ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB

SEGURANÇA DE REDES SEM FIO BASEADA NO PADRÃO IEEE 802.11

Cristiano Alves Pimentel[1]
Hudson Ramos[2]

Resumo

O presente artigo tem por objetivo analisar como atua uma rede sem fio baseada no padrão IEEE 802.11, demonstrando suas vulnerabilidades e as principais ferramentas de defesa, que podem variar de soluções simples até as mais estruturadas e custosas, a fim de melhor atender suas necessidades e manter a integridade das informações. Este padrão possui variações que, para cada uma delas, existe uma determinada configuração: 802.11a (54Mbps a 5Ghz) e 802.11b (11Mbps a 2,4Ghz). Existe o tipo de rede, cuja realização tem sido as ondas de rádio, no qual não é limitado quanto ao perímetro, encontrado no *access point*, cruzando as paredes para que o sinal chegue e alcance a área externa do estabelecimento, para facilitar o acesso impróprio. Diante disso, evita-se que um *host* tenha obtenção quanto a promoção imprópria da rede ou capturação das informações trafegadas. Conclui-se que deve existir uma demonstração dos métodos e ações que são implementados na busca assegurada na maior confiabilidade e autenticidade, utilizando assim, a criptografia como o WEP (*Wired Equivalency Privacy*) ou o WPA (*Wi-Fi Protected Access*), para assegurar a confiabilidade das informações.

Palavras-chave: IEEE 802.11, Wireless, Wi-fi, Segurança de Redes Sem Fio.

1 Introdução

As tecnologias sem fio tem sido uma realidade no qual tem crescido muito nos últimos dias, sendo acelerado e conquistado cada vez mais, tornando-se adeptos para aqueles usuários residenciais até mesmo a aqueles que fazem uso dessa tecnologia em seu ambiente de trabalho.

[1] Pós Graduando do Curso de Pós Graduação em Rede de Computadores na Escola Superior Aberta do Brasil – ESAB. (cristian.alves2011@hotmail.com)
[2] Mestre em Engenharia de Software - UFES Bacharel em Ciência da Computação - UFES Técnico em Processamento de Dados - IFES Sócio Fundador da Projetas Sistemas de Informação Ltda Consultor de Tecnologia do SEBRAE-ES Professor do CEAD - IFES Professor Titular da Universidade de Vila Velha - UVV Professor (Orientação de TCC) ESAB.

Considera-se que as redes sem fio variam em seu modelo estrutural, podendo implementar de uma maneira mais complexa, baseada em estações interligadas por um ou muitos pontos de acesso, ou de maneira mais simples, cujas estações comunicadas entre si, através de modelo ponto-a-ponto, caracterizando a mobilidade para tornar flexíveis as alterações necessárias para completar mais as necessidades dos usuários, mesmo que haja mobilidade necessária, quanto a garantia dos dados no qual podem ser circuladas na rede, sendo um alvo de grande estima para as empresas, cujas soluções podem se tornar mais adequadas (MENESES, 2009).

O ambiente de transmissão quanto a rede sem fio, tem sido considerado o ar, caracterizando sua total ausência de fios ou cabos, transmitindo por ambiente de ondas eletromagnéticas. Uma grande característica deste meio é que o sinal se difunde igualmente em todas as direções, a menos que seja restringido, e continua a se propagar indefinidamente. Na medida que à distância da origem aumenta, a energia se difunde por uma área maior, tornando o sinal cada vez mais fraco. No caminho do sinal eletromagnético, ele é afetado por distúrbios naturais que podem interferir com o sinal (SPERANDIO, 2008).

Symantec (2006) quando descreve sobre a motivação, traz-se o uso das redes sem fio, no qual pode ser multiplicado à medida que a qualidade das mesmas possam melhorar os preços dos equipamentos, tornando-se até mesmo mais acessíveis.

Com um simples uso na configuração, pode ser considerado que é trazido elemento para o tipo de rede, cuja pessoa mal intencionada, obtém geralmente o acesso fácil para os s*oftwares* específicos para cada situação

O presente artigo teve por objetivo analisar como atua uma rede sem fio baseada no padrão IEEE 802.11, demonstrando suas vulnerabilidades e as principais ferramentas de defesa, que podem variar de soluções simples até as mais estruturadas e custosas, a fim de melhor atender suas necessidades e manter a integridade das informações.

A metodologia utilizada foi exploratória, onde buscou-se explorar as vulnerabilidades da rede sem fio e descrever seus principais métodos de segurança. Ainda, foi realizado através do método e procedimentos técnicos de Levantamento Bibliográfico, apurando, comparando, constatando, observando, todos os dados pertinentes à estrutura histórica e contemporânea no que concerne a segurança de redes. Ainda, o método da pesquisa foi a qualitativa, pois ao fazer o levantamento bibliográfico de pesquisas, houve à material suficiente para tirar deduções acerca dos problemas levantado.

2 Redes sem fio (WI-FI)

Segundo Engst & Flsieshman (2007), descrevem que *Wireless* traz o significado de SEM FIO, cujas redes podem ser supridos por ondas de rádio, usando a simplicidade da instalação, proporcionando seu aumento quanto ao uso diariamente.

Há diversos tipos e padrões de redes *wireless*, exemplificando assim, o *WiMax, Bluetooth, Wi-Fi(Wireless Fidelity), InfraRed*(Infravermelho) (ARTHAS, 2006)

Sabe-se que a rede *wireless* é reconhecida por ser sem fio, pois o transmissor e o receptor geralmente se comunicam sem a presença de fios e por através também por ondas de rádio. (ENGST & FLEISHMAN, 2007)

São encaixadas na categoria os seguintes tipos de rede quanto a: Locais Sem Fio ou WLAN (*Wireless Local Area Network*), Redes Metropolitanas sem Fio ou WMAN (*Wireless Metropolitan Area Network*), por exemplo o WiMAX (*Worldwide Interoperability for Microwave Access*), Redes de Longa Distância sem Fio ou WWAN (*Wireless Wide Area Network*), redes WLL (*Wireless Local Loop*) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (*Wireless Personal Area Network*). (ARTHAS, 2006)

Engst e Fleishman (2007) descrevem que os modelos para redes sem fio, durante o mundo da tecnologia, é padronizado por aparelhamentos de redes sem fio no qual podem funcionar em conjunto por equipamentos padrões ajustados com outros aparelhos suportados com o próprio padrão. Na tecnologia, considera-se o padrão como um nome específico, para ser confirmado por um órgão da indústria.

É conhecido atualmente o IEEE (*Institute of Electrical and Electronics Engineers*), sendo uma agregação profissional desenvolvida por padrões técnicos baseados consequentemente aos fabricantes, definindo a transmissão entre dispositivos clientes de rede. Com um tempo, foram criados muitos padrões, destacando e desenvolvendo o 802.11, conhecido também como Wi-Fi - *Wireless Fidelity* – Fidelidade sem fio (RUFINO, 2007).

3 Padrões para redes sem fio

O padrão 802.11a é considerado como padrão frequentemente de 5 GHz, surgido em 1999, mesmo que não tenha sido utilizado atualmente, mesmo que não haja vários dispositivos fabricados na tecnologia (DUARTE, 2003).

Os aparelhamentos do padrão 802.11a surgiram no ano de 2002, logo após o padrão 802.11b, ocorrendo a aparição do padrão 802.11a não permanecia disponível, bem como certas tecnologias para o desenvolvimento (ENGST e FLEISHMAN, 2007).

Rufino (2007, p. 34) afirmou que as características principais quanto ao padrão 802.11a ocorrem quanto:

> - O aumento de sua velocidade para utilização em 54 Mbps ou aproximadamente 25 Mbps de throughput real (108 Mbps em modo turbo), porém podendo ser utilizado para transmissões em velocidades mais baixas.
> - Trabalha na faixa de 5 GHz, com pouquíssimos concorrentes, porém o alcance é reduzido, mas com melhores protocolos que o 802.11b.
> - A quantidade de clientes conectados pode chegar a 64;
> - Possui 12 canais não sobrepostos, que permite que os pontos de acessos possam cobrir a área um do outro sem causar interferências ou conflitos.

Considera-se como principal desvantagem a incompatibilidade padrão 802.11b, que vem possuindo um grande terraço no qual instala o cenário tecnológico, onde os padrões podem utilizar faixas de frequências diferentes (ENGST e FLEISHMAN, 2007).

O 802.11b aproveita o espalhamento espectral por sequência direta (DSSS - Direct-Sequence Spread Spectrum) para receber e transmitir os dados a uma velocidade máxima de 11 Mbps por segundo, mesmo que não haja velocidade real, pode ser incluso todo o *overhead* (sobrecarga) de rede, iniciando e findando os pacotes. A taxa real tem variado através das configurações do equipamento e do espectro em que se encontra, porém pode variar entre 4 a 7 Mbps aproximadamente (SOUZA JR., 2007).

O padrão 802.11g traz certa lentidão do que o 802.11a, principalmente quando é balanceado o carregamento de transmissão com o 802.11b. Não tem sido compatível a opção para o fabricante, não sendo aceito o aumento de qualquer produto da linha 802.11g, na compatibilidade com o 802.11b, que é obrigado a especificação do padrão (ENGST e FLEISHMAN, 2007).

As características tem sido as velocidades, chegando atingir 54 Mbps; e tendo a compatibilidade total com os equipamentos do protocolo 802.11b que atuam na frequência de 2.4 GHz.

Quanto ao padrão 802.16 (WiMax), tem visto que, a utilização e finalização quanto a criação das longas distâncias utilizada por ondas de rádio, por cabos de rede, sendo praticado numa rede de dados de alta velocidade, por uma longa distância, como por exemplo, entre cidades, em uma residência ou em uma área rural (ENGST e FLEISHMAN, 2007).

O padrão 802.11n, tem trazido grande aumento quanto a taxa de transmissão dos dados, que é aproximado por 100 a 500 Mbps, sendo conhecido como WWiSE (*World Wide Spectrum Efficiency*). Seu objetivo é alcançar grande cobertura do sinal, através dos canais de 40 Mhz, no qual é mantido a compatibilidade trabalhada nos 20 Mhz, cujas velocidades são osciladas em torno de135 Mbps (RUFINO, 2007).

O padrão 802.1x é referido por dois pontos de segurança fundamentais por uma rede sem fio, no qual traz a Privacidade e a Autenticação. Na aparição regularizada, é seguido ao nível de porta, quando referido por um ponto de vinculação a uma LAN, conexa física ou lógica, para utilizar assim, os dispositivos sem fio e AP (SILVA e DUARTE, 2006)

O padrão IEEE 802.1x pode ser especificado através do mecanismo para autenticar os dispositivos ou até mesmo os usuários, com a utilização de muitos tipos de protocolo EAP – Extensible Authentication Protocol, onde é definido a permissão da utilização de uma enorme variedade de mecanismos de autenticação (PERES e WEBER, 2006).

4 Tipos de rede sem fio

A WLAN (*Wireless Local Area Networks*) é definido por padrão IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 (PERES & WEBER, 2006).

Considera-se que a rede convencional, quando comparada por uma rede cabeada, pode ser oferecido funcionalidades, exceto quando há flexibilidade e conectividade de muitos ambientes, sendo transmissores e receptores das estações dos clientes ligadas a pontos de acesso diretamente ligada a uma rede cabeada ou a outros pontos de acesso (BEZERRA, 2004).

As WPAN (*Wireless Personal Area Networks)* são definidas pelo padrão *Bluetooth*, que atualmente é incorporado no padrão IEEE 802.15. O bluetooth começou pelos estudos na Ericsson Mobile Communication em meados do ano de 1994, criando por finalidade uma transmisão de baixo custo e consumo entre celulares e seus acessórios. Em 1998, cinco empresas formaram um grupo chamado SIG (*Bluetooth Special Interest Group*), que era composto por Ericsson, Nokia, IBM, Toshiba e Intel, como a 3COM e a Lucent, juntando por fim, para a criação de um certificado para um novo padrão (ARAÚJO e ANDRADE, 2005).

A utilização do Bluetooh tem sido realizada em celulares, palm tops, notebooks, microfones, fones de ouvidos, entre muitos outros dispositivos, visando a facilitação do usuário.

O Bluetooth trabalha na frequência de 2,45 Ghz, no qual são utilizados nos padrões 802.11b e 802.11g, mas não é um substituto do Wi-Fi, pois a rede Bluetooth é mais lenta e possui poucos dispositivos tolerados. Quanto a distância, este chega a aproximadamente 10 metros, sendo uma distância curta comparada com outros protocolos (KOBAYASHI, 2004).

A WMAN (*Wireless Metropolitan Area Networks*) tem sido definida pelo padrão IEEE 802.16, conhecida também como rede sem fio de banda larga, sendo concorrente da fibra óptica, por possuir diferença de mobilidade, abrangência e disponibilidade, onde os serviços superiores aos serviços de DSL (*Digital Subscriber Line* – Linha Digital para Assinantes) são existentes, havendo certo limite na classificação dos alcances e custos (CAMARA & SILVA, 2005).

5 Tipos de transmissão

Na Radiofrequência, a comunicação é utilizada nas redes locais com bandas não autorizadas, utilizando uma modulação do tipo *spread spectrum*, que pode ser adequado aos requerimentos para operação em muitos países. Os padrões aproveitados pela comunicação em radiofrequência são o FHSS (*Frequency Hopping Spread Spectrum*) e o DSSS (*Direct Sequence Spread Spectrum*), tem sido utilizada pela frequência de 2.4 GHz (ZANETTI & GONÇALVES, 2003).

Quanto a tecnologia *spread spectrum* desenvolveu para ser usado em militar, cuja função é a distribuição quanto ao sinal de maneira uniforme em toda a faixa de frequência. A desvantagem da utilização tem sido o consumo da banda, garantindo a integridade das informações trafegadas, por diminuir a sensibilidade dos ruídos e também pelas interferências de outros meios tecnológicos no qual podem ser utilizados na mesma frequência para transmissão (RUFINO, 2007).

O DSSS tem sido utilizado pelo padrão 802.11b, e, sua denominação é *code chips*, no qual separa cada bit de dados, sendo em 11 bits, nos quais são enviados de forma redundante pelo canal de comunicação. O processo pode espalhar energia de radiofrequência em torno de uma banda larga, tornando-se necessário para transmitir o dado (RUFINO, 2007).

Quanto ao infravermelho, considera-se uma tecnologia pouco utilizada para fins comerciais, trabalhando em altas frequências e transmissão direta dos dados, no qual não pode possuir objeto entre o transmissor e o receptor, sendo exigido uma visada direta ou quase direta entre ambos (ALBUQUERQUE, 2008).

Há dois tipos de propagação do infravermelho, sendo a direta e a difusa, cuja propagação do sinal direto, tem necessitado de uma transmissão sem assoreamento física entre as unidades, trocada por informações. Na longa transmissão, pode ser emitido sinais para uma superfície reflexiva, sendo incluso o teto, paredes, piso, ou seja, todo o ambiente repercurtido por sinal, sendo eliminado pela necessidade de alinhamento conciso com o receptor (ALBUQUERQUE, 2008).

A tecnologia laser tem sido similar ao infravermelho, sendo diferentemente utilizado por um comprimento de onda diferente. A transmissão laser é muito direto, onde os equipamentos de transmissão e recepção são obrigados alinhar a comunicação completa. Quanto ao infravermelho, este possui um ângulo de abertura, cuja vantagem é considerado do laser sobre o infravermelho, sendo o alcance que é superior, onde este é obtido conforme a potência aplicada no transmissor (TORRES, 2001 apud ALBUQUERQUE, 2008).

Sobre o Wi-Max (*Worldwide Interoperability for Microwave Access*) ou padrão 802.16 (sub-pdrões do Wi-Max), é considerado que o futuro da tecnologia sem fio pode revolucionar todas tecnologias de rede sem fio, incluindo a telefonia fixa e móvel.

6 Segurança em redes sem fio

Considera-se que a segurança em redes sem fio traz algumas desvantagens e também a segurança principal delas. Em estudos, Laura Garcia-Manrique, gerente da *Group Product - Wireless* da Symantec, descreve que a segurança considera-se como um dos três grandes problemas enfrentados por gerentes de TI, com relação às redes sem fio e computação remota (GIMENES, 2005).

Gimenes (2005, p. 20), nos estudos de Laura Garcia-Manrique, afirma que os principais problemas de segurança com relação aos sistemas sem fio incluem:

> - Intercessão de transmissão sem fio à medida que viaja via aérea.
> - Perda de um dispositivo portátil, comprometendo os dados nele contidos.
> - "Relacionamentos de confiança" quando os dispositivos sem fio são usados para comércio (por exemplo, para a o envio de pedidos ou compras).

Diante dessas considerações, para lidar com os problemas, Garcia-Manrique afirma que as empresas tem necessitado de procedência especificamente o uso de dispositivos sem fio, incluindo as funções para as quais os mesmos podem ser usados, ou até mesmo pode ou não ser armazenado e qual a tecnologia de segurança que deve estar instalada, para evitar que os dados sejam comprometidos, no caso de roubo do dispositivo (GIMENES, 2005).

Geralmente as configurações de fábricas não traz habilitação quanto aos mecanismos de segurança, tornando-se assim, a rede mais vulnerável a um ataque, onde os aparelhos possuem configurações quanto ao padrão de fábrica, desde do SSID (*service set identifier*), endereços IPs e senhas, e ainda, aos acessos indevidos para a rede ser facilmente simples (RUFINO, 2007)

Sabe-se que o tipo de configuração pode ser caracterizado através do envio do SSID da rede pelo concentrador, sendo aceito por conexões de qualquer pessoa cuja compatibilidade de *hardware* seja consentida. Requisitando a conexão, o concentrador pode possuir um servidor DHCP (*Dynamic Host Configuration Protocol*), equiparando-se por um endereço IP válido para a rede, para liberar acesso à ela. Diante disso, quanto ao modo de configuração, o concentrador não envia o seu SSID, permitindo apenas a conexão daqueles que sabem o SSID da rede (RUFINO, 2007).

Quando há um atacante, basta "escutar" o tráfego da rede para determinar seu SSID correto, acessando assim, a mesma. Para proteção, há outra forma de acesso a uma rede *wi-fi*, no qual tem definido os endereços físicos acessíveis a rede (RUFINO, 2007).

Quanto ao endereço físico, ocorre também o endereço MAC, no qual tem feito parte da camada de Enlace do modelo OSI (*Open Systems Interconection*). (GUERRA, 2002)

Qualquer dispositivo de rede tem possuido um endereço físico (*Media Access Control*). Antes, os endereços físicos não eram considerados únicos, cujos fabricantes geralmente produzem placas e os endereços físicos são iguais para ocasionar seus conflitos. Atualmente, todo dispositivo de rede possui um endereço físico único. (GUERRA, 2002).

Configura-se que há um concentrador para conexão dos endereços físicos no qual é definido pelo administrador, cujo dispositivo traz autenticação para o equipamento e não o usuário, que, possivelmente uma pessoa não é autorizada para realizar a utilização da rede por meio de um equipamento, no qual o acesso liberado à mesma. (RUFINO, 2007)

Há certas desvantagens para utilização do tipo de autenticação, sendo necessariamente obtida manualmente os endereços físicos e também o cadastro no concentrador, onde as alterações são frequentemente alternado entre os usuários (RUFINO, 2007).

Para realizar tal conexão a uma rede *w-fi*, tem sido necessário haver um dispositivo, atendendo os padrões da rede, como placas PCI (internas), adaptadores USB, adaptadores *Ethernet* e cartões e placas PCMCIA (GIMENES, 2005).

Geralmente, os dispositivos são considerados portáteis e removíveis, cuja pessoa sendo mal intencionada, obtém um *hardware*, permitindo o acesso a rede e plugá-lo no computador para tal acesso a rede.

Outra desvantagem pode ser a obtenção do tráfego, contendo o endereço MAC dos dispositivos, cujo atacante com um endereço físico válido de acesso à rede, renomeia o endereço físico de sua placa e obter o acesso. Alterando o endereço físico no *Windows* (somente as versões 2000, XP e 2003), é utilizado o caminho das conexões de rede, propriedades da rede local, configurar, avançado e *NetwrokAddress* (RUFINO, 2007).

Ainda, existe outro modo para obtenção do endereço MAC, havendo validade para utilização da força bruta, repetindo os testes dos endereços MAC aleatórios, criando uma lista para acessar determinada rede.

6 Proposta de implementação de uma rede sem fio segura

A proposta de implementação de uma rede sem fio segura tem trazido grande utilidade para um ambiente coorporativo de pequeno e médio porte, através das redes domésticas. O levantamento estrutural de rede pode ser analisada através do reaproveitamento da própria infraestrutura, dispositivos e equipamentos existentes. Sabe-se que a rede agregada a rede sem fio, pode criar uma rede mista, como também, pode haver reserva de casos quanto a falha de muitos motivos da comunicação sem fio.

A posição dos aparelhos responsáveis pela comunicação da rede, ou seja, os pontos de acesso, são posicionados em locais limitados por sinal num ambiente, cujas alterações das configurações, principalmente de fábrica, traz dispositivos como por exemplo, o nome do usuário e a senha para promoção às configurações do Ponto de Acesso, o SSID e o *broadcast* SSID.

A potência do Ponto de acesso tem sido também regulada conforme a necessidade, até porque o ambiente pequeno, como uma sala ou uma seção de 12 ou 15 metros quadrados, podem atuar cinco ou seis computadores, não sendo imprescindível por uma alta do sinal de radiofrequência, cujos dispositivos clientes devem estar próximos do ponto de acesso.

A compra dos equipamentos necessários, tem atualmente previsto por possíveis mudanças e adaptações futuras, necessitando de reestruturação ou evolução da quantidade de clientes que terão acesso à rede. Sabe-se que a compra por equipamentos com o padrão 802.11a tem sido um dos pontos mais seguros, cuja a maioria dos equipamentos existentes utilizam o padrão 802.11b/g.

No entanto, o custo com a aquisição dos equipamentos não tem existido em muitos dispositivos, como por exemplo, os Notebooks, que tem o padrão 802.11a já incorporados aos mesmos.

Diante disso, independente do padrão para configurar, é trazido a proteção da rede com a utilização de mecanismos de segurança. O WEP com criptografia de 128 bits, traz uma chave compartilhada, considerando a rede livre de intrusos, cujos invasores descobrem chaves da rede, podendo ter acesso à mesma em questão de poucas horas.

A utilização do WPA com chave compartilhada tem sido configurado intermediária, recomendada por várias situações, como ambientes domésticos, empresas ou organizações de pequeno porte. A segurança tem sido grande com a do WEP, sendo vantajoso na configuração e administração. Ainda, tem sido considerada para médias empresas em que o tráfego dos elementos não tem sido de costume sigiloso, utilizado por conexões do tipo VPN, protegendo assim, informações circulares na rede.

O protocolo WPA tem possuído método para utilizar segurança da rede, considerado EAP, cuja dependência necessita do nível de segurança, exigidos pela empresa ou organização, sendo recomendado a segurança para autenticar o Radius ou a utilização de certificações digitais.

Apresentado as três linhas, tem sido possivelmente configurado para o ambiente aplicável quanto a utilização de redes sem fio, cujo administrador da rede deve sempre estar atento para buscar os testes na rede com as ferramentas existentes, surgindo possivelmente as falhas e soluções mantidas pela segurança das informações e a confiabilidade no acesso às redes sem fio.

7 Conclusão

O presente artigo teve por objetivo principal analisar como atua uma rede sem fio baseada no padrão IEEE 802.11, demonstrando suas vulnerabilidades e as principais ferramentas de defesa, que podem variar de soluções simples até as mais estruturadas e custosas, a fim de melhor atender suas necessidades e manter a integridade das informações.

Os riscos e as vulneráveis tipos de rede de computadores, pode resultar em diversos problemas para as empresas, sendo implantado a necessidade de várias reformas, cuja rede cabeada precisa de fios por paredes ou caneletas, sendo facilmente atraída cada vez mais por usuários.

Como todo ambiente lógico não é totalmente seguro, as redes sem fio ter suas vulnerabilidades, no qual, há atualmente vários processos que ajudam a tornar um ambiente *Wireless* seguro, mesmo não garantindo que a rede seja totalmente segura.

Apesar de existir precauções, podem ser adotadas e aplicada as redes sem fio, quanto a possibilidade de haver um invasor bem motivado para o sucesso em seu ataque.

E, diante disso, é com o propósito de analisar a tecnologia de redes sem fio, o que foi alcançado, a possível apresentação de um trabalho, de forma que pessoas leigas queiram ter contato, tanto no entendimento da tecnologia quanto em seu uso.

Em relação às análises, principalmente em relação aos padrões apresentados, foram feitas baseadas nos módulos efetivamente firmados pelo comitê IEEE que por sua vez dão suporte a redes sem fio.

Ressalta-se que pode haver melhores buscas de metodologias de segurança para os padrões, visto que o padrão IEEE 802.11, tem sido uma base para os demais, sendo constantemente alterado por grupos de estudos e até mesmo por profissionais de informática, aperfeiçoando o encontro estabelecido por padrão de segurança aceitável, ideal e confiável.

A segurança de redes é constantemente manipulada pelos inúmeros processos de protocolos em que frequentemente esses são tidos somente muitas vezes como um erro da etapa de aplicação. E a partir do surgimento das redes locais sem fio (WLANs – Wireless Local Area Networks) este modelo de segurança por si deixa ser adequado para estas redes.

Já que a comunicação dessas redes acontece através de ondas de rádio. Desta forma a pessoa que tiver um receptor de rádio pode interceptar a comunicação deixando-a vulnerável. Ou mais, uma pessoa que um possua um transmissor de rádio também pode injetar esses dados na rede. Tendo em vista tais necessidades que as WLANs precisam de elementos de segurança presentes na etapa transição dos dados para proteger esse acesso à rede e assegurando a proteção dos dados que passam na mesma.

Para o padrão IEEE 802.11 sendo introduzido um protocolo de segurança chamado WEP (*Wired Equivalent Privacy*). Tendo por objetivo dar maior segurança aos usuários deste serviço, ou seja, uma privacidade equivalente ao das redes locais (LANs – Local Area Networks) Ethernet. Na qual está ligada a componente de segurança físicos que se referem a um espaço físico controlado. Quando falamos das WLANs, se torna ineficiente, pois as ondas de rádio usadas para a comunicação não ficam necessariamente restritas aos espaços físicos da área onde se encontram os mecanismos que formam a rede.

O WEP (criptografia de dados) é um mecanismo de segurança equivalente ao mecanismo de segurança físico, ou seja, tem por objetivo dar segurança aos dados que irão passar pelo canal de comunicação entre o ponto de acesso e os clientes/ clientes e o ponto de acesso. E a partir destas medidas, pode fazer uso de outros mecanismos de segurança LANs

como: MAC (Medium Access Control – proteção por meio de senhas, filtro de endenreço) e a utilização redes VPNs (Virtual Private Networks - privadas virtuais).

Os problemas de segurança no modelo IEEE 802.11. E expõe que em 2003, o WEP foi substituído pelo WPA (Wi-Fi Protected Access) e também apresentar alguns erros na sua implementação, acabou sendo atualizado até mesmo por outros modelos de IEEE 802.11.

Notadamente, existem barreiras físicas que impedem ou atenuam demasiadamente a passagem do sinal deixando-o imperceptível ou altamente instável para impedir que o sinal transponha os limites da corporação barreiras físicas poderiam ser construídas, a utilização de equipamentos que sobrecarreguem a faixa de freqüência com ruído destrutivo também pode ser uma alternativa.

As principais contribuições tem sido o crescimento do uso de redes sem fio, que trouxe um inegável aumento de produtividade para as empresas, mas, ao mesmo tempo, desafiando os administradores quanto a infraestrutura de rede, sendo possivelmente fornecido o acesso aos recursos necessários e também para os usuários que realmente deveriam obter este acesso.

A padronização através do padrão IEEE 802.11, pode permitir interoperabilidade entre dispositivos de diversos fabricantes, que além disso, pode definir um protocolo de segurança - o WEP- que pouco tempo foi alvo de duras críticas por conta das vulnerabilidades.

Diante do exposto, o presente trabalho pode ser indicado para futuros trabalhos acadêmicos e entre outras fontes de pesquisa, por existir informações de autores que descrevem sobre a segurança de redes sem fio, no qual foi baseado no padrão IEEE 802.11.

ABSTRACT

This article aims to analyze how it operates a wireless network based on the IEEE 802.11 standard, demonstrating their vulnerabilities and the main advocacy tools, which can range from simple solutions to the most structured and costly in order to better meet your needs and maintain the integrity of the information. This pattern has variations which, for each of them, there is a specific configuration: 802.11a (5GHz 54Mbps) and 802.11b (11Mbps in 2.4Ghz). There is the type of network, the performance of which has been the radio waves, which is not limited in scope, found on the access point, crossing the walls for the signal to flow and reach the outside of the establishment, to facilitate the improper access . Therefore, it is avoided that a host has obtained for improper network promotion or image snapshot of trafficked information. It follows that there must be a demonstration of the methods and actions that are implemented in the search for the most assured reliability and authenticity, using thus the encryption like WEP (Wired Equivalency Privacy) or WPA (Wi-Fi Protected Access), to ensure the reliability of information.

Key-words: IEEE 802.11,Wireless, Wi-Fi, Security of Wi-fi.

Referências

ALBUQUERQUE, Alessandro Ferreira de. **Estudo de métodos de proteção de Redes Wireless.** Monografia. Ministério Da Educação - Universidade Tecnológica Federal Do Paraná – UTFPR - Campus Medianeira, Medianeira – PR, 2008.

ARTHAS, Kael. **Tutorial Wireless.** 2006. Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=269602. Acesso em 02 jan. 2015.

BEZERRA, Fábio Fernandes. **Ferramenta de Análise Modal de Protocolos de Segurança para Redes Sem Fio**. Monografia apresentada como conclusão do curso de Engenheiro de Telecomunicações. Universidade Regional de Blumenau, Santa Catarina, 2004.

CERT. **Práticas de Segurança para Administradores de Redes *Internet,*** 4.13.6. Monitoração da Rede *Wireless*. 2003. Disponível em: http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#sec2 . Acesso em 02 jan. 2015.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão do Curso de Bacharel em Ciência da Computação. UNESP São José do Rio Preto. 2003. Disponível em: http://www.apostilando.com/download.php?cod=230&categoria=Redes. Acesso em 02 jan. 2015.

ENGST, Adam; FLEISHMAN, Glenn. **Kit do Iniciante em Redes Sem Fio:** O guia prático sobre redes *Wi-Fi* para Windows e Macintosh. 3ª ed.: São Paulo. Ed.: Pearson Makron Books. 2007.

GIMENES, Eder Coral. **Segurança de redes wirelles**. Monografia apresentada a FATEC Mauá, como parte dos requisitos para obtenção do título de Tecnólogo em Informática com ênfase em Gestão de Negócios. Centro de Educação Tecnológica Paula Souza - Faculdade de Tecnologia de Mauá, 2005.

MENESES, Emerson Barros de. **Rede Wirelless:** Uma solução sem fios. Trabalho de Conclusão de Curso. Rio de Janeiro, Dezembro, 2009.

PALMELA, Pedro Nuno Lopes; RODRIGUES, António Afonso. **Rede de Infravermelhos a Alta Velocidade**. Universidade de Oveiro. Portugal 2002.

PERES, André; WEBER, Raul Fernando. **Considerações sobre Segurança em Redes Sem Fio**. ULBRA - Universidade Luterana do Brasil, RS - 2006.

RUFINO, Nelson Murilo de Oliveira. **Segurança de Redes Sem Fio**. 2ª ed. São Paulo: Ed.: Novatec, 2007.

SILVA, Luiz Antonio F. da, DUARTE, Otto Carlos M. B. **RADIUS em Redes sem Fio**. Universidade Federal do Rio de Janeiro. RJ – 2006.

SPERANDIO, Dircelene Jussara. **A tecnologia computacional móvel na sistematização da assistência de enfermagem**: Avaliação de um Software-protótipo. Tese de Doutorado - Enfermagem de Ribeira Preto - USP - Ribeirão Preto, 2008.

SOUZA JÚNIOR, Pedro Ismar Maia de. **Redes de Comunicação.** Campo Grande – MS, 2007. Disponível em http://cpan.sites.ufms.br/wp-content/blogs.dir/125/files/2014/01/4109914apostila.pdf. Acesso em 02 jan. 2015.

SYMANTEC. **Implementando Uma LAN Sem Fio Segura.** 2006. Disponível em: http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html. Acesso em 02 jan. 2015.

ZANETTI, Alberto René & GONÇALVES, Leandro de Carvalho. **Redes Locais Sem Fio**. Trabalho apresentado na Pós-Graduação em Ciência da Computação - Universidade Federal de São Carlos, São Paulo, 2003.