ANÁSLISE DE SEGURANÇA DE ACESSO A REDE SEM FIO

***José Roberto dos Santos*[1], *Claudineia Helena Recco*[1], Marcelo Eloy Fernandes[1]**

[1]Departamento de Pós-Graduação– *Universidade Nove de Julho, UNINOVE*
01156-050, São Paulo - SP – Brazil

jrobert_santos@hotmail.com, {chrecco, marceloeloyfernandes}@gmail.com

Abstract. *The technological breakthrough brought the need for mobility, to achieve this mobility was necessary evolution in use of cabled network computers, bringing a method that allows people to use their devices anywhere in your house and not only next to the router. By means of this challenge was developed wireless network, with network came the security trouble. The objective of this study is to give broad science which is the wireless network, evolution, problem and simplistic methods of data protection. Through research were suggested several protection modes, and also the identification of attacks that can be performed using a wireless network and the network evolution and its variations to evade risks.*

Resumo. *O grande avanço tecnológico trouxe a necessidade da flexibilidade, para atingirmos essa mobilidade foi necessária evolução em utilização da rede de computadores cabeada, trazendo um método que possibilite as pessoas usarem seus dispositivos em qualquer parte de sua casa e não somente ao lado do roteador. Através deste desafio foi desenvolvida a rede sem fio, porém junto com está rede vieram os problemas de segurança. O objetivo deste estudo é dar ampla ciência do que é a rede sem fio, evolução, problema e métodos simplista de proteção dos dados. Através de pesquisas foram sugeridos diversos modos de proteção, e também a identificação dos ataques que podem ser realizados utilizando uma rede sem fio bem como a evolução da rede e suas variações para driblar os riscos.*

1. Introdução

Atualmente possuímos dispositivos que fazem acesso à *web* através da palma da mão, o que significa que podemos estar conectados à internet em qualquer lugar e a qualquer hora.

Vivemos no mundo onde tudo está conectado a tudo, por conta disso vem se tornando mais forte os dispositivos que possuem internet, existindo geladeira, rádio, televisores e muitos outros equipamentos dentro das residências que podem ou devem acessar a rede mundial.

Por conta dessa necessidade de estarmos conectados todo o tempo surge a necessidade de termos internet, para isso podemos contar com acesso a rede através de cabo ou através do ar, onde o primeiro chamamos de *LAN* e a segunda chamamos de *WLAN*.

Hoje é difícil ir a uma residência e nela não termos acesso sem fio, mas este conceito não se restringe apenas em casas, mas também em qualquer estabelecimento, isso se tornou uma forma de atrair clientes.

Com a grande utilização da rede sem fio, vieram os riscos e estes podem ser diversos desde o roubo de uma imagem ou outro tipo de informações importantes, como por exemplo, senhas, dados bancários ou pessoais, endereço e/ou outras informações.

Levando em conta isso devemos tomar cuidados ao acessar redes públicas e evitar fazer transações financeiras e quaisquer outros dados que possa pôr em risco a integridade do dispositivo.

2. Rede sem fio – O que é

Rede sem fio ou wireless tem como conceito principal a mobilidade, como o nome já diz é uma tecnologia que permite a utilização de equipamentos para a transmissão e recepção de dados sem o uso de cabos, utilizando ondas propagadas através do ar, uma das vantagens dessa rede é que ela não é licenciada.

Para o funcionamento são necessários poucos itens, um dispositivo que servirá de fornecedor da onda podendo ser um *AP* sem fio do mais simples, e um dispositivo que receberá essa onda que pode ser um computador com uma placa de rede sem fio instalada. Os notebooks já vêm com essa placa instalada e pronta para o uso.

Esse sistema está tão difundido que quase todos os equipamentos que compramos já vêm com uma conexão sem fio e também é comum cada casa, escritório, prédios terem sua própria rede sem fio, nas grandes cidades encontramos ponto de acesso sem fio onde só é necessário se cadastrar e acessar e em alguns casos nem o cadastro é necessário.

Essas redes recebem o nome de WLANs (*Wireless Local Area Network* – Área local de rede sem fio), normalmente essas redes são para uma área não muito grande onde diversas pessoas podem se conectar. Mesmo sendo uma rede que não necessita de cabo podemos considerar que é possível ter acesso à internet de forma tranquila e eficaz.

Muitas operadoras que fornecem serviços de internet no país distribuem roteadores sem fio para os clientes que contratam pacotes com estas, o que vem incentivando o aumento do uso de equipamentos sem fio.

Podemos encontrar dois tipos de conexão de rede sem fio são elas infraestrutura e ponto-a-ponto, o mais comum de vermos hoje é a utilização da conexão através da infraestrutura, onde computadores se conectar a um ponto de acesso (*AP – Access Point*), esses *APs* são responsáveis pela retransmissão e direcionamento da informação, de modo que uma estação não converse com outra, esses *APs* também servem de pontes para comunicação da rede com fio para a rede sem fio e vice-versa, caso haja um desligamento desse *AP* as estações ficam sem comunicação umas com as outras. Com isso limitasse um pouco a utilização de todo o poder da rede sem fio. (Battisti, 2014)

Já no modelo ponto-a-ponto (*ad Hoc*) permite que as máquinas se comuniquem sem um intermediador (*Access Point*), ou seja, têm permissão de comunicação umas com as outras desde que estejam livres para receber a informação, este método é comumente usados em grupos pequenos de equipamentos. (Battisti, 2014)

Para a transmissão de dados é necessário o uso de um canal de transmissão às tecnologias mais usadas é infravermelho, laser e frequências de rádio. (Redes de computadores, 2011).

A transmissão através do infravermelho é bem simples e comum encontramos esse tipo de transmissão no controle remoto da TV que cria uma linha entre o transmissor e o receptor onde usa o canal completo para a transferência a velocidade máxima de transferência é de 16 Mbps. (Redes de computadores, 2011)

A transmissão a *laser* é mais utilizada através de fibra ótica o que não elimina o cabo, porém estudos mostram possibilidade de utilização sem o uso dos cabos, porém ainda não está em uso. (Redes de computadores, 2011)

Já a transmissão de rádio frequência é feita através de fios de cobre que a ligam a uma antena que por sua vez faz a dispersão do sinal através do ar. A rede sem fio usa todos os conceitos da transmissão por rádio frequência, porém uma não interfere na outra. (Redes de computadores, 2011)

Segundo Rufino (2015, p. 22) o espectro de radiofrequência é dividido em faixas, que são intervalos reservados, normalmente, para um determinado tipo de serviço, definido por convenções internacionais e/ou por agências reguladoras.

O que acontece é que essas faixas são divididas em partes para que possa haver a transmissão simultânea de sinais diferentes, os quais são semelhantes as estações de rádio e canais de televisão analógicos.

Essa ideia, fica visível quando se fala em redes sem fio, pois nos canais usados pela rede sem fio frequências próximas podem causar interferência. (Rufino, 2015)

Por tanto existem diversos tipos de técnicas de codificação para a transmissão sem maiores interferências.

Um deles é a *Spread Spectrum* que foi criada para uso militar e utiliza toda a faixa da frequência, ela possui a desvantagem de consumir mais banda, porém tem a vantagem de garantir a integridade das informações. Atualmente esse é o padrão usado para todos os tipos de redes sem fio. (Reis, 2012)

Outra técnica é a FHSS (*Frequency-Hopping Spread-Spectrum*) que usa a banda 2,4 Ghz que se divide em 75 canais, e de forma aleatória envia as informações por todos esses canais. Segundo Rufino (2015, p. 23) essa sequência segue um padrão conhecido pelo transmissor e pelo receptor, que, uma vez sincronizados, estabelecem um canal lógico. Uma desvantagem desse modelo é que a velocidade de transmissão chega até 2 Mbps.

Temos também o *Direct Sequence Spread Spectrum* (DSSS) esse modelo também se limita a 1 ou 2 Mbps, porém é utilizado em padrões atuais como o 802.11b, esse tem a característica de separar cada bit de dados em 11 sub-bits, e transmite esses dados em forma redundante, enviando todos os dados pelo mesmo canal, a banda 2,4 é dividida em 3 canais, o que torna esse modelo um alvo para ataques a uma banda fixa. (Reis, 2012)

Outro método de transmissão recebe o nome de *Orthogonal Frequency division Multiplexing/Modulation* (OFDM), atualmente os padrões de rede sem fio utilizam este método por conta de ser capaz de identificar interferências ou ruídos, com isso permite também a troca e ou isolamento de uma faixa de frequência ou alteração de velocidade de transmissão. Segundo Rufino (2015, p. 24) este método é utilizado não somente por

equipamentos sem fio, mas também por redes cabeadas, como ADSL, devido a sua possibilidade de isolação de interferência.

Também possuímos bandas públicas que através de convenções são determinadas para diversos usos no Brasil esse órgão regulamentador é a Anatel, faixas foram reservadas para uso industrial, científico e médico, com isso essas frequências podem ser usadas por qualquer aplicação que se adapte a uma dessas categorias. Segundo Rufino (2015, p. 24) as frequências disponíveis em cada uma das três faixas são:

902 – 928 MHz;

2,4 – 2,485 GHz (2,4 a 2,5 GHz no Brasil);

5,150 – 5,825 GHz.

A primeira faixa informada é reservada para telecomunicação em geral (móvel ou fixa), radioamador, radiolocalização. (Rufino, 2015)

A segunda faixa é utilizada por muitos equipamentos o que torna essa carregada, pode ser usada pelos padrões 802.11b e 802.11g, o que acarreta a utilização dessa faixa por babás eletrônicas e qualquer dispositivo que possua IOT (*Internet of Things* – Internet das coisas), também pode ser usada por aparelhos Bluetooth. (Rufino, 2015)

Já a terceira faixa é usada para redes menores, pois o alcance de distância não é muito grande, tornando isso uma vantagem ou uma desvantagem para essa faixa. (Rufino, 2015)

Temos também as frequências licenciadas, ou seja, as frequências que possuem empresas donas delas e que só deve ser usado pelas empresas detentoras do seu direito, podemos citar o padrão 802.16 (WiMax) que utiliza a faixa de 2 a 11GHz e tem poder para atingir um raio de 50 Km a uma velocidade entre 10 a 70 Mb, e também a faixa 1,8 GHz utilizada no Brasil para telefonia móvel com o padrão GSM, em outros países a frequência usada é a 1,9 GHz. (Anatel, 2015)

3. Rede sem fio – História

O conceito de redes sem fio parece algo novo e com pouco tempo de uso, porém a ideia de comunicação através do ar é antiga, com a segunda guerra mundial houve uma

explosão atrás de novas tecnologias e junto essa tecnologia veio a transmissão através de ondas de rádios, os Estados Unidos da América foi o primeiro a utilizar dessa inovação na guerra onde mandava informações da guerra sem necessitar de fios. (Rocha, 2006)

Na década de 80, vieram mais aprimoramentos dessa tecnologia usada anteriormente das quais estavam infravermelhos e rádios de micro-ondas, o mais utilizado era o infravermelho por conta da fácil comunicação e por não ser necessário o uso de licença, mesmo sendo o mais utilizado ele ainda tinha um problema que perdura até a atualidade, precisava ter um local sem barreiras para que os dispositivos pudessem se comunicar. (Rocha, 2006)

No começo da década de 90 empresas começaram a explorar a oferta de redes sem fio e começaram a ofertar produtos os principais países eram os da América do Norte, porém logo começaram a ofertar também esse serviço na Europa, porém não havia um padrão solido e consistente, onde todos os equipamentos se comunicassem com tudo que estivesse ligado na rede sem fio. (Rocha, 2006)

Com isso o interesse dos fabricantes de equipamentos sem fio começou a cair, e a utilização por parte da população se tornava impossível, com isso surgiu a necessidade de estipular um padrão, em 1997 à IEEE (*Institute of Electrical and Electronic Engineers*), publicou o padrão para as redes sem fio, recebeu o nome de 801.11, na mesma época também lançaram o padrão para utilização do Bluetooth, com a padronização veio uma enorme gama de empresas interessadas em começar a desenvolver para este tipo de tecnologia. (Rocha, 2006)

Mesmo com esse avanço todo não foi fácil chegar à evolução citada, as primeiras redes sem fio foram caras, lentas e com muitos problemas relacionado à interferência e o principal sem nenhuma segurança. Alguns dos problemas enfrentados eram Taxa de transmissão baixa, equipamentos proprietários, sem softwares móveis para garantir o funcionamento do equipamento, perda de qualidade de sinal ao afastar o equipamento receptor do transmissor. (Rocha, 2006)

O avanço alcançado pelo padrão é indiscutível, e a criação desse padrão permitiu que empresas diferentes fizessem o equipamento delas se comunicarem o que também atraiu muitos utilizados, porém a velocidade inicial de acesso era baixa de apenas 2 Mbps o que torna a rede uma rede de transmissão lenta. (Rocha, 2006)

Para solucionar o problema foi feito um estudo que apontou a necessidade de evolução do padrão, porém o próprio comitê de desenvolvimento acabou entrando em conflito sobre as suas decisões e a evolução acabou sendo dividida em outros padrões o 802.11a e 802.11b com velocidades bem superiores a anterior que pode chegar a 54 Mbps também existem o padrão 802.11g e 802.11f, onde cada um possui uma característica determinante e diferente. (Rocha, 2006)

4. Padrão 802.11

Recebe o nome de 802.11 o padrão desenvolvido pela IEEE(*Institut of Eletrical and Electronics Engineers*) para a tecnologia de internet sem fio ou WLAN, existem diversas especificações para este padrão, esse padrão é a referência tanto para o receptor quanto para o transmissor, a norma foi aceita em 1997 visando o aumento dos dispositivos e evolução dos equipamentos sem fio. O padrão 802.11 usa o método de transmissão FHSS ou DSSS, nele possuímos mais variações, entre estas estão as 802.11 a/b/e/g/n. (Alecrim, 2013)

O PARÃO 802.11 A veio a ser usado em 1999, com alguns meses depois apareceu o 802.11 b, o padrão 802.11a tem a possibilidade de transmitir com as taxas de 6 Mb/s, 9 Mb/s, 12 Mb/s, 18 Mb/s, 24 Mb/s, 36 Mb/s, 48 Mb/s e 54 Mb/s, este ainda tem uma área de abrangência de cerca de 50 metros, e trabalha com uma frequência diferente do padrão 802.11 original, trabalhando com a faixa de 5 GHz e com canais de 20 MHz dentro da faixa. A vantagem é que pelo padrão não trabalhar na frequência original, não existe tanta interferência, por conta do pouco uso. Já o principal problema é a possível incompatibilidade com outros dispositivos que não usam esse padrão, outra curiosidade é que esse padrão não utiliza as técnicas conhecidas como DSSS ou FHSS ele utiliza OFDM. (Alecrim, 2013)

Com o avança ainda em 1999, foi lançada uma atualização do padrão ele passou a ser chamado 802.11b por sua vez a atualização incluiu a possibilidade de manter conexão coma s seguintes velocidades 1 Mb/s, 2 Mb/s, 5,5 Mb/s e 11 Mb/s, a técnica de transmissão utilizada é a DSSS, porém ao usar velocidade acima de 5,5 Mb/s este utiliza uma técnica chamada CCK (*Complementary Code Keying*). O raio de atendimento desse padrão passou a ser de 400 metros em áreas abertas em locais com barreiras ou fechados

pode atingir até 50 metros, porém essa transmissão pode sofrer influência, podemos citar paredes. Esse padrão foi o primeiro a ser utilizado em grandes escalas, e deu início a popularização das redes sem fio. (Alecrim, 2013)

O padrão 802.11c não é comum falarmos dela, pois nela foi definido padrões de acesso as pontes (*Bridges*) de modo apropriado, suportando pondes em utilização a nível de MAC (*Media Access Control address* – endereço físico de rede) os dispositivos que utilizam esse padrão são os que possuem função para realizar ponto a ponto. (Alecrim, 2013)

Outro padrão que serviu de atualização foi o 802.11d que atualiza o padrão para a normatização do uso do padrão 802.11 internacionalmente, isso significa que o padrão 802.11d permite que todos os equipamentos se comuniquem trocando informação em várias frequências. (CCM, 2016)

Já o padrão 802.11e teve como objetivo principal introduzir a possibilidade de QoS (*Qulity of Services*) em dispositivos que usavam a comunicação em redes sem fio, tornando assim possível a utilização de serviços como voz, vídeo e áudio. (CCM, 2016)

O padrão 802.11f veio com o intuito de facilitar os fabricantes de pontos de acesso por meio de fornecer métodos que torne fácil a troca de ponto de acesso pelos dispositivos sem que seja necessária a interação do usuário, para isso foi implementado o protocolo *inter access point roaming protocol*. (CCM,2016)

O protocolo 802.11g é um dos mais versáteis que possui, ele pode interagir com equipamento que utilizam padrões 802.11b. A técnica de transmissão padrão é a OFDM que é a esma do protocolo 802.11a, o 802.11g opera na faixa da frequência 2,4 GHz, contando com o mesmo campo de cobertura do 802.11b, quando vai transmitir para o padrão 802.11b é alterada sua forma de comunicação passando a operar por DSSS. Qualquer dispositivo que opera om o padrão 802.11g deverá se comunicar com os outros equipamentos que operam no padrão 802.11b sem grandes problemas. (Alecrim, 2013)

O 802.11h é uma atualização que proporciona compatibilidade das normas europeias.

Já o padrão 802.11i tem o objetivo de incluir mais segurança no protocolo adicionando uma gestão de chaves de acesso, codificações e autenticação, baseando-se no AES

(*Advaced Encryption Standard*), defendendo uma codificação para todas as transmissões realizadas pelos diversos padrões 802.11. (Alecrim, 2013)

O padrão 802.11j é uma atualização do padrão para a utilização da faixa de 4,9 à 5 Ghz seguindo as normas japonesas de acesso as frequências de rádios, o objetivo principal foi criar um padrão para que os dispositivos pudessem trocar de frequência ou largura de canal afim de disponibilizar maior desempenho e menor interferência com outros dispositivos sem fio. (CCM, 2016)

O padrão 802.11n é o mais compatível de todos já citados, pois é uma evolução do 802.11g podendo transmitir informações para o 802.11b, 802.11a e 802.11g. O padrão utiliza as frequências de 2,4 e 5 Ghz por conta disso é a sua capacidade em se comunicar com as versões anteriores, usa técnica de transmissão OFDS, e usa um esquema chamado MIMO (*Multiple-Input Multipe-Output*) que é a capacidade do agregar velocidade de transmissão quando possuem mais de uma antena (Aps) e receptores (STAs), podendo chegar a faixa de 300 Mbps e com essa combinação bem alinhada produtos prometem chegar a uma taxa de 600 Mbps. Com isso também podemos dizer que o 802.11n usa a técnica de transmissão MIMO-OFDM. (CCM, 2016)

Atualmente o padrão mais falado é o 802.11ac que deve ser o sucessor do padrão 802.11n, foi praticamente desenvolvido entre 2011 e 2013 com lançamento em 2014. Existem equipamentos que já estão sendo vendidos que permitem a utilização do 802.11ac, a principal mudança é o aumento da velocidade para que isso fosse possível foi unido três fundamentos que são, aumento de largura de banda, aumento de eficiência e relação de sinal/ruído. (Alecrim, 2013)

Esse protocolo usa o OFDM com possibilidade de usar o MIMO tornando possível o alcance de velocidades de 1300 Mbps, usando a frequência de 5 GHz diferente do 802.11n que poderia operar em frequências 2,4 e 5 GHz, o 802.11ac pode agrupar números maiores de canais e utilizá-los simultaneamente e será compatível com equipamentos do padrão 802.11n.

Segundo Rufino(2015, p. 35), vários fornecedores estão optando por fabricar equipamentos que podem operar em ambos os padrões, o que pode ser afirmado com isso que o consumidor ou o usuário final que não tem total domínio sobre a ferramenta não vai ter

uma experiência traumática quando tiver que optar por um dispositivo que atenda a um padrão específico.

5. Segurança em redes sem fio

A segurança da informação deve estar presente em qualquer rede, porém em uma rede sem fio ela se torna obrigatória por conta do fácil acesso e levando em conta que todos nós temos dispositivos móveis que podem acessar qualquer rede sem fio que esteja visível.

Para isso devemos implementar mecanismos que permitam essa segurança, pensando sempre que a segurança deve se basear nos pilares que são confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade. Somente quando garantirmos essas cinco situações podemos dizer que estamos protegidos. (Alecrim, 2013)

E o quão importante são os seus dados, vemos diversas pessoas que tem informações roubadas e através dessas informações muitas coisas acontece. Como exemplo, a exposição e a perda de capital financeiro.

Existem alguns métodos que garante uma certa segurança para a rede sem fio, tais como, *WEP* (*Wired Equivalent Privacy*)*, WAP (Wi-Fi Protected Access), WAP2* (versão 2 de *Wi-Fi Protected Access II*)*, TKIP* (Temporal Key Integrity Protocol), *AES* (*Advaced Encryption Standard*)*, WPA-PSK* (Pre-Shared Key) *e WPA2-PSK* (Pre-Shared Key versão 2). A grande maioria dos dispositivos de APs permite configuração para todos os métodos, porém não ao mesmo tempo.

Um método de segurança eficaz é o de controlar acesso por MAC *address,* porém esse método requer manutenções periódicas devido à necessidade de acrescentar ou retirar MAC dos *Access Point*, essa solução é uma solução boa para ambientes pequenos e com mudanças pontuais onde é possível prever e previr por eventuais mudanças de equipamentos, para uma empresa de grande ou médio porte já se torna um método complicado de se manter. (Alecrim, 2013)

O WEP (*Wired Equivalent Privacy*) é um protocolo que tem a funcionalidade de cifrar os dados e está presente em todos os equipamentos sem fio.

Segundo Rufino (2015, p. 40), WEP é um protocolo que utiliza algoritmos simétricos, isso significa que os dispositivos compartilham uma chave de acesso entre todos da rede e os equipamentos tem o objetivo de cifrar e decifrarem o código para a tramitação das informações.

Esse protocolo foi desenhado seguindo os seguintes critérios:

- Suficientemente forte – deve ser adequado as necessidades do usuário.
- Autossincronismo – deve permitir que um equipamento entre a área de cobertura e funcionar sem nenhuma intervenção.
- Requer poucos recursos computacionais – pode ser usado em equipamentos com o mínimo poder de processamento onde este pode ser instalado através de software ou diretamente no hardware.
- Exportável – deve ser exportável para qualquer país.
- De uso opcional – pode ou não ser usado.

O funcionamento é um tanto quanto simples são necessárias duas chaves onde uma é estática que deve existir em todos os equipamentos da rede, e uma outra dinâmica que juntos formam a chave para decifrar e cifrar os dados trafegados. Depois de autenticado é feito um processo que essa chave estática se divide em outras 4 que podem ser de 40 à 104 bits, algo suscetível a um ataque de força bruta, para tentar reduzir as chances de ataque é incluído um segundo elemento que pode conter cerca de 24 bits. (Rufino, 2015)

Com os problemas apresentados no método WEP (*Wired Equivalent Privacy*), foi criado uma nova forma de autenticação que recebeu o nome de WPA (*W-Fi Protectes Access*), com este novo método de acesso veio alguns avanços principalmente mais segurança, uma mudança entre o WPA e o WEP foi que o WPA não permite acesso a configuração *ad hoc*, com isso as redes que foram configuradas por esse último método não podem contar com a utilização do WPA.

O protocolo foi disponibilizado ainda em 2003, o objetivo além de implementar mais segurança era manter os dispositivos que utilizavam WEP em atividade, na verdade podemos dizer que o WPA é uma atualização do WEP, com isso o método manteve alguns

problemas, pois partes de códigos foram herdados do anterior e com isso o método de ataque através de força bruta não foi resolvia, outros tipos de ataques eram ainda muito utilizados para a quebra desse tipo de autenticação.

O WPA tinha áreas distintas de atuação, segundo Rufino (2015) divide-se essas áreas em dois tipos de chaves, a chave compartilhada e a troca dinâmica da chave.

Antes de entendermos essas dois tipos de chaves devemos entender a criptografia usada no WPA, a criptografia tinha o objetivo de melhorar os mecanismos usados pelo WEP, no WPA combina algoritmo e temporalidade da chave, como sabemos as redes sem fios podem estar ativas em diversos ambientes sendo eles domésticos, corporativos de pequeno, médio ou grande porte, foi imaginado que o WPA devesse ter diversos tipos de segurança através de chaves cadastramento manual de chaves, porém isso se torna trabalhoso, repetitivo e de difícil gerenciamento. (Alecrim, 2013)

O protocolo para cifrar os dados pode ser dividido em dois, um para pequenas redes, que tem uma chave mestre que segundo Rufino (2015, p. 42) existirá uma chave compartilhada previamente (Pre-Shared Key, ou WPA-PSK) que será responsável pelo reconhecimento do equipamento pelo concentrador. Já o segundo protocolo pode ser denominado infraestrutura, que terá um centralizador de autenticação.

Segundo Rufino (2015, p. 42) poderá ser necessário de uma infraestrutura de chaves públicas (ICP), caso utilize certificado digital para promover a autenticação do usuário, podemos dizer que esse segundo ponto será mais indicado para empresas, pois será necessário acrescentar mais um equipamento sendo este um servidor de chaves o que eleva o custo dessa estrutura.

Uma vantagem no protocolo WPA sobre o WEP é o uso de um protocolo que recebeu o nome de TKIP (Temporal Key Integrity Protocol), tem a função de gerenciar as chaves temporárias que são utilizadas pelos diversos dispositivos que se comunicam usando esse protocolo, outra vantagem citada por Rufino (2015, p. 43) é o aumento significativo do tamanho do vetor de iniciação (Inicialization Vector), que passou dos originais 24 para 48 bits, com isso os ataques a esses vetores se tornaram inúteis pela quantidade de possibilidade de combinações. Mesmo com todas essas vantagens este protocolo possui vulnerabilidades.

Cada ano que passa usamos mais dispositivos móveis que necessitam de internet também móvel, por conta disso os protocolos continuam a evoluir em 2004 foi feita a evolução do protocolo WPA, com isso criaram um protocolo mais seguro, que leva o nome de WPA2, Rufino afirma que este protocolo é o protocolo mais seguro, devido à grande evolução e também ser o último protocolo que foi lançado e continua em uso, para equipamentos, mas simples tem boa utilização e também é um protocolo leve e estável, surgiu com a homologação do 802.11i diferentes dos outros usa o protocolo AES para cifrar e decifrar os dados, utilizando esse método faz a criptografia em forma de blocos com cerca de 128 bits. (Rufino, 2015)

Uma das vantagens desse padrão é que ele permite a comunicação por diversos outros padrões 80211x conhecidos e já usados, uma novidade é a possibilidade de utilizar certificação digital, que até então não era possível nos seus antecessores, o modelo de autenticação utilizado é o EAP (*extensible Authentication Protocol*), porém este método não é utilizado sozinho e sim em conjunto com o TKIP, com essa junção dos dois protocolos é permitido a utilização de criptografia até 256 bits. Por ser um padrão relativamente novo, muitos equipamentos obsoletos ou com data de lançamento anterior ao do protocolo não permitem a utilização desse método. (Rufino, 2015)

A autenticação de uma rede sem fio é algo muito importante devemos lembrar que existem diversos métodos de autenticação, além das possibilidades de autenticação do WPA / 2 temos outros que também podem ser usados tais como autenticação por MAC (endereço físico) dos equipamentos, senhas fixas, senhas dinâmicas (*one time password*) e até certificados digitais. (Rufino, 2015)

Não podemos definir qual é o melhor, pois cada um tem suas vantagens e desvantagens, porém o que devemos ressaltar é que é necessário criar uma barreira como proteção para que a rede sem fio não fique expostas a qualquer risco, mesmo criando essas barreiras devemos saber que ainda existe risco. (Rufino, 2015)

6. Ameaças e Riscos

Conforme já falamos anteriormente com o crescimento da utilização dos dispositivos móveis, e com o crescente incentivo e facilidade de acesso à internet vieram os perigos delas. Com recentes casos de sequestro de dados, exposição de dados pessoais em redes públicas, fica a pergunta o quanto nós estamos preparados e seguros para navegar, essa é uma pergunta que podem ter diversas respostas.

Qual o maior problema que uma intrusão e exposição dos seus dados podem causar. Tivemos casos de extrema importância, onde o ataque conseguiu afetar muitas pessoas, um deles e bem conhecido foi o ataque à rede PSN da empresa Sony, que aconteceu em 2011 e foram roubados dados de pelo menos 24 milhões de pessoas, esses dados continham número de cartão de crédito, senha, histórico de compras na rede, os dados não eram criptografados. A empresa tentou recompensar os usuários, porém ficou com uma marca negativa. (Rohr, 2011)

Se isso acontece com empresas que investem em segurança, imagina com consumidores convencionais que não se preocupam tanto com a segurança dos seus dados.

Segundo o dicionário Michaelis ameaça quer dizer aceno, gesto, sinal ou palavra, cujo fim é advertir, amedrontar, atemorizar ou promessa de castigo ou de malefícios. Já risco eles definem como possibilidade de perigo, incerto, mas previsível, que ameaça de dano a pessoa ou a coisa.

Em informática a ideia é a mesma, a ameaça é a possibilidade de alguém explorar uma falha sendo de sistema ou de hardware, já risco tende a ser uma possível falha de sistema que um agente tente explorar para trazer impactos à organização, esse impacto nem sempre negativo. (Rufino, 2015)

É oportuno entender que a rede sem fio requer cuidados adicionais em comparação a uma rede cabeada, falaremos sobre hackers, ataques físicos, war drivers, rogue AP e pessoas que fazem parte e já possuem acesso a essas redes.

Ataques físicos não são ataques que irão causar danos físicos a pessoa dona da rede, e sim ao equipamento que utiliza em sua rede. Quando chegamos em um prédio comercial é comum encontramos barreiras físicas como catracas, atendentes e câmeras, com a infraestrutura é a mesma coisa ao entrar em um centro de processamento de dados, iremos encontrar diversas barreiras. Com a rede sem fio já não conseguimos controlar a frequência para não ser vista pelos equipamentos, o que torna mais inseguro o processo de colocarmos uma rede sem fio na empresa. (Rufino, 2015)

Não deve ser esquecido dos problemas causados pela não configuração correta dos equipamentos, muitos problemas estão em ambientes que mantém a configuração de fabrica dos equipamentos onde com usuários e senha padrão conseguem acessar esse dis-

positivo ou até mesmo onde deixam a rede aberta. Podemos comparar essa atitude a deixar o portão da sua casa aberto, entra qualquer pessoa e não é possível saber o intuito que a pessoa está acessando. (Rufino, 2015)

O ataque de war drivers é buscando redes sem segurança nenhuma o que o atacante quer é achar uma rede sem segurança ou sem nenhuma senha para o acesso, estes ataques podem ser feitos usando um notebook, celular, ou qualquer dispositivo que tenha acesso sem fio. (No mundo das redes, 2011)

Hackers a intenção de acesso a uma rede sempre está vinculado a alguma conquista pessoal, podendo ser valor financeiro (atrás de dados financeiros), ou por prazer motivacional, fez algo que não queria e acaba virando alvo. Em empresas é comum os ataques serem de ex-funcionários ou funcionários insatisfeitos com a empresa e que demonstrar o descontentamento. Existem muitas possibilidades que levam uma pessoa a fazer um ataque entre essas possibilidades estão os seguintes: curiosidade, diversão, desafio, ativismo e dinheiro. (No mundo das redes, 2011)

Rogue AP, nada mais é do que criar um clone do dispositivo emissor de rede sem fio, isso pode ser feito através de captura de frames emitidos pela rede sem fio e posteriormente usando um software de força bruta conseguir as chaves de acesso, assim o atacante torna esse ponto de acesso "clone" em um ponto de acesso reconhecido pelos demais, tornando assim possível que usuários da rede se conectem nele e com isso os dados navegados nesse ponto de acesso pirata podem ser captados. Posteriormente o atacante faz a seleção dos dados que são críticos e podem valer a pena e dos dados que são considerados descartáveis. (No mundo das redes, 2011)

Interceptação de dados, uma rede sem fio por si só já dá a ideia que os dados não possuem um caminho para seguir como acontece na rede cabeada, com isso se torna mais fácil conseguir interceptar uma sequência de dados, por conta do raio de abrangência do sinal, com isso qualquer pessoa que estiver nesse raio e souber como utilizar a ferramenta para a captura desses dados terá acesso, para usuários domésticos esse é um medo menor, pois dificilmente utilizamos dados confidenciais, os dados mais confidenciais que usamos são: internet *bank* e redes sociais. (Rufino, 2015)

Outro ponto em que redes sem fio são bem sensíveis é com relação a interferência, podemos dizer que caso uma pessoa queira deixar o serviço da rede sem fio indisponível

é necessário que apenas cause uma interferência ao emissor de ondas ou a simples utilização do micro-ondas pode ocasionar uma queda de qualidade de sinal ou perda total de sinal.

7. Defendendo a rede sem fio

O *access point* é um dos meios de comunicação mais importante nas redes sem fio, por esse motivo devemos manter atenção especial para suas configurações. Não podemos descuidar dele, se um hacker chegar a invadir o *access point* estará a um passo de conseguir o principal meio de acesso ao computador ou dispositivo móvel que utilizamos para fazer nossas transações. (Rufino, 2015)

Para tentar criar barreiras de segurança para dificultar a vida do hacker devemos tomar algumas atitudes com relação ao nosso ponto de acesso.

A primeira e que boa parte das pessoas não se preocupa é as configurações de fabricas dos equipamentos, a primeira coisa a se fazer com o equipamento após tirar da caixa e modificar as suas configurações. Tornando esse equipamento um pouco mais seguro. (Alecrim, 2013)

Uma possibilidade válida também é retirar a difusão do nome da rede, a ideia aqui é não deixar a rede visível a tudo e a todos, mantê-la escondida com isso dificulta a possibilidade de o atacante acessar sua rede, não podemos atacar o que não vemos. (Rufino, 2015)

A troca do MAC também pode ser feita em muitos equipamentos, ou seja, mudará o método de procura de MAC, caso esse procedimento seja feito no começo da configuração do dispositivo não trará nenhum transtorno aos futuros utilizadores. (Rufino, 2015)

Desabilitar o acesso ao *access point* via rede sem fio, ou seja, para acessar as configurações do roteador sem fio, será necessário estar conectado através de um cabo UTP, isso reduz a chance dos atacantes acessarem as configurações do seu *access point*. (Rufino, 2015)

Outro método que pode ser utilizado é a autenticação mútua, ou seja, é configurada uma senha nos equipamentos que irão se conectar à rede sem fio e configurado também no *access point*, através de algoritmos sofisticados, o processo de checagem da senha

é feito dos dois lados e quando é identificado ambos como idôneos é feita a comunicação. (No mundo das redes, 2011)

Configuração por MAC, ou seja, é feito o cadastro do MAC do dispositivo que será integrado a rede no *access point*, posteriormente é definida uma senha no *access* point e os equipamentos que irão ingressar na rede deverão fornecer as duas credenciais corretas (senha e MAC previamente cadastrado). (Rufino, 2015)

Essas são soluções que podem ser utilizadas em qualquer ambiente de qualquer tamanho, claro que cabe a cada administrador verificar a sua necessidade e adequar às soluções.

CONSIDERAÇÕES FINAIS

Os métodos de ataques são variáveis e não estáticos, ou seja, evoluem ou são adaptados, de modo que é necessário que o utilizador sempre se atualize com informações de fontes fidedignas. Isso é o que não acontece com a maioria dos usuários da rede sem fio.

A rede sem fio se tornou tão popular que as pessoas veem isso apenas como um facilitador e acabam esquecendo que existem riscos.

Muitos dos riscos quem proporciona são os usuários tendo um equipamento desatualizado, não estruturado adequadamente e acessando sites não confiáveis ou até mesmo utilizando softwares de antivírus com serial pirata.

Por mais que os protocolos de rede evoluíram e se tornaram mais seguros, podemos ver que ainda não é o suficiente para extinguir os ataques de crackers ou hackers.

O que resta para os usuários desse sistema é se prevenir tomando cuidado de como, quando e onde acessar informações importantes com seus equipamentos. Outra possibilidade é realizar processos simples para tentar se proteger colocando, por exemplo, uma senha forte que deve conter caracteres em maiúsculo, em minúsculo, especiais e números, não que apenas com isso irão acabar com todas as possibilidades de uma invasão ou roubo de informação, mas vai dificultar o ataque.

Claro que quanto mais métodos de segurança vão se implementando nos equipamentos, mais seguros estes vão ficando. Simplesmente retirar um equipamento da caixa e usar e esperar que nada acontece é um risco imensurável.

REFERÊNCIAS BIBLIOGRÁFICAS

Altieres Rohr. 2011. “Vazamento de dados da PSN é considerado o 5º maior da história.” Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/04/vazamento-de-dados-da-psn-e-considerado-o-5-maior-da-historia.html>. Acesso em 19/05/2016.

Anatel. 2015. “Região 2.” Disponível em: <http://sistemas.anatel.gov.br/pdff/Consulta/FreqConsulta.Asp?inpNumFaixa=527&intPagina=18&intLivro=1>. Acesso em 17/05/2016.

CCM. 2016. “Introdução ao Wi-Fi (802.11 ou WiFi).” Disponível em: <http://br.ccm.net/contents/790-introducao-ao-wi-fi-802-11-ou-wifi>. Acesso em 19/05/2016.

Emerson Alecrim. 2013. “O que é Wi-Fi (IEEE 802.11)?”. Disponível em: <http://www.infowester.com/wifi.php#80211b>. Acesso em 19/05/2016.

Gustavo Henrique da Rocha Reis. “Redes de Computadores”. 2012. Disponível em: <https://sistemas.riopomba.ifsudestemg.edu.br/dcc/materiais/1042283583_redes-sem-fio.pdf>. Acesso em 28/07/2016

João Wilson Vieira Rocha. “Redes WLAN de Alta Velocidade.” 2006. Disponível em <http://www.teleco.com.br/tutoriais/tutorialredeswlanI/default.asp>. Acesso em 03/05/2016

Júlio Battisti. “Rede Wireless – Parte III.” 2014. Disponível em: <http://juliobattisti.com.br/tutoriais/paulocfarias/redeswireless001.asp>. Acesso em 03/05/2016.

Michaelis. “Moderno Dicionário da Língua Portuguesa.” Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php>. Acesso em 05/04/2016.

No mundo das redes. “Segurança de Redes sem fio”. 2011. Disponível em: <http://no-mundodasredes.blogspot.com.br/2011/07/seguranca-de-redes-wireless.html>. Acesso em 25/05/2016.

Redes de computadores. “Infravermelho.” 2011. Disponível em: <http://meios-de-trans-missao-de-dados.blogspot.com.br/2011/04/infravermelho.html>. Acesso em 03/05/2016.

Rufino, N. M. O. “Segurança em redes sem fio.” 5. Ed. São Paulo: Novadata, 2015. 287 p.