Um Método para Minimizar Falhas de Segurança em Redes WLAN 802.11b/g: Controlando Acessos Provenientes de Dispositivos Móveis

Leandro Ferreira Paz3, Rodrigo Petter Daniel1, Vinícius Maran2, Cristiane Ellwanger1

[1] Departamento de Ciências Exatas e Engenharias – Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUÍ)
Caixa Postal 489 – 98.900-000 – Santa Rosa RS – Brasil

[2] Coordenadoria Acadêmica – Universidade Federal de Santa Maria (UFSM)
Av. Presidente Vargas, 1958 – Cachoeira do Sul – RS – Brasil

[3] Instituto Federal de Educação, Ciência e Tecnologia Farroupilha
Rua Uruguai, 1675, Bairro Central, Santa Rosa – RS – Brasil

{rodrigo.daniel, cristiane.ellwanger}@unijui.edu.br,
viniciusm@inf.ufsm.br, leandro.paz@iffarroupilha.edu.br

Abstract. *Wireless networks play a fundamental role for organizations to evolve both technologically and economically. Allied to this, the proliferation of mobile devices has brought the convenience of connection between devices, anytime, anywhere. However, in this scenario the vulnerability of wireless networks has become a worrying factor because often access to corporate networks does not provide levels of security required for sensitive data traffic. With this, this paper proposes a method for implementing a wireless 802.11b/g secure with a focus on mobile devices in order to protect the confidential information of companies.*

Resumo. *Redes sem fio possuem papel fundamental para que as organizações consigam evoluir tanto tecnologicamente como economicamente. Aliado a isto, a proliferação dos dispositivos móveis trouxe a comodidade de conexão entre dispositivos, a qualquer momento, em qualquer lugar. No entanto, neste cenário, a vulnerabilidade das redes sem fio tornou-se um fator preocupante, pois muitas vezes o acesso interno às redes corporativas não oferecem níveis de segurança necessários para o tráfego de dados sigilosos. Com isto, este artigo propõe um método para implementar redes sem fio 802.11b/g segura com foco em dispositivos móveis a fim de proteger as informações confidenciais de empresas.*

1. Introdução

Em 2015, uma pesquisa realizada pela Fortinet [Fortinet, 2015] levantou que as redes sem fio representam o ponto mais vulnerável da infraestrutura de tecnologia da informação. Os dados apontam que 49% das organizações classificam a infraestrutura sem fio como o elemento de maior exposição as atividades de roubo de dados. Além disso, 43% das empresas fornecem acesso a dispositivos móveis meramente como convidados e 13% permitem isso sem aplicar nenhum controle de acesso.

Vários trabalhos se direcionam a proteção de informações organizacionais a partir de dispositivos móveis. Silva & Ludwig [2011] propõem uma metodologia para auditar redes sem fio 802.11b/g, com base em seis fases de auditoria, abordando um planejamento que vai desde o desenho do mapa topográfico da rede, que contém o leiaute onde a auditoria será feita até a captura de dados para análise por ferramentas, emprego de protocolos de segurança, monitoração da rede e aumento da segurança das aplicações, entre outros. Trabalhos como os de Cansian et al., [2004] e Pinto & Gomes [2011] ressaltam as vulnerabilidades e ameaças das redes wireless tais como as falhas no protocolo WEP, relatam as susceptibilidades às invasões externas e a descriptografia de pacotes.

Embora tais trabalhos sejam de suma relevância para a área de segurança das informações, eles não demonstram de forma clara como ela pode ser preservada. Diante do exposto, o presente artigo propõe um método de implementação de uma rede WLAN local 802.11b/g para dispositivos móveis, cujo acesso externo é segurado por uma conexão criptografada através de uma Virtual Private Network (VPN). A vantagem de usar uma VPN para dispositivos móveis é garantir um nível adequado de segurança para os sistemas críticos conectados quando uma infraestrutura de rede subjacente por si só não pode fornecê-la.

O artigo está estruturado da seguinte forma: Na Seção 2 é apresentada uma descrição das redes sem fio e suas classificações e características. Na Seção 3 é demonstrado como o método proposto foi concebido. Na Seção 4 são descritos os cenários e ferramentas utilizadas. Na Seção 5 são apresentados os resultados da aplicação do método e na Seção 6 são apresentadas as conclusões deste trabalho e trabalhos futuros.

2. Redes Sem Fio 802.11: Classificações e Características

O padrão IEEE 802.11 tem por objetivo documentar e padronizar Wireless Local Area Network (WLAN). Esse padrão é constituído por diversos subgrupos, onde cada um deles possui novos implementos e melhorias. Esses subgrupos recebem uma letra, em ordem alfabética, conforme são desenvolvidos ou planejados, referenciados como 802.11b, 802.11g e 802.11i. Em redes sem fio as topologias que seguem o padrão IEEE 802.11 são duas: ad hoc e infraestruturadas. A primeira é independente, ou seja, não necessita de um ponto de acesso para que exista comunicação entre os dispositivos conectados. Já a segunda, que é abordada nesta pesquisa, possui a necessidade que toda a comunicação entre os dispositivos móveis passe por um ponto central como um Access Point (AP) ou um roteador.

Redes infraestruturadas sem fio são similares ao da telefonia celular, onde há obrigatoriedade de que a comunicação passe por um ponto central, ou seja, ainda que os dispositivos conectados na rede estejam bastante próximos, os mesmos não podem se comunicar diretamente. Duas premissas são utilizadas neste contexto, ou se usa uma comunicação ad hoc, ou se utiliza uma estação de suporte à mobilidade da rede infraestruturada, neste caso.

2.1. Propriedades do IEEE 802.11b/g Relacionadas à Segurança

O IEEE 802.11b é o padrão mais utilizado atualmente [Pinto & Gomes, 2011], embora desatualizado ele ainda fornece acesso para muitos dispositivos antigos. Operando numa frequência de 2.4 GHz e utilizando o protocolo Wired Equivalent Privacy (WEP), o 802.11b possui limite para 32 usuários conectados, com taxa de transmissão de 11 Mbps. O padrão 802.11g trabalha na faixa de 2.4 GHz, transmitindo a 54 Mbps. Embora

o padrão 802.11n tenha aumentado seu uso, os padrões 802.11b/g ainda são usados em muitas configurações [Morimoto, 2011]. Uma característica importante do padrão 802.11n é poder operar na mesma faixa de frequência do 802.11b, desta forma duas configurações podem trabalhar juntas.

O principal problema apontado no padrão 802.11b/g é seu protocolo de criptografia [Cansian et al., 2004]. Este protocolo propõe uma forma de conexão semelhante das redes cabeadas, cuja segurança é baixa. O protocolo WEP utiliza um vetor pseudorrandômico de 24 bits em conjunto com uma senha de 40 ou 104 bits programada pelo usuário, para criptografar os pacotes enviados pelos dispositivos sem fio. Tal falha é ocasionada na geração dos vetores de inicialização, quando ocorrem vetores com uma estrutura singular de modo que se possa prevê-los. Estes são chamados de "vetores de inicialização fracos" [Cansian et al, 2004].

3. Método Proposto para Implementação de rede VPN

O método proposto neste trabalho tem por intuito minimizar os impactos das vulnerabilidades existentes em sistemas críticos, se apoiando nos trabalhos realizados por Cansian et al., [2004]; e Pinto & Gomes [2011], ressaltando a metodologia apresentada por de Silva e Ludwig [2011], para auditoria de redes sem fio 802.11b/g a fim de auxiliar os profissionais a identificarem as vulnerabilidades da rede. A abordagem do presente método (Figura 1) permite ao usuário não somente a análise da solução implementada, mas também salientar aspectos importantes na efetividade da segurança de redes wi-fi.

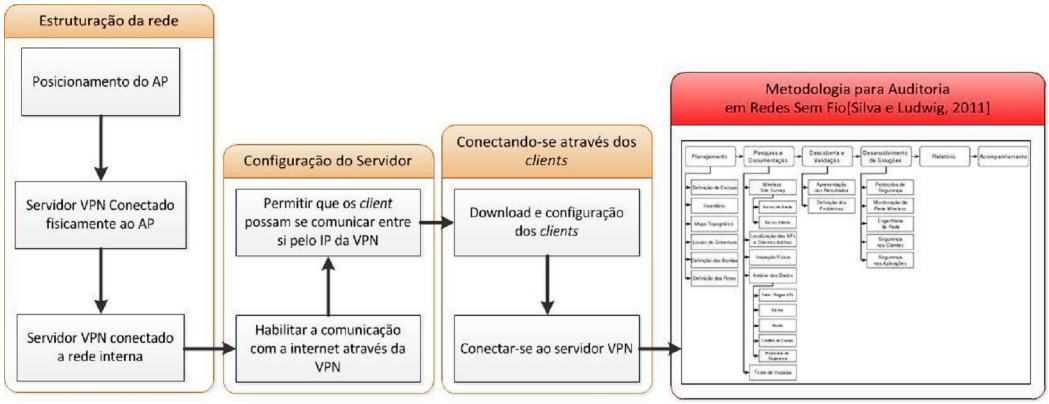

Figura 1: Método para implementação da rede VPN.

O método apresentado na Figura 1 constitui-se de quatro etapas: Estruturação da rede, Configuração estabelecida com o servidor, Conexão com os clientes e Aplicação da metodologia proposta por Silva & Ludwig [2011]. Esta quarta etapa é considerada um processo contínuo, então sua posição pode ser tanto no fim como no início do método.

A Fase de **Estruturação da Rede** refere-se à forma em que a rede é montada. O AP necessita estar conectado diretamente ao servidor VPN e este, por sua vez, deve estar conectado à rede interna da empresa. Essa estruturação em duas redes distintas possibilitará somente aos dispositivos autenticados na VPN, acesso aos demais recursos.

Já a Fase de **Configuração com o Servidor** tem por intuito minimizar as vulnerabilidades do protocolo WEP, utilizando-se de um servidor VPN. Para isto, optou-se pela utilização do software OpenVPN (https://openvpn.net/). Após, foi realizado o download do OpenVPN Access Server Virtual Appliance, e foram

realizadas as configurações de rede básicas do servidor. Primeiramente é necessário configurar o OpenVPN para que todas as requisições de internet passem pelo servidor. Fazendo isto, os dados transmitidos via wireless estarão encapsulados na conexão VPN.

Por fim, a Fase de Conexão com os Clientes tem por intuito estabelecer em elo de comunicação entre os mesmos de forma mais efetiva em termos de segurança, ou seja, após o servidor ser configurado para receber o tráfego de internet e disponibilizar os serviços de rede que estejam depois dele. O estabelecimento da conexão a partir de um computador (independentemente de sistema operacional) é realizado acessando o endereço IP do servidor a partir de qualquer navegador, fazendo a autenticação e realizando o download o OpenVPNClient (https://openvpn.net/). Para conectar-se a VPN utilizando um smartphone com sistema operacional Android, é necessário baixar, instalar e configurar o OpenVPN. Após a instalação, o procedimento para conectar-se é semelhante ao do Linux, ou seja, necessário acessar o IP do servidor através de um navegador, autenticar-se e baixar o arquivo de configuração.

Para validação do método proposto com o estabelecimento das fases acima apresentadas, e os procedimentos a elas relacionados, a metodologia foi aplicada em um estudo de caso, no qual se especificou um contexto de aplicação, a seleção das ferramentas mais adequadas para a extração de informações realmente úteis e a análise dos resultados provenientes da realização do mesmo, sendo estes descritos nas seções subsequentes.

4. Cenário e Ferramentas Utilizadas

O escopo do ambiente de estudo é constituído de uma rede infraestruturada composta por: um Access Point (AP), um servidor VPN, um switch e recursos da rede protegida e os dispositivos móveis (Figura 2). Como também para utilizar as ferramentas da organização e ainda manipular arquivos como num servidor File Transfer Protocol (FTP), por exemplo, o acesso também será feito pela VPN. Isto é considerado um ponto importante com relação à segurança de sistemas corporativos, assim, a prática de uma rede privada virtual aumenta significativamente a segurança nos acessos a sistemas críticos [Klein, 2012].

A VPN é uma forma de a segurança interna da rede, pois ela permite a criptografia por tunelamento garantindo a confidencialidade, autenticação e integridade das informações recebidas e enviadas [Rossi & Franzin, 2000]. O objetivo é combater algumas vulnerabilidades que o protocolo WEP apresenta usado no padrão 802.11b/g como injeção de tráfego, redirecionamento de mensagens, obtenção do segredo compartilhado [Catafesta, 2004].

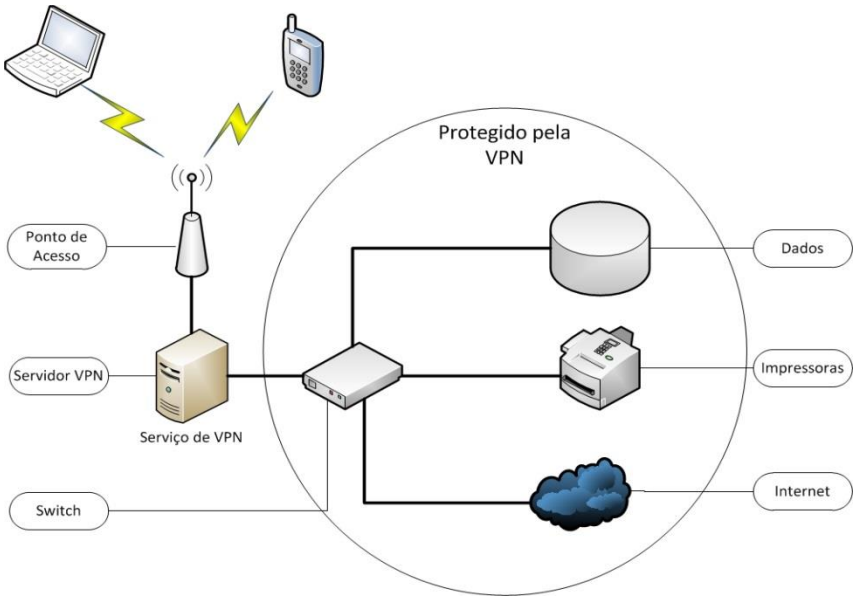

Figura 2: Rede VPN.

Neste cenário a realização de testes de segurança e a implementação do método foram utilizados alguns aplicativos, conforme demonstra a Tabela 1. A utilização, para concretização do método proposto, justifica-se por serem softwares gratuitos, multiplataforma e de fácil instalação.

Tabela 1: Ferramentas utilizadas nos testes de implementação.

Aplicativo	**Categoria**	**Versão**	**Plataforma**	**Valor**
Aircrack-ngSuite	*Sniffer*	1.1	Linux/Windows	Gratuito
Kismet	*Sniffer*	2011-03-R2	Linux	Gratuito
OpenVPN	*Server e Client*	1.8.4	Linux/Windows	Gratuito
Wireshark	*Sniffer*	1.8.3	Linux/Windows	Gratuito

A ferramenta Aircrack-ng (http://www.aircrack-ng.org/) é uma suíte de aplicativos para verificação de redes sem fio. Um de seus aplicativos é o Airodump-ng (http://www.aircrack-ng.org/) que captura pacotes, gerando um arquivo com extensão cap. A leitura deste arquivo é feita pelo Aircrack-ng, que tem o objetivo de quebrar a senha de encriptação WEP. Já a ferramenta Kismet (http://www.kismetwireless.net/) é usado para descoberta das redes sem fio, enquanto o Wireshark (https://www.wireshark.org/) captura os pacotes de uma determinada rede.

5. Resultados Advindos da Aplicação do Método

Para demonstrar a viabilidade do método proposto, foram realizados testes no cenário apresentado na Figura 2. Em um primeiro momento, foram feitas tentativas de invasão na rede wi-fi. Como resultado obteve-se a confidencialidade da informação comprometida quando a senha WEP pôde ser descoberta com o uso do Aircrack-ng Suite e o Kismet. Este último conseguiu interceptar o BSSID e SSID da rede e o canal que estava operando. Com esses dados foi possível capturar pacotes com Airodump-ng e, com 40.000 pacotes a chave foi descoberta com o Aircrack-ng (Figura 3).

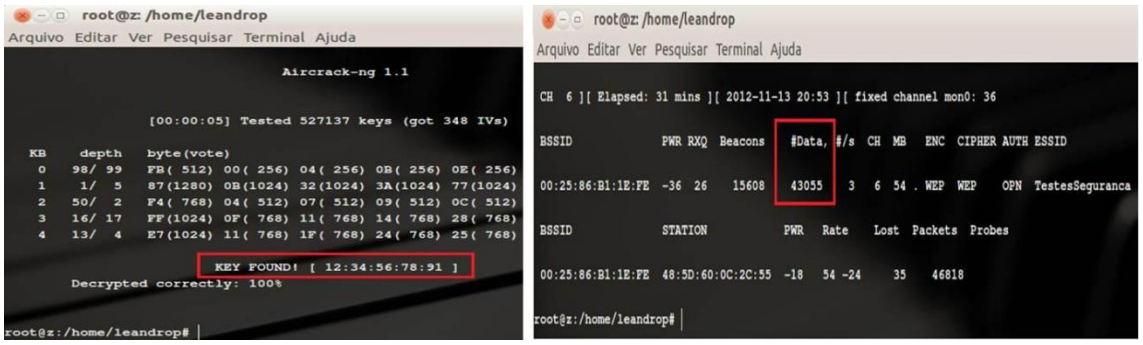

Figura 3: Captura de pacotes (A) e descoberta de senha (B), respectivamente, com Airodump-ng e Aircrack-ng.

A Figura 3 demonstra as vulnerabilidades do protocolo WEP para fornecer segurança nas redes sem fio 802.11b/g. Assim, faz-se necessário o uso de uma camada adicional de segurança na rede quando se utiliza criptografia WEP. A análise e filtragem do trafego da rede foi feita utilizando-se do software Wireshark, o que permitiu acompanhar a ocorrência da criptografia no túnel no tráfego de dados durante a VPN. O funcionamento da VPN foi verificada a partir do estabelecimento de uma sessão File Transfer Protocol (FTP).

É possível verificar (Figura 4 A) que os dados trafegados na VPN estão criptografados. Em outro teste (Figura 4 B) a VPN foi desativada e a sessão FTP foi iniciada. O Wireshark foi ativado para captura dos pacotes. Nota-se que os dados que trafegam pela rede estão totalmente descriptografados, contendo informações confidenciais tais como o nome do usuário da sessão, senha e comando efetuados durante a sessão FTP.

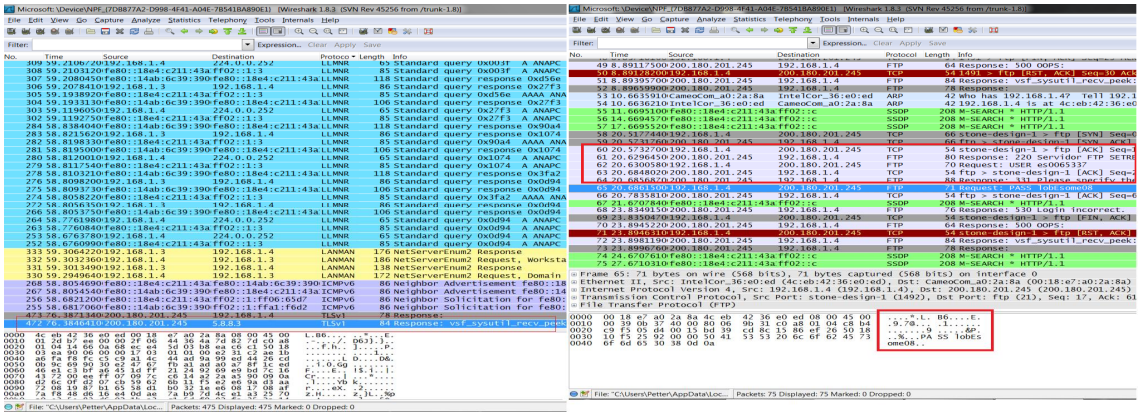

Figura 4: Dados criptografados pela VPN capturados pelo Wireshark (A) e desprotegidos (B).

Atualmente, o OpenVPN tem destaque como uma implementação open source sobre TLS. A criptografia de chave pública é o método mais conhecido do protocolo TLS. A outra forma é a convencional, a criptografia com a chave que foi distribuída. Nos testes realizados a autenticação do cliente foi feita por password, em casos de VPN host LAN isto é permitido. A senha é enviada diretamente para o servidor através de uma conexão segura, ou seja, há uma preautenticação do servidor perante o cliente.

Desta forma, o risco de a senha ser capturada durante o transporte por um desconhecido é descartada. Esta autenticação é feita através do certificado de chave pública do servidor, cuja instalação é feita manualmente [Moreira, 2010]. Alguns pontos com relação à segurança proposta ficaram sem proteção como Engenharia Social, falsos

APs e ataques internos, demonstrado na Figura 5. Por outro lado, a captura de dados, invasões externas e utilização de recursos por pessoas não autorizadas tiveram proteção com o uso da VPN.

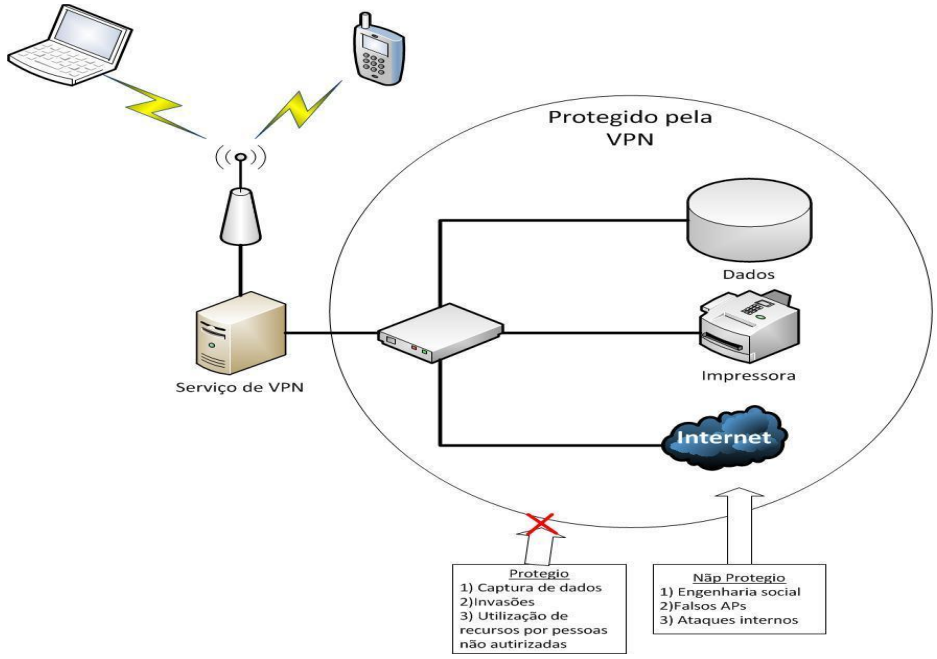

Figura 5: Pontos protegidos e desprotegidos da rede implementada.

Ainda que alguns fatores estejam desprotegidos, minimizaram-se as vulnerabilidades do protocolo WEP onde as chaves de segurança trocadas podem ser previstas. O uso de uma VPN neste caso fornece uma melhor efetividade na proteção dos dados, pois a criptografia no túnel garante a autenticidade, a integridade e o sigilo das informações. Se for comparado com os trabalhos de autores citados neste artigo, eles somente utilizam o protocolo WEP como camada de proteção.

6. Conclusão e Trabalhos Futuros

É de fundamental importância manter os dados confidenciais fora do alcance de usuários mal intencionados, protegendo as informações de ataques passivos e ativos. Assim, é aconselhável utilizar uma camada a mais de segurança e que a mesma esteja configurada de maneira adequada. Pois, como foram relatadas, algumas das propriedades das tecnologias wireless atuais mais utilizadas (IEEE 802.11b/g) não são capazes de prover tal segurança, deixando os dados trafegados à disposição de qualquer usuário que souber como interceptá-los.

Neste artigo foi proposto um método para implementar uma VPN diretamente sobre um AP que repassa o sinal para os usuários, ao contrário dos demais que utilizam algum meio de comunicação sem fio em conjunto com uma VPN para interligar duas LANs distintas. O objetivo é garantir que a comunicação dos dispositivos móveis (notebooks, smartfones, tablets, etc) com os pontos de acessos sem fios seja feita de forma segura e restrita apenas a quem tiver autorização.

Como trabalhos futuros, sugere-se pesquisar um método que programe o mesmo tipo de segurança em uma rede doméstica, visto que atualmente a quantidade de hotspots inseguros de uso particular é superior aos corporativos.

7. Referências Bibliográficas

Cansian et al. Falhas Políticas de Configuração: uma análise dos riscos para as redes sem fio na cidade de São Paulo. In: SIMPÓSIO DE SEGURANÇA EM INFORMÁTICA, 6, 2004, São José dos Campos. Anais. São Paulo: IFSJC. Disponível em:<http://www.acmesecurity.org/sites/default/files/publicacoes/artigos/acme-artigo-ssi-2004-wlan.pdf>. Acesso em: 20 ago. 2015.

Catafesta, Márcio. Implementação de um Mecanismo de Filtragem de Pacotes para um Ponto de Acesso Sem Fio. 2004. Disponível em:<http://guaiba.ulbra.tche.br/pesquisa/2004/resum os/sistemas/seminario/173.PDF>. Acesso em: 19 ago. 2015.

Fortinet. Wireless Network the Weakest Security Link in Enterprise IT Infrastructure, According to Fortinet Global Survey of IT Leaders. 2015. Disponível em:<http://www.fortinet.com/press_releases/2015/global-survey-wireless-network-weakest-security-link.html>. Acesso em: 26 ago. 2015.

IEEE 802. Wireless Local Area Network: the working group for WLAN standarts. 2010. Disponível em:<http://www.ieee802.org/11/index.shtml>. Acesso em: 24 ago. 2015.

Klein, Eduardo. Gestão de Segurança de Dispositivos Móveis. 2012. Disponível em:< http://www.mobiltec.com.br/blog/index.php/gestao-de-seguranca-de-dispositivos-moveis/>. Acesso em: 03 ago. 2015.

Moreira, André. Redes de Computadores – Redes Privadas Virtuais (VPN) Protocolo PPP. 2010. Disponível em: <http://www.dei.isep.ipp.pt/~andre/documentos/RCOMP/T9.pdf>. Acesso em: 10 jul. 2015.

Morimoto, Carlos E. Redes Wireless atualizado (sétima e última parte). 2011. Disponível em:<http://www.hardware.com.br/guias/redes-wireless/80211g-1.html>. Acesso em: 26 jul. 2015.

Pinto, Pedro MicaelT.L.N; Gomes, Antônio Ricardo Leocádio. Segurança na Conectividade Wifi em Dispositivos Móveis: estudo de caso do iPhone. RevistaE-xacta. Belo Horizonte, n. 3, dez. 2011. Disponível em:<http://revistas.unibh.br/index.php/dcet/article/view/331/406>. Acesso em: 01 jul. 2015.

Rossi, Marco Antonio G.; Franzin, Oswaldo. VPN – Virtual Private Nwtwork.2000. Disponível em:<http://www.gpr.com.br/download/vpn.pdf>. Acesso em: 06 jul. 2015.

Silva, Fabiano; Ludwig, Glauco Antonio. Desenvolvimento de uma Metodologia para Auditoria em Redes Sem Fio IEEE 802.11b/g. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 8, Gramado. Anais. Rio Grande do Sul: UFRGS. Disponível em:<http://labcom.inf.ufrgs.br/ceseg/anais/2008/data/pdf/st02_02_wticg.pdf>. Acesso em: 30 jun. 2015.