REDES WIRELESS DOMÉSTICA

JOÊNIA OLIVEIRA LOPES
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMA

Paracatu, novembro de 2016

RESUMO

Com a necessidade de mobilidade a tecnologia wireless vem ganhando cada vez mais usuários tanto em rede empresariais, como em rede doméstica. Mas a dúvida é se esta tecnologia dispõe de mecanismos que garantam segurança aos seus usuários? Existindo tais mecanismos seria fácil a qualquer usuário implementá-los? Quais seriam as dificuldades encontradas? Neste artigo iremos buscar responder a tais duvidas e tentar enumerar alguns riscos no uso desta tecnologia.

Palavras chaves: Wireless, Segurança de Redes.

1 - INTRODUÇÃO

Wireless – E a tecnologia que permite a conexão de dispositivos eletrônicos sem a necessidade de cabos, a comunicação se dá por meio de radiofrequência, a distância varia de acordo com a tecnologia empregada e a potência dos dispositivos. O termo wireless em si significa “sem fio”, toda e qualquer comunicação que se propaga sem a utilização de fios ou cabos trata-se de uma conexão wireless. Em nosso cotidiano utilizamos diversos meios de wireless, como por exemplo o Bluetooth, a conexão existente entre diversos aparelhos e o seu respectivo controle remoto, entre o celular e as torres das operadoras e até o rádio da polícia com as centrais de operação.

Já no ano de 1901, o físico italiano Guglielmo Marconi demonstrou o funcionamento de um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código Morse(infoescola.com).

Mas neste artigo trataremos da conexão de dispositivos móveis à rede mundial de computadores por via wireless. Nos dias atuais é muito comum na maioria dos lugares a disponibilidade de rede móveis, por vários motivos: não é caro, relativamente simples de instalar e concede aos seus usuários a vantagem de estar conectado sem precisar ficar preso a uma mesa ou a um conector fixo basta apenas estar ao alcance do ponto de acesso. Vamos neste artigo buscar e analisar alguns prós e contras desta conexão em ambiente doméstico. A natureza desta pesquisa é exploratória o método de pesquisa utilizado para este trabalho foi a pesquisa documental, através de referências bibliográficas disponíveis em sites e artigos online.

1.1 – O PROBLEMA

O problema a ser abordado é de que forma podemos implementar uma conexão wireless que nos garanta segurança de acesso e manipulação de dados. Se você possui um computador um celular e uma smart TV estes dispositivos vão se conectar através de um roteador, se este roteador não está seguro nenhuma destas conexões estarão.

1.2 – OBJETIVOS

O presente artigo propõe os seguintes objetivos, divididos em geral e específicos:

1.2.1 – Objetivo Geral

Neste artigo buscaremos orientar usuários comuns na configuração de uma rede doméstica que seja segura, demostraremos alguns riscos e possíveis soluções.

1.2.2 – Objetivo Específicos

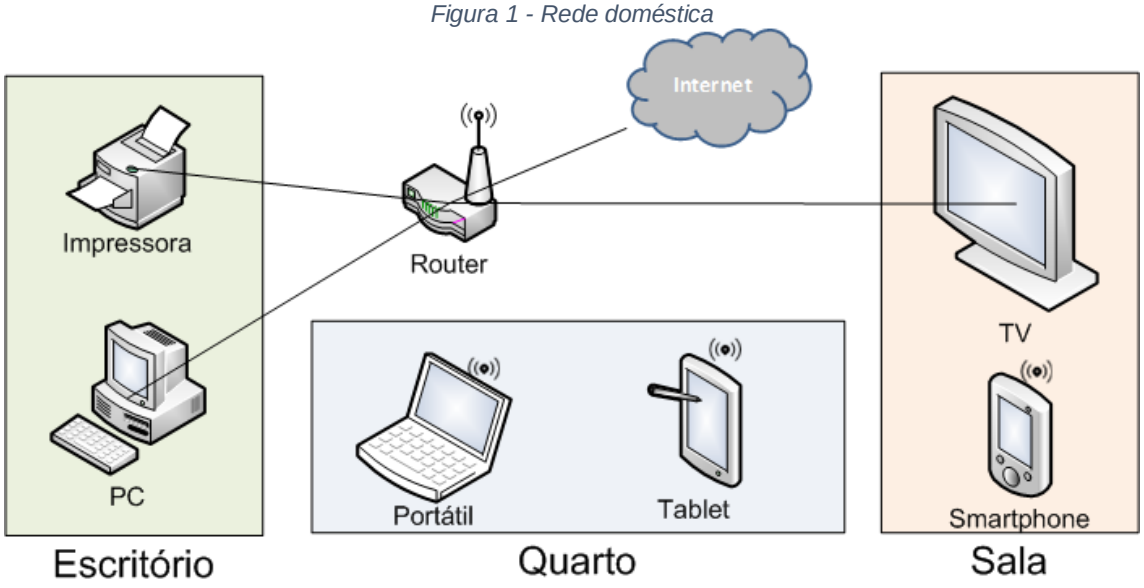
- Definir uma rede wireless e seus padrões;
- Definir a hierarquia da rede wireless;
- Enumeração de algumas ameaças e técnicas de ataque;
- Listar algumas soluções de fácil implementação que nos garanta uma solução viável;

2 – REDE DOMÉSTICA

Na realidade do mundo atual a palavra de ordem é mobilidade e nos deparamos com um crescente desenvolvimento de dispositivos móveis tais como smartphones, tablets e notebooks e não faria sentido utilizar estes equipamentos em uma rede cabeada.

A poucos anos atrás as famílias não tinham necessidade ou não tinha condições de adquirir mais de um dispositivo como estes, no entanto, hoje um único computador não é mais suficiente na maioria das famílias. Numa casa com alguns computadores e dispositivos moveis e até smart tvs que necessitam conexão à rede uma rede doméstica tornou-se uma mais que uma necessidade. Se você possui dois ou mais dispositivos em casa, uma rede doméstica permite o compartilhamento de arquivos, documentos, impressoras etc.

Figura 1 - Rede doméstica



Fonte - http://www.newcompany.pt/paginas.php?idpagina=19

3 - PADRÕES DE REDE WIRELESS

Vamos primeiramente definir os padrões de redes Wireless. Todas os diferentes padrões wireless começam com o número 802.11, seguido por uma ou duas letras que, servem para diferenciar as propriedades da conexão como velocidade de transmissão e alcance do sinal. Vamos ver muitas vezes que os produtos suportam múltiplos, se não de todos os padrões, ao mesmo tempo. Você pode ter visto uma listagem como Wi-Fi (Wireless-Fidelity) 802.11 a / b / g / n / ac sobre a folha de especificações para muitos smartphones, que abrange todos os padrões modernos mais antigos e mais comuns. Segundo o site www.oficinadanet.com.br/post/8619-qual-a-diferenca-entre-redes-wifi-a-b-g-n os padrões se dividem da seguinte maneira:

IEEE 802.11a: Padrão utilizado em empresas que necessitam grande tráfego de informações. A principal vantagem desse tipo de padrão é a alta velocidade, como também a ausência de interferências. Esse padrão Wi-Fi é para frequência 5 GHz com capacidade teórica de 54 Mbps. O único problema encontrado nesse tipo de padrão é o seu alcance, que não costuma ser muito grande.

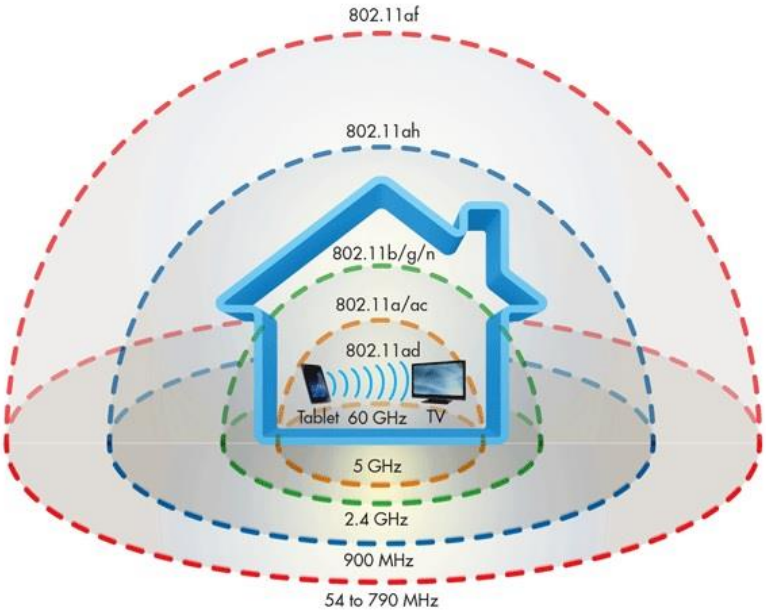
IEEE 802.11b: Padrão de rede utilizado no ambiente doméstico. Também é encontrado em pequenas empresas. A sua principal vantagem realmente é o seu alcance. Porém, como desvantagem, a sua velocidade, que costuma ser inferior se comparada às outras. O padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 11 Mbps.

IEEE 802.11g: Esse padrão poder ser comparado ao (b), porém, se comparado a velocidade, esse padrão costuma responder melhor. Igualmente ao padrão (b), é amplamente usado em residência e empresas de porte pequeno. Para tanto, como desvantagem, o alcance costuma ser menor ao padrão (b). O padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 54 Mbps.

IEEE 802.11n: Este é o mais recente padrão, poucos equipamentos fazem uso dessa tecnologia, porém, com o decorrer do tempo, a tendência é aumentar. A

Apple, famosa pela qualidade de seus produtos, já possui alguns aparelhos com essa tecnologia, como por exemplo, o iPhone de quarta geração e alguns modelos de MacBooks. O padrão Wi-Fi para frequência 2,4 GHz e/ou 5 GHz com capacidade teórica de 65 a 600 Mbps.

Figura 2 - Padrões de rede wireless



Fonte - http://mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah

3.1 HIERARQUIA DA REDE - No contexto da informática, uma rede é formada por vários dispositivos interligados que compartilham recurso. A algum tempo este conceito estava restrito a escritórios ou ambientes corporativos, mas atualmente também em ambiente doméstico existe esta necessidade de conexão, existem vária designações de rede vejamos algumas:

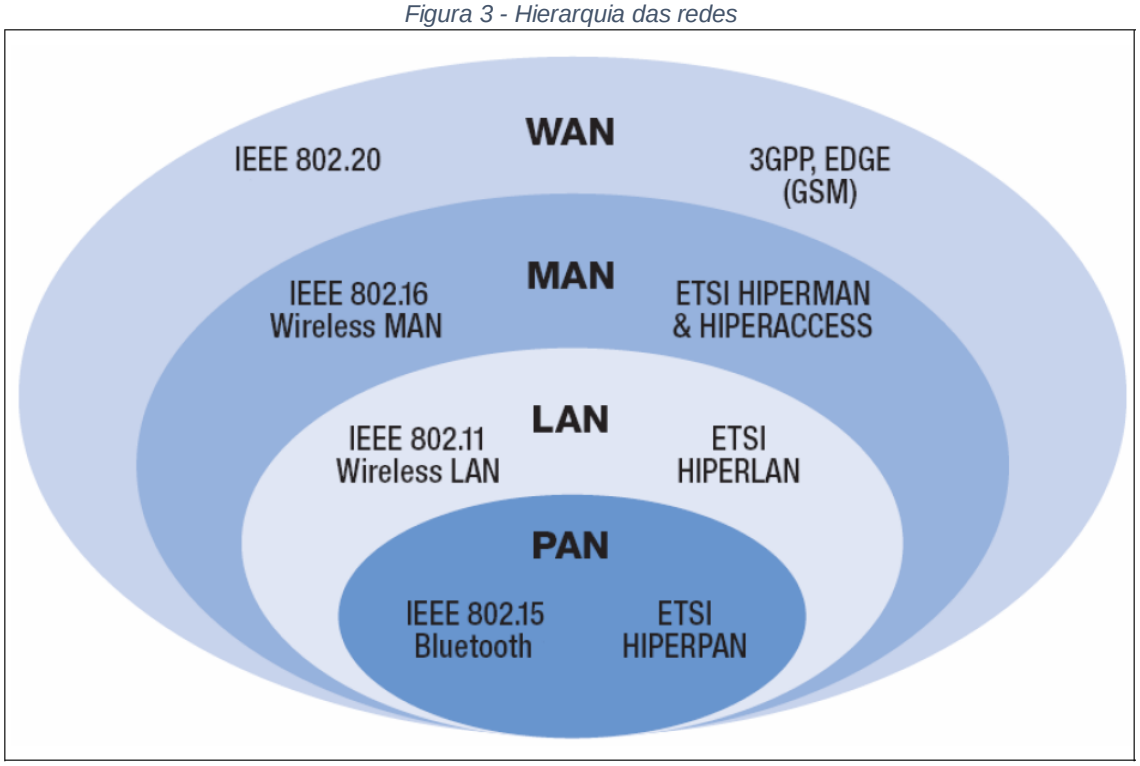
PAN – As redes do tipo PAN, ou Redes de Área Pessoal, são usadas para que dispositivos se comuniquem dentro de uma distância curta. Um exemplo disso são as redes Bluetooth e UWB(Ultra-wide-band). Definido pelo padrão 802.15. (Barcelar, 2006)

WLAN – Rede Local Sem Fio. Esse tipo de rede é bastante utilizado tanto em ambientes residenciais quanto em empresas e lugares públicos. Definido pelo padrão 802.11. (Barcelar, 2006)

WMAN – Rede Metropolitana Sem Fio com um alcance de dezenas de quilômetros, sendo possível conectar redes de escritórios de uma mesma empresa ou de campus de universidades. Definido pelo Padrão 802.16. (Barcelar, 2006)

WWAN – Rede de Longa Distância Sem Fio. Com um alcance ainda maior, a WWAN alcança diversas partes do mundo. Justamente por isso, a WWAN está mais sujeita a ruídos. Definido pelo padrão 802.20. (Barcelar, 2006)

Figura 3 - Hierarquia das redes



Fonte: http://docplayer.com.br/81260-Leandro-lavagnini-barrozo.html

4 – SEGURANÇA

Segurança segundo o dicionário Aurélio é: ‘Qualidade do que é ou está seguro. Conjunto das ações e dos recursos utilizados para proteger algo ou alguém. O que serve para diminuir os riscos ou os perigos. ’ Em segurança da informação esse conceito não muda. Na verdade, ela está apoiada em três princípios básicos: Confidencialidade, Integridade e Disponibilidade.

Confidencialidade – é um princípio que garante que o acesso a determinada informação será concedido apenas a quem tem esse direito.

Integridade – esse princípio garante que a informação será armazenada sem mantendo-se suas características originais estabelecida por seu proprietário.

Disponibilidade – garante que a informação estará sempre disponível ao proprietário ou usuários por ele autorizados.

Talvez possamos imaginar que não exista o interesse de violar esses princípios quando se trata de uma conexão no ambiente doméstico, mas mesmo aí esses princípios devem ser assegurados. A rede wireless é por natureza vulnerável a ataques, pois qualquer pessoa que esteja no raio de alcance da sua rede pode interceptar o seu sinal, o perigo vai desde a utilização não autorizada do seu sinal a um ataque propriamente dito. Informação é sempre valiosa e talvez você nem saiba o que um intruso pode fazer com os seus dados caso tenha acesso a eles.

5 - TIPOS DE ATAQUES EM REDES WIRELESS

Segundo o site http://www.contractti.com.br/portal/dicas/wireless-dicas/66-tipos-de-ataque-wireless.html esses são os tipos mais frequentes de ataque:

5.1 - ENGENHARIA SOCIAL - A mais simples e muito eficaz maneira de conseguir informações é perguntando, nesta tática a pessoa simplesmente faz perguntas que podem ser aparentemente inofensivas, mas que se trata de uma coleta de informações, às vezes por excesso de confiança e falta de malicia, podemos passar informações valiosas numa conversa aparentemente boba. E a eficácia está no fato de a vítima nem se dar conta que está sob ataque.

5.2 - PONTO DE ACESSO FALSO - Este ataque aproveita falhas nos sistemas operacionais e da falta de atenção do usuário. Utilizando um software que transforme uma placa wireless em um ponto de acesso o notebook se comporta como um AP (Access Point) assim ao ser ligado em uma rede cabeada pode dar acesso à internet a vítima. Isto é possível porque ao configurar um notebook com o mesmo nome do AP, este gera um sinal que é mais forte que o sinal do AP verdadeiro. O sistema operacional se conecta com o sinal mais forte então acaba se conectando no ponto falso. Deste jeito o invasor obtém acesso aos dados de acesso do verdadeiro AP verdadeiro e outras informações importantes que estão trafegando na rede.

5.3 - FORÇA BRUTA - Uma das técnicas mais antigas de invasão de um sistema é o ataque de força bruta, vulgo *brutal force*. Todo sistema de acesso restrito é acessível através do conjunto nome de login e senha e um ataque de força bruta significa tentar adivinhar o conjunto por meio de tentativa e erro. Se o invasor souber pelo menos do nome do usuário já tem um bom caminho andado, pois só irá precisar descobrir a senha e surpreendente como existem senhas óbvias. O programa receberá um arquivo com uma lista de senhas chutadas e tentará se conectar ao servidor usando cada uma delas.

5.4 - WLAN SCANNERS – Esta técnica de ataque ocorre quando um dispositivo opera na mesma frequência do AP dentro do alcance, pode captar os sinais transmitidos. Mesmo desabilitado o envio de broadcasts no AP não impede que scanners detectem uma rede sem fio, pois está enviando pacotes mesmo sem nenhum usuário conectado, os scanners enviam pacotes de solicitação de SSID (Service Set Identifier) para todos os canais e é aguardada a resposta do AP. Dessa forma as informações de rede são captadas.

5.5 - MAC SPOOFING - Nessa técnica o endereço físico da sua placa sem fio ou placa de rede é clonado. A técnica de falsificação de endereços não é utilizada apenas para falsificação de endereços, mas serve também para evitar que o endereço real de um ataque seja reconhecido durante uma tentativa de invasão. Pode ser também usado para acesso não autorizado em redes que não usam senhas e sim apenas controle de acesso por MAC (Media Access Control).

5.6 - MAN IN THE MIDDLE - Conhecido como ataque de 'penetra', porque ficar entre o cliente e o servidor observando os dados sigilosos que estão trafegando. O 'penetra' assume o controle da conexão após a autenticação entre usuário e AP. Existem duas formas de assumir o controle da conexão: a primeira é durante os passos iniciais da comunicação TCP, a outra acontece quando dois hosts não estão sincronizados, e descartam pacotes uns dos outros, neste momento o 'penetra' injeta pacotes falsos, mas que possuem os números de sequência correta e desta forma pode ver e reproduzir os pacotes originais que estão sendo enviados. Este ataque permite ao 'penetra' ver e alterar os dados sigilosos tais como senhas e demais dados sigilosos.

5.7 - ATAQUE DE INUNDAÇÃO UDP – A inundação é um ataque que sequer precisa de conexão, pois inicia-se quando o invasor envia pacotes UDP para sua vítima. Ao receber um pacote nosso sistema busca um destino e mesmo quando não o encontra por protocolo envia uma resposta ICMP com a mensagem destino não encontrado ao remetente. Quando é enviado uma grande quantidade de pacotes UDP as portas são abertas e concedem acesso ao invasor.

5.8 - IP SPOOFING – O IP Spoofing usa uma técnica muito simples de falsificação de IP (Internet Protocolo ou Protocolo de Endereço do internauta na

Web). Assim o invasor assume a identidade de qualquer máquina na rede. Este ataque pode criar centenas de usuários não existentes dentro de um sistema, isto causa aumento do consumo da largura de banda, uso inútil do processador com processos desnecessários e sobrecarga os equipamentos em uso na rede.

O invasor usa o spoofing quando quer sequestrar alguma conexão entre o computador do cliente e o servidor. No caso do usuário doméstico, ele falsifica o IP da vítima e pode realizar um ataque via Web.

6 - MECANISMOS DE SEGURANÇA

Vamos com calma não é necessário se desesperar nem abandonar o uso de rede wireless. Basta a adoção de técnicas de segurança que estão ao alcance de qualquer usuário que esteja disposto a dedicar algum tempo na busca de entender alguns conceitos próprios da rede.

Implementar uma configuração adequada, pode possibilitar um ambiente mais seguro e estável.

6.1 – SENHAS E LOGIN – Por padrão a maioria dos dispositivos vem pré-configurados de fábrica usuário admin e senha admin, precisamos é claro trocar esses padrões e ao definir uma senha não colocar nenhuma palavra de fácil dedução, ou algo que esteja obviamente ligado à nossa pessoa. Anova senha deve respeitar um tamanho mínimo e conter letras, números e caracteres especiais para dificultar um ataque de força bruta ou torna-lo inviável. (Silva 2010)

6.2 – CRIPTOGRAFIA – A palavra criptografia define a ciência de escrever em código, de forma que seja incompreensível a todos que não possuem a chave para decodificar a mensagem. Há basicamente três níveis de segurança em um roteador doméstico. Estes níveis estão de acordo com os tipos de criptografia: WEP (Wired Encriptation Protocol), WPA (Wi-Fi Protected Access) e WPA2.

O WEP Este protocolo foi lançado como um padrão de segurança em 1997 e tornou-se o pioneiro no assunto de proteção de redes sem fio. Ele utiliza o algoritmo RC4 para criptografar os pacotes que serão trocados numa rede sem fios e usa também uma função que detecta erros e verifica se a mensagem recebida foi corrompida ou alterada no meio do caminho. Este protocolo já está obsoleto e é facilmente quebrado até mesmo por um invasor inexperiente, se seu roteador usa esta configuração você deve troca-la imediatamente.

O WPA pode ser considerado um protocolo WEP melhorado, já que ele surgiu a partir de um esforço conjunto de membros da Aliança Wi-Fi e do IEEE (Institute of Eletrical and Eletronic Engineers) para combater algumas das vulnerabilidades do WEP e aumentar o nível de segurança das redes sem fio.

Mas já foi substituído pelo WPA2 que trouxe os últimos padrões de segurança, especialmente no que diz respeito à criptografia dos dados com um poderoso algoritmo de criptografia. (Silva, 2010)

6.2 – MODIFICAR O SSID – O SSID nada mais é do que o nome que você dá à sua rede wireless, uma medida básica de segurança seria ocultar o SIDD da sua conexão assim apenas os usuários a quem você informar saberão o SSID e poderão estabelecer a conexão. (Silva 2010)

6.3 – ATIVAR O FILTRO MAC – O MAC identifica cada AP e é único para cada hardware e está gravado no firmware do dispositivo, dessa maneira é impossível mudá-lo. No entanto, é possível falsificá-lo temporariamente. Ao habilitar o filtro de endereço MAC criamos uma lista com os MACs autorizados a se conectar em nossa rede, assim apenas os equipamentos incluídos na lista poderão se conectar. Porém, na utilização da criptografia WEP este mecanismo se torna vulnerável porque os endereços MAC dos equipamentos conectados são transmitidos sem criptografia, dessa maneira um invasor que tenha um pode falsificar o seu MAC acessar a rede. (Silva 2010)

6.4 – LIMITAR O ACESSO SIMULTÂNEO – Se o AP permitir limitar o número de conexões é uma boa prática de segurança pois ao atingir o limite um invasor não conseguirá estabelecer uma conexão, essa configuração é feita nas configurações de DHCP(Dynamic Host Configuration Protocol) basta limitar o range de endereços distribuídos. (Silva 2010)

6.5 – DESATIVAR SERVIDOR DHCP – O DHCP é um protocolo que configura de forma dinâmica um endereço IP a cada host na nossa rede, esse endereço é renovado em determinado espaço de tempo, ao desativar esse servidor, cada host que desejar se conectar deve informar manualmente um IP que pertença a nossa rede. (Silva 2010)

6.6 – FIREWALL – Outra medida que pode ser adotada e a configuração e ativação do firewall, esta talvez seja a medida que mais exigirá conhecimento

para ser implementada, o firewall pode ser baseado em hardware ou software e a partir de regras e instruções analisa o trafego e bloqueia ou libera o acesso de acordo com as regras. O firewall é um filtro de pacotes que controla tudo que entra e sai. Também é possível filtrar o trafego a partir das portas que serão utilizadas.

CONCLUSÃO

A rede Wireless sem dúvida nos traz inúmeros benefícios, porém também encontraremos desvantagens o quesito segurança é uma delas. Uma análise das vulnerabilidades em nossa rede se faz necessária e baseado em tais características devemos adotar as medidas que melhor nos atendam.

Os métodos de invasão apresentados neste artigo são utilizados por indivíduos maliciosos que procuram explorar as fragilidades da rede. Uma política de senhas mais seguras e de difíceis dedução que, juntamente com padrões de criptografia, formam um conjunto eficaz contra ações de um possível invasor.

Mas como criar senhas de uma maneira que garanta sua força? Quais garantias teremos para que ela não seja facilmente quebrada? Temos que ter em mente que não há uma regra fixa que sirva para todos os casos e infelizmente não existem garantias, uma das principais falhas de segurança é o fator humano, portanto não se trata de uma questão meramente tecnológica, mas também de procedimento, estamos sempre sujeitos a moral de outras pessoas a única solução é estar sempre alerta e nunca baixar a guarda.

.

REFERÊNCIAS:

BARCELAR, RICARDO RODRIGUES. **Padrão IEEE 802.16**. **Uma Visão Geral sobre o WIMAX**. Artigo Pós-Graduação CEFETMT. Cuiabá 2006. Disponível em < http://www.profiscientia.ifmt.edu.br/profiscientia/index.php/profiscientia/article/view/14/13>. Acesso em 28 de outubro de 2016.

BARROZO, LEANDRO LAVAGNINI. **SEGURANÇA NAS REDES SEM FIO: WIRELESS E WIMAX.** Marília 2009. Disponível em< http://aberto.univem.edu.br/bitstream/handle/11077/285/Segurança%20nas%20redes%20sem%20fio%3a%20Wireless%20e%20Wimax.pdf?sequence=1>. Acesso em 29 de outubro de 2016.

GIMENES, EDER CORAL. **Segurança de Redes Wireless.** Monografia de Curso Tecnólogo em Informática com ênfase em Gestão de Negócios. Mauá 2005. Disponível em <http://www.tvprudente.com.br/apostilas/Rede/Redes.pdf>. Acesso em 26 de outubro de 2016.

SILVA, LEANDRO RODRIGUES. **Segurança Em Redes Sem Fio (WIRELESS).** Monografia de Pós Graduação em Redes e Segurança de Sistemas. Curitiba 2010. Disponível em <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Leandro%20Rodrigues%20Silva%20-%20Artigo.pdf> Acesso em 26 de outubro de 2016.

* https://www.oficinadanet.com.br/post/8619-qual-a-diferenca-entre-redes-wifi-a-b-g-n. Acesso em 28 de outubro de 2016.

* http://www.androidauthority.com/wifi-standards-explained-802-11b-g-n-ac-ad-ah-af-666245/. Acesso em 28 de outubro de 2016.

* http://www.contractti.com.br/portal/dicas/wireless-dicas/66-tipos-de-ataque-wireless.html. Acesso em 29 de outubro de 2016.