

A criptografia compartilhada é uma técnica de criptografia de dados extremamente antiga usada desde o tempo dos romanos. Ela usa a mesma chave tanto criptografar quanto para descriptografar os dados e, portanto, às vezes é chamada de criptografia simétrica. (WRIGHTSON, 2014).

De acordo com o Wrightson, (2014) no protocolo WEP usa a criptografia da chave compartilhada na qual é preciso inserir uma chave de criptografia no ponto de acesso e, então, inserir a mesma chave em qualquer cliente que precise de acesso à rede. (WRIGHTSON, 2014).

O WEP é usado não só para autenticação, mas também para a criptografia. Inclusive, já dissemos anteriormente, a mesma chave é utilizada em ambos os processos. A criptografia é feita utilizando-se uma chave compartilhada que é previamente configurada em todos os APs e clientes. O processo de distribuição manual da chave leva muito tempo e é extremamente contraprodutivo. O uso de soluções de distribuições automatizadas da chave (como o SNMP) pode levar a problemas de segurança por causa de técnicas como *Sniffing e Man in the Middle* (mesmo em teoria a chave sendo criptografada). (ASSUNÇÃO, 2013)

O padrão original é a chave WEP de 40 bits, apesar de algumas implementações hoje utilizarem um valor de 104 bits para a chave. A chave WEP é adicionado um Vetor de Inicialização (IV) de 24 bits.

A princípio o WEP parecia ser um protocolo que de fato garantiria a segurança dos usuários da internet, porém, os engenheiros descobriram falhas tanto da autenticação, quanto da criptografia do WEP as quais ASSUNÇÃO, (2013) enumera:

A mesma chave WEP é usada para autenticação e Criptografia; WEP não utiliza autenticação mútua; não há integridade real dos dados ao usar um valor de *checksum* (CRC); a chave do WEP 40 bits é muito curta para sobreviver a um ataque de força bruta, e mesmo se “sobreviver” existem falhas conhecidas no RC4 que permitem a quebras de praticamente qualquer chave; o WEP não provê geração e o gerenciamento de chave dinâmicas; o Vetor de Inicialização de 24 bits do WEP é muito pequeno para evitar colisões em um pequeno espaço de tempo. Isso resulta em mensagens com XOR aplicadas com o mesmo IV, dando aos atacantes muita informação para realizar as criptoanálise e permitindo deduzir a chave. (ASSUNÇÃO, 2013, p.34 e 35)

Portanto, segundo Wrightson (2014) apesar de a chave compartilhada poder ser usada com rapidez e de forma simples, ela não é totalmente segura, por outro lado, a infraestrutura de chaves públicas é extremamente segura.

A infraestrutura das chaves públicas (também chamadas de criptografia assimétrica) usa uma chave separada para criptografar e descriptografar dados. Isso pode ser um pouco confuso para as pessoas que estão iniciando na ICP, mas só é preciso saber que alguns cálculos bem complexos são usados em segundo planos. Esta é considerada a maneira mais confiável de criptografar dados. (WRIGHTSON, 2014).

Os dois métodos básicos da criptografia de dados são as cifras de fluxo e as cifras de bloco. Em cifra de fluxo, normalmente os dados são criptografados um byte de cada vez e o texto cifrado as saídas tem o mesmo tamanho (ou quase) do texto sem a criptografia de entrada. Em cifra de bloco, o algoritmo de criptografia trabalha com blocos de dados de tamanho fixo. Por exemplo, se um algoritmo de criptografia trabalhar com blocos de dados de 32 bytes, uma mensagem criptografia de 128 bytes será dividida em quatro blocos exclusivos de texto cifrado. (WRIGHTSON, 2014).

O WEP fazia parte do padrão sem fio 802.11 originais introduzido em 1999, o qual fornece uma criptografia na camada 2 no modelo OSI, a camada MAC ou de enlace. Utiliza o algoritmo de criptografia RC4 para criptografar dados de um sistema e usa um sistema de chave compartilhada. (WRIGHTSON, 2014)

De acordo com Wrightson, (2014, p.57) o algoritmo RC4 que foi projetado em 1987 por Ron Rivest da RSA Security, é um algoritmo de criptografia muito forte quando implementado de maneira segura para outros protocolos como o WPA.

A norma IEEE 802.11i consistia de três partes principais TKIP, CCMP, 802.1X e gerenciamento das chaves, sua implementação completa também conhecida como RSN faz uso da cifra de bloco Advanced Encryption Standard (AES) em oposição a cifra de fluxo RC4 usada no WEP e no WPA (IEEE 802.11i-2004, 2008).

Ninguém pode com legitimidade afirmar que um sistema de segurança é inquebrável, contudo as redes sem fio RSN/WPA foram desenvolvidas com profundo envolvimento de especialistas e receberam muito mais análise e testes da comunidade que trabalha com criptografia do que o WEP recebeu quando foi desenvolvido. (CORRÊA, 2008)

O IEEE, já sabendo das fragilidades de segurança existentes no WEP, estava trabalhando em um novo padrão que pudesse garantir, dentre outras coisas, o sigilo das informações que trafegavam pelas ondas eletromagnéticas através do ar. (CORRÊA, 2008)

A Wi-Fi Alliance criou o WPA que vinha a ser, portanto, esse subconjunto do trabalho que estava sendo desenvolvido pelo IEEE, nesse subconjunto apenas o TKIP era especificado. A Wi-Fi Alliance fez um planejamento para garantir a interoperabilidade entre os diversos fabricantes, e que esse novo padrão fosse adotado em dispositivos capazes de suportar o padrão de segurança anterior, portanto, os dispositivos deveriam estar preparados para trabalhar com o WEP, bem como suportar inovações que ainda estavam por surgir fruto do trabalho do IEEE, reforçando assim o caráter transitório do WPA quando foi concebido. (CORRÊA, 2008)

O WPA foi projetado para aperfeiçoar a segurança das redes sem fio. Ele foi desenvolvido de duas formas, podemos dizer: WPA para uso pessoal e o WPA para uso empresarial. (CORRÊA, 2008)

Para utilizar o protocolo WPA ou WPA2 você deve usar o modo OSA (Open System Authentication – Autenticação do sistema aberto). A opção de SKA (Shared Key- chave compartilhada) exige o uso do WEP. (ASSUNÇÃO, 2013)

O padrão 802,11i define dois modos de operação o *Personal* e o *Enterprise.* Quando operando no modo Personal, o uso da chave pré- compartilhada (PSK) é obrigatório. É o conhecimento da PSK que faz com que a estação wireless seja autenticada. Esse conhecimento é obtido através de um processo, onde ambos os lados utilizam a PSK para gerar chaves de criptografia. Com essas chaves já geradas, os dois dispositivos serão capazes de criptografar/descriptografar toda a comunicação entre eles. (ASSUNÇÃO, 2013)

A chave pré-compartilhada (PSK) é gerada com base em uma “senha” (passphrese) que pode variar entre 8 e 63 caracteres ASCIL, podendo também usar números binários de 256 bits. Ao criar a *passphrase* é importante tomar algumas precauções.como: não usar palavras que possam ser usadas com um ataque de dicionário, não usar nomes e datas associadas à sua pessoa; combine letras, maiúsculas, minúsculas e números; use ao menos 20 caracteres. (ASSUNÇÃO, 2013)

É válido ressaltar que apesar de todas as precauções ainda é possível “quebrar” uma chave WPA1/WPA2 ou descobrir a *passphrase.* (ASSUNÇÃO, 2013)

A PSK não tem nada a ver com o modo SKA que é usado no protocolo WEP, contudo, seja WEP ou WPA PSK, a chave deve ser configurada nos dispositivos que querem comunicar entre si. Por isso, o modo de operação (Personal) é recomendado apenas para redes pequenas e ainda assim deve tomar muito cuidado para não deixar a *passphrase* configurada por muito tempo. (ASSUNÇÃO, 2013)

Para criptografar os dados, o Access Point utiliza uma tecnologia chamada TKIP (Temporal Key Integrity Protocol). O TKIP usa a PSK para gerar chaves de criptografia individuais para cada estação cliente. Estas chaves de criptografia estão constantemente mudando (ao contrário das chaves estáticas WEP). Essa solução é muito melhor do que a WEP, pois mesmo se uma chave for quebrada não irá comprometer toda sessão. (ASSUNÇÃO, 2013)

O WPA- Enterprise é muito mais difícil de configurar em comparação com o WPA- PSK. Ele requer servidores adicionais no *backend* para a autenticação de cada usuário (em geral um servidor RADUIUS). Embora inicialmente o WPA- Enterprise seja mais difícil de configurar, é mais fácil de administrar em empresas maiores e fornece uma camada melhor de segurança. (WRIGHTSON, 2014)

Quando utilizamos o modo Enterprise, o padrão 802.1X nos fornece uma interface para controle de acesso baseado em portas além de outros recursos úteis. Basicamente, o 802.1X é um protocolo da camada de enlace (modelo OSI), no qual o propósito é prevenir acessos não autorizados a serviços, como uma rede Wi-Fi. Uma das características mais curiosas é a utilização de um servidor Radius externos para tirar a “responsabilidade” da autenticação da chave PSK local do AP. Este protocolo é composto por três componentes principais: Suplicante, Autenticador e Servidor de Autenticação. (ASSUNÇÃO, 2013)

Suplicante: esse papel é adotado por um dispositivo que deseja acessar recursos providos pelo Autenticador. Normalmente é uma estação cliente. Autenticador: esse papel é adotado por um dispositivo que deseja restringir acesso aos seus recursos, libertando-os apenas para as estações *wireless* que possam provar a sua identidade. Normalmente é o Access Point. Servidor de autenticação: esse papel é adotado pelo dispositivo que realiza a função de autenticação para validar a identidade do suplicante. Normalmente é um servidor Radius. (ASSUNÇÃO, 2013)

Numa rede Wi-Fi o suplicante tipicamente é uma estação Wi-Fi tentando se conectar a uma infraestrutura. O autenticador (normalmente o AP) repassa a comunicação de autenticação recebida do suplicante para o servidor de autenticação. É no Servidor de Autenticação (no caso o Radius) que as credenciais serão checadas o resultado da autenticação, seja sucesso ou falha, é passado para o autenticador. Baseado nesse resultado o acesso é permitido ou negado. (ASSUNÇÃO, 2013)

O Wi-Fi de acesso protegido 2 (WPA2) foi uma substituição ao protocolo WPA, embora este fosse bastante seguro em relação ao padrão anterior WEP. O WPA2 utiliza um protocolo denominado Advanced Encryption Standard (AES), que é muito eficiente, mas possui a desvantagem de exigir bastante processamento. (HOROVITS, 2013)

O seu uso é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de equipamentos de redes pouco sofisticadas. O principal objetivo do WPA2 é suportar as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e codificação, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio. (HOROVITS, 2013)

 Enfim, o Protocolo de Integridade da Chave Temporal (TKIP- TEMPORAL Key Integrity Protocol) é obrigatório na implementação do WPA (WPA1) e opcional no WPA2. Mesmo que o TKIP seja baseado no RC4, ele é um protocolo muito superior. Já o CCMP (Counter Mode with CBC-MAC Protocol) é obrigatório para o WPA2. É o conjunto de iniciais mais bizarras e confusas que existe. “Counter Mode” refere-se ao modo de operação do AES, que é a cifra utilizada ao invés do RC4. Atualmente é considerado um dos algoritmos de criptografia de bloco mais confiáveis. O Código de Autenticação de Mensagens de Bloco (CBC-MAC-Cipher Block Chaining Message Authentication Code) (ASSUNÇÃO, 2013)

2.3.3 Ataques às Redes Sem Fio

Os ataques contra as redes sem fio decorrem da sua própria estrutura, uma vez que ponto de acesso precisa anunciar a existência da rede, de modo que os clientes possam se conectar e usufruir todos os serviços e recursos fornecidos. Para isso, frames especiais, conhecidos como *beacons* (balizas), são enviados periodicamente, facilitando a descoberta de uma rede sem fio, inclusive por pessoas mal-intencionadas. Na realidade, o objetivo dos ataques não é apenas comprometer a rede sem fio, mas também ganhar acesso ou comprometer a rede cabeada, podendo levar à exploração de todos os recursos que a rede oferece. (ANDRADE; SOARES; COUTINHO E ABELÉM, 2015)

Redes mal configuradas tornam-se vulneráveis a ataques de intrusos mal-intencionados. Essas redes dispõem de algumas facilidades aos invasores, como: impossibilidade de identificação da origem do ataque. Na maioria dos casos, as tentativas são realizadas a partir de uma análise de tráfego, que pode ser ativa (pacotes são enviados para a rede alvo) ou passiva (não há introdução de pacotes na rede) (PIZON, 2009)

No ataque passivo uma pessoa não autorizada obtém acesso a uma rede, mas não altera o conteúdo dos dados. Armado com um adaptador wireless em modo promíscuo, um intruso pode capturar pacotes de dados e fazer análise do tráfego da rede. Ataques desse tipo não deixam indícios da presença de um intruso na rede, uma vez que não é preciso se associar a um *access point* para tentar monitorar os pacotes. Os dois tipos de ataques passivos são: escuta: monitoramento da transmissão para obter o conteúdo que está sendo transmitido, análise do tráfego: monitoramento da transmissão para entender os padrões de comunicação. (REIS; GOULART; MENDES, 2015)

No ataque ativo uma pessoa desautorizada obtém acesso à rede e modifica o conteúdo da mensagem que está sendo transmitida. Uma vez conectado a WLAN um indivíduo pode alterar sua configuração. Ataques ativos podem ser detectados, mas nem sempre impedidos. Por exemplo, um intruso que conseguir clonar um endereço MAC autorizado, poderia navegar pelos access point e remover todos os filtros de MAC, facilitando seu acesso. (REIS; GOULART; MENDES, 2015)

Estes são os tipos de ataques ativos, que podem ser usados combinados: disfarce: o atacante personifica um usuário e com isso obtém algum dos recursos desautorizados da rede; repetição: o atacante intercepta a transmissão e envia como se fosse o usuário legítimo; modificação de mensagem: o atacante altera uma mensagem legítima, apagando, adicionando, editando ou reordenando a própria mensagem; negação de serviço: o atacante dificulta o uso normal ou o gerenciamento dos dispositivos da rede, através de sobrecarga, impossibilitando que ele atenda a todas as requisições que lhe são feitas.(REIS; GOULART; MENDES, 2015)

 Na literatura há diversos ataques inerentes a redes sem fio, porém, os são executados são: *Sniffing*, *Hijacking* e DoS. Originalmente, a escuta de rede (Sniffing) foi concebida como uma ferramenta de análise de tráfego. (MAGALHÃES, 2011).

As ferramentas de escuta foram desenvolvidas inicialmente em uma época em que as tecnologias de rede cabeadas disponíveis, como hubs e repetidores, não direcionavam os pacotes diretamente ao seu destinatário. Os dados eram enviados em broadcast. Tendo isso em mente, o *Sniffing* se tornou uma ferramenta importante também para as redes sem fio, uma vez que os dados também não são enviados para uma determinada estação e sim para o meio de transmissão, o ar, não sendo nem mesmo necessário estar associado à rede para interceptar os dados. (MAGALHÃES, 2011)

O principal motivo deste tipo de ataque é invadir redes fechadas. Uma rede pode ser fechada por filtro de MAC, filtro de IP e autenticação. No caso de uma rede fechada apenas por MAC e/ou IP, pode-se fazer uma análise das estações conectadas e então simplesmente trocar o endereço MAC e/ou IP da estação invasora. (MAGALHÃES, 2011)

 Sobre os ataques de *Hijacking* ou roubo de sessão, compreende-se que são executados falsificando a tabela ARP do equipamento wireless (um AP, por exemplo). O atacante então pode se associar a um IP válido na rede. A partir daí todos os dados direcionados para o AP passam pelo atacante primeiro. Esse ataque também é conhecido como o ataque do homem do meio, ou interceptador (ULBRICH; VALLE, 2009).

O ataque força bruta é um dos ataques mais famosos no que diz respeito à autenticação. Este tipo de ataque consiste na tentativa sistemática de encontrar chaves possíveis, até que a chave correta seja encontrada. No pior dos casos, este método tem de percorrer todo o espaço de pesquisa até encontrar a chave correta. O tamanho da chave é um dos aspetos a considerar que determina a fiabilidade de efetuar um ataque de força bruta. Basicamente, quanto maior for o tamanho da chave, maior vai ser a dificuldade de efetuar um ataque deste tipo. Também se pode dificultar este tipo de ataques ao ofuscar os dados, sendo assim, mais complicado para o atacante de reconhecer quando é que descodificou o código. (GONÇALVES; SILVA, 2015)

2.3.4 Ferramentas para Ataques nas Redes Sem Fio

As ferramentas de auditoria e testes de segurança em redes sem fio são também amplamente utilizadas para realizar ataques. Também são apresentadas algumas ferramentas com a função específica de ataque. (MAGALHÃES, 2011)

Uma das primeiras ferramentas desenvolvidas para mapeamento de Wi-Fi para ambiente Windows foi a Netstumbler, que tem como característica: possibilitar interação com equipamentos GPS, produzindo um mapa preciso de acessos identificados. (HOROVITS, 2013)

Uma grande vantagem desse aplicativo é estar atualizado em relação aos padrões do mercado. Antes, tal modelo era limitado ao padrão 802.11b. Atualmente, com as atualizações sofridas, tornou-se viável para tal ferramenta identificar redes em todos os padrões comerciais (802.11/a/b/g). (HOROVITS, 2013)

Essa ferramenta possui uma boa flexibilidade, possibilita identificar as redes, nomes, endereços MAC e demais informações disponíveis. Entretanto, não possibilita a captura de tráfego e nem possui métodos para quebrar senhas WEP, WPA e WPA2. Uma das funcionalidades exclusivas é a capacidade de continuar uma análise salva anteriormente, o que permite adicionar informações acerca de redes já catalogadas e paralelamente de novas redes detectadas a formar um só conteúdo. (RUFINO, 2005).

Já a Ferramenta Airsnort é uma ferramenta antiga, mas ainda bastante utilizada, mesmo com algumas limitações em termos de quantidades de placas e chipsets diretamente suportados como (Orinoco/Proxim, Prism2 e Atheros). O Airsnort tem uma característica ímpar, que é a possibilidade da quebra de chave WEP ser feita em meio à captura do tráfego. Dessa maneira, a quantidade de pacotes coletados não precisa ser previamente definida como ocorre com outras ferramentas, nas quais primeiro é feita a captura dos pacotes e, em seguida, o processamento, visando à quebra da chave. Outras funcionalidades dessa ferramenta incluem informações relacionadas (SSID e endereço MAC) na identificação de redes, e possibilita uma varredura em todos os canais ou apenas em um canal de interesse. (HOROVITS, 2013)

O Wireshark é um analisador de rede com suporte aos mais variados protocolos, sendo também utilizado como *sniffe*r. É um programa portável a sistemas operacionais como Windows, Linux, BSDs, Solaris e MAC OS (WIRESHARK FOUNDATION, 2011).

A ferramenta Weplab, realiza ataques utilizando um dicionário de senhas ou ataques estatísticos para a quebra de senhas. Para tal é 42 necessário um arquivo de captura com pacotes de dados suficientes. Uma interface gráfica encontra-se disponível no site do projeto (MARTÍN, 2005).

2.4 Teste de Invasão do WEP

Para Lima; Lijó; Souza, (2014) devido às características da tecnologia de comunicação sem fio a segurança é a principal barreira contra a rede e a sua utilização o que requer habilidades especiais por parte do usuário.

Os testes de intrusão o em redes sem fio (*Pentest Wireless*) têm como objetivo atestar falhas existentes nos principais protocolos, devido ao uso inadequado da tecnologia ou a falta de conhecimento na elaboração de configurações que possam comprometer a segurança dos dados que trafegam em uma rede. (LIMA; LIJÓ; SOUZA, 2014)

Redes mal configuradas tornam-se vulneráveis a ataques de intrusos mal-intencionados. Essas redes dispõem de algumas facilidades aos invasores, como: impossibilidade de identificação da origem do ataque. Por isso, políticas de segurança devem ser adotadas para certificar e diminuir os riscos envolvendo serviços por meio de redes sem fio. (LIMA; LIJÓ; SOUZA, 2014)

De uma forma completa, as fases que compreendem um teste de intrusão são: aquisição de Informações, varredura, obter acesso, manter acesso e limpar rastros. S. Ali and T. Heriyanto, 2011, *apud* Lima; Lijó; Souza, 2014)

Na primeira etapa são coletadas todas as informações sobre o alvo, é possível identificar os protocolos de segurança, nível de potência do sinal do ponto de acesso, endereço físico de rede, entre outros. Para realizar o procedimento de identificação é necessário configurar a placa de rede em modo monitor com a utilização do airmon-ng (especifica a interface da rede sem fio) no terminal Linux (LIMA; LIJÓ; SOUZA, 2014)

A varredura verifica os hosts ativos na rede e identifica a versão dos sistemas operacionais e os serviços em execução, na sequência se obtém o acesso - o objetivo nessa etapa é conseguir acesso a um determinado host da rede; manter o Acesso - Essa fase visa manter o acesso, explorando portas abertas do sistema alvo; Limpar Rastros- nessa etapa os rastros que identificam a intrusão são apagados. (LIMA; LIJÓ; SOUZA, 2014).

Umas das ferramentas para quebrar senha WEP, é o aircrack-ng que possui melhor compatibilidade com o Linux.

 Sendo assim, de acordo com Pasa (2015) é preciso identificar interface wireless com o comando “iwconfig”; colocar interface wireless em modo de captura (monitor)

 airmon-ng start wlan0



 Após este comando cria automaticamente a interface “mon0”

1ºPasso para começar a captura

 airodump-ng -w captura\_wep-c 4 --bssid 00:1D:0F:F5:8D:E0 mon0



2º realizar falsa autenticação no AP (abrir outro terminal)

 aireplay-ng -1 0 -a 00:1D:0F:F5:8D:E0 mon0



3º gerar tráfego para captura (abrir outro terminal)

 aireplay-ng -3 -b 00:1D:0F:F5:8D:E0 mon0



 Objetivo de gerar pacotes ARP na rede e acelerar o processo de captura até ter a quantidade necessária de IVs (Inicialization Vector) para realizar a descriptografia da senha.



Após a captura de cerca de 20.000 IVs já é possível tentar realizar a quebra da senha com o aircrack-ng,

4ºDescriptografar os dados obtidos no arquivo “captura\_wep-01.cap”



aircrack-ng “captura\_wep-01”



Key found! [52:45:44:45:53] (ASCII: REDES)

 Senha “redes”.

A figura mostra a decriptação com sucesso senha configurada com o protocolo WEP.

O tempo necessário para descobrir uma senha com protocolo wep variar de 3 a 20 minutos nos melhores caso dependendo da distância entre o roteador e o invasor, assim como, da quantidade de trafego existente e que se pode gerar com a injeção de pacotes. Ao contrario o WPA não possuem falhas conhecidas de segurança, que permitam descobrir a chave rapidamente. Apesar disso, ainda é possível usar ataques de força bruta para descobrir passphrases fáceis, baseadas em palavras do dicionário ou sequências numéricas simples.

O WPA aumenta o nível de segurança embora não seja 100% confiável (PAIM,2014)

2.5 Segurança da Informação: física e lógica

Hoje em dia há uma grande preocupação em como manter os dados seguros em meio a essa revolução tecnológica dos instrumentos de informação, este é um tema bastante atual que tem gerado diversos debates. Desta forma, vão sendo criado elementos para garantir um poço de tranquilidade aos usuários da rede.

A política de segurança deve ser estabelecida visando à prevenção de incidentes, inviabilizando acessos indevidos, risco aos equipamentos e a estrutura lógica dos ativos de TI (Tecnologia da Informação). (LEITE, 2011)

Devido à facilidade em acessar equipamentos de informática e à grande evolução de conhecimento técnico, as fraudes estão se disseminando, pois normalmente tornam-se lucrativa delimitando assim um grande investimento. Os especialistas em crimes cibernéticos possuem uma visão estratégica e planejamento para aplicar golpes e lesionar os concorrentes do mercado comercial, afinal uma simples falha de segurança pode representar uma infiltração e consequentemente o roubo de informação ou falha no procedimento habitual das instituições. (LEITE, 2011)

Portanto, a Gestão de Segurança da Informação é “a ação que protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio” (ABNT ISO/IEC 17799).

Neste contexto, algumas medidas preventivas de ordem física e lógica devem ser tomadas.

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Este tipo de segurança deve se basear em perímetros predefinidos nas imediações dos recursos computacionais, podendo ser explícita como uma sala cofre, ou implícita, como áreas de acesso restrito. (PINHEIRO, 2009)

A segurança física pode ser abordada sob duas formas: segurança de acesso - trata das medidas de proteção contra o acesso físico não autorizado; segurança ambiental – trata da prevenção de danos por causas naturais.

Quanto à segurança lógica pode-se dizer que é um processo em que um sujeito ativo deseja acessar um objeto passivo. O sujeito é um usuário ou um processo da rede e o objeto pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc.). (PINHEIRO, 2009)

A segurança lógica compreende um conjunto de medida e procedimentos, adotados pela empresa ou intrínsecos aos sistemas utilizados. O objetivo é proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas. (PINHEIRO, 2009)

2.6 Computação Forense

A Forense Computacional pode ser definida como a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional. (FORENSE DIGITAL/COMPUTACIONAL, 2007)

Atualmente, existem peritos especializados em diversas áreas científicas, entre elas: Análise de documentos (documentos cópia); Criminalística (Balística, Impressões digitais, substâncias controladas); Computação (Forense Computacional ou Forense Digital); entre outras como: Patologia, Psicologia, Toxicologia, Metrologia. FORENSE DIGITAL/COMPUTACIONAL, 2007)

A Forense Digital/Computacional tem como objetivo suprir as necessidades das instituições legais no que se refere à manipulação das novas formas de evidências eletrônicas. Ela é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional. Através da utilização de métodos científicos e sistemáticos, para que essas informações passem a ser caracterizadas como evidências e, posteriormente, como provas legais de fato. (FORENSE DIGITAL/COMPUTACIONAL, 2007)

É utilizada com fins: legais, como por exemplo: investigação de casos de espionagem industrial, roubo de identidade, extorsão ou ameaças; ações disciplinares internas. As etapas da investigação forense são: coleta, exame, análise e resultados. FORENSE DIGITAL/COMPUTACIONAL, 2007)

A Coleta de dados consiste na identificação de possíveis fontes de dados: computadores pessoais, laptops; Dispositivos de armazenamento em rede; – CDs, DVDs; portas de comunicação: USB, Firewire, Flash card e PCMCIA; – Máquina fotográfica, relógio com comunicação via USB, etc. O Exame tem por finalidade localizar, filtrar e extrair somente as informações relevantes à investigação, neste processo se deve considerar: capacidade de armazenamento dos dispositivos atuais; quantidade de diferentes formatos de arquivos existentes Ex.: imagens, áudio, arquivos criptografados e compactados; muitos formatos de arquivos possibilitam o uso de esteganografia para ocultar dados, o que exige que o perito esteja atento e apto a identificar e recuperar esses dados; em meio aos dados recuperados podem estar informações irrelevantes e que devem ser filtradas. Ex.: o arquivo de log do sistema de um servidor pode conter milhares de entradas, sendo que somente algumas delas podem interessar à investigação. Após a restauração da cópia dos dados, o perito faz uma avaliação dos dados encontrados. FORENSE DIGITAL/COMPUTACIONAL, 2007)

Após a extração dos dados considerados relevantes, o perito deve concentrar suas habilidades e conhecimentos na etapa de análise e interpretação das informações, com a finalidade de identificar pessoas, locais e eventos; determinar como esses elementos estão inter-relacionados. A interpretação e apresentação dos resultados obtidos é a etapa conclusiva da investigação, na qual o perito elabora um laudo pericial que deve ser escrito de forma clara e concisa, listando todas as evidências localizadas e analisadas. FORENSE DIGITAL/COMPUTACIONAL, 2007)

**CONCLUSÃO**

Esta pesquisa foi importante, porque possibilitou a compreensão sobre a importância dos protocolos de segurança na prevenção contra os ataques nas redes sem fio.

O Wi-Fi é um elemento que facilita a vida do ser humano, porém, o indivíduo deve saber utilizá-lo para não se expor aos perigos da internet.

Além disso, ficou claro que é viável buscar o conhecimento sobre os mecanismos de segurança no mundo virtual, porque, a internet não só proporciona praticidade e rapidez ao ser humano, como também, expõe os usuários a diversos perigos.

De acordo com a pesquisa entende-se que os crimes na internet têm aumentado consideravelmente, entretanto, deve-se destacar que muitas pessoas também fazem uso das redes sem fio sem considerar os perigos.

Sendo assim, esta pesquisa teve o propósito de mostrar que a precaução e o conhecimento sobre medidas de segurança no universo virtual são alternativas de grande valia contra os ataques virtuais.

Foi dada ênfase ao protocolo WPA, que é objeto de estudo desta pesquisa e, neste processo de segurança entende-se que à medida que o tempo passa, novas ameaças vão surgindo e o IEEE precisa criar novos protocolos para conter os ataques de hackers mal-intencionados nas redes.

Portanto, conclui-se que o WPA solucionou praticamente todas as vulnerabilidades apresentadas pelo protocolo WEP, porém, falhas em sua implementação como a fraqueza no algoritmo de combinação de chave; PSK susceptível a ataques de dicionário e a negação de serviço, ainda, o tornam vulnerável, contudo, esta modalidade de protocolo proporciona diversos benefícios aos usuários da rede. (LINHARES; GONÇALVES, 2015)

 O WPA introduz diversos mecanismos para resolver os problemas de segurança associados ao WEP: Regras para o IV e IV estendido de 48; regras para a escolha e verificação de IVs para tornar ataques de reinjeção de pacotes ineficazes; usa um novo campo de 64 bits, o MIC (Message Integrity Code), para verificar se o conteúdo de um quadro de dados possui alterações por erros de transmissão ou manipulação de dados, entre outros (LINHARES; GONÇALVES, 2015)

Para o momento o protocolo WPA tem sido eficiente e auxilia muitas pessoas a manterem a integridade de seus dados particulares na internet.

Assim, acredita-se que se as pessoas começarem a tomar medidas preventivas, aliadas aos benefícios proporcionados pelos protocolos de segurança, certamente, poderão usar as redes sem fio de forma mais segura.

**REFERÊNCIAS**

ABELÉM, Antônio Jorge Gomes. Análise Das Vulnerabilidades De Segurança Existentes Nas Redes Locais Sem Fio: Um Estudo De Caso Do Projeto Wlaca. Disponível em: [www.researchgate.net/profile/Mauro\_Coutinho/publication/228757441.\_deec52e1065ef3222000000.pdf](http://www.researchgate.net/profile/Mauro_Coutinho/publication/228757441._deec52e1065ef3222000000.pdf). Acesso em 20 de nov. de 2015

ANDRADE, Lidiane Parente; SOARES, Daniel Nelo; COUTINHO, Mauro Margalho;

ASSUNÇÃO, Marcos Flávio Araújo. **Wireless Hacking ataques e segurança de redes sem fio Wi – Fi**. Florianópolis: Visual Books, 2013.

BARCELLOS, Gianfrancesca Cutini; BARANAUSKAS, Maria Cecília Calani. **Uma Análise de Metáforas em Interfaces para Comunicação Eletrônica.** Disponível em:<http://www.c5.cl/tise99/memoriatise99/html/papers/metaforas/>. Acesso em 25 de Nov de 2015.

CARVALHO, Daltro Oliveira de. **A internet na sociedade**: um estudo com professores e alunos da comunidade acadêmica de nível superior na cidade de Franca-SP /. Tese – Doutorado – Franca: UNESP, 2005.

COMITÊ Gestor da Internet no Brasil. **Cartilha de Segurança para Internet Versão 4.0.** São Paulo, 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em 10 de Nov de 2015.

CORRÊA, Marcos Antonio Costa Júnior. **Evolução da Segurança em Redes Sem Fio**. Pernambuco: UFP/Centro de Informática, 2008. Disponível em: <http://www.cin.ufpe.br/~tg/2008-1/maccj.pdf>. Acesso em 20 de Nov. de 2008

COSTA, Rogério da. **A cultura digital**. São Paulo: Publifolia, 2003

Escola Superior de Redes RNP. **Redes sem fio**. Cartilha Projeto UCA: Universidade Federal Fluminense (UFF), 2010.

**Forense Digital** / Computacional CIn – UFPE, 2007. Disponível em: [http://www.cin.ufpe.br/~ruy/crypto/seguranca/Forense\_Computacional(UFPE).pdf](http://www.cin.ufpe.br/~ruy/crypto/seguranca/Forense_Computacional%28UFPE%29.pdf). Acesso em 20 de Nov. de 2015

GIAVAROTO, Silvio César Roxo; SANTOS, Gerson Raimundo dos. **Backtrack Linux Auditoria e Teste De Invasão em Redes de Computadores**. Rio de Janeiro: Editora Ciência Moderna, 2013.

GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 2002.

GONÇALVES, João de Melo Feio Pinheiro; SILVA Rodolfo Paulo Teixeira Tavares da. Autenticação.Universidade do Porto/ Faculdade de Engenharia. Disponível em: <http://web.fe.up.pt/~jmcruz/ssi/ssi.1112/trabs-als/final/G6T3-user.auth.feup-final.pdf>. Acesso em 20 de Nov. de 2011.

HOROVITS, Henrique Daniel. **Explorando vulnerabilidades em Redes sem Fio: Usando as principais ferramentas de ataque e configurações de defesa.** Brasília- DF: Faculdade Senac, 2013. Disponível em: [file:///C:/Users/Giol/Downloads/seg02%20Henrique%20Daniel%20Horovits%20-TCC.pdf](file:///C%3A/Users/Giol/Downloads/seg02%20Henrique%20Daniel%20Horovits%20-TCC.pdf). Acesso em 20 de Nov. de 2015

IEEE. IEEE Std 802.11i-2004. 2004. Disponível em: <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>. Acessado em 20 de Nov. de 2008.

LINHARES, André Guedes; GONÇALVES, PAULO ANDRÉ DA S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w∗**. Disponível em: <http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf>. Acesso em 20 de Nov. de 2015.

LEITE, Cristiano Monteiro. **Políticas de segurança física e lógica em ambientes institucionais que utilizam tecnologia da informação. 2011.** Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede) – Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em:<http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/400/1/CT_GESER_1_2011_08.pdf>. Acesso em 20 de Nov. de 2015

LIMA, Vanderson Ramos Diniz de, LIJÓ, Maria Camila; SOUSA Marcelo Portela. **Segurança em Redes sem Fio**: Princípios, Ataques e Defesas. Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), Campina Grande, PB, Brasil,Laboratório de Sistemas Cognitivos e Redes Pessoais (LABee), Campina Grande, PB, Brasil.

**Live- CD**. Disponível em: <http://www.hardware.com.br/termos/livecd>. Acesso em 25 de Nov de 2015.

MAGALHÃES, Pedro Diniz de. **Integração De Ferramentas De Análise E Auditoria Em Redes Wi-Fi Com A Finalidade De Quebra De Chaves WEP/WPA LAVRAS – MG:** Universidade Federal de Larvas, 2011. Disponível em: <http://repositorio.ufla.br/bitstream/1/4992/1/MONOGRAFIA_Integracao_de_ferramentas_de_analise_e_auditoria_em_redes_wi-fi_com_a_finalidade_de_quebra_de_chaves>. Acesso em 20 de Nov. de 2015

MORAES, Alexandre Fernandes de. **Redes de Computadores**: fundamentos. São Paulo: Érica, 2004.

### MORAN, José Manuel. ****Como utilizar a Internet na educação**. Ciência da Informação. Versão on line.** ISSN 1518-8353 Ci. Inf. v. 26 n. 2 Brasília May/Aug. 1997. Disponível em: <http://www.scielo.br/scielo.php?pid=s010019651997000200006&script=sci_arttext>. Acesso em 10 de ago de 2015.

MORIMOTO, Carlos E. Segurança em Redes Wireless.Disponível em: <http://www.hardware.com.br/tutoriais/entendendo-quebrando-seguranca-redes-wireless/pagina4.html>. Acesso em 20 de dezembro de 2015.

PASA, Tiago. Roteiro – Aircrack-ng. Disponível em [http://187.7.106.14/emmonks/seguranca4/Pratica3/alunos/Roteiro%20ferramentas%20de%](http://187.7.106.14/emmonks/seguranca4/Pratica3/alunos/Roteiro%20ferramentas%20de%25). Acesso 20 de dezembro de 2015

PINHEIRO, José Maurício S. **Auditoria e Análise de Segurança da Informação Segurança Física e Lógica**. UGB – 2009. Disponível em: [www.projetoderedes.com.br/aulas/ugb\_auditoria\_e\_analise/ugb\_apoio\_auditoria\_e\_analise\_de\_seguranca\_aula\_02.pdf](http://www.projetoderedes.com.br/aulas/ugb_auditoria_e_analise/ugb_apoio_auditoria_e_analise_de_seguranca_aula_02.pdf). Acesso em 20 de Nov. de 2015

PIZON, A. **Vulnerabilidade da segurança em Redes Sem Fio**. 2009. 68f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação). Faculdade de Informática - Centro Universitário Ritter dos Reis, Porto Alegre, 2009. Disponível em: <https://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k9/TCCII_2009_1_Alexandre.pdf>. Acesso em 10 de set ago de 2015.

REIS, João Victor do Carmo, GOULART, Paula, MENDES, Luís Augusto Mattos. Redes Wireless: **Segurança Uma Questão Gerencial**. Disponível em: <http://fsd.edu.br/revistaeletronica/arquivos/2Edicao/artigo12.pdf>. Acesso em 20 de Nov. de 2015

ROBERTO, Laís Maciel. **A Influência Das Redes Sociais Na Comunicação Organizacional**. São Paulo: Universidade Nove De Julho (UNINOVE), 2009.

ROSS, Jonh. **O livro do wireless**: um guia definitivo para o Wi-Fi e redes sem fio. Rio de Janeiro: Atlas Books, 2009. RUFINO, Nelson Murilo de Oliveira. Seguranças em Redes sem fio. São Paulo: Novatec, 2005.

**Redes Sem Fio – Wireless Networks**. Disponível [file:///C:/Users/Giol/Downloads/redes-sem-fio-wireless-networks-819-kt7wa2.pdf](file:///C%3A/Users/Giol/Downloads/redes-sem-fio-wireless-networks-819-kt7wa2.pdf). Acesso em 20 de dezembro de 2015.

**Rede Wireless, parte 3. Configurando o ponto de acesso.** Disponível em: <http://www.hardware.com.br/tutoriais/configurando-ponto-acesso/>. Acesso em 25 de Nov de 2015.

RUFINO, N. M. O. **Segurança em Redes sem Fio**. São Paulo: Novatec, 2005. 206

SILVA, Leandro Rodrigues**. SEGURANÇA EM REDES SEM FIO (WIRELESS)** Pós-Graduação em Redes e Segurança de Sistemas Pontifícia Universidade Católica do Paraná Curitiba, 2010. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Leandro%20Rodrigues%20Silva%20-%20Artigo.pdf>. Acesso em 10 de set de 2015.

SCHIAVONI, Jaqueline E**. Mídia**: o papel das novas tecnologias na sociedade do conhecimento. Disponível em: <http://www4.faac.unesp.br/publicacoes/anais-comunicacao/textos/01.pdf>. Acesso em 25 de Nov de 2015.

TEIXEIRA, Fábio de Aquino Galvão; GOMES, Lucélia. **Análise de Vulnerabilidade em Redes Wi-fi 802.11.** Estudo de Caso: Protocolo de Segurança do Iesam. Instituto de Estudos Superiores da Amazônia –Nazaré - Belém-PA. Disponível em: <http://www3.iesam-pa.edu.br/ojs/index.php/computacao/article/view/241/232>. Acesso em 10 de out de 2015.

TEMP, Vivian Beatriz; MÜLLER, Karla Maria. **Comunicação instantânea**: uma nova prática sociocultural no contexto organizacional. Universidade Federal do Rio Grande do Sul. Disponível em: <http://www.abrapcorp.org.br/anais2007/trabalhos/gt3/gt3_temp.pdf>. Acesso em 10 de out. de 2015.

TERRA, Carolina Frazon. **Comunicação Corporativa Digital**: o futuro das relações públicas na rede. São Paulo: Universidade de São Paulo/ Escola de Comunicação e Artes/ Departamento de Reações Públicas/ Propaganda e Turismo, 2006.

TERRA, C. A **Comunicação Bidirecional, Direta e Instantânea como o Padrão dos Relacionamentos Organizacionais com seus Públicos**. Revista Eletrônica PRODAM Tecnologia (2), 15. 2009.

ULBRICH, H. C.; VALLE, J. D. **Universidade Hacker**. [S.l.]: Digerati Books, 2009.

**Wireless.** Disponível em: <http://fesppr.br/~airton/2010/redes/AP06-WIRELESS.pdf>. Acesso em 25 de Nov de 2015.

WIRESHARK FOUNDATION. **Wireshark. 2011**. Disponível em: [WWW.Wireshark.org](http://WWW.Wireshark.org). Acesso em 20 de Nov. de 2015

WRIGHTSON, Tyler. **Segurança** **de redes sem fio**: guia do iniciante. tradução: Aldair José Coelho Corrêa da Silva. Porto Alegre: Bookman, 2014

**GLOSSÁRIO**

AP ou Access Point - é um dispositivo que conecta dispositivos de comunicação sem fio para criar uma rede sem fio. Em uma rede sem fio infraestruturada é através do AP que os dispositivos *wireless* se comunicam.

Blackhat –é um termo utilizado na informática para se referir as pessoas ou técnicas que visam atingir um objetivo sem a autorização do órgão, empresa ou pessoa responsável. Esse objetivo pode ser a entrada em um sistema protegido, monetização por meios não autorizados ou o acesso às informações confidenciais.

Backtrack – é uma distribuição Linux que ajuda a garantir a segurança permitindo inclusive efetuar auditoria no sistema operacional, tudo com o objetivo de manter a informação segura contra terceiros (crackers)

Beacon – é um frame de sincronismo enviado periodicamente pelo ponto de acesso. Tem a função de avisar os clientes de que a rede está presente, avisar sobre frames gravados no buffer do access point (aguardando transmissão) e também sincronizar a transmissão dos dados.

Chat –é uma palavra em língua inglesa que significa conversa. Quando aplicamos o conceito de chat no mundo das redes de computadores, continuamos a usar o mesmo significado só que o ambiente no qual a conversa se desenvolverá é agora mediado pelo computador. Em português, esse ambiente é conhecido como "bate-papo" e é equivalente ao termo em inglês aplicado no contexto da Internet. (Barcellos; Baranauskas, 2015)

E - mail – correio eletrônico ou simplesmente e-mail (abreviaturas de eletronic mail) é uma ferramenta que permite compor, enviar e receber mensagens de textos, figuras e outros arquivos através da internet.

Enterprise – empresa, empreendimento.

Firewalls – na informática, os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade deles. .

Live – CD – num Live- CD o sistema roda sobre um ramdisk, um disco virtual criado usando parte da memória RAM. Partes do sistema que precisam de permissões de escrita, como os diretórios/ dev/TPM,/ home e arquivos de configuração no diretório. São copiados durante o boot para o ramdisk, permitindo que o sistema rode quase normalmente, enquanto o grosso dos arquivos é acessado diretamente a partir do CD (somente leitura) de modo que o sistema não consuma um caminhão de memória.

Netbank – internet para Banco

Sniffing – é um método de espionagem, que permite interceptar os pacotes de dados transmitidos por outros micros, através da rede. Em redes Ethernet os pacotes são transmitidos a todos os micros da rede, daí dizer-se que as redes Ethernet usam uma topologia lógica de barramento.

Wireless – a palavra wireless provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios. Wireless então caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar.

Wireshark – o Wireshark (anteriormente conhecido como Ethereal) é um programa que analisa o tráfego de rede, e o organiza por [protocolos](https://pt.wikipedia.org/wiki/Protocolo). As funcionalidades do Wireshark são parecidas com o [tcp dump](https://pt.wikipedia.org/wiki/Tcpdump%22%20%5Co%20%22Tcpdump), mas com uma [interface](https://pt.wikipedia.org/wiki/Interface_gr%C3%A1fica) [GUI](https://pt.wikipedia.org/wiki/GUI), com mais informação e com a possibilidade da utilização de filtros.