SEGURANÇA EM REDES WIRELESS

Diogo Gomes Faria Douglas Felipe do Amaral Silva, Diogo Chaud.

Palavras-chave: Redes, Wireless, Segurança, Wlans, WEP, WPA, Firewall, IEEE.
Área do Conhecimento: Engenharia Elétrica

Resumo – Este TCC busca explicar as funcionalidades de uma rede sem fio que utiliza radiofreqüência em sua comunicação. Este tipo de rede, normalizado pelo IEEE (Institute of Eletrical and Eletronic Engineers), utiliza o padrão 802.11. Este padrão possui variações que, para cada uma delas, existe uma determinada configuração: 802.11a (54Mbps a 5Ghz); 802.11b (11Mbps a 2,4GHz) e 802.11g (54Mbps a 2,4GHz). Este tipo de rede, por ser realizada através de ondas de rádio, atravessando paredes o sinal pode chegar a alcançar a área externa do estabelecimento, facilitando o acesso indevido. Para se evitar que um servidor obtenha acesso indevido à rede ou capture as informações ali trafegadas, este trabalho demonstra os métodos e ações que podem ser implementados em busca de assegurar uma maior confiabilidade e autenticidade, se utilizando, por exemplo, de criptografia como o WEP (Wired Equivalency Privacy) ou o WPA (Wi-Fi Protected Access), assegurando a confiabilidade das informações. Este tipo de rede, quando sua segurança é bem configurada, é uma excelente opção a ser implementada, pois sua configuração é simples, o que justifica o aumento de usuários à melhor difusão desta tecnologia.

1. Introdução

As redes sem fio, segundo ENGST & FLSIESHMAN (2005) iniciou-se de um projeto que ligou as universidades do Havaí em 1971, que conectavam os computadores. Elas entraram para o uso da computação pessoal em 1980, quando a idéia de compartilhar dados entre computadores começava a se tornar popular. As primeiras redes sem fio baseadas em ondas de rádio ganharam notoriedade no início dos anos 90, quando os processadores se tornaram mais rápidos a ponto de suportar tal aplicação. As redes existentes na época eram patenteadas e incompatíveis, por isso, no meio da década de 90 as atenções se voltaram para o novo modelo do IEEE (Institute of Eletrical and Eletronic Engineers), o 802.11. (ENGST & FLEISHMAN, 2005). Atualmente este tipo de rede já se tornou bem popular, e seu futuro parece ser ainda mais difundido do que no atual presente.

Nessa nova era surgiu as redes Wireless, cujo objetivo é substituir ou adicionar mobilidade a redes convencionais. A tecnologia Wireless constitui-se como uma alternativa a essas redes, fornecendo as mesmas funcionalidades, mas de forma flexível, e com boa conectividade eliminando os problemas dos cabos, entre outros. Redes locais sem fio combinam conectividade de dados com mobilidade do usuário. Esse tipo de rede possui um grande mercado, trazendo benefícios como: mobilidade, agilidade, flexibilidade, baixo custo. Apesar da facilidade de uso deste tipo de rede, suas vulnerabilidades devem ser tratadas de forma a melhorar a proteção da rede.

Nosso objetivo nesse projeto é demonstrar como atua uma rede sem fio baseada no padrão IEEE 802.11, demonstrando suas vulnerabilidades e as principais ferramentas de defesa, que podem variar de soluções simples até as mais estruturadas e custosas.

Por ser uma tecnologia relativamente recente, muitas vulnerabilidades podem ser encontradas e outras ainda serão descobertas. É justamente explorando estas vulnerabilidades que “hackers” se infiltram nas redes sem fio. A forma comum utilizada para explorar estas falhas é através do uso de ferramentas desenvolvidas especificamente para esta finalidade. Ataques direcionados às redes sem fio além de comprometer os recursos destas, podem comprometer os recursos de outras redes com as quais esta se interconecta. Outro fator determinante da segurança em redes sem fio é relacionado com a origem dos ataques. Estes podem ser originados de qualquer posição dentro da área de cobertura da rede em questão, o que dificulta a tarefa de localização precisa da origem do ataque.

Esta rede tornou-se um alvo fácil e almejado por pessoas mal intencionadas para o comprometimento de sistemas, pois disponibiliza inúmeros atrativos como dificuldade na identificação da origem exata do ataque, imaturidade das opções e protocolos de segurança para esse tipo de tecnologia, facilidade em obter acesso a rede guiada através de uma conexão de rede sem fio e principalmente a falta de conhecimento técnico do gerente desta rede.

Para que os ataques dirigidos às redes sem fio possam ser identificados e as contra-

medidas possam ser tomadas eficazmente, é necessário que haja a análise das vulnerabilidades inerentes às redes 802.11x. Para isso, é preciso um estudo exaustivo sobre os protocolos que dão suporte às mesmas. Com isso as falhas nestes protocolos são apontadas e as mudanças cabíveis podem ser introduzidas. O trabalho, portanto, analisa as falhas, o grau de comprometimento atingido por cada uma delas, como pode ser explorado e como podem ser eliminadas.

2. Arquitetura

A topologia de uma rede Wireless é composta pelos seguintes elementos:
BSS - Basic Service Set - corresponde a uma célula de comunicação wireless.
STA - Stations - são as estações de trabalho que comunicam-se entre si dentro da BSS.
AP - Access Point - funciona como uma bridge(ponte) entre a rede wireless e a rede tradicional. Coordena a comunicação entre as STA dentro da BSS. Existem APs que também atuam como roteador, possibilitando o compartilhamento de Internet pelos outros micros da rede. Eles vêem de fábrica como servidores DHCP (Dynamic Host Configuration Protocol), facilitando a obtenção de um endereço IP na rede. Também conhecido como concentrador.
Bridge - Faz a ligação entre diferentes redes, por exemplo, uma rede sem fio para uma rede cabeada.

ESS - Estended Service Set - consiste de várias células BSS vizinhas que se interceptam e cujos AP estão conectados a uma mesma rede tradicional. Nestas condições uma STA pode movimentar-se de um BSS para outro permanecendo conectada à rede. Este processo é denominado Roaming.
Dois modos de operação são previstos:
Modo Infra - estrutura - quando existe a presença de um AP coordenando a comunicação entre as estações de uma célula (BSS).

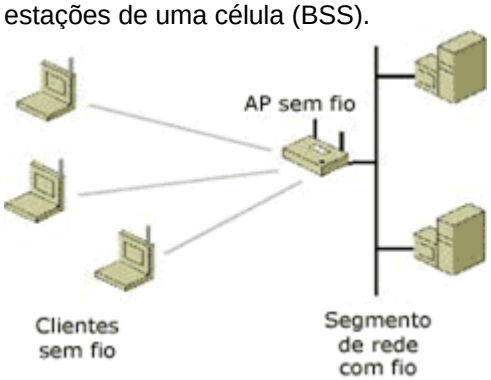

Figura 1: Rede sem fio no modo de infra-estrutura
Fonte: Microsoft Brasil (2005)

Modo Ad-Hoc - quando não existe AP e as estações se comunicam entre si diretamente. Este modo não é recomendado pelo padrão.

Figura 2: Rede sem fio no modo Ad Hoc
Fonte: Microsoft Brasil (2005)

Existem vários tipos de hardwares para acessar uma rede sem fio, como placas USB (externas), placas PCI(internas) e adaptadores de placas de rede.

3. Segurança em Redes Wireless

O surgimento das redes sem fio não é nenhuma surpresa para as empresas atuais. Isso se deve ao grande aumento de produtividade que as tecnologias sem fio proporcionam o que é difícil de ser ignorado. Em um recente estudo, a Gartner descobriu que funcionários com notebooks atingiram um aumento de produtividade de meia hora a três horas, comparado aos usuários de desktops. Quando a conexão sem fio é adicionada a esses notebooks, ocorre um aumento de até 11 horas de produtividade adicional por semana.

Porém, as redes sem fio vêm também acompanhadas de desvantagens significativas e talvez a segurança seja a principal delas. A segurança é um dos três maiores problemas enfrentados por gerentes de TI, com relação às redes sem fio e computação remota.

Os principais problemas de segurança com relação aos sistemas sem fio incluem:
Perda de um dispositivo portátil, comprometendo os dados nele contidos. Relacionamentos de confiança" quando os dispositivos sem fio são usados para comércio (por exemplo, para a o envio de pedidos ou compras).

Para lidar com esses problemas, as empresas precisam determinar procedimentos muito específicos para o uso de dispositivos sem fio, incluindo as funções para as quais os mesmos podem ser usados, o que pode ou não ser armazenado e qual a tecnologia de segurança que deve estar instalada, para evitar que os dados sejam comprometidos, no caso de roubo do dispositivo.

A definição de políticas de segurança e padrões para os dispositivos sem fio é muito importante. Por exemplo, notebooks com recursos sem fio devem ter proteção antivírus e de firewall instaladas. Uma rede sem fio pode realizar transmissões em distâncias muito além de um prédio, permitindo a qualquer um que esteja por perto ou até mesmo passando perto de uma instalação, acessar dados. Basta uma antena potente e um software de hacker facilmente disponível no mercado. **(SYMANTEC, 2003)**

A rede deve estar operante e garantir:

Confiabilidade - O sinal transmitido pela rede pode ser captado por qualquer receptor atuante na área em que o sinal estiver ativo.

Integridade da Informação - Garantir que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor.

Disponibilidade da Rede - Manter a rede acessível.

Autenticidade - Fazer com que a autenticação para o acesso à rede ocorra.

4. Metodologia e Materiais

Criptografia: Uma forma de proteção aos dados trafegados na rede é a criptografia. Caso um atacante tente obter os dados trafegados na rede, a criptografia vai cuidar de deixar todos os dados fora de uma ordem lógica e entendível. **(ENGST & FLEISHMAN, 2005)**

WEP (Wired Equivalency Privacy): Segundo a Microsoft, é o método criptográfico usado nas redes wireless 802.11. O WEP opera na camada de enlace de dados e fornece criptografia entre o cliente e o Access Point. O WEP é baseado no método criptográfico que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (secret shared key) de 40 ou 104 bits. O WEP que traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática, o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o SSID e a lista de endereços físicos permitidos, também conhecido por endereço MAC (Media Access Control).

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os pontos que suportarem apenas o padrão de 64 bits ficarão fora da rede. ***(MICROSOFT , 2004)***

Alguns programas já largamente disponíveis são capazes de quebrar as chaves de criptografia caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. Assim sendo, o WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas por softwares como AirSnort ou WEPCrack. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.O WEP vem desativado na maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que será preciso definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. Nas estações a chave, assim como o endereço SSID e outras configurações de rede podem ser definidas através de outro utilitário, fornecida pelo fabricante da placa. **(RUFINO, 2005)**

WPA(Wi-Fi Protected Access): com os problemas de segurança no WEP, a Wi-Fi Alliance adiantou a parte de autenticação e certificação elaboradas para o 802.11i e liberou o protocolo WPA.

Apesar de avanços terem ocorridos nesse protocolo, a maioria deles requer novos elementos na infra-estrutura da rede e ainda deve trabalhar em conjunto com outros protocolos, como o 802.1x. O WPA atua em duas áreas. A primeira é a qual substitui o WEP, cifrando os dados e garantindo a privacidade do tráfego, e a segunda, autentica o usuário, utilizando para isso padrões 802.1x e EAP (Extensible Authentication Protocol).

Mecanismos de Criptografia WPA: O WPA possui diferentes modelos de segurança, adaptável ao tipo do uso em que ele será implementado, uma para aplicações pequenas, como redes domésticas e pequenos escritórios, utilizando uma chave previamente compartilhada, sendo responsável pelo reconhecimento do aparelho. O método de chave compartilhada é semelhante ao WEP, onde a troca de chaves é feita manualmente, fazendo com que seu uso se torne melhor adequado em redes pequenas onde os participantes estão acessíveis na maior parte do tempo. Não existem ainda problemas divulgados nos protocolos usados com WPA-

PSK.TKIP, responsável pela troca dinâmica das chaves. **(RUFINO, 2005)**

O protocolo TKIP (Temporal Key Integrity Protocol) é o responsável pelo gerenciamento da troca de chaves, no WEP as chaves eram estáticas e seu vetor de inicialização era de apenas 24bits, passando agora para 48bits. **(RUFINO, 2005)**

"Com 802.11 e WEP, a integridade dos dados é fornecida por um valor de verificação de integridade, o ICV (Integrity Check Value) de 32-bit que aparece com a carga útil 802.11 e é criptografado com WEP. Embora o ICV esteja criptografado, pode-se alterar os bits na carga criptografada e atualizar o ICV criptografado sem ser detectado pelo receptor.

Com WPA, um método conhecido como Michael, específica um novo algoritmo que calcula um código de integridade da mensagem, o MIC (Message Integrity Code) de 8 bytes usando os recursos de cálculo disponíveis nos dispositivos existentes. O MIC está localizado entre a parte de dados do quadro 802.11 do IEEE e o ICV de 4 bytes. O campo MIC é criptografado com os dados do quadro e o ICV.

Michael também ajuda a fornecer proteção à reexecução. Para ajudar a evitar ataques de repetição, é usado um novo contador de quadros no IEEE 802.11." **(SUPPORT MICROSOFT, 2005)**

No WPA também foi inserido um modelo para autenticação de usuários, conhecido como EAP (Extensible Authentication Protocol), que utiliza o padrão 802.11x e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital. Este padrão pode ser utilizado em conjunto com outras tecnologias existentes, como o servidor de autenticação RADIUS. **(SUPPORT MICROSOFT, 2005)**

Uma das vantagens em se utilizar equipamentos adicionais para a autenticação do usuário é de ter uma base centralizada, onde todos os métodos de acesso (não apenas wi-fi, mas cabeadas e/ou discadas também) utilizem a mesma forma, sem a necessidade de manter uma sincronização. **(SUPPORT MICROSOFT, 2005)**

Existem 3 participantes em uma transação usando o 802.1X:

- ***O suplicante*** - Um usuário ou um cliente que quer ser autenticado. Ele pode ser qualquer dispositivo sem fio.
- ***O servidor de autenticação*** - Um sistema de autenticação, tipo RADIUS, que faz a autenticação dos clientes autorizados.
- ***O autenticador*** - O dispositivo que age como um intermediário na transação, entre o suplicante e o servidor de autenticação. O ponto de acesso, na maioria dos casos.

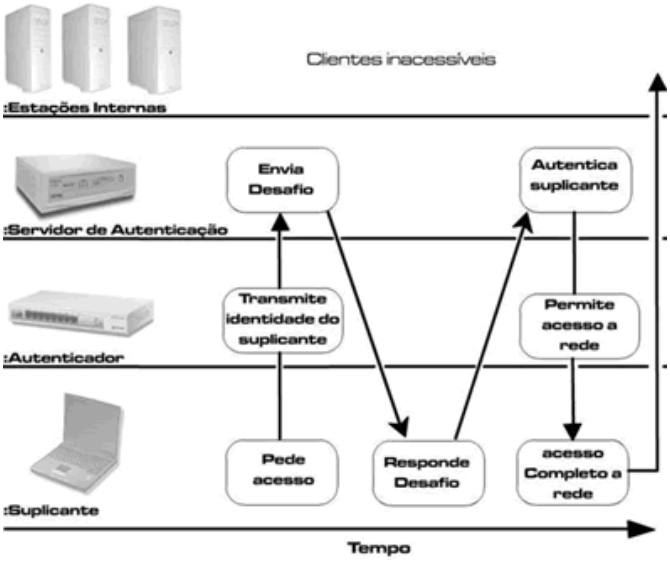

Figura 5: Simulação de acesso a uma rede sem fio. **Fonte: Lockabit (2003)**

Criptografia WPA2: De acordo com a publicação da Microsoft (2005) WPA2 é uma certificação de produto disponível por meio da Wi-Fi Alliance que certifica equipamentos sem fio como sendo compatíveis com o padrão 802.11i. O WPA2 oferece suporte aos recursos de segurança obrigatórios adicionais do padrão 802.11i que não estão incluídos em produtos que oferecem suporte ao WPA. Com o WPA2, a criptografia é realizada com o AES (Advanced Encryption Standard), que também substitui o WEP por um algoritmo de criptografia bem mais forte. Como o TKIP do WPA, o AES permite a descoberta de uma chave de criptografia de difusão ponto a ponto inicial exclusiva para cada autenticação, bem como a alteração sincronizada da chave de criptografia de difusão ponto a ponto para cada quadro.

Como as chaves AES são descobertas automaticamente, não há necessidade de se configurar uma chave de criptografia para o WPA2. O WPA2 é a modalidade de segurança sem fio mais forte.

Como talvez não seja possível agregar suporte AES por meio de uma atualização de firmware ao equipamento existente, o suporte a

AES é opcional e depende do suporte ao driver do fornecedor. **(MICROSOFT, 2005)**

5. Softwares Complementares

***Firewall*:** Segundo Luiz Carlos dos Santos, firewall é o mecanismo de segurança interposto entre a rede interna e a rede externa com a finalidade de liberar ou bloquear o acesso de computadores remotos aos serviços que são oferecidos em um perímetro ou dentro da rede corporativa. Este mecanismo de segurança pode ser baseado em hardware, software ou uma mistura dos dois.

A função do firewall é bloquear tráfego malicioso, que poderia colocar em risco os computadores da rede. Eles examinam o tráfego a fim de procurar por certos padrões ou se tem por alvo recursos vulneráveis. O trafego que possui os padrões definidos são descartados para que não cheguem ao seu destino final. **(ENGST & FLEISHMAN, 2005)**

A maioria dos Gateways (access point) oferece recursos de firewall que permitem filtrar tipos específicos de tráfego, como aquele destinado a um dado serviço Internet. A maioria desses firewalls é simples, permitindo limitar todo o tráfego que entra que não seja uma resposta a uma solicitação feita ou a serviços Internet específicos, como FTP.

Como boa parte dos gateways também inclui múltiplas portas Ethernet, você pode criar um firewall não apenas entre sua conexão Internet de banda larga - conectada à porta de rede remota - e seus computadores e dispositivos sem fio, mas também entre a rede sem fio e quaisquer máquinas conectadas a portas Ethernet da rede local (LAN) no gateway". **(ENGST & FLEISHMAN, 2005)**

Monitoramento da Rede Wi-Fi

Da mesma forma que muitos administradores monitoram o seu ambiente de rede convencional (com o uso de IDSs, por exemplo), a monitoração da rede wireless também é importante. Essa monitoração pode detectar:

- Clientes conectados em um dado instante (em horários improváveis ou simplesmente para acompanhamento);
- Instalação de APs não autorizados;
- Dispositivos que não estejam usando WEP;
- Ataques contra os clientes wireless;
- Acessos não autorizados;
- Mudanças de endereços MAC;
- Mudanças de canal;
- DoS. (CERT, 2003)

6. Métodos de Acesso Seguros

VPN: Virtual Private Network ou Rede Privada Virtual é uma rede privada construída sobre a infra-estrutura de uma rede pública, normalmente a Internet.

O sigilo do tráfego da rede, a autenticação inicial dos usuários, a integridade das mensagens da rede sem fio serão garantidos através da implementação de uma VPN segura, para tanto utiliza-se do protocolo IPSec a fim de garantir a privacidade virtual da rede e a segurança das eletrôncias que por ela passam.

Nesta arquitetura todo o tráfego entre as estações e o AP é encriptado independente do destino dos pacotes enviados pelas estações. A VPN poderia ser configurada de forma que somente alguns pacotes com endereços de destino definidos fossem encriptados.

O servidor VPN pode se tornar um gargalo. Todo o acesso do cliente WLAN será canalizado pelo servidor. Os dispositivos VPN tradicionalmente atendem muitos clientes remotos de baixa velocidade. Ser solicitado a controlar a taxa de transferência de um grande número de clientes que funcionam na velocidade total da LAN significará que muitos dispositivos VPN não conseguirão atender mais de poucas dezenas ou centenas de clientes. **(MICROSOFT, 2004)**

O foco deste trabalho se prende a estudar métodos e processos que tornam uma comunicação sem fio no padrão IEEE 802.11. Uma VPN pode ser usada para qualquer tipo de meio de transmissão de dados (redes cabeadas, wi-fi, infravermelho, etc), portanto, para proteger as informações de uma rede wi-fi recomenda-se que se utilize dos protocolos de criptografia específicos para este tipo de rede (WEP ou WPA), pois possuem um determinado nível de segurança e não causam tanto impacto a performance da rede quanto uma VPN causa.

RADIUS: O primeiro passo é realizado pelo usuário que deseja acessar a rede, encaminhando uma mensagem contendo seu login e senha para o cliente RADIU4S (Remote Authentication Dial-In User Server).

Ao receber a mensagem do usuário o cliente RADIUS gera uma requisição contendo os dados do usuário, encaminhando-a para o servidor RADIUS. Uma mensagem de resposta é aguarda por um determinado tempo, porém caso essa mensagem não chegue, o cliente poderá encaminhar uma nova requisição para o mesmo servidor ou para um servidor RADIUS alternativo.

Quando recebe uma requisição a primeira ação do servidor é validar o cliente RADIUS o qual encaminhou a mensagem de requisição, evitando dessa forma que um "falso" cliente consiga realizar alguma operação. Tratando-se de um cliente válido, os dados referentes ao usuário, encaminhados na requisição, serão verificados. Não apenas seu login e senha, mas também a porta através da qual o usuário entrou em contato com o cliente RADIUS será validada.

Após validar as informações a respeito do usuário o servidor RADIUS encaminha uma resposta para o cliente, negando o acesso caso as informações não sejam válidas, ou permitindo o acesso a rede caso contrário. Quando o servidor permite o acesso encaminha junto a resposta enviada ao cliente, os direitos e permissões referentes ao tipo/nível de acesso permitido ao usuário em questão. **(ALBUQUERQUE, 2003)**

7. Conclusão

Este trabalho conclui que as rede wireless proporciona facilidade de instalção e maior mobiliade e conforto para seus usuários,e empresas que buscam um diferencial e conforto em seu trabalho.

Possui uma grande flexibilidade pra instalação reduzindo os custos com cabos, e de fácil configuração em qualquer escritório.

E como demonstramos nesse artigo as redes wireless assim como as outras requer uma proteção e um nível de segurança para que bem estruturada e monitorada funcione de uma forma segura, e os dados de seus usuários em sigilo absoluto. Usuários de rede sem fio se prevenindo com os métodos de segurança para essas redes podem assim garantir sua integridade sem nenhuma preocupação e mostrar de que a tecnologia wireless é segura.

Usando os métodos ja explicados e considerando as orientações do fabricante é possível se obter um bom nível de segurança, respeitando as limitações técnicas e econômicas de cada usuário.

8. Bibliográfia

ABDO, JOSÉ MÁRIO MIRANDA. Agência Nacional de Energia Elétrica. Disponível em http://www.aneel.gov.br, de 2006.

FRANCO, EDGARD. Engecomp Tecnologia em Automação e Controle LTDA. Disponível em: http://www.engecomp.com.br/pow_qual.htm. Acesso em 2006.

GUERRINI, IRIA MÜLLER. Setor de Física da Universidade de São Paulo. Disponível em física.cdcc.sc.usp.br/olimpíadas/01/artigo/fontes_elétricas.htm/, de 24/08/2001.

INEE. Instituto Nacional de Eficiência Energética. Disponível em http://www.inee.org.br/ forum_sobre_gd cg.asp, de 2005.

KELMAN, JERSON. Agência Nacional de Energia Elétrica. Disponível em http://www.aneel.gov.br, de 2006.

MME. Ministério de Minas e Energia. Disponível em http://www.mme.gov.br/site/select_main_menu_item.do. Ano base 2004.

SILVEIRA, JOSÉ LUIZ. Revista Eletrônica de Jornalismo Científico. Disponível em http://www.comciencia.br/reportagens/energiaeletrica/energia13.htm, de 10/07/2001.

BALIEIRO, Silva. Na Rua Com As Redes Sem Fio. São Paulo. INFO Exame, ano 19, n° 218, pp.: 46-48. Maio/2004.

CARDOSO, Rogério. WLANS São Inseguras?. Disponível em: http://www.ciscoredacaovirtual.com/redacao/perfistecnologicos/conectividad.asp?Id=24 .

CARRIÓN, Demetrio de Souza Diaz. Implementação De Um Ponto De Acesso Seguro Para Redes 802.11b Baseado No Sistema Operacional OPENBSD. Trabalho de Conclusão do Curso de Engenharia Elétrica, Universidade Federal do Rio de Janeiro. 2003. Disponível em: http://www.ravel.ufrj.br/arquivosPublicacoes/demetrio_projfinal.pdf .

DUARTE, Luiz Otávio. Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x. Trabalho de Conclusão do Curso de Bacharel em Ciência da Computação. UNESP São José do Rio Preto. 2003. Disponível

em:
http://www.apostilando.com/download.php?cod=230&categoria=Redes .

MICROSOFT. Decisão sobre uma Estratégia de Rede sem Fio Protegida. 2004. Disponível em: http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx .

MICROSOFT. Usando o 802.1X e a Criptografia Para Proteger WLANs. Disponível em: http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod172.mspx .

MICROSOFT. Visão Geral da Atualização de Segurança WPA Sem Fio no Windows XP. 2005. Disponível em: http://support.microsoft.com/kb/815485/pt-br .

PRADO, Eduardo. Segurança em WLAN. 2004. Disponível em: http://www.wirelessbrasil.org/eduardo_prado/wifi_bible/seguranca.html .

RUFINO, **Nelson Murilo de Oliveira**. Segurança de Redes Sem Fio. 1ª ed. São Paulo: Ed.: Novatec, 2005.

SANTOS, Luiz Carlos. Como funciona a VPN?. 2001. Disponível em: http://www.clubedasredes.eti.br/rede0004.htm.

SANTOS, Luiz Carlos. Uma Combinação Ideal, DSL/Cable Modem e WLAN. 2003. Disponível em: http://www.clubedasredes.eti.br/hard0007.htm .

SYMANTEC. Implementando Uma LAN Sem Fio Segura. 2003. Disponível em: http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html .

TEIXEIRA, Edson Rodrigues Duffles. Tutoriais: Banda larga e VOIP. 2005. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp .

VERÍSSIMO, Fernando. O Problema de Segurança em Redes Baseadas no Padrão 802.11. 2003. Disponível em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=82 .