ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB

OS RISCOS DE SEGURANÇA DAS INFORMAÇÕES COMPARTILHADAS NO USO DE TECNOLOGIAS WIRELESS EM AMBIENTES DOMÉSTICOS

Paulo da Silva Filho[1]
Hudson Ramos[2]

RESUMO

Esse artigo tem o intuito de analisar os riscos de segurança oriundos do uso indevido das informações compartilhadas através das tecnologias *wireless* nos ambientes domésticos, proporcionados pela crescente expansão dos equipamentos móveis, tais como: *tablets*, *smartphones*, notebooks e computadores pessoais que fazem uso desse padrão de comunicação. Com a utilização desses dispositivos móveis totalmente compatíveis com essa tecnologia, principalmente com os padrões IEEE 802.11 b/g/n, nota-se a inevitabilidade de criar mecanismos de defesa em suas redes sem fios (WLAN). Por isso, é fundamental explorar e analisar soluções para minimizar as exponenciais ameaças de invasão a WLAN, seus arquivos e recursos de multimídia. Utilizando como um estudo de caso uma rede doméstica planejada, adotando ferramentas de projeto, s*ite Survey*, implantação e monitoração, pormenorizando o status de cada etapa com o intuito de promover a compreensão e a usabilidade dos recursos da tecnologia sem fio com diversos tipos de dispositivos nos ambientes domésticos, fomentará ao usuário que usufrui dessa tecnologia a possibilidade de ter um senso perscrutador sobre os conceitos e o compartilhamento de informações nesse ambiente tão prático e comum no cotidiano.

Palavras-chave: Wireless. WLAN. Projeto. Riscos. Segurança.

[1] Pós-Graduando *Latu Sensu* em Rede de Computadores na Escola Superior Aberta do Brasil – ESAB. profpaulofilho@gmail.com

[2] Mestrado em Informática

1 Introdução

A rede sem fio tornou-se rapidamente a forma de comunicação mais utilizada em ambientes domésticos e segundo Engst e Flsieshman (2005, p. 13) "A liberdade oferecida pelas redes sem fio não para quando você sai de casa", as redes cabeadas LANS e os antigos computadores com placas de rede *ethernet/fastethernet*[3], com cabos espalhados em todo o ambiente deixam suscetíveis a tropeços, acidentes de trabalho, além de aumentar a poluição visual.

Basta olhar atrás de um desktop que encontrará um emaranhado de fios (ENGST; FLSIESHMAN, 2005), de maneira que todos aqueles cabos conectados aos outros computadores tornam-se obsoletos em comparação aos dispositivos móveis que dominam o gosto dos usuários, devido a mobilidade propiciada pela liberdade de não necessitar de fios para estabelecer conexões.

Segundo Brentano (2012, np):

> Um estudo revelou que 71% dos usuários de banda larga no Brasil acham que a rede Wi-Fi oferece uma melhor velocidade de internet em comparação com o acesso via rede móvel celular (2G/3G). A pesquisa conduzida pela fabricante de equipamentos de telecomunicações Cisco e apresentada nesta quarta-feira (10) na Futurecom, no Rio de Janeiro, mostrou que o Wi-Fi é a rede preferida dos brasileiros para acessar a internet por dispositivos móveis: 78% dos usuários de notebooks, 75% de tablets e 57% de smartphones preferem a conexão via Wi-Fi. A pesquisa envolveu 650 entrevistas com consumidores de banda larga no Brasil, em maio deste ano. O estudo também foi realizado no Canadá, Estados Unidos, México e Reino Unido. Conforme o levantamento, embora o usuário se conecte mais à web em casa, ele gostaria de ter acesso Wi-Fi em todos os locais que frequenta. O estudo revelou que 52% dos entrevistados gostariam de ter acesso Wi-Fi em qualquer lugar, e 33% têm interesse em acessar a rede em ruas e rodovias.

Geralmente os ambientes de redes locais podem ser: WLAN – *Wireless Local Area Network* – Rede de Area Local sem Fio, e LAN – *Local Area Network* (Rede de Area Local). Os meios de conexão e acesso a informações destas redes são distintos, ou seja, LAN utiliza *switches* para concentrar, distribuir e regenerar os sinais para o computador até seu NIC – *Network interface card*, popularmente conhecida como placa de rede, concebendo uma dificuldade física, pois necessita de cabos para o acesso a esse tipo de conexão.

---

[3] *Ethernet* – Tecnologia de enlace físico com transmissão de dados até 10Mbps e segundo Kurose e Ross (2013. p. 348) A ethernet é uma LAN de transmissão por difusão – todos os quadros transmitidos movem-se para, e são processados por todos os adaptadores conectados ao barramento.

Fastethernet – É a atualização tecnológica do ethernet com transmissão até 100Mbps.

Enquanto a WLAN utiliza *Access Point* (AP) ou *Wireless Router* (roteador sem fio) para emitir ondas de rádio que se propagam pelo ambiente com a finalidade de conectar outros equipamentos que utilizam esta tecnologia.

Segundo Kurose e Ross (2013, p. 14):

> Os meios físicos se enquadram em duas categorias: meios guiados e meios não guiados. Nos meios guiados, as ondas são dirigidas ao longo de um meio sólido, tal como um cabo de fibra ótica, um par de fios de cobre ou um cabo coaxial. Nos meios não guiados, as ondas se propagam na atmosfera e no espaço, como é o caso de uma LAN sem fio ou um canal digital de satélite.

E também segundo Tanenbaum e Wetherall (2011, p. 214):

> Os switchs são bridges modernas com outro nome (na verdade, um conjunto de bridges forma um switch). As diferenças são mais por questão de marketing do que técnicas, mas existem alguns pontos que precisam ser conhecidos. As bridges foram desenvolvidas quando a Ethernet clássica estava em uso, de modo que tendem a unir relativamente poucas LANs e, portanto, ter relativamente poucas portas. O termo switch é mais popular hoje em dia. Além disso, todas as instalações modernas usam enlaces ponto a ponto, como cabos de par trançado, de modo que computadores individuais se conectam diretamente a um switch e, portanto, este costuma ter muitas portas.

Segundo Moraes (2010, p. 183) Access Point ou ponto de acesso é uma estação de rede wireless responsável por gerenciaras conexões entre usuários e a rede cabeada.

Por sua vez os equipamentos possuem *Wireless card*, no qual o usuário desse ambiente associa seu equipamento através do SSID - *Service Set Identifier,* cujo propósito é conectar o equipamento por meio de autenticação de credencial, podendo ser aberta (sem autenticação segura) ou com uma senha utilizando ou não requisitos de complexidade de métodos para autenticação, como por exemplo: WEP - *Wired Equivalent Privacy* e o WPA – *Wi-Fi Protected Access*.

O vasto uso de equipamentos móveis pela população devido ao baixo custo e também sendo compatível com os padrões *wireless*, tornaram-se definitivamente os preferidos para acesso a Internet. Hoje, a maioria dos usuários de ambientes sem fio utilizam dispositivos móveis conectados à WAN até pelo amadurecimento dessa tecnologia, porém ficam vulneráveis a ataques e invasões em suas WLANS.

Segundo Moraes (2010, p. 191):

> Como nem tudo é perfeito, o ponto segurança ainda deixa muito a desejar em redes antigas (pré – IEEE 802.11i). Elas são uma ameaça, pois ampliam o perímetro de segurança e, consequentemente, aumentam a vulnerabilidade, pois se elas não estiverem bem protegidas, um hacker pode invadi-las, usando algumas técnicas relativamente simples.

Os usuários preferem utilizar tecnologia a sem fio por conta da praticidade e taxa de dados utilizados neste tipo de conexão, pois em sua maioria são mais velozes do que as tecnologias proporcionadas pelas empresas de telefonia aos seus clientes, como o 3G[4] e 4G[5].

A utilização de redes sociais e de mensagens instantâneas, como Facebook®, Instagram® e WhatsAp® faz com que os usuários permaneçam conectados em seus equipamentos o tempo todo através destes aplicativos. Os dispositivos sem fio mais comuns utilizados hoje por usuários de ambientes domésticos são *smartphones*, *notebooks* e *tablets*.

Segundo Kurose e Ross (2013, p. 48):

> A onipresença cada vez maior das redes Wi-Fi públicas de alta velocidade (54 Mbits/s) e o acesso à Internet com velocidade média (até alguns Mbits/s) por redes de telefonia celular 3G e 4G não apenas está possibilitando permanecer constantemente conectado enquanto se desloca, mas também permite novas aplicações específicas à localização. O número de dispositivos sem fio conectados ultrapassou o número de dispositivos com fio em 2011. Esse acesso sem fio em alta velocidade preparou a cena para o rápido surgimento de computadores portáteis (iPhones, Androids, iPads etc.), que possuem acesso constante e livre a Internet.
> Redes sociais on-line, como Facebook e Twitter, criaram redes de pessoas maciças em cima da Internet. Muitos usuários hoje" vivem" principalmente dentro do Facebook. Através de suas APIs, as redes sociais on-line criaram plataformas para novas aplicações em rede e jogos distribuídos

Apesar da maioria dos usuários de redes sem fio não conhecerem a tecnologia a ponto de criarem um ambiente compartilhado que lhes proporcione certo conforto quanto à segurança, usufruem mesmo assim sem critérios os recursos que conhecem, compartilhando pastas, arquivos, impressoras e conexão com a Internet com outros usuários em seu próprio domicílio e residências adjacentes, sem a preocupação de monitorar a segurança desses recursos.

Um caso recente amplamente divulgado de intrusão a rede sem fio foi observado com a ferramenta Google Stret View® da empresa Google®. enquanto mapeava as ruas, não só do Brasil, mas também de outros países, obteve-se acessos indevidos de APs e Hotspots que estavam com a autenticação aberta ou sem segurança a esses equipamentos (ALMEIDA, 2013, np).

Diante deste cenário, é possível criar mecanismos para aumentar a segurança nos compartilhamentos de informações via Wireless coletando informações em um ambiente

---

[4] 3G é a terceira geração da tecnologia que permite acessar a Internet com o celular, segundo Kurose e Ross (2013, p. 13) "empregam a mesma estrutura sem fios usada para telefonia celular para enviar/receber pacotes por estação-base que é controlada pela operadora da rede celular".

[5] 4G é uma evolução da tecnologia de conexão pelos celulares, até 100 vezes mais rápida que a 3G. Além de mais qualidade nas chamadas de voz, vídeo chamadas e navegação, comporta mais conexões em uma mesma antena (CAMILO, 2012, np)

doméstico com amostragem de usuário padrão, com o objetivo de analisar e planejar uma rede mais segura. Por fim, a implantação e monitoração desta nova amostragem apresentará ~~os~~ resultados de redução de ataques e intrusão no ambiente doméstico compartilhado por Wireless.

2 Conhecendo as Características do Ambiente sem Fio

O propósito das redes sem fio é a eliminação de cabos visando a mobilidade e a conectividade em qualquer ambiente (ENGST; FLSIESHMAN, 2005). O termo *Wireless* abordado por Engst e Flsieshman (2005) significa sem fio, ou seja, são redes que substituem cabos por ondas de rádio. Segundo Moraes (2010, p.174) "As redes sem fio são hoje largamente utilizadas devido principalmente à facilidade de uso e de instalação".

Utiliza-se a rede *wireless* como extensão de uma rede cabeada, logo, em algum ponto, haverá um cabo de rede para realizar as conexões entre as redes sem fio e cabeada. De acordo com Tanenbaum e Watherall (2011), a largura de banda de rede e as capacidades de dispositivos aumentaram tremendamente com a implantação dos serviços 3G, telefones móveis com telas maiores, melhoria dos processadores e a capacidade das redes sem fios 802.11.

Conforme Edwards (2011 apud EDWARDS; KUROSE; ROSS, 2013, p. 13):

> Embora as redes de acesso por ethernet e Wi-Fi fossem implantadas no início em ambientes corporativos (empresas, universidades), elas há pouco se tornaram componentes bastante comuns das redes residenciais. Muitas casas unem o acesso residencial banda larga (ou seja, modens a cabo ou DSL) com a tecnologia LAN sem fio a um custo acessível para criar redes residenciais potentes.

A rede sem fio não é uma tecnologia nova, apesar da sua utilização parecer recente e os usuários acharem que essa inovação tecnológica seja muito contemporânea, seu conceito já foi utilizado a mais de um século, segundo Tanenbaum (2003, p. 23):

> A comunicação digital sem fio não é uma ideia nova. Em 1901, o físico Guglielmo Marconi demonstrou como funcionava um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código morse (afinal de contas, os pontos e traços são binários). Os modernos sistemas digitais sem fio têm desempenho melhor, mas a ideia é a mesma.

No final da década de 80, a rede sem fio já era uma realidade, só que onerosa, com falhas de segurança e pouco utilizada, mas com uma proposta que agradava pela praticidade e mobilidade. Existiam diversos equipamentos de diversos fabricantes, o grande problema era

encontrar compatibilidade entre equipamentos que fossem de fabricantes diferentes, dificultando assim, a utilização das redes sem fio.

Corroborando com essa informação, Tanenbaum e Wetherall (2011, p. 43):

> Esse trabalho levou rapidamente à comercialização de LANS sem fio por várias empresas. O problema era encontrar duas delas que fossem compatíveis. Essa proliferação de padrões significava que um computador equipado com um rádio da marca X não funcionaria em uma sala equipada com uma estação-base da marca Y. Em meados da década de 1990, a indústria decidiu que um padrão de LAN sem fios poderia ser uma boa ideia, e assim o comitê do IEEE que padronizou as LANS com fios recebeu a tarefa de elaborar um padrão de LANS sem fios.

Segundo Engst e Flsieshman (2005, p. 9):

> O IEEE *Institute of Eletrical and Eletronics Engeneers* é associação profissional técnica sem fins lucrativos com 380 mil membros. A missão do IEEE é desenvolver padrões técnicos com base no consenso para a eletrônica em várias indústrias. Muito dos fabricantes de equipamentos 802.11b participam do subcomitê do IEEE. O comitê do IEEE 802 lida com redes: o grupo de trabalho do 802.11 trata de redes locais sem fio (*wireless local area networks* - WLANS) e os vários grupos de tarefa (a, b, c, f, g, h, i entre outros) tratam tipos de WLANS específicos ou problemas específicos relacionados a redes sem fio, como *streaming* de dados multimídia, comunicação por ponto de Inter acesso e segurança.

Esse padrão ~~o~~ recebeu o nome de 802.11 que também é conhecido como WIFI[6] *Wireless Fidelity*. Ele opera com banda não licenciada ISM (Industrial, Scientific, and Medical) a exemplo de 900MHz, 2,4GHz e 5,75GHz, diferente das redes de telefonia móvel com bandas licenciadas onerosas (TANENBAUM; WETHERALL, 2011). Dessa forma, o IEEE regulamentou os padrões de conectividade sem fio com o IEEE 802.11.

Entretanto, necessitava-se de uma interoperabilidade entre os equipamentos no qual não existia até o final dos anos 90. Surgiu a WECA Wireless *Ethernet Compatibility Alliance* que tem a função de garantir a interação entre equipamentos com tecnologia sem fio de diversos fabricantes. Assim foram implantados os padrões IEEE 802.11b e 802.11a com taxas de transferência entre 11Mbps e 54Mbps respectivamente. Conforme quadro 1 de quadro comparativo dos padrões 802.11:

IEEE 802.11	Padrão primordial, com taxas de transferência de 2 Mbps, não mais utilizados pela criação dos novos padrões
IEEE 802.11b	Ainda utilizada atualmente em menor proporção pela sua obsolescência, taxas de transmissão de 11Mbps, opera na frequência de 2,4Ghz.
IEEE 802.11a	Padrão pouco utilizado, incompatibilidade com o padrão 802.11b, taxa de transferência em 54Mbps, opera na frequência de 5Ghz.
IEEE 802.11g	Padrão ainda utilizado atualmente, taxa de transferência entre 54Mbps e 108Mbps, opera na frequência de 2,4Ghz.

[6] Wi-Fi é uma abreviatura de wireless fidelity, termo que transmite a noção de dados com alta qualidade, uma marca comercial da WECA, também conhecida como Wi-Fi Alliance que tem a responsabilidade de garantir a interoperabilidade entre os dispositivos de diversos fabricantes. (ENGST; FLSIESHMAN 2005)

IEEE 802.11n	Padrão utilizado em maior proporção atualmente, taxa de transferência entre 300Mbps. E 600Mbps, opera nas frequências de 2,4Ghz. e 5Ghz.

Quadro 1 - Comparativo de Padrões 802.11
Fonte:Engst; Flsieshman (2005)

Com os padrões estabelecidos e sendo amplamente utilizados, tornou-se comum encontrar redes sem fio em ambientes de escritórios e domésticos com conexões compartilhadas. As redes ad hoc e de infraestrutura para conexão de clientes sem fio móveis, como por exemplo, notebooks e telefones móveis tornaram-se totalmente triviais e de fácil instalação, segundo Tanenbaum e Wetherall (2011, p.43):

> As redes 802.11 são compostas de clientes, como notebooks e telefones móveis, e infraestrutura chamada pontos de acesso, ou APS (Access Points), que são instalados nos prédios. Os pontos de acesso também são chamados de estações-base. Os pontos de acesso se conectam à rede com fios, e toda a comunicação entre os clientes passa por um ponto de acesso. Também é possível que os clientes no alcance do rádio falem diretamente, como dois computadores em um escritório sem um ponto de acesso. Esse arranjo é chamado de rede ocasional (ou rede ad hoc). Ele é usado com muito menos frequência do que o modo ponto de acesso.

Os padrões IEEE 802.b/g/n possuem algumas particularidades nos métodos de conexão, esses padrões utilizam o mesmo protocolo de acesso ao meio, a mesma estrutura de quadros para os seus quadros de camada de enlace, possuem a mesma capacidade de reduzir a sua taxa de transmissão para alcançar distâncias maiores e permitem modo de infraestrutura e modo ad hoc (KUROSE; ROSS, 2013).

A tecnologia de rede sem fio mais utilizada no momento é a do padrão IEEE 802.11n, desenvolvida a partir de 2004 e publicada no final de 2009. Encontra-se esse padrão na maioria dos novos equipamentos que os usuários de dispositivos móveis utilizam.

De acordo com o estudo realizado pela Cisco segundo Barros (2012, np):

> A maioria dos usuários conecta seus dispositivos via WIFI de algum ponto em algum momento, incluindo 80% daqueles que se conectam à internet por smartphones e que 78% dos usuários de laptops, 75% de tablets e 57% de smartphones preferem a conexão via Wi-Fi

O ambiente sem fio doméstico geralmente é composto por um AP ou um Wireless Router - roteador sem fio e seus dispositivos conectados, como, *tablets, smartphones e notebooks*. Essa conexão criadas pelos usuários, geralmente compartilham acesso à Internet, pastas de arquivos, unidades de disco e impressoras.

Um compartilhamento padrão é comumente usado por usuário doméstico por conta da praticidade, é também usual os utilizadores dessa rede disponibilizarem esse acesso para pessoas que usufruem desse ambiente, ou até não possui uma segurança, potencializando os

riscos de invasão ou o que chamamos de sequestro[7] no ambiente sem fio, a próxima etapa é analisar seu impacto nesse ambiente.

3 Os Riscos das Redes sem Fio

Os riscos para os ambientes sem fio são diversos, deve-se analisar o que compartilha e principalmente seguir os requisitos básicos de segurança. A rede sem fio é utilizada sem muita proteção, seus utilizadores não preocupam-se em proteger o que estão transmitindo.

Segundo Kurose e Ross (2013, p. 43):

> Muitos usuários hoje acessam a Internet por meio de aparelhos sem fio, como laptops conectados à tecnologia Wi-Fi ou aparelhos portáteis com conexões à Internet via telefone celular. Embora o acesso onipresente à Internet seja de extrema conveniência a disponibilize novas aplicações sensacionais aos usuários móveis, ele também cria uma grande vulnerabilidade de segurança – posicionando um receptor passivo nas proximidades do transmissor sem fio, o receptor pode obter uma cópia de cada pacote transmitido!
> Esses pacotes podem conter todo o tipo de informações confidenciais, incluindo senhas, número de identificação, segredos comerciais e mensagens pessoais.

O ambiente sem fio já tem o grande problema de propagar os dados pelo ambiente utilizando os campos eletromagnéticos, sua exposição é notória. E com muitos usuários sem conhecimento ou usando indiscriminadamente seus recursos de rede, esses problemas como falhas de segurança, sequestro ou até de negação de acesso tendem a aumentar.

Essas redes wireless devem seguir requisitos de segurança, tais como Campos (2014) relata que um sistema de segurança da informação baseia-se em três princípios básicos: Confidencialidade, Integridade e Disponibilidade. Infelizmente em muitos casos as redes domesticas estão abertas e prontas para serem atacadas, não observando os pontos de segurança.

As redes desprotegidas e disponíveis no ambiente tornam-se um chamariz para invasores que tem seus métodos de garimpar recursos alheios para obtenção de dados que facilitem seu acesso. Os potenciais invasores utilizam uma serie de técnicas e ferramentas, assim como a segurança baseia-se em princípios, os invasores também o tem, e são utilizados em 4 fases: Reconhecimento, *Scanning*, Enumeração e Ataque.

Munido com essas informações, a potencial ameaça está pronta para invadir redes com as ferramentas corretas para essa intrusão (Moraes, 2010).

---

[7] Sequestro de rede Wi-Fi segundo a cert.br entende-se uma situação em que um terceiro ganha acesso à rede e altera configurações no AP para que somente ele consiga acessá-la.

Dessa forma, é preciso se proteger evitando ao máximo o risco de intrusão em redes. Deve-se verificar a confiabilidade da rede, com os arquivos compartilhados íntegros e disponíveis sempre que requisitado acesso, ou seja, não devem existir falhas de segurança e somente os usuários autorizados devem ter acesso aos arquivos e recursos compartilhados.

Para analisar melhor os requisitos de segurança, uma pesquisa de campo foi realizada com o objetivo de gerar uma amostragem estatística e analisar as formas de configuração de segurança mais adotadas nas redes domésticas que possibilitem a diminuição dos riscos de invasão do compartilhamento das informações dos usuários.

Segundo Rufino (2007), no processo de pesquisa de campo, é necessário realizar um esquema do ambiente. Esse método possibilita lograr maior êxito de obtenção de informações sobre redes distintas, tendo acesso a detalhes importantes com aspectos mais precisos e com menos riscos de ser descoberto. O sucesso de tal ação depende do nível de proteção configurado na rede alvo.

Por motivos como esse, é essencial o conhecimento do perfil desses usuários, então no período de 14 de outubro à 7 de Novembro de 2014, foi realizada uma pesquisa no bairro popular de Plataforma localizado em Salvador, Bahia, Brasil, onde encontra-se como em qualquer lugar povoado diversas residências com redes sem fio.

Para a pesquisa de campo foi proposta uma entrevista utilizando amostragem de 5 (cinco) residências que adotam o ambiente sem fio compartilhado, composta por um questionário que segue no apêndice desse artigo, contendo nove perguntas, conforme quadro 2:

Quantos dispositivos wireless são utilizados em sua rede doméstica?
Qual o padrão Wireless utilizado? 802.11 b, a, g ou n?
Disponibiliza algum recurso para usuários externos?
O que compartilha para os usuários externos?
Variam a senha de acesso periodicamente (trocam de senha) e se usavam complexidade (adotam senhas com letras número e caracteres especiais, como por exemplo: P&$qu1s@)?
Já sofreu algum tipo de ataque em sua rede?
Possui conhecimento técnico para realizar configurações nos equipamentos?
Utilizam endereçamento IP estático ou dinâmico?
Preocupam-se com a segurança em sua rede sem fio?

Quadro 2 - Questões da pesquisa
Fonte: Elaboração própria (2014)

Cada residência foi analisada tendo acesso às essas redes, e o questionário respondido por seus usuários, os resultados foram satisfatórios para essa linha de pesquisa e significantemente preocupantes. A amostragem revelou que 100% dos entrevistados compartilham conexão com 03 ou mais dispositivos moveis em suas residências conforme

gráfico da figura 1. Foi possível verificar também que 60% utilizam o padrão 802.11n e 40% utilizam o padrão 802.11g.

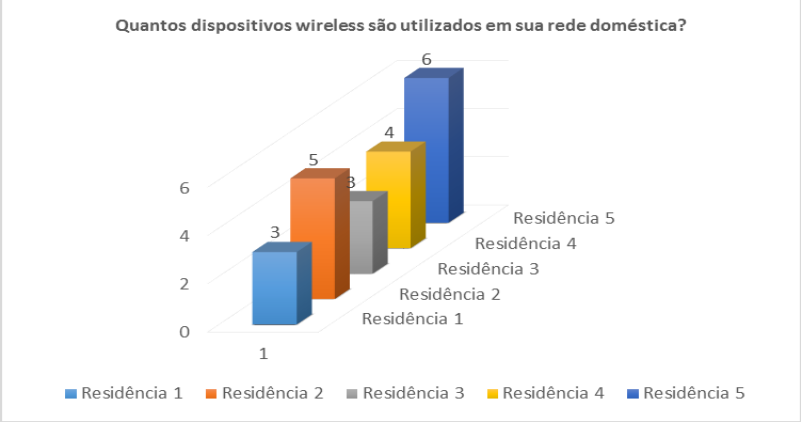

Figura 1: Quantidade de dispositivos móveis por residência.
Fonte: Elaboração própria (2014)

Também verificou-se que 60% disponibilizam recursos para usuários externos, 60% compartilham recursos e disponibilizam conexão com a internet para usuários externos e 10% disponibilizam acesso à pasta compartilhada de arquivos multimídia.

Do total também foi constatado que apenas 40% das residências seguem requisitos mínimos de segurança como troca periódica de senha, 40% não possui sequer requisitos mínimos de segurança e apenas 20% seguem requisitos básicos de segurança.

Quando perguntados se já sofreram algum tipo de ataque em sua rede, 80% disseram que não sabiam e 20% disseram que sim, foram atacados, com invasão de sua rede para obtenção de provavelmente acesso gratuito à Internet.

O conhecimento técnico necessário para criar-se o mínimo de segurança também é preocupante. Apenas 30% informaram possuir tais habilidades, os 70% restantes informaram que utilizavam os padrões de configuração de fábrica ou utilizavam os serviços de terceiros para elaboração de tais configurações.

Quanto ao endereçamento IP de equipamentos e dispositivos, 100% dos entrevistados utilizam o endereçamento IP dinâmico, através dos serviços de DHCP[8] disponibilizados pelos equipamentos e surpreendentemente utilizando o range alocado de endereço que já vem configurado por padrão nos equipamentos.

[8] DHCP Segundo Kurose e Ross (2013. p, 255) O DHCP (Protocolo de configuração Dinâmica de Hospedeiro) permite que um hospedeiro obtenha (seja alocado a) um endereço IP de maneira automática. Um administrador de rede pode configurar o DHCP para que determinado hospedeiro receba o mesmo endereço IP toda vez que se conectar, ou hospedeiro pode receber um endereço IP temporário diferente sempre que se conectar.

A última pergunta foi se existia alguma preocupação com a segurança de sua rede e 30% disseram que sim, enquanto os 70% disseram que nunca haviam se preocupado com conceitos de segurança. Um dos entrevistados respondeu da seguinte forma: “na verdade eu uso a rede sem fio para compartilhar o que preciso, o que importa é ela funcionar, mas depois dessas perguntas estou muito preocupado”.

Com esses dados pode-se observar que ainda são muito poucos os usuários que utilizam redes sem fio de forma segura e correta. Os princípios básicos de confidencialidade, disponibilidade e integridade são praticamente esquecidos, por aspectos de falta de habilidade técnica dos usuários ou até pior, por falta de relevância para com esses requisitos importantíssimos.

Observa-se também que as senhas sem complexidade utilizadas para autenticação é a causa mais comum de vulnerabilidade para acessar as redes sem fio. A autenticação é o método usado para confirmação da veracidade da identidade do dispositivo wireless pelo AP ou *Wireless Router*. Esse processo ocorre todas às vezes que um dispositivo tentar conectar nessa rede. Para autenticar o cliente é necessária essa verificação, conexão alguma será efetuada sem essa verificação primeiro (JARDIM, 2007). Um outro problema encontrado nas redes sem fio da pesquisa é a utilização de criptografia WEP, que é obsoleta e muito vulnerável a ataques.

Segundo Moraes (2010, p. 204):

> Alguns estudos realizados pela Universidade de Berkeley na Califórnia e pela Universidade de Maryland provaram a existência de grandes problemas de segurança com o WEP, demonstrando que ele não é adequando para prover privacidade em redes sem fio em camada de enlace.
> O WEP possui algumas vulnerabilidades. A primeira delas é que ele trabalha com vetor de inicialização muito pequeno, o que o torna ainda mais vulnerável a ataques que buscam descobrir a chave criptográfica.

Também foi encontrado nas redes sem fio da pesquisa endereçamento disponibilizado de forma dinâmica sem controle na quantidade de dispositivos conectados, SSID visíveis por todos, sem métodos e sem técnicas de segurança na maioria das redes. São apenas alguns dos aspectos, os quais contribuem para que um ambiente compartilhado sem fio esteja vulnerável a ataques e intrusões, culminando, assim, nas investidas de invasão por terceiros.

O próximo passo desse artigo é um projeto de uma rede sem fio planejado e monitorado, ratificando que pode-se manter uma estrutura mais segura, minimizando assim, os resultados negativos obtidos na pesquisa. Dentro do cenário da pesquisa, foi escolhida como objeto de estudo a rede sem fio da Residência 5, que foi concedida pelo proprietário, por ter apresentado na estatística geral a maior colocação de possíveis riscos em seu ambiente.

O entrevistado compartilha sua senha de acesso ao seu ambiente sem fio com pessoas que não residem no mesmo local, aumentando assim, o risco de intrusão ou sequestro de sinal. Um risco maior ainda foi detectado nesta rede, pois um dos utilizadores participa de uma rede social de compartilhamento de senhas de rede sem fio.

4 Projeto, Implantação e Monitoramento com Segurança de uma Rede Compartilhada sem Fio

O projeto e implantação da rede doméstica sem fio desse estudo de caso segue o conceito baseado em análise e gerenciamento de riscos do ambiente de rede escolhido.

Segundo Moraes (2010, p. 32):

> O princípio básico de gerenciamento de risco é: não podemos proteger algo que não conhecemos. Com o conhecimento dos riscos envolvidos é possível planejar as políticas e técnicas a serem implementadas para a sua redução. Por exemplo, se disponibilidade é importante, e existe o risco de o sistema ficar fora do ar devido a uma queda de energia, então o risco pode ser reduzido com a utilização de um sistema ininterrupto de força.

Nesse caso todo o projeto será para a residência escolhida. Este ambiente de rede possui 6 dispositivos sem fio e 2 com fio conectados a WLAN, conforme figura 2.

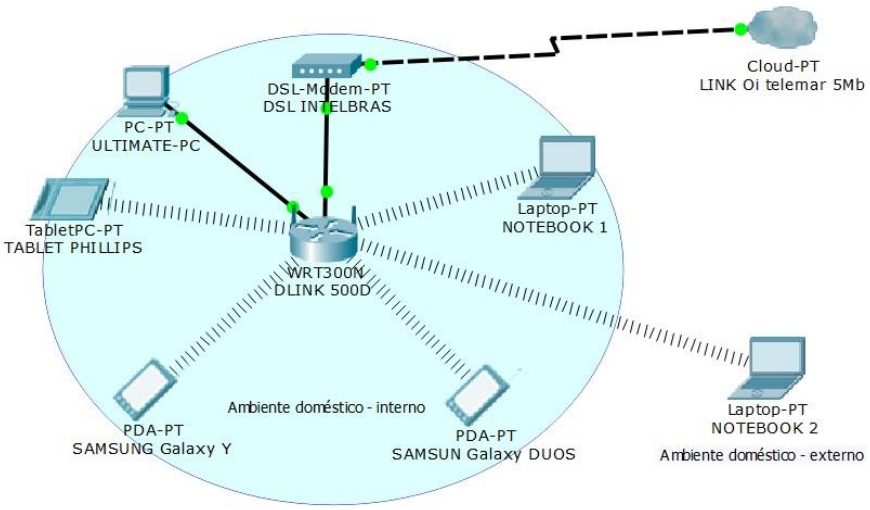

Figura 2: Ambiente WLAN da pesquisa.
Fonte: Elaboração própria

Este ambiente foi mapeado com um programa de Site Survey, o qual possui funcionalidades para obter uma visão ampla da propagação do sinal da rede sem fio, catalogando até o limite da propagação do sinal. Com o objetivo de coletar, analisar e elaborar um relatório do referido estudo de caso, alguns programas foram utilizados para as seguintes finalidades apresentadas na tabela 3:

Programas	Finalidade
Tamograph® Site Survey versão de teste 4.0	Executar do *Site Survey*
Microsoft Visio® 2013	Arquitetar o ambiente interno e externo
Cisco Packet Tracer® versão 6	Simular conectividade antes da implantação
Cisco Network Magic®	Monitorar a rede após a implantação

Quadro 2: Aplicativos utilizados para o projeto.
Fonte: Elaboração própria (2014)

Foi utilizado para esse estudo de caso os dispositivos e equipamentos existentes do proprietário da residência 5, além da adição de mais um dispositivo pessoal para a criação de todo o projeto, abaixo suas características conforme quadro 3:

01	Computador Pessoal com processador Intel core 2 DUO 2.6GHz, 8GB RAM. com NIC fastethernet Realtek 8229.
01	Notebook Itautec W7535 com processador Intel Dual core 1,55GHz, 3GB RAM placa de rede sem fio Atheros 802.11g
01	Notebook HP Pavilion (Usuário adjacente)
01	Smartphone Samsung Galaxy Y 802.11g
01	Smartphone Samsung Galaxy DUOS 802.11n
01	Tablet Phillips 802.11n
01	Notebook HP G42 (pesquisador) com Pentium Dual-core 2,30GHz, 4GB RAM placa de rede sem fio Realtek RTL8191SE 802.11 b/g/n
01	Modem ADSL Dlink 500B
01	Wireless Router Dlink 500D 802.11n

Quadro 3: Especificações de equipamentos e dispositivos para o projeto.
Fonte: Elaboração própria (2014)

Ao iniciar o projeto foi necessário criar uma planta baixa da Residência 5, conforme figura 2, para lograr a localização dos equipamentos do ambiente compartilhado sem fio. Também houve a necessidade de criar o ambiente externo adjacente, porque o usuário compartilha sua conexão com a Internet com um vizinho.

O software para diagramação do ambiente é o *Microsoft® Visio 2013* conforme a figura 2:

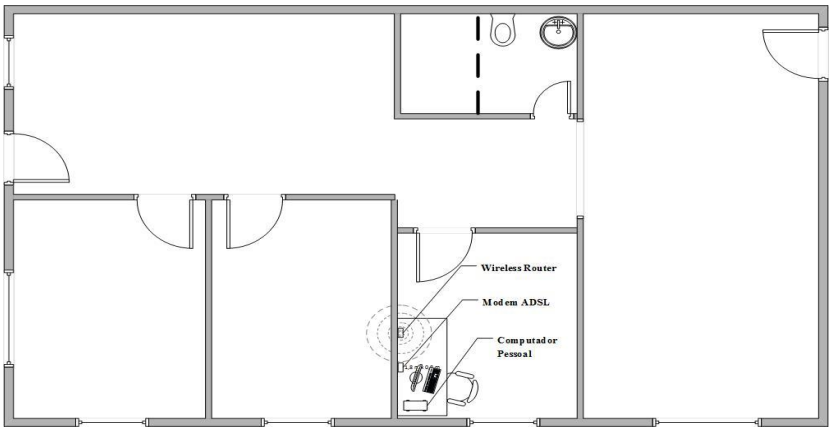

Figura 2: Planta Baixa Residência 5
Fonte: Elaboração própria

O *Tamograph® Site survey* foi utilizado para visualização do alcance do equipamento, através da simulação de propagação do sinal e ruído dentro das áreas com cobertura da rede sem fio analisada, conforme figura 3.

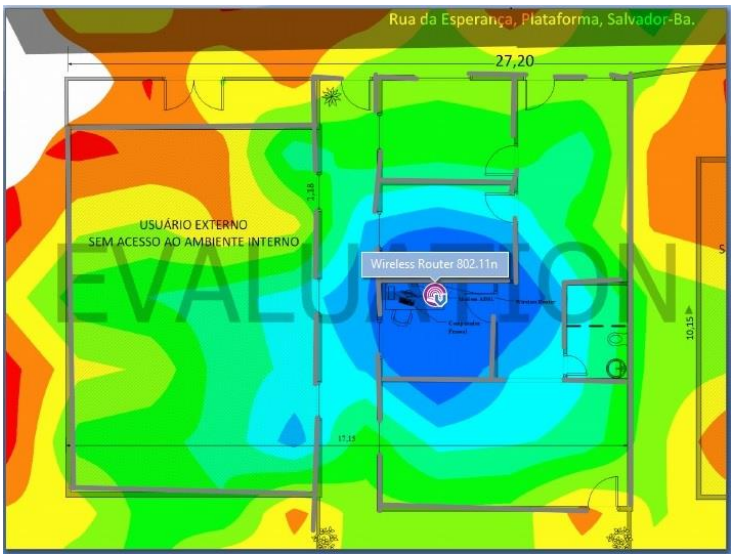

Figura 3: Área coberta pelo sinal sem fio em ralação ao sinal e ruído
Fonte: Elaboração própria

Observa-se na figura 3 que as áreas cobertas em azul e verde mesmo com obstáculos existentes, como: paredes e janelas, possuem um sinal excelente devido à proximidade dos locais com os equipamentos envolvidos nesta análise.

A rede sem fio criada no projeto possui método de autenticação WPA2 com AES *Advanced Encryption Standard* que segundo Moraes (2010, p. 209) “O WPA2 com o AES é a solução mais segura existente, uma vez que o AES é um algoritmo criptográfico até hoje inviolável. Estima-se que seriam necessários milhares de anos para quebrar a chave de 256 bits do AES”.

Implementou-se também a funcionalidade de ocultar o SSID, fazendo com que todos os usuários sejam obrigados a conhecer o nome da rede, criando e prevenindo assim o ataque a rede sem fio. Essa é a primeira linha defensiva, sem a rede com seu SSID propagado pelo ambiente cria-se uma forma de dificultar a primeira fase da invasão que é o reconhecimento. Sem esse ponto exposto uma intrusão ou sequestro de sinal torna-se mais difícil, esse é realmente o intuito de criar mecanismos que dificultem o acesso a rede sem fio.

O próximo passo da configuração foi a criação de senhas mais seguras para os usuários acessarem a rede sem fio projetada. A senha de acesso/autenticação dos dispositivos deve possuir uma sequência de 08 caracteres, possuindo complexidade e baseada em uma palavra, como por exemplo, a palavra password que após aplicado os requisitos de complexidade de letras maiúsculas e minúsculas, números e caracteres especiais poderiam ser elaborada da seguinte forma: P@$$w0rd, PaSSW0rd, pA$$w0Rd, criando mais uma camada para que se utilize com segurança esse requisito e com regras de alteração de senhas periódicas.

Filtros de acesso para autenticação de usuários foram utilizados nas regras de segurança adotadas. Os equipamentos e dispositivos sem fio foram para a documentação e monitoramento sua especificação de endereço físico MAC (*Media Access Control*), para se obter mais controle sobre os dispositivos que pertencem a essa rede compartilhada, a qual será configurada no *Wireless Router*.

Esse processo chama-se MAC Filter, um filtro em que pode-se permitir ou negar o acesso de dispositivos a conectar-se a essa rede sem fio utilizando para isso o endereço físico do equipamento, resultando em mais uma camada de segurança. O MAC Filter tem suas vantagens, que segundo Moraes (2010, p. 202) explica, “É um recurso interessante que auxilia a aumentar a segurança e a realizar um filtro nos Access Points, permitindo que apenas estações que possuam endereço MAC registrado tenham acesso a rede”.

Foi criado um range de endereçamento IP de classe A 10.255.255.0/28 para a rede sem fio, que dá a possibilidade de se obter 14 endereços IPs por rede, 1 endereço será atribuído ao *Wireless Router*, que disponibilizará por DHCP apenas os 7 endereços necessários para os dispositivos, reservando os outros 6 endereços para futura expansão, também foi designado um endereçamento IP de classe C 192.168.0.0/30 com a possibilidade de 02 endereços por rede para conexão do modem ADSL com o Wireless Router.

O escopo de endereçamento segue a seguinte estrutura conforme tabela 1:

Endereçamento IP			
Equipamento	Tipo de Interface	Endereçamento/Atribuição	Máscara
Modem ADSL	LAN	192.168.0.1/Estático	255.255.255.252
Wireless Router	WAN	192.168.0.2/Estático	255.255.255.252
Wireless Router	WLAN/LAN	10.255.255.14/Estático	255.255.255.240
Serviço DHCP	IP inicial	IP Final	Máscara
Wireless Router	10.255.255.1	10.255.255.7	255.255.255.240
Expansão futura	10.255.255.8	10.255.255.13	255.255.255.240

Tabela 1: Escopo de Endereçamento IP
Fonte: Elaboração própria (2014)

Esse endereçamento foi criado seguindo o VLSM *Variable Lenght Subnet Mask* – máscara de sub-rede de tamanho variável, com o propósito de reduzir a quantidade de endereços disponibilizados pelo serviço de DHCP para que um determinado número de clientes possam receber esses endereços, sem ter desperdício de endereços e proporciona outra linha defensiva.

O VLSM é um método de cálculo de sub-redes em que pode-se manipular a quantidade de binários reservados para rede e para host, utilizando máscaras de tamanho variáveis (Odom, 2008). No método tradicional só é possível disponibilizar blocos inteiros de endereços IP, já no método de sub-redes com VLSM é utilizado uma máscara de sub-rede variável para reduzir os blocos de endereços, é mais eficiente para pequenas redes, pois atribui-se a rede uma quantidade menor de hosts por sub-rede.

Após as configurações de equipamentos com filtro de endereço físico, ocultamento de SSID, complexidade de senhas e endereçamento com alocação reduzida, o esquema da rede doméstica sem fio ficou apropriado para uma rede segura, reduzindo bastante os riscos de intrusão, de acordo com a figura 4.

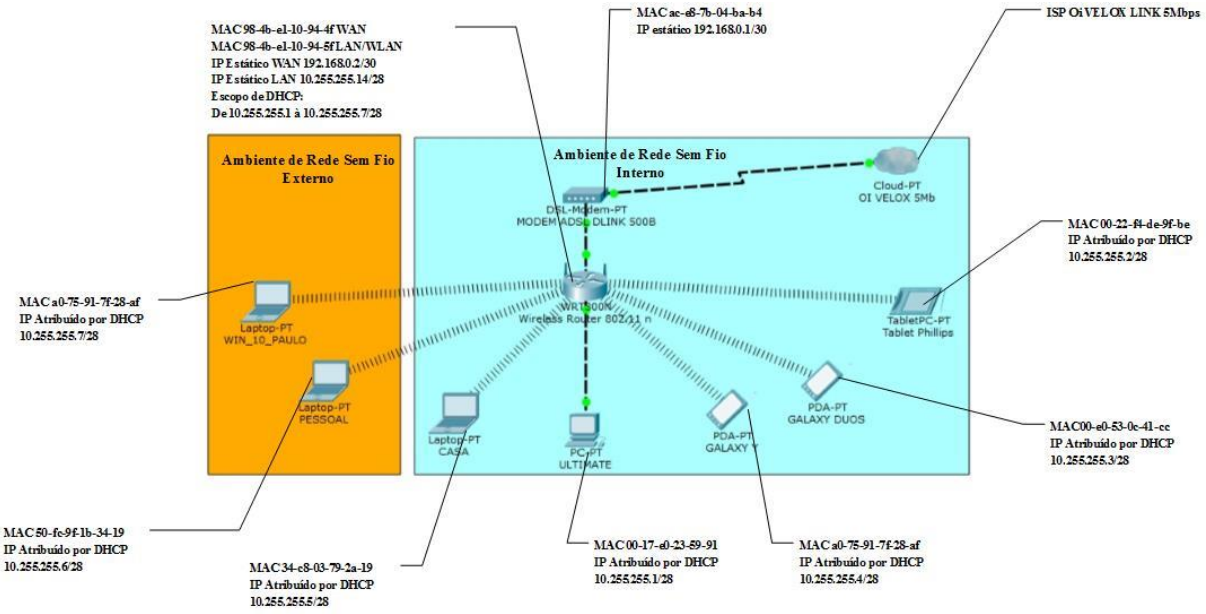

Figura 4: Simulação de ambiente com o Cisco Packet Tracer®, antes da implantação
Fonte: Elaboração própria (2014)

Para monitoramento de seus dispositivos, utilizou-se o aplicativo *Cisco Network Magic*®, pois, possui funções de IDS *Intrusion Detection System*, um sistema de detecção de intrusão de forma gráfica e simples de manusear é possível visualizar todos os dispositivos do ambiente sem fio, com essa implementação consegue-se uma rede mais segura monitorada e controlada, minimizando riscos de intrusão para o ambiente doméstico de rede sem fio, como mostrado na figura 5.

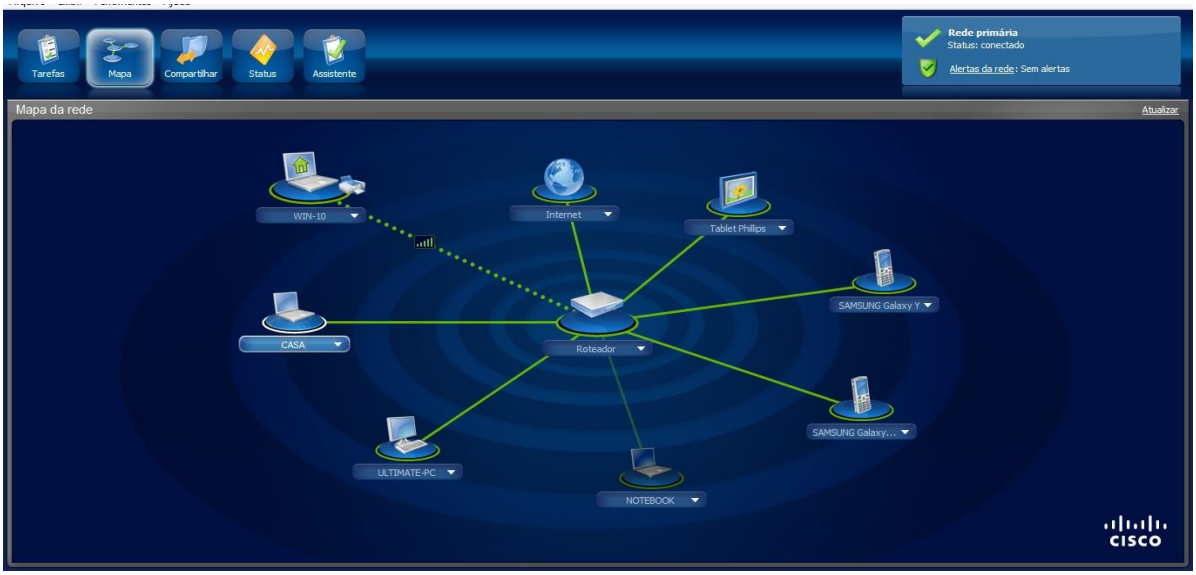

Figura 5: Visualização do ambiente controlado com o Cisco Network Magic®
Fonte: Elaboração própria (2014)

5 Conclusão

As redes sem fio são de fato uma realidade no cotidiano das pessoas, utiliza-se para todo o tipo de acesso e necessita de monitoramento constante para evitar falhas de segurança. Desde sua criação proporciona aos seus usuários o conforto de acessar seus recursos sem estar preso aos cabos, mobilidade é o que se torna valoroso nos dias de hoje por termos acesso às informações em tempo real.

A forma que os usuários do ambiente sem fio utilizam os recursos de rede, através de seus dispositivos móveis, apenas fascinados pelo acesso à Internet com as redes sócias disponíveis a qualquer momento, jogos e entretenimento no geral, estão satisfeitos por estarem conectado à Internet, demonstra somente o lado bom da mobilidade de acesso sem fio, porém deixa de observar o mais importante, como usufruir de toda essa maravilha móvel em tempo real com o mínimo de segurança.

É notável que em um ambiente doméstico de redes sem fio planejado e seguro, é exequível utilizar recursos de redes com uma redução muito grande dos riscos, adotando-se uma linha básica de defesa ou até mínima possível. Porém alguns pontos de segurança devem ser reforçados, como por exemplo: não compartilhar o sinal da rede sem fio com usuários, os quais não sejam domiciliados no mesmo ambiente e não divulgar a senha de acesso à rede sem fio. Quanto mais camada de segurança forem atribuídas a esse ambiente, mais seguro ele será.

Seguir os principais requisitos de segurança, ajuda bastante a reduzir as falhas inerentes do ambiente sem fio. Novos mecanismos para reduzir vulnerabilidades serão implantados para acessar esse ambiente e proporcionará aos seus utilizadores confiabilidade para aproveitar toda a praticidade e comodidade que essa tecnologia impar tem a oferecer.

De qualquer modo, o risco existe. Se os métodos de autenticação criados dão uma relativa segurança em compartilhar o ambiente sem fio. Por outro lado, existe o problema da inexperiência ou falta de conhecimento técnico dos usuários das redes sem fio, que por essa carência técnica acaba por enveredar em configurações sem segurança e por consequência cria pontos falhos neste ambiente, os quais proporcionando, assim a facilidade para invasão por terceiros aos recursos compartilhados.

Essa tecnologia escalável é muito importante para usuários domésticos e está no seu auge de popularidade. É inimaginável o nosso cotidiano sem acesso a algum tipo de recurso

proporcionado pela tecnologia de comunicação móvel, o ambiente compartilhado sem fio é indispensável nos dias de hoje.

Sua utilização é quase unânime em ambientes compartilhados, e estão disponíveis em 100% dos dispositivos móveis atuais conectados à rede sem fio e requer novos momentos de pesquisas para melhorias e evoluções de seus aspectos de acesso e de segurança, proporcionando assim num futuro próximo novos meios de acesso seguro a essas informações.

Como trabalhos futuros, continuar com essa linha de exploração é essencial e imprescindível para dar continuidade a elaboração de novas pesquisas, questionários, estudos de caso e novos métodos de segurança com aplicativos, configurações e dispositivos, evoluindo e aumentando a segurança no ambiente sem fio.

Além disso, como docente, disseminar os resultados das pesquisas para que os alunos possam compartilhar desta segurança. Aumentando o número de pessoas com conhecimentos aplicáveis, por si mesmo, sobre como manter uma rede segura, diminuir e até dirimir os riscos neste meio.

Neste artigo foram abordados alguns pontos comuns de riscos, porém importantes para um ambiente sem fio compartilhado, atribuindo técnicas de planejamento, segurança e monitoramento para o conforto dos usuários desse ambiente.

Abstract

This article is my intent to evaluate security risks that could happen from the misuse of all the information shared nowadays by wireless technologies in domestic environments, provided by the growing development of mobile equipment, such as: tablets, smartphones, notebooks and last but not last, personal computers that’s depend on this technology of communication. With the use of these mobile devices fully compatible with this technology, with special focus in the IEEE 802.11 b/g/n, we notice that is inevitable the creation of some defense mechanisms to protect the wireless networks (WLAN) system. This consideration shows how it is crucial to explore and analyze possibilities of reducing to the minimum the threat of potential invasion of the files in multimedia WLAN structures.

For this research a domestic and planned network was used as a study case, adopting design tools, site Survey, implementation and monitoring, detailing the status of each step with the aim of promoting understanding and usability of wireless technology resources having quite different types of devices in domestic environments, this will certainly

encourage the user to enjoy this technology that will give to them the possibility of having a sharp sense over the concepts and information shared in this very practical and common environment in a everyday life.

Keywords: Wireless. WLAN. Project. Risks. Security.

Referências

ALMEIDA, MARIA, Justiça cobra informações do Google sobre captura de redes Wi-Fi no Brasil**, Tecnologia iG** São Paulo, julho de 2013.
Disponível em: <http://tecnologia.ig.com.br/2013-07-16/justica-cobra-informacoes-do-google-sobre-invasao-de-redes-wi-fi-no-brasil.html> Acessado em: 12 out. 2014.

BARROS, FABIO, Brasil responde por apenas 0,5% dos hotspots WiFi, **Convergência Digital Uol** São Paulo outubro de 2012.Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32060&sid=116#.VD2oEkGv-fc> Acesso em 14 out. 2014.

BRENTANO, LAURA, Brasileiros preferem acesso sem fio Wi-Fi ao 3G, diz pesquisa, **G1** Rio de Janeiro, outubro de 2012.
Disponível em: < http://g1.globo.com/tecnologia/noticia/2012/10/brasileiros-preferem-acesso-sem-fio-por-wi-fi-ao-3g-diz-pesquisa.html >Acesso em 14 out. 2014.

CAMILO, CAMILA, 3G, 4G, Banda larga, wi-fi, wimax: entenda o que significam, **Revista Escola FVC** São Paulo, outubro de 2012.
Disponível em: <http://revistaescola.abril.com.br/gestao-escolar/conexao-acesso-internet-709513.shtml> Acesso em 12 out. 2014.

CAMPOS, A. L. N. **Sistema de Segurança da Informação:** Controlando os Riscos. 3 ed. Florianópolis: Editora Visual books, 2014.

CERT.BR, **Centro de Estudos Respostas Tratamento e Incidentes de Segurança no Brasil**, Segurança de Redes
Disponível em: <http://cartilha.cert.br/redes/ >Acesso em 14 out. 2014

ENGST, A.; FLSIESHMAN, G. **Kit do iniciante em Redes sem fio**: O Guia Prático sobre redes Wi-Fi para Windows e Macintosh. 2. ed. São Paulo: Pearson Makron Books, 2005

JARDIM, F. de M. **Treinamento Avançado de Redes Wireless.** 1. ed. São Paulo: Digerati, 2007.

KUROSE, J. F.; ROSS, K. W. **Rede de Computadores e a Internet**: Uma Abordagem Top-down. 6 ed. São Paulo: Pearson Education do Brasil, 2013

MORAES, A. F. de. **Segurança em Redes:** Fundamentos. 1. ed. São Paulo: Érica, 2010

_____, A. F. de. **Rede de Computadores:** Fundamentos. 7. ed. São Paulo: Érica, 2010

ODOM, W. **CCNA ICND2**:Guia Oficial de Certificação do Exame. 2. ed. Rio de Janeiro: Alta Books, 2008

RUFINO, N. M. de O. **Segurança em Redes sem Fio**: Aprenda a proteger suas Informações em ambientes Wi-Fi e Bluetooth. 2. ed. São Paulo: Novatec, 2007.

TANEMBAUM, A. S.; WATHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011

TANEMBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier, 2003

Apêndice

ESAB – ESCOLA SUPERIOR ABERTA DO BRASIL
CURSO LATO SENSU EM REDE DE COMPUTADORES

Prezado Sr._____, meu nome é **Paulo da Silva Filho**, sou estudante do curso de **Pós-Graduação em Rede de Computadores da ESAB** e estou fazendo uma pesquisa para meu artigo científico, cujo o tema é **"Os riscos de segurança das informações compartilhadas no uso de tecnologias wireless em Ambientes domésticos"**. E o objetivo é verificar o nível de segurança nas redes domésticas. Necessito de sua atenção para responder a algumas perguntas.

1- Quantos dispositivos wireless são utilizados em sua rede doméstica?

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

2- Qual o padrão Wireless utilizado? 802.11 b, a, g ou n?

A	**B**	**G**	**N**

3- Disponibiliza algum recurso para usuários externos?

( ) sim ( ) não

4- O que compartilha para os usuários externos?

Internet	Música	Documentos	Filmes	Imagens	Outros

5- Variam a senha de acesso periodicamente (trocam de senha) e usam complexidade? (adotam senhas com letras número e caracteres especiais, como por exemplo: P&$qu1s@)

( ) sim ( ) não

6- Já sofreu algum tipo de ataque em sua rede?

( ) sim ( ) não

7- Possui conhecimento técnico para realizar configurações nos equipamentos?

( ) sim ( ) não

8- Utiliza endereçamento IP estático ou dinâmico?

( ) sim ( ) não

9- Preocupa-se com a segurança em sua rede sem fio?

( ) sim ( ) não