Iêda Paula de Farias Teixeira

Maria das Graças Maciel Silva

SEGURANÇA EM REDES SEM FIO

Olho d’ Água das Flores-AL , Novembro de 2012.

Iêda Paula de Farias Teixeira

Maria das Graças Maciel Silva

SEGURANÇA EM REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Instituto de Computação, sob a orientação do professor Breno Jacinto Duarte da Costa e co-orientação do professor Marcus de Melo Braga.

INSTITUTO DE COMPUTAÇÃO- IC
UNIVERSIDADE FEDERAL DE ALAGOAS - UFAL
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Olho d' Água das Flores- AL, Novembro de 2012.

Iêda Paula de Farias Teixeira

Maria das Graças Maciel Silva

A comissão examinadora abaixo aprova e assina a monografia.

SEGURANÇA EM REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Instituto de Computação, sob a orientação do professor Breno Jacinto Duarte da Costa e co-orientação do professor Marcus de Melo Braga.

Olho d' Água das Flores- AL, Novembro de 2012.

Banca Examinadora:

_____

Prof. Marcus de Melo Braga

_____

Prof. Edmilson Fialho

_____

Profa. Leide Jane de Sá Araújo

RESUMO

As redes sem fio tornam-se, a cada dia, mais populares. A conveniência de sua utilização em lugares como conferências, aeroportos e hotéis, shopping Center é inegável, oferecendo, também, serviços através da internet que podem ser utilizados através de laptops, PDAs e smartphones. Como acontece com toda tecnologia recente, muitos usuários estão mais interessados na novidade da tecnologia do que nas suas reais vantagens. Com toda essa inovação e comodidade surgem preocupações de segurança com a adoção dessa nova tecnologia. Constatam-se basicamente dois tipos de reação principais, por parte dos administradores de rede, com relação a redes sem fio: a não-adoção, por receio das implicações de segurança que tal procedimento possa ocasionar à rede; ou a adoção impulsiva, sem compreender a tecnologia, os riscos e as medidas de segurança recomendáveis. É fundamental que o administrador de redes ou usuário doméstico entenda as implicações de segurança de cada escolha tomada. Da mesma forma que nas redes cabeadas, os riscos das redes sem fio precisam ser conhecidos para serem minimizados por meio do entendimento das soluções disponíveis e da aplicação de boas práticas. Essas decisões envolvem não apenas questões de configuração, mas também de planejamento, tanto de projeto como de compra de equipamentos que tenham certas características desejáveis. Este é o foco desta monografia, que aborda as fragilidades, os possíveis ataques e algumas estratégias para combatê-los, através de diversas técnicas de defesa, que incluem não apenas tecnologia, mas também ações proativas por parte do administrador.

Palavras-chave: Internet, rede sem fio, planejamento, segurança.

ABSTRACT

The advance of the wireless networking becomes more popular each day. The convenience of its use in places as conferences, airports, hotels and shopping centers is unquestionable, by offering services in the World Wide Web that can be used through laptops, PDAs and smartphones. As it usually occurs with all recent technology, many users are more interested in the newness of the technology, rather than in its real advantages. Besides the newness and facilities, certainly many worries arise concerning the security in adopting a new technology. Basically, two types of reactions are evidenced by the net administrators, with respect to wireless networking: the no-adoption for fear of safety's implications that such procedure can cause to the net; or the impulsive adoption, without understanding the technology, the risks and the advisable measures of safety. It is essential, that the networking administrator or home user understands the implications of safety for any taken choice. As in the traditional networking, the risks of the wireless networking needs to be known, so they could be minimized by means of understanding all available solutions and good practices. These decisions not only involve questions of configuration, but also on planning the project and purchasing equipments with desirable characteristics. This is the main focus of this monograph, that shows the fragilities and the existing attacks and how to deal with them, using several techniques of defenses, that not only includes technology, but also proactive actions by the net administrator.

Key words: Internet, wireless networking, planning, security.

ÍNDICE DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Em se tratando de segurança da informação é sempre importante lembrar que tais atividades abrangem um conjunto de medidas que envolvem, entre outros fatores, procedimentos técnicos. Porém, há ainda diversas atividades que envolvem outros tipos de procedimentos, tais como medidas cautelares de classificação de material, descarte de documentos, cópias de segurança, treinamento e educação do usuário, princípios éticos dos administradores, segurança física, políticas de segurança, entre outros. Os temas que serão aqui abordados correspondem a uma pequena parte de segurança da informação, concentrando-se apenas na parte técnica da questão.

Redes sem fio é algo novo na vida da maioria das pessoas, e diferentemente das redes cabeadas, onde era necessário conhecimento técnico um pouco mais específico, a montagem e instalação de redes Wi-Fi são absolutamente factíveis por um usuário iniciante. Toda essa simplicidade de instalação tem feito com que muitas redes sem fio sejam montadas com padrões de fábrica, ou seja, completamente expostas a vários tipos de ataques.

O objetivo geral desta monografia é proporcionar uma visão abrangente das características e peculiaridades de redes sem fio, mas também permitir entendimento das vulnerabilidades comuns associadas à tecnologia, seus riscos e a sua utilização com maior segurança. Tendo como objetivos específicos: Prover segurança para usuário de rede sem fio e Aumentar o uso de práticas de segurança.

A monografia é composta de cinco capítulos. O primeiro capítulo descreve o surgimento da tecnologia Wi-Fi; no segundo apresenta-se a tecnologia Wireless; no terceiro capítulo abordam-se os riscos, as ameaças e as técnicas de ataque às redes sem fio; no quarto capítulo discutem-se os métodos de defesa; no quinto capítulo apresenta-se um estudo de caso, cenário doméstico/pequena empresa, este que servirá de base para trabalhos futuros e,

finalmente, na conclusão, são apresentadas as considerações finais e sugestões para trabalhos futuros.

CAPÍTULO I

O NASCIMENTO DA TECNOLOGIA WI-FI

1.1 Histórico da tecnologia Wi-Fi

Os primórdios das comunicações sem fio datam do início do século XIX, numa época quando Guglielmo Marconi, "O Pai do Rádio", deixou a sua marca no mundo das tecnologias sem fios. Por volta de 1894, Marconi começou a fazer testes com ondas rádio (Ondas Hertzianas). O seu objetivo era o de produzir e detectar ondas rádio de longa distância. Em 1896, Marconi conseguiu e obteve a patente criando a primeira fabrica de rádios no mundo, a Wireless Telegraph and Signal Company Limited. Em 1901, foram recebidos sinais do outro lado do atlântico e em 1905 o primeiro sinal de socorro sem fios foi enviado usando o famoso Código Morse [COR 07]. A tecnologia sem fios progrediu eventualmente como uma ferramenta valiosa, ao ser utilizada pelo exército norte-americano durante a 2ª Guerra Mundial, quando o exército começou a enviar planos de batalha sob as linhas do inimigo e quando os navios da Marinha enviavam instruções para as suas frotas de costa a costa.

A idéia constituída por Hedy Lamarr que recebeu a patente de nº 2.292.387 dos EUA, em 11/08/1942. Sobre a criação do Spread Spectrum (espectro espalhado) "Não importava que os navios inimigos executassem manobras evasivas, uma vez que ainda assim lhes conseguiria acertar, a não ser que o inimigo conseguisse perturbar o sinal de controle" [FOR 04]. Com isso Lamarr pensou na possibilidade de fazer com que o transmissor e o receptor usassem várias freqüências de rádio, alternando entre elas várias vezes por segundo.

Esta era, sem sombra de dúvida, uma idéia brilhante, mas bastante à frente do seu tempo, considerando que o sistema de controle que Lamarr havia projetado era demasiadamente complexo e arrojado para tal época. O aparecimento dos transistores (componentes eletrônicos que fazem a amplificação e o chaveamento de sinais elétricos) tornou a idéia de Lamarr mais prática, "e mais tarde o projeto de Lamarr foi utilizado nas comunicações militares durante o bloqueio naval a Cuba em 1962", sendo ainda utilizado nos dias de hoje [FOR 04].

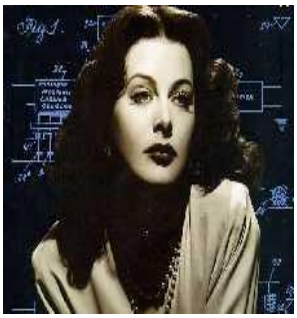

Fig. 1.1 - Guglielmo Marconi **Fig.1.2** - Hedy Lamarr
Fontes: http://media-2.web.britannica.com/eb-media/20/2320-004-F984545E.jpg
http://www.rfid-weblog.com/archives/hedy%20lamarr.jpg

A norma original, IEEE 802.11 Wi-Fi, define duas formas de Spread Spectrum. A primeira trata-se do FHSS (Frequency Hopping Spread Spectrum), que funciona do modo que Lamarr havia idealizado, com um transmissor e um receptor alternando rapidamente entre várias freqüências [FOR 04].

1.2 O surgimento da 1ª geração Wireless e das redes sem fio

"O trabalho com sistemas comercias começou em 1980, quando o órgão regulador de telecomunicações dos EUA (*FCC – Federal Communications Commission*) autorizou o uso de três faixas de rádio-freqüência (RF) para finalidades industriais, científicas e médicas"

[MAI 03]. A partir daí houve um interesse na tecnologia e começaram a surgir sistemas de comunicação, tais como: telefone sem fio, bips, celulares, etc.

Os sistemas de telecomunicação móvel (celulares) surgiram no final da década de 70. Junto a esses sistemas surgiu a primeira geração Wireless (sem fio). Nessa geração os sistemas de telecomunicação móvel usavam sinais analógicos (sinais que variam continuamente com o tempo) para transmissão.

Fig.1.3 - Sistemas de telecomunicação móvel
Fontes: bp1.blogger.com/.../s400/motorola+analógico.jpg
www.aboutlife.com/files/pager.jpg

1.3 O surgimento da 2ª geração Wireless

O Surgimento da segunda geração Wireless surgiu no início da década de 90. Nessa geração começou a se utilizar a codificação digital (o sinal digital é caracterizado pela presença de pulsos, nos quais a amplitude da onda é fixa, ou seja, a altura ou crista da onda tem tamanho fixo). Os celulares digitais eram usados, principalmente para comunicação de voz, mas alguns serviços de mensagens já começavam a ser desenvolvidos, como por exemplo, SMS (*Short Messaging Service*).

Já as redes sem fio começavam a receber mais atenção. Padrões começaram a ser desenvolvidos e equipamentos para transmissão digital começaram a se tornar disponíveis no mercado, mas a efetiva implantação das redes sem fio ainda estava restrita às áreas onde a conexão tradicional configurava-se inviável.

Conforme Maia:

> Hoje vivemos na metade da segunda geração Wireless (2.5G), e a impressão de que a tecnologia Wi-Fi é novidade, deve-se ao fato de que só agora ela vem se tornando viável e vem ganhando mercado. Além disso, está havendo um grande investimento no desenvolvimento de novos produtos, melhoria e otimização dos existentes para serem aplicados na próxima geração [MAI 03].

1.4 A 3ª geração Wireless

A terceira geração Wireless está em funcionamento desde 2002, e tem como objetivo fornecer serviços de áudio e vídeo de alta qualidade e total liberdade de movimentação do usuário. O 3G significa "terceira geração" de tecnologia de comunicação sem fio. Refere-se a aperfeiçoamentos pendentes na comunicação wireless de dados e voz através de qualquer um dos vários padrões propostos. A comunicação wireless proporcionará qualidade de voz superior e serviços de dados que suportam conteúdo de vídeo e multimídia enviado sem fio a laptops, handhelds e smartphones.

1.5 A geração wireless de alta velocidade (3G)

Alguns especialistas consideram a atual comunicação wireless ainda lenta demais. À medida que aumenta o número de dispositivos *handhelds* em wireless projetados para acessar a Internet, cresce também a necessidade de tecnologias mais velozes e mais eficientes de comunicação sem fio. O objetivo imediato é aumentar a velocidade de transmissão de 9,5 Kbps para 2 Mbps.

“A importância da 3G para a corporação é clara", afirma o analista Craig Mathias, do The Farpoint Group. "3G significa que tudo que as linhas terrestres podem fazer, wireless também pode" [COM 08]. Com um potencial tão grandioso, diz Mathias, as

empresas deveriam começar a planejar como a tecnologia sem fio influenciará seus mundos.

CAPÍTULO II

REDES SEM FIO – WIRELESS

2.1 Conceitos de Wireless

"Wireless pode ser entendido como a transmissão de voz e dados através de ondas de rádio, luz ou outro meio que dispense o cabeamento convencional, ou seja, a comunicação sem fio" [PIN 05]. "Nas redes sem fio (Wireless Networks) os pacotes são transmitidos, "através do ar", em canais de freqüência de rádio (freqüências na faixa de KHz até GHz) ou infravermelho (freqüências da ordem THz)" [SOA 95]. Dentro deste modelo de comunicação enquadram-se várias tecnologias, como Wi-Fi, Infrared (infravermelho), Bluetooth (padrão sem fio para redes pessoais de curto alcance criado pela Ericsson em meados da década de 90) e Wi-Max (conexão sem fio de alta velocidade que permite um alcance de até 48 km). O controle remoto da televisão ou do aparelho de som, o celular e uma infinidade de aparelhos trabalham com conexões sem fio. Podemos dizer, como exemplo lúcido, que durante uma conversa entre duas pessoas, temos uma conexão wireless, partindo do principio de que sua voz não utiliza cabos para chegar até o receptor da mensagem.

As redes sem fio trazem como benefícios uma maior flexibilidade e mobilidade, uma vez que as pessoas não ficam mais presas as suas mesas, podendo se movimentar facilmente, sem se desconectar da rede. Outro benefício, é que a tecnologia Wi-Fi permite conexões mais rápidas e estáveis.

2.2 O crescimento do uso das redes sem fio

Com o grande crescimento do uso das redes sem fio no Brasil, “que vem ganhando força na versão IEEE802.11b, 802.11a ou 802.11g, utilizando freqüência de 2.4GHz e velocidade de até 11Mbps” [3EL 04], muitas pessoas e empresas vêm aderindo a este tipo de rede diariamente, pois existe a possibilidade de abolir a utilização de cabos. Nos últimos anos, houve rápido crescimento no uso de laptops acompanhado de rápido desenvolvimento da tecnologia de redes em fio [SHE 08]. Com isso, tornou-se tecnológica e financeiramente viável a criação de redes sem fio (wireless) de acesso público à internet.

A utilização das redes sem fio vem crescendo cada vez mais devido à facilidade de fazer a sua montagem (não precisando ter conhecimentos técnicos mais específicos sobre os equipamentos), mas principalmente pela estabilidade e rapidez da conexão. Outro atrativo é a facilidade de deslocamento, graças a não utilização de cabos.

2.3 Tipos de redes sem fio

Para as redes sem fio existem vários tipos, relacionados a seguir [SIL 98]: redes locais sem fio (WLAN – Wireless Local Area Network), redes metropolitanas sem fio (WMAN – Wireless Metropolitan Area Network), redes de longa distância sem fio (WWAN – Wireless Wide Area Network), circuito local sem fio (WLL – Wireless Local Loop) e o novo conceito de redes pessoais sem fio (WPAN – Wireless Personal Area Network).

2.4 Aplicações das redes sem fio

As aplicações estão divididas em dois tipos: Indoor e Outdoor. Se a rede precisa de uma comunicação entre dois prédios é usada uma aplicação Outdoor. No caso de uma aplicação Indoor a comunicação ocorre dentro do mesmo prédio. O mais utilizado são as aplicações Indoor, como é o caso do Hospital do Coração em São Paulo (HCor), onde os médicos possuem equipamentos móveis com acesso Wi-Fi.

No ambiente corporativo existem diversas aplicações possíveis para as redes sem fio, assim como qualquer outra tecnologia tem seu lugar dentro da infra-estrutura das redes locais. Entretanto, como todo projeto de rede deve apresentar seus benefícios, torna-se necessário justificar sua utilização. A seguir estão alguns exemplos de quando é justificável disponibilizar as redes sem fio em lugar de uma rede estruturada:

- Locais onde não é possível instalar o cabeamento convencional, como prédios tombados pelo patrimônio histórico, por exemplo;
- Aplicações que envolvam soluções de software mais computadores portáveis como coletores de dados, leitores RFID ou códigos de barra;
- Acesso a internet em locais públicos, como hotspots, Wi-Fi, por exemplo.

O principal ponto é verificar a dimensão necessária para cada solução de rede disponível e, dependendo dos custos das soluções selecionadas, é que poderemos considerar as possibilidades de combinação de tecnologias para a aquisição dos equipamentos necessários.

2.5 Redes locais sem fio (WLAN)

Os sistemas de redes locais sem fio utilizam rádio-freqüência porque as ondas de rádio têm grande poder de penetração. O alcance ou raio de cobertura de sistemas WLAN característicos chega a 200 metros, dependendo do número e do tipo de obstáculos encontrados [ART 10].

Através da utilização de rádio-freqüência ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas. Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza em uma freqüência específica e rejeita as outras portadoras de freqüências diferentes.

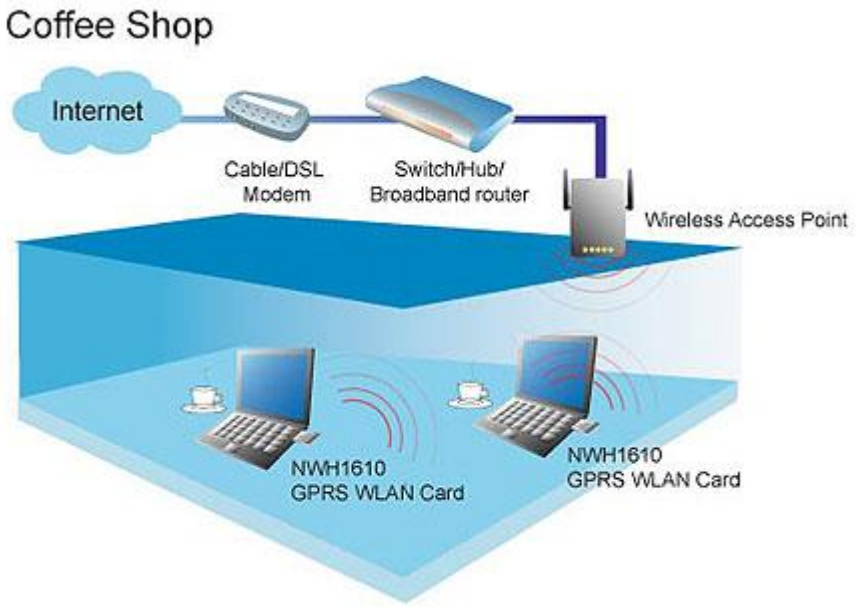

Fig.2.1 - Rede local sem fio (WLAN)
Fonte: http://www.ndclan.com/Products/images/nwh1610-2.jpg

2.6 Tecnologia das redes sem fio

Existem várias tecnologias envolvidas nas redes sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. A seguir são relacionadas algumas das mais empregadas.

2.6.1 Sistemas Narrowband

"Os Sistemas Narrowband (banda estreita) operam em uma freqüência de rádio específica, mantendo o sinal de rádio o mais estreito possível, o suficiente para passar as informações" [SIL 98]. O Crosstalk (interferência elétrica gerada por um campo eletromagnético próximo a outro) é indesejável entre os vários canais de comunicação, pode ser evitado coordenando cuidadosamente os diferentes usuários nos diferentes canais de freqüência.

2.6.2 Spread Spectrum

Esse tipo de tecnologia, originalmente desenvolvida para uso militar, distribui o sinal através de toda a faixa de freqüência de maneira uniforme. Consome mais banda, porém garante maior integridade ao tráfego das informações e está muito menos sujeita a ruídos e interferências que outras tecnologias que utilizam freqüência fixa predeterminada, já que a presença de ruído em uma determinada freqüência irá afetar apenas a transmissão nessa freqüência, e não a faixa inteira [RUF 05]. Desta maneira, o sinal necessitaria ser retransmitido somente quando se fizer uso daquela freqüência. Pelo fato de preencher toda a faixa, o sinal pode ser facilmente detectado, mas se o receptor não conhecer o padrão de

alteração da freqüência, tudo que receber será entendido como ruído. A maioria dos padrões para comunicação, nas redes sem fio, utiliza essa tecnologia.

Com base nos dados de Rufino existem dois tipos de Spread Spectrum, são eles: DSSS (Direct Sequence Spread Spectrum), que é o mais utilizado, e o FHSS (Frequency Hopping Spread Spectrum).

2.6.2.1 Direct Sequence Spread Spectrum (DSSS)

DSSS (Direct Sequence Spread Spectrum) – Utilizado no padrão IEEE 802.11b, o DSSS utiliza uma técnica denominada Code Chips, "que consiste em separar cada bit de dados em 11 subbits, que são enviados de forma redundante por um mesmo canal em diferentes freqüências, e a banda 2,4GHz é dividida em três canais" [RUF 05]. Essa característica torna o DSSS mais susceptível a ataques diretos em uma freqüência fixa e a ruídos que ocupem parte da banda utilizada.

2.6.2.2 Frequency Hopping Spread Spectrum (FHSS)

FHSS (Frequency Hopping Spread Spectrum) – Neste modelo, a banda 2,4GHz é dividida em 75 canais e o transmissor e receptor são sincronizados por saltos de canal em uma seqüência pseudo-aleatória pré-determinada. O FHSS comuta as freqüências de algumas vezes por segundo a milhares de vezes por segundo, dependendo do padrão conhecido pelo transmissor e receptor [RUF 05]. O sinal é recebido por quem conhece a seqüência de saltos e aparece como ruído para outros possíveis receptores.

2.7 Configurações das redes sem fio

As redes sem fio podem ser configuradas através de dois métodos. Um deles é a configuração *Ad-Hoc Mode – Independent Basic Service Set* (IBSS), e o outro é a configuração *Infrastructure Mode - Infrastructure Basic Service Set*.

2.7.1 Ad-Hoc Mode – Independent Basic Service Set (IBSS)

São "compostas por estações independentes, sendo criadas de maneira espontânea, por estes dispositivos. Este tipo de rede se caracteriza pela topologia altamente variável, existência por um período de tempo determinado e baixa abrangência" [PIN 04]. "Estas são redes sem topologia definida, cujos nós são móveis e comunicam-se através de canais de rádio" [GRA 04]. A comunicação entre as estações de trabalho é estabelecida diretamente, sem a necessidade de um AP (*Access Point* – ponto de acesso) e de uma rede física para conectar as estações. Essa rede também é conhecida como uma rede sem fio Ad-hoc.

2.7.2 Infrastructure Mode – Basic Service Set (BSS)

"Uma Rede BSS consiste de um simples *Access Point* (AP) que suporta um ou mais clientes sem fio. Nessa rede, todas as estações comunicam-se entre si através de um AP. Esse tipo de rede tem o inconveniente de consumir o dobro de banda. Mas um dos seus grandes benefícios é o armazenamento dos dados enquanto as estações estão em modo de economia de energia (Power Save). A rede possui pontos de acesso (APs) fixos que conectam a rede sem fio à rede convencional e estabelecem a comunicação entre os diversos clientes da rede" [CAB 12].

2.8 Arquitetura para redes sem fio

A arquitetura adotada pelo projeto IEEE 802.11 (*Institute of Electrical and Electronic Engineers*) para redes sem fio baseia-se na divisão da área coberta pela rede em células. As células são chamadas BSA (*Basic Service Area*). "Um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA, constitui um BSS (Basic Service Set)" [SOA 95].

O tamanho da BSA depende das características e do alcance do sinal dos transmissores/receptores usados nas estações. Para permitir a construção de redes cobrindo áreas maiores que uma célula, múltiplas BSAs são interligadas através de um sistema de distribuição (que pode ser uma rede baseada em outro meio de transmissão, por exemplo, fios metálicos ou fibra óptica) via Access Points (APs). Os APs são estações especiais responsáveis pela captura das transmissões realizadas pelas estações de sua BSA, destinadas às estações localizadas em outras BSAs, retransmitindo-as, usando o sistema de distribuição (*DS – Distribution System*).

"Os BSAs interligados por um sistema de distribuição através de APs definem uma ESA (*Extended Service Area*)" [SOA 95]. O conjunto de estações formado pela união dos vários BSSs conectados por um sistema de distribuição define um ESS (*Extended Service Set*). Cada ESS é identificado por um BSS-ID. Esses dois identificadores formam o Network-ID de uma rede sem fio IEEE 802.11.

> Um ESS formado pela interconexão de múltiplos BSSs constitui uma rede local sem fio com infra-estrutura. A infra-estrutura consiste nas estações especiais denominadas pontos de acesso, e no sistema de distribuição que interliga os pontos de acesso. O sistema de distribuição, além de interligar os vários APs, pode fornecer os recursos necessários para interligar a rede sem fio a outras redes [SOA 95].

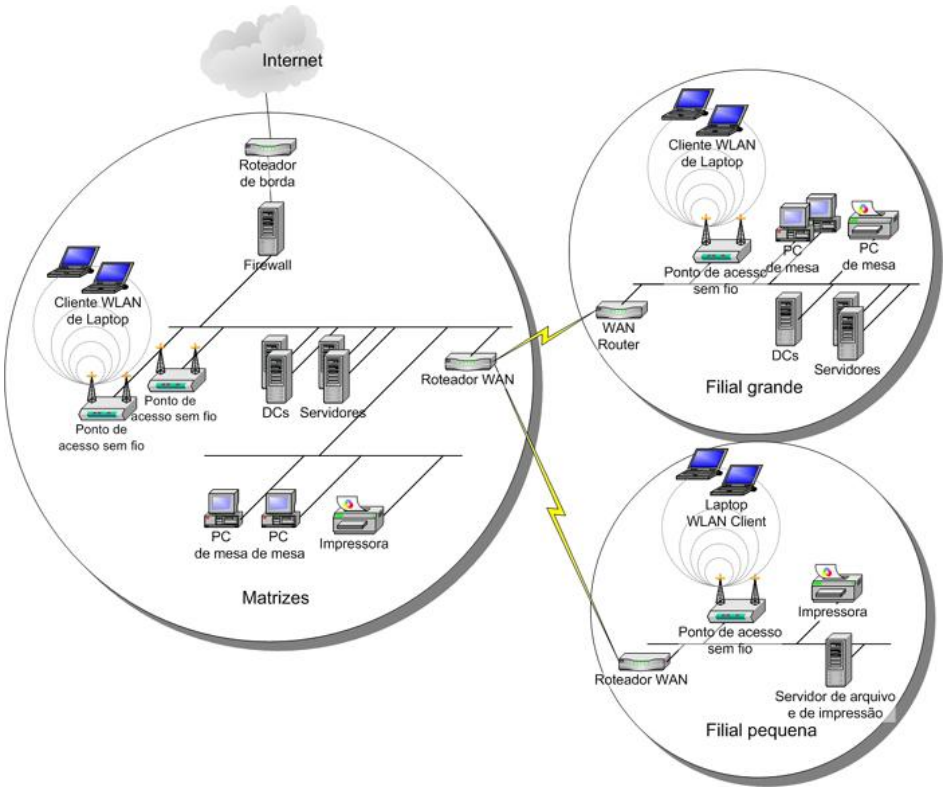

Fig.2.2 - Rede sem fio com infra-estrutura
Fonte: http://www.microsoft.com/brasil/security/guidance/topics/wireless/images%5CSGFG17104.jpg

2.9 Padrões para redes sem fio

Quando se discute a configuração de uma WLAN existem alguns padrões desenvolvidos ou em desenvolvimento que devem ser considerados [RUF 05]:

IEEE 802.11: é o primeiro padrão firmado para redes sem fio. Apresenta suporte ao WEP e sistema de rádio na banda ISM (*Industrial Scientifical Medical*) de 900 MHz.

IEEE 802.11a: é o padrão para redes sem fio que atua na banda ISM de 5GHz e provê taxas de transferência até 54 Mbps, porém a freqüência superior significa um alcance menor. Apesar de ter sido firmado em 1999 não existem muitos dispositivos que atuam nesta freqüência.

IEEE 802.11b: padrão dos produtos WLAN mais comuns no Brasil atualmente, incluindo aspectos de sistema de rádio e também especificação de segurança utilizando o protocolo WEP. Trabalha na banda ISM de 2.4 GHz e provê taxas de transferência até 11 Mbps. Foi aprovado em julho de 2003 pelo IEEE.

IEEE 802.11g: padrão para redes sem fio compatível com o IEEE 802.11b. Atua na banda ISM de 2.4 GHz e provê taxas de transferências até 54 Mbps.

IEEE 802.11e: fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e o 802.11a. Os melhoramentos incluem capacidade multimídia possibilitada com a adesão da funcionalidade de qualidade de serviços (*QoS – Quality of Service),* como também melhoramentos em aspectos de segurança. O que significa isto aos ISP's? Isto significa a habilidade de oferecer vídeo e áudio sob demanda (on demand), serviços de acesso de alta velocidade a Internet e Voz sobre IP (*VoIP – Voice over Internet Protocol).* O que significa isto ao cliente final? Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

Grupos do IEEE que estão desenvolvendo outros protocolos [MAN 06]:

Grupo 802.11d – Está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O protocolo 802.11 só define operações WLAN em alguns países).

Grupo 802.11f – Está a desenvolver o *Inter-Access Point Protocol* (Protocolo de acesso entre pontos), por causa da atual limitação de proibir *roaming* entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.

Grupo 802.11g – Estão trabalhando para conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.

Grupo 802.11h – Está em desenvolvimento do espectro e gestão de extensões de potência para o 802.11a do IEEE para ser utilizado na Europa.

O comitê 802 do IEEE tem os seguintes grupos de trabalho ativos trabalhando na elaboração de normas de redes sem fio (Wireless):

- 802.11 *Wireless LAN* (WLAN) WIFI
- 802.15 *Wireless Personal Area Network* (WPAN) Bluetooth entre outros.
- 802.16 *Broadband Wireless Access* (BBWA) WiMax
- 802.20 *Mobile Wireless Access* Mobile - Fi

2.10 Topologias das redes sem fio

A topologia das redes sem fio é composta por [RUF 05]:

- BSS (Basic Service Set) – Corresponde a uma célula de comunicação da rede sem fio;

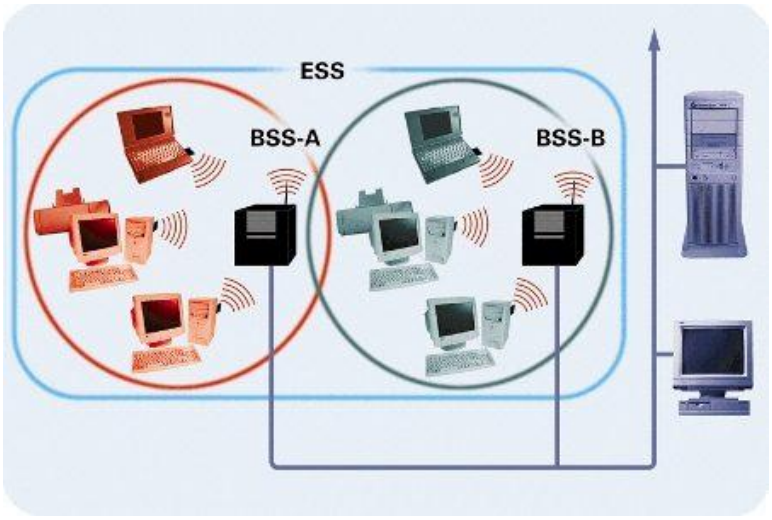

Fig.2.3 - BSS (Basic Service Set)
Fonte: http://www.vivasemfio.com/blog_images/bss_ess_architecture.jpg

- STA (Wireless Lan Stations) – Representa os diversos clientes da rede;

Fig.2.4 - STA (Wireless Lan Stations)
Fonte: http://www.gdzsqy.com/syssite/home/shop/1/pictures/productsimg/small/163.jpg

- AP (*Access Point*) – É o nó que coordena a comunicação entre os clientes dentro da célula. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional;

Fig.2.5 - AP (Access Point)
Fonte: http://www.ahead-computers.com/images
/MICD/normal/networking/wireless/netdlidwlg2100ap.jpg

- DS (*Distribution System*) – Corresponde ao Backbone da WLAN, realizando a comunicação entre os APs;

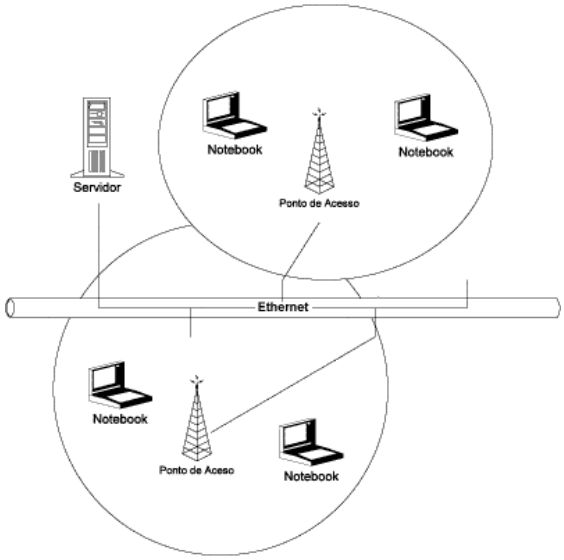

Fig.2.6 - DS (*Distribution System*)
Fonte: http://img507.imageshack.us/img507/2734/wirelessredeby5.gif

- ESS (*Extended Service Set*) – É o conjunto de células cujos APs estão conectados a uma mesma rede convencional. Nestas condições um cliente (STA) pode se movimentar de uma célula para outra, permanecendo conectado à rede.

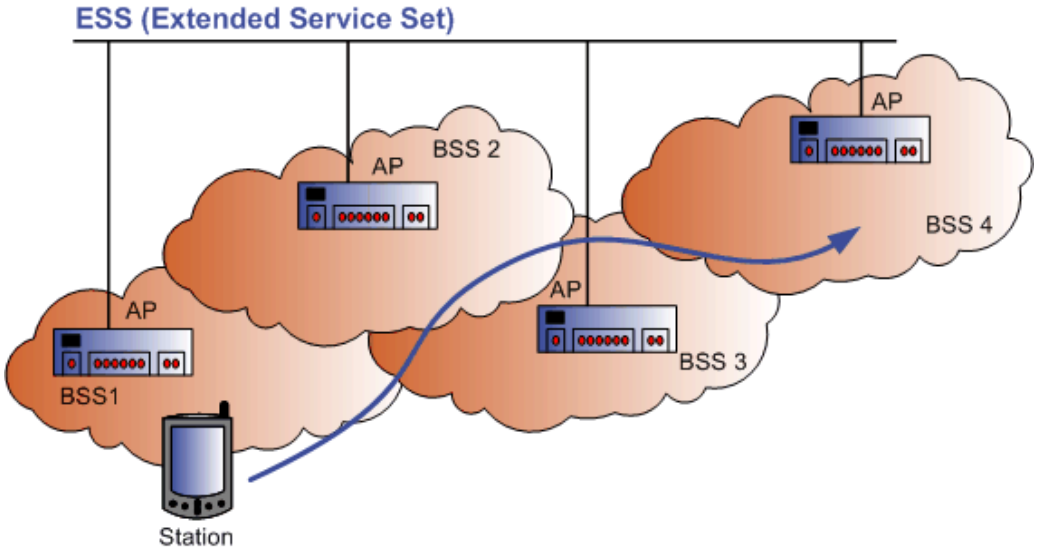

Fig.2.7 - ESS (*Extended Service Set*)
Fonte: http://www.mpirical.com/companion/UMTS/ESS.gif

CAPÍTULO III

RISCOS, AMEAÇAS E TÉCNICAS DE ATAQUE

3.1 Ameaças e ataques

A ameaça consiste em uma possível violação da segurança de um sistema. Algumas das principais ameaças às redes de computadores são [SOA 95]:

- Destruição de informação ou de outros recursos;
- Interrupção de serviços;
- Modificação da informação;
- Revelação de informação;
- Roubo, remoção ou perda de informação ou de outros recursos;

Há vários tipos de ameaças:

> As ameaças podem ser classificadas como acidentais ou intencionais. Ameaças acidentais são as que não estão associadas à intenção premeditada. As concretizações das ameaças intencionais variam desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema. A realização de uma ameaça intencional configura um ataque [SOA 95].

Na seção seguinte veremos as principais questões sobre segurança em redes de computadores. Serão abordados os principais tipos de ataque.

3.2 Problemas de segurança física

Administradores de rede tendem a cuidar muito da segurança lógica e, em geral, dão pouca atenção à segurança física, até porque a maioria das organizações tem a área de segurança física vinculada a outros departamentos que não são subordinados à área de

tecnologia de informação, o que é um erro estratégico. “Se a segurança física é um importante componente de risco quando se trata de redes cabeadas, em redes sem fio esse aspecto é ainda mais relevante, visto que a área de abrangência “física” aumenta substancialmente” [RUF 05]. O posicionamento de determinados componentes de rede, agora deve ser cuidadosamente estudado, sob o risco de comprometer o bom funcionamento da rede e, principalmente, facilitar o acesso não autorizado e outros tipos de ataque.

3.3 Envio e recepção de sinal

Essa característica é fácil de ser percebida quando se sabe o sinal (a menos que se utilizem antenas direcionais ou setoriais) a ser enviado em várias direções, portanto, um concentrador colocado em uma parede enviará sinal tanto para dentro do ambiente quanto para fora deste, o que pode não ser o desejado pelo administrador. “É regra geral que quanto mais ao centro estiver o concentrador melhor será o aproveitamento, pelas estações, do sinal irradiado por ele” [RUF 05]. Deve-se lembrar ainda que, mesmo que o sinal seja fraco fora do ambiente desejado, equipamentos com melhor recepção podem fazer uso dele, até porque sinal baixo permite conexão, mesmo que a baixas velocidades, mas que podem ser suficiente para os propósitos do invasor.

3.4 Negação de serviço (Denial of Service - DoS)

Este tipo de ataque consiste em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador. Para isso, são usadas técnicas que podem: sobrecarregar uma rede a tal ponto que os verdadeiros usuários dela não consigam usá-la;

derrubar uma conexão entre dois ou mais computadores; negar acesso a um sistema ou a determinados usuários; fazer tantas requisições a um site até que este não consiga mais ser acessado.

3.5 Mapeamento do ambiente

Uma das primeiras ações realizadas pelos atacantes é sem dúvida, promover o mapeamento do ambiente. Esse procedimento possibilita obter o maior número de informações sobre uma determinada rede, permitindo conhecer detalhes que lhe permitam lançar ataques de fora mais precisos e com menos riscos de serem identificados.

3.6 Criptografias de segurança da rede sem fio

Os seguintes tipos de criptografia estão disponíveis para uso em redes 802.11 [RUF 05].

- WEP
- WPA
- WPA2

Nas seções seguintes veremos cada um desses tipos de criptografia com mais detalhes.

3.7 Wired Equivalent Privacy (WEP)

Algumas das vantagens do algoritmo usado no WEP, é a facilidade na implementação e o baixo consumo de recursos, e já que no caso do WEP as fases de iniciação e cifragem ocorrem para cada pacote e a leveza do protocolo usado em ambas permite ganho significativo. O WEP faz a utilização do algoritmo RC4 para a implementação de sua criptografia.

Sendo a única opção de segurança, o WEP caiu em descrédito quando "pesquisadores descobriram que era possível ter acesso à chave utilizada na criptografia provocando o surgimento de diversas ferramentas para a quebra do WEP na Internet" [BIC 05]. Muitas pessoas, mesmo sem entender em que circunstâncias essa quebra pode ocorrer, condenaram-no para qualquer caso.

3.8 Wi-Fi Protected Access (WPA)

"O WPA vem sendo apontado como um substituto mais robusto que o seu antecessor, o WEP, já que vários dos problemas apontados para o WEP não existem mais e grande parte dos equipamentos legados pode passar a usar WPA sem maiores problemas" [RUF 05]. O WPA-Personal utiliza uma chave pré-compartilhada chamada PSK (*Pre-shared Key*) e criptografia TKIP (chave temporária). O WPA-*Enterprise* utiliza o método de autenticação 802.1x com criptografia TKIP. O WPA2-Personal e WPA2-Enterprise surgiram recentemente com um algoritmo de criptografia AES (padrão avançado de criptografia). Alguns fabricantes têm como padrão senhas pequenas imaginando que o administrador irá

modificá-la quando colocar o equipamento em produção, porém isso não ocorre na prática, tornando as redes com WPA tão vulneráveis quanto as que utilizam WEP.

3.9 Wi-Fi Protected Access 2 (WPA2)

De acordo com a publicação da [MIC 12] WPA2 é uma certificação de produto disponível por meio de *Wi-Fi Alliance* que certifica equipamentos sem fio como sendo com sendo compatíveis com o padrão 802.11i. O WPA2 oferece suporte aos recursos de segurança obrigatórios adicionais do padrão 802.11i que estão incluídos em produtos que oferecem suporte ao WPA. Com o WPA2, a criptografia é realizada como 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.

3.10 Configurações de fábrica

"A segurança das redes sem fio é elaborada desde a sua concepção, e desde esse momento tem evoluído rapidamente. Porém, a despeito dos equipamentos possuírem vários, e muitas vezes modernos, mecanismos de segurança, eles não vêm habilitados de fábrica" [RUF 05]. Tal fato faz com que os administradores com pouca experiência em redes sem fio e/ou com os prazos de implantação vencidos coloquem os equipamentos e produção sem qualquer mudança. É certo que os equipamentos de fábrica, em que os mecanismos de segurança não estejam habilitados, serão alvos fáceis de ataques.

Praticamente todos os equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados, poderão permitir a um ataque utilizá-los em uma rede-alvo e ter condições de identificar todas as configurações, podendo até mesmo

modificá-las. Portanto, contas administrativas devem ser trocadas, como as chaves WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), WPA2 (*Wi-Fi Protected Access*) e o *SSID – Service Set ID* (código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede) de modo a não permitir identificar a rede.

3.11 Técnicas e ferramentas de ataque

3.11.1 Preparação do ambiente

Há aspectos a serem considerados ao se promover análise de um ambiente de redes sem fio. Dentre estes, deve-se cogitar quais equipamentos e ferramentas serão úteis para cada caso. “Necessidade ou foco de investigação certamente será diferente em ambientes distintos, daí ser desejável um planejamento antecipado dos equipamentos e programas que realmente se encaixam em cada objetivo” [RUF 05]. Porém, para isso é necessário conhecer as características dos equipamentos e ferramentas disponíveis, usá-las corretamente ou justificar a sua aquisição.

3.11.2 Wardriving

Para efetuar essa prática é necessário um automóvel, um computador móvel, uma placa Wi-Fi configurada no modo “promíscuo” (o dispositivo efetua a interceptação e leitura dos pacotes de comunicação de maneira completa) e um tipo de antena que pode ser posicionada dentro ou fora do veículo (como por exemplo, utilizar uma lata da famosa marca de batatas frita norte-americana, Pringles). Tal atividade não é danosa em si, pois alguns se

contentam em encontrar a rede sem fio desprotegida, enquanto outros efetuam login e uso destas redes.

"Wardriving é o nome dado à técnica de dar um pequeno "passeio" de carro, rastreando e invadindo redes à rádio" [ASS 05].

Fig.3.1 – Wardriving
Fontes: http://www.esquemadf.xpg.com.br/wi1.jpg
http://www.marieval.com/training/opennetwork/gtnet/_1860241_pringleisec300.jpg
http://www.airtouchnetworks.com/images/kitpic.jpg

3.11.3 Escuta de tráfego

A escuta de redes sem fio é um ataque de simples execução, mas muito poderoso em vista dos danos que causa: a perda de privacidade, integridade e confidencialidade dos dados do sistema.

Para ter acesso ao conteúdo de um tráfego não é necessário nenhuma ferramenta específica para redes sem fio. Ao se utilizar ferramentas tradicionais é possível capturar grande parte do tráfego de uma rede cujo sinal esteja suficientemente próximo. Há diferentes tipos de dados que podem ser capturados em redes sem fio, essas informações podem ser

capturadas através de programas conhecidos por Sniffers. Sniffing (escuta) é o ato de monitorar o tráfego na rede para dados como senhas em texto puro ou informações de configurações [MIC 04].

3.11.4 Algumas ferramentas disponíveis

A seguir serão descritas algumas ferramentas gratuitamente disponíveis, suas principais características e possibilidades de uso [RUF 05]:

- **Airtraf –** Permite coletar uma vasta quantidade de informações sobre as redes identificadas, tais como clientes conectados, serviços utilizados e várias totalizações, tudo em tempo real;
- **Airsnort –** Mesmo com algumas limitações em termos de quantidade de placas e chipsets diretamente suportados, sua popularidade talvez seja, em parte, explicada por conta desses padrões de placa. As funcionalidades dessa ferramenta incluem: identificação de redes e informações relacionadas; uso ou não de WEP; possibilidade de varredura em todos os canais ou apenas em um canal de interesse;
- **Netstumbler –** Uma das primeiras ferramentas para o mapeamento e identificação de redes sem fio em ambiente Windows, similar a ferramenta Kismet, o Netstumbler possui algumas características úteis, como permitir integração com equipamentos GPS (Global Positioning System) e, desta maneira, obter um mapa preciso de pontos de acesso identificados. Por ele é

possível identificar as redes, seus nomes, endereços MAC e outras informações, tais como nível de sinal de propagação de cada rede detectada;

- **Hotspotter –** Criado para identificar uma vulnerabilidade em Windows XP, que permitia re-conexão sem criptografia com um concentrador falso, após a autenticação com um concentrador legítimo, o Hotspotter pode ser utilizado para forjar concentradores e fazer com que os clientes se conectem a ele em vez de ao verdadeiro.

3.11.5 Warchalking

"Inventado nos Estados Unidos há aproximadamente 70 anos, durante a época da depressão, o *Warchalking* era uma forma de comunicação usada pelos "Hobos" (andarilhos desempregados)" [MEN 04]. Os Hobos criaram uma linguagem de marcas de giz em cercas, calçadas e paredes, indicando um ao outro o que esperar de determinados lugares, casas ou instituições onde poderiam conseguir comida e abrigo temporário.

O *Warchalking* é a prática de escrever símbolos indicando a existência de redes sem fio e informando sobre suas configurações. As marcas usualmente feitas em giz nas calçadas indicam a posição das redes sem fio, facilitando a localização para o uso de conexões alheias pelos simpatizantes da idéia.

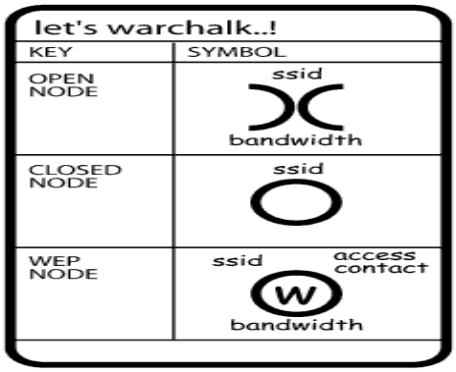

Fig.3.2 – Warchalking
Fonte: http://news.bbc.co.uk/media/images/38150000/jpg/_38150554_wchalk-300.jpg
http://www.wlan-project.com/images/warchalking.gif

3.11.6 Endereçamento MAC

Algumas medidas de segurança fazem o uso do prévio cadastramento dos endereços MAC, de equipamentos que poderão ser utilizados em uma determinada rede sem fio. Partem da suposição de que os endereços MAC são únicos, desta forma poderão distinguir inequivocadamente um equipamento registrado. Porém, na prática, esta solução pode ser burlada facilmente por uma estação clandestina, que identifique o tráfego (que inclui o endereço MAC de uma determinada estação cliente) e perceba quando uma estação cessar a comunicação, para então alterar o seu próprio endereço MAC para se fazer passar pela estação legítima.

CAPÍTULO IV

MÉTODOS DE DEFESA

4.1 Segurança

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus periféricos. “A necessidade de proteção deve ser definida em termo das possíveis ameaças e riscos e dos objetivos de uma organização, formalizada nos termos de uma política de segurança” [SOA 95].

A segurança é um dos temas mais importantes abordados nas redes sem fio. Desde seu início, os fabricantes e órgãos internacionais vêm tentando disponibilizar protocolos que garantam as comunicações:

> A política de segurança é o conjunto de diretrizes, normas e procedimentos que devem ser seguidos e visa conscientizar e orientar os funcionários, clientes, parceiros e fornecedores para o uso seguro do ambiente informatizado, com informações sobre como gerenciar, distribuir e proteger seus principais ativos [3EL 05].

Com relação às redes sem fio e redes estruturadas é possível disponibilizar meios para garantir a segurança destas através de mecanismos de autenticação, embora na prática o que se vê nas implantações das redes sem fio são apenas chaves de criptografia, com listas de acesso restringindo os endereços de hardware que podem associar-se às redes sem fio. Com a realização da autenticação, “ela irá garantir que os dados recebidos correspondam àqueles originalmente enviados, assim como garante a identidade do emissor” [CHI 98]. Já com a utilização da criptografia os dados irão trafegar na rede pública ou privada em formato cifrado

e, caso sejam interceptados, não deverão ser decodificados, garantindo a privacidade da informação.

Para que a rede sem fio criada esteja com o nível correto de segurança, primeiramente é preciso conhecer os padrões disponíveis, o que eles podem oferecer e então, de acordo com a sua aplicação, política de segurança e objetivo, implementar o nível correto e desejado.

Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar, com um transmissor irradiando os dados transmitidos através da rede em todas as direções; daí o problema de como impedir que qualquer um possa se conectar a rede e roubar os dados.Um ponto de acesso instalado próximo à janela da sala provavelmente permitirá que um vizinho a dois quarteirões de sua casa consiga captar o sinal da sua rede, uma preocupação agravada pela popularidade que as redes sem fio vêm ganhando nos últimos anos[BUL 12].

4.2 Serviços de segurança dos dados

O padrão IEEE 802.11 fornece o serviço de segurança dos dados através de dois métodos: autenticação e criptografia [RUF 05].

4.2.1 Autenticação

A maneira tradicional de adicionar segurança ao ambiente é promover autenticação do usuário e/ou do equipamento que deseja utilizar recursos da rede. Da mesma forma, a

maioria dos mecanismos de autenticação em redes sem fio baseia-se em senha fixas, porém existem alternativas que vão desde a associação com endereços MAC dos equipamentos, senhas dinâmicas, até o uso de certificados digitais, logicamente, cada uma delas, com diferentes níveis de riscos associados.

Sobre essa questão Rufino comenta:

> As senhas fixas são as mais utilizadas por serem mais simples de implementar, dado que é um mecanismo que o usuário já conhece e tem costume de utilizar. Esse método tem sido usado para autenticar usuários de serviços comerciais de acesso à Internet (Hotspots) e também em redes locais [RUF 05].

A Figura 4.1 apresenta uma tela de autenticação:

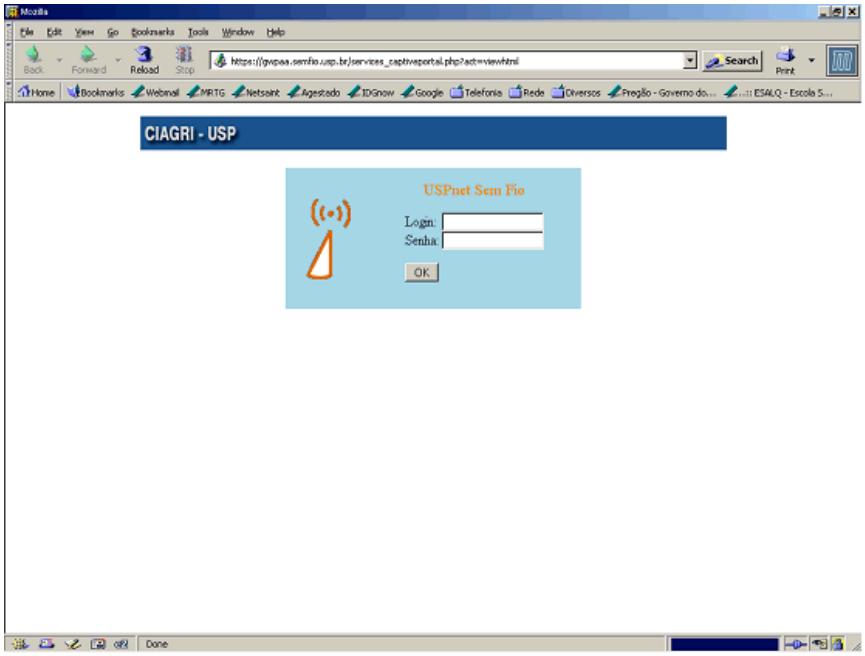

Fig.4.1 – Autenticação
Fonte: http://www.ciagri.usp.br/recursos/uspnetsemfio-autenticacao.png

4.2.2 Criptografia

A criptografia representa a transformação de informação inteligível numa forma aparentemente ilegível, a fim de ocultar informação de pessoas não autorizadas, garantindo privacidade [TRI 98].

Segundo Aldeia, "a palavra criptografia tem sua origem no grego: *kryptos* significa oculto, envolto, escondido, secreto; *graphos* significa escrever, gravar. Portanto criptografia significa escrita secreta ou escrita oculta" [ALD 03].

Há duas maneiras básicas de se criptografar mensagens: através de códigos ou de cifras. A primeira delas procura esconder o conteúdo da mensagem através de códigos predefinidos entre as partes envolvidas na troca de mensagens. O outro método usado para criptografar mensagens é através da cifra, técnica na qual o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original, a mensagem é decifrada fazendo-se o processo inverso ao ciframento.

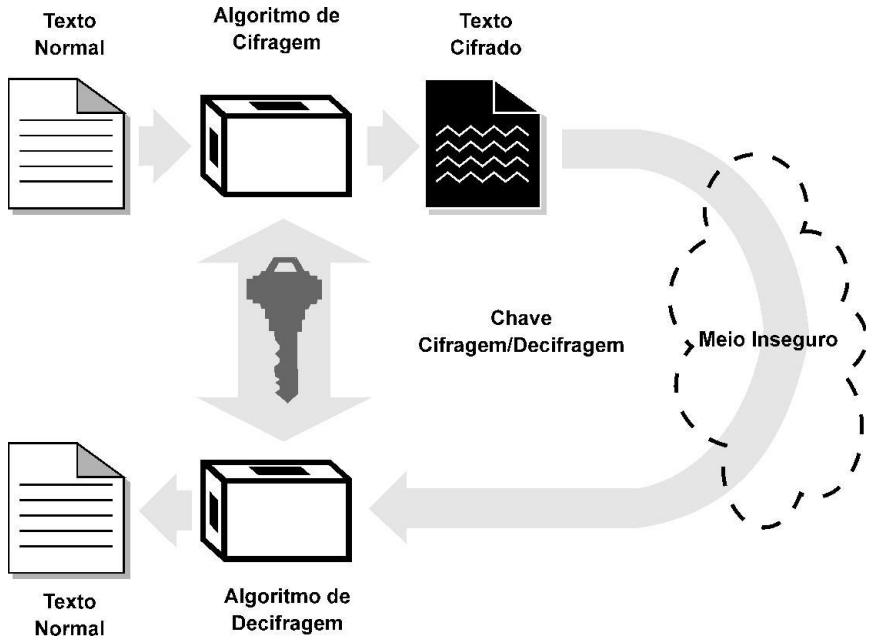

Fig.4.2 - Cifragem e decifragem
Fonte: http://www.di.ufpe.br/~flash/ais98/cripto/Image3.gif

A principal vantagem das cifras em relação aos códigos é a não limitação das possíveis mensagens a serem enviadas, além de se tornarem mais difíceis de serem decifradas. As cifras são implementadas através de algoritmos associados a chaves, longas seqüências de números e/ou letras que determinarão o formato do texto cifrado.

Segundo Duarte [DUA 03]: "O conceito de chave é um tanto abstrato, mas se pensarmos no criptosistema como um conjunto de algoritmos, as chaves são elementos fundamentais que interagem com os algoritmos para a cifragem/decifragem das mensagens".

4.2.2.1 Criptografia de chave simétrica

Na criptografia de chave simétrica, a mesma chave utilizada na codificação deve ser usada na decodificação. Para que este tipo de criptografia funcione, "todas as pessoas envolvidas devem conhecer a chave, pois quando uma mensagem criptografada chega à caixa de entrada, ela só pode ser aberta por quem possui a chave" [LOP 05]

4.2.2.2 Criptografia de chave assimétrica

"Criptografia assimétrica é o conjunto de condições para a possibilidade de identificação dos emissores e receptores de conteúdos semânticos, e da integridade da transmissão desses conteúdos, numa rede de comunicação aberta" [REZ 00]. A criptografia assimétrica trabalha com duas chaves: uma denominada privada e a outra denominada pública. Nesse método uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar as informações. Uma outra chave deve ser criada para a decodificação, esta é uma chave privada.

4.3 Técnicas de segurança

Dentro do utilitário de configuração poderão ser habilitados recursos de segurança. Na maioria dos casos os recursos relacionados abaixo vêm desativados por padrão a fim de que a rede funcione imediatamente, mesmo antes de qualquer coisa ser configurada. Para os fabricantes, quanto mais simples for à instalação da rede melhor, pois haverá um número menor de usuários insatisfeitos por não conseguir fazer a rede funcionar. Porém, a segurança da rede fica baixa, possibilitando uma maior facilidade a acessos não autorizados. Para garantir uma segurança melhor da rede é preciso realizar configurações extras.

4.3.1 Service Set ID (SSID)

A primeira linha de defesa é o SSID, um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede. Cada fabricante utiliza um valor padrão para esta opção, mas deve-se alterá-la para um valor alfanumérico qualquer, que seja difícil de adivinhar. Geralmente estará disponível no utilitário de configuração do ponto de acesso, a opção “Broadcast SSID”. Ao ativar esta opção o ponto de acesso envia periodicamente o código SSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber previamente o código. Esta é uma opção desejável em redes de acesso público, mas caso sua preocupação maior seja a segurança, o melhor é desativar a opção. Desta forma, apenas quem souber o valor ESSID (Extended Service Set ID) poderá acessar a rede.

4.3.2 Wired Equivalent Privacy (WEP)

O WEP é ainda a única possibilidade de aumentar o nível de segurança em algumas instalações, quer seja pela existência de equipamentos legados, por problemas de política de uso, quer ainda por dificuldades técnicas.

Ainda segundo Rufino:

> Considerar o WEP robusto e, por causa disso, não se preocupar em implementar mais nenhuma proteção e não proceder a um correto monitoramento do ambiente pode ser um erro tão grande quanto deixar de utilizá-lo pelo simples fato de ter lido sobre suas vulnerabilidades, sem fazer uma avaliação do seu ambiente e das possibilidades que os seus recursos computacionais oferecem [RUF 05].

4.3.3 Wi-Fi Protected Access (WPA)

O WPA pode ser utilizado para a obtenção de soluções de segurança mais robustas, já que dispõe de recursos de segurança nativos e também os que podem trabalhar de forma integrada a outras tecnologias, tais como IEEE 802.1x (permite autenticação) e certificados digitais. Deve-se ter em mente que a maioria dos recursos do WPA não está disponível em modo Ad-Hoc, mas apenas com a topologia tradicional de infra-estrutura.

A maneira mais simples de utilizar os recursos nativos do WPA é por meio de chaves compartilhadas, pois assim se estabelece negociação entre o cliente e o concentrador, o qual ao usar uma chave pré-estabelecida, faz com que a chave de seção seja trocada periodicamente, de forma confiável.

4.3.4 Wi-Fi Protected Access 2 (WPA2)

Criptografia WPA2 com TKIP e AES 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. É modalidade de segurança sem fio mais forte. O WPA2 oferece também um método de autenticação de chave pré- compartilhada em redes sem fio no modo de infra-estrutura. A chave pré-compartilhada é configurada no Acess Point(AP) sem fio e em cada cliente sem fio.

4.3.5 Permissões de acesso

Além da encriptação pode-se considerar a implantação de um sistema de segurança baseado em permissões de acesso. O Windows 95/98/ME/XP/VISTA permite colocar senhas nos compartilhamentos, enquanto o Windows NT/2000/2003/2008 Server, já permite uma segurança mais refinada, baseada em permissões de acesso por endereço IP (endereço lógico da placa de rede), por usuário, por grupo etc. Usando esses recursos, mesmo que alguém consiga penetrar na rede, ainda terá que quebrar a segurança do sistema operacional para conseguir chegar aos arquivos. Isso vale não apenas para redes sem fio, mas também para redes cabeadas, onde qualquer um que tenha acesso a um dos cabos ou a um computador conectado à rede é um invasor em potencial.

Somando o uso de todos os recursos acima, a rede sem fio pode tornar-se até mais segura do que uma rede cabeada, embora colocar tantas camadas de proteção torne a implantação da rede muita mais trabalhosa.

CAPÍTULO V

ESTUDO DE CASO

5.1 Cenário doméstico/pequena empresa

Como já vimos anteriormente, por mais simples que seja o ambiente, a segurança não deve ser negligenciada, pois não é difícil imaginar que muita informação sensível pode trafegar ou estar armazenada em computadores pessoais, mesmo em ambientes domésticos. É recomendado preservar as tradicionais preocupações dos clientes quanto à existência de produtos de segurança tais como, antivírus, Firewall pessoal etc.

Um dos casos mais usuais são as redes sem fio domésticas ou em escritórios, onde existe conexão banda larga compartilhada para menos de 20 equipamentos. Neste modelo seria suficiente um concentrador com características de roteamento e interfaces de rede sem fio para estações, notebooks, impressoras e outros. Uma ligação convencional seria um concentrador ligado ao roteador/modem ADSL e três ou quatro estações com interfaces sem fio.

É necessário, primeiramente, adquirir um concentrador e placas que permitam uso de WPA, logo em seguida habilitar o WPA na modalidade de chaves previamente compartilhadas. Um esforço inicial ocorrerá para configurar equipamentos envolvidos, mas a partir daí nada mais precisará ser alterado, a menos que uma chave seja descoberta e seja necessário trocá-la. É importante deixar claro que a qualidade da chave-mestra é fundamental para que a quebra seja difícil, é sempre bom evitar chaves pequenas ou existentes em dicionários.

O acesso às configurações do concentrador se dá por meio do serviço HTTP (Hyper Text Transfer Protocol) ou TELNET (é um protocolo utilizado para abrir uma sessão em uma máquina remota ou concentrador). É possível, na maioria dos casos restringirem o acesso aos serviços (HTTP e TELNET), deixando apenas o acesso disponível pela placa cabeada. Se não for possível, pode-se ainda restringir o endereço IP do equipamento que terá acesso autorizado, deixando esse endereço fora do bloco de IPs dinâmicos (DHCP), sem entrar em conflito com os demais.

Caso o concentrador não permita nenhum tipo de limitação de acesso, será recomendado desabilitar o acesso ao serviço, e somente após o reset do concentrador, ter novamente a possibilidade de acesso recuperada, deste modo perder-se-ia toda a configuração feita anteriormente. Alguns modelos de concentrador têm a opção de salvar as configurações e restaurá-las posteriormente.

A segurança das estações clientes é que garantirá a segurança da rede como um todo, pois um ataque bem sucedido a uma estação cliente terá implicações sérias na segurança do ambiente, já que estará sob o controle do atacante um equipamento que tem credenciais para acessar recursos da rede.

Caso o administrador procure uma solução melhor, mas sem a complexidade de um servidor RADIUS - *Remote Authentication Dial In User Service* (serviço de autenticação remota de usuários discados), pode-se adotar o Tinypeap, que consiste em um servidor RADIUS com funcionalidades bem reduzidas, as quais podem rodar nos próprios concentradores, porém o único concentrador que suporta o Tinypeap disponível é o (WRT54G) do fabricante Linksys.

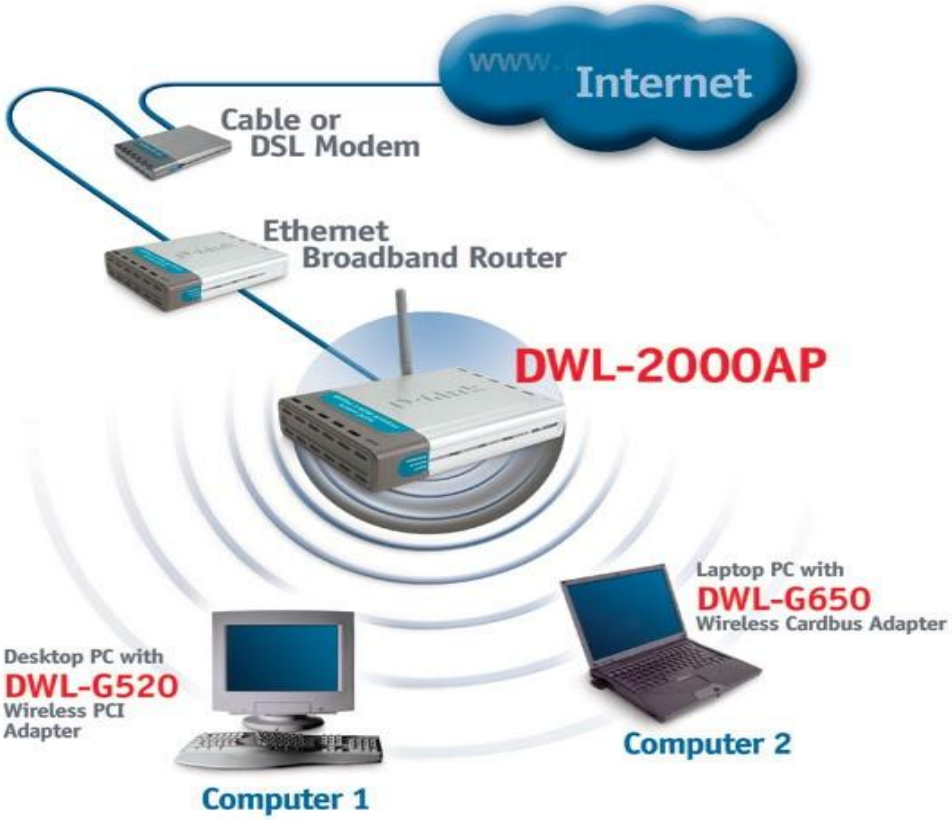

Fig.5.1 - Modelo de Configuração
Fonte: http://users.swing.be/id-phy/WLAN/WLAN-DLINK.jpg

CONCLUSÃO

Qualquer que seja o nível de segurança em redes sem fio escolhido ou possível de ser adotado, apresentará riscos e vulnerabilidades envolvidas. O interessante é que quanto maior a complexidade da solução, maior será a quantidade de pontos de falha, ou seja, em um modelo robusto onde existam servidores de autenticação, serviços de diretório, banco de dados etc., cada um desses elementos passa a ser um risco potencial, tanto pela rede sem fio quanto por uma possível rede cabeada. Mas, por outro lado, quanto menos elementos existirem para compor a segurança, mais a rede em si passará a ser o ponto de maior risco. Em qualquer caso, o cliente e o concentrador são sempre pontos de possíveis vulnerabilidades e devem receber atenção especial e constante.

Alguns problemas ainda estão sendo resolvidos, como o que se relaciona ao armazenamento da senha, tanto do lado cliente quanto dos servidores. Em alguns modelos de autenticação até a senha para acesso a chave privada fica exposta em arquivos ou armazenada no próprio disco, sujeito à cópia e à recuperação do seu conteúdo.

O principal relaciona-se a autenticação, visto que outros elementos já estão razoavelmente solucionados, como algoritmos para cifragem do tráfego, protocolos e freqüências utilizadas.

A rede sem fio é um avanço tecnológico inegável e proporciona facilidades antes inimagináveis, como, por exemplo, implantar rede em um prédio tombado, local onde seria impraticável quebrar paredes para a passagem de cabos, onde outras tecnologias podem não ser completamente adequadas, e permitir acesso em parques e áreas abertas, entre muitos outros ambientes. Todavia, apresenta muito mais riscos de segurança envolvidos, sabendo que boa parte da proteção adotada está calcada na segurança física, o que não existe em redes sem fio, pelo menos no que diz respeito às informações em trânsito.

Outro problema grave em redes sem fio é a relativa facilidade em se promover ataques do tipo negação de serviço. Não há solução definitiva para esse problema, mas este pode ser monitorado, e com o uso das ferramentas certas, a origem do ataque pode ser mais fácil e rapidamente identificada.

Trabalhos futuros poderão explorar, por exemplo, a questão da segurança nas redes sem fio, fazendo um comparativo entre a eficiência das diversas técnicas de defesa.

Outros trabalhos poderão abordar os novos padrões de redes sem fio, ainda em fase de pesquisa e desenvolvimento, apesar das dificuldades de obtenção de material bibliográfico devido as questões de segredo industrial implícitas nessas atividades de pesquisa.

REFERÊNCIAS BIBLIOGRÁFICAS

[3EL 04] 3ELOS. **Política de segurança da informação,** disponível em <http://www.3elos.com.br/produtos/politicadeseguranca.php>, acesso em 15 de dezembro, 2011.

[ALD 03] ALDEIA, Vicki. **Criptografia,** disponível em <http://www.numaboa.com.br/criptografia >, acesso em 17 de dezembro, 2011.

[ART 10] ARTHAS, Kael**. Tutorial Redes Wireless**, disponível em < http://www.babooforum.com.br/forum/index.php?/topic/269602-redes-wireless/ >, acesso em 01 de março, 2012.

[ASS 05] ASSUNÇÃO, Marcos. **Detonando redes de rádio,** disponível em < http://www.invasao.com.br/coluna-marcos-17.htm >, acesso em 15 de Janeiro, 2012.

[BIC 05] BICE, Bryan. **Wired Equivalent Privacy,** disponível em <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549087,00.html>, acesso em 10 de fevereiro, 2012.

[CAB 12] CABIANCA, Luís Antonio. **Redes LAN/MAN Wireless II: Tipos de Rede**, disponível em <http://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_2.asp >, acesso em 12 de março, 2012.

[COR 07] CORDEIRO, Ricardo. **Rede sem fios**, disponível em < www.leak.pt/rede-sem-fios/ >, acesso em 15 de dezembro, 2011.

[BUL 12] BULHMAN, Haroldo José. **Tutoriais Redes Opticas**, disponível em <http://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_2.asp >, acesso em 17 de março, 2012.

http://www.teleco.com.br/tutoriais/tutorialcdigital/pagina_2.asp

[CHI 98] CHIN, Liou Kuo. **Rede privada virtual,** disponível em <http://www.rnp.br/newsgen/9811/vpn.html>, acesso em 15 de fevereiro, 2012.

[COM 08] ComputerWorld EUA. **3G: a geração wireless de alta velocidade**, acesso em 11 de Janeiro, 2012.

[DUA 03] DUARTE, Luiz Otávio. **Análise de vulnerabilidades e ataques a redes sem fio,** disponível em <http://www.apostilando.com/download.php?cod=230&categoria=Redes>, acesso em 20 de fevereiro, 2012.

[FOR 04] FORUMPCS. **O nascimento do Wi-Fi – parte 1,** disponível em <http://www.forumpcs.com.br/noticia.php?b=83772>, acesso em 27 de fevereiro, 2012.

[GRA 04] GRANVILLE, Lisandro Zambenedetti; ALMEIDA, Mª Janilce Bosquiroli. **Simpósio brasileiro de redes de computadores – anais volume 1,** Rio Grande do Sul, 2004.

[LOP 05] LOPES, Janaina da Silva. **CRIPTOGRAFIA**, disponível em < http://www.jsl.siteonline.com.br/interna.jsp?lnk=32706> , acesso em 13 de março, 2012.

[MAI 03] MAIA, Roberto M. Franklin. **Bluetooth – promessas de uma nova** Trabalho de conclusão de curso de graduação. Faculdade Integrado do Recife. Recife: 2003.

[MAN 06] MANDARINO ,Marco Antonio. **Rede Wirelles**, disponível em <http://www.mandarino.pro.br/Sites/wireless/osprotocolos.html>, acesso em 12 de fevereiro, 2012.

[MEN 04] MENEZES, Ricardo. **Warchalking: de qual lado você está?**

[MIC 12] MICROSOFT. **Guia de Planejamento para Conformidade com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento**, disponível em <http://technet.microsoft.com/pt-br/library/bb821241.aspx> acesso em 20 de fevereiro, 2012.

[MIC 04] MICROSOFT. **Ameaças e Contramedidas de Segurança na Web**, disponível em <http://technet.microsoft.com/pt-br/library/dd569900.aspx> acesso em 06 de março, 2012.

[PIN 04] PINHEIRO, José Mauricio Santos.**Vulnerabilidades em Redes Wireless**, disponível em<http://www.projetoderedes.com.br/artigos/artigo_vulnerabilidades_em_redes_wireless.php>, acesso em 01 de março, 2012.

[REZ 00] REZENDE, Pedro Antônio Dourado. **1ª conferência internacional de direito na internet e na informática,** disponível em <http://www.cic.unb.br/docentes/pedro/trabs/gesso.htm>, acesso em 02 de março, 2012.

[RUF 05] RUFINO, Nelson Murilo O. **Segurança em redes sem fio,** São Paulo, Novatec, 2007.

[SHE 08] SHELLENROX. **Redes Wi-Fi**, disponível em <http://www.htmlstaff.org/ver.php?id=20443>, acesso em 10 de Janeiro, 2012.

[SIL 98] SILVA, Adailton J. S. **As tecnologias de redes wireless,** disponível em <http://www.rnp.br/newsgen/9805/wireless.html>, acesso em 05 de março, 2012.

[SOA 95] SOARES, L. F. G; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores: das LANs, MANs e WANs às redes ATM.** 2ª Edição, Rio de Janeiro, Elsevier, 1995.

[TRI 98] TRINTA, Fernando Antonio Mota; DE MACÊDO, Rodrigo Cavalcanti. **Um Estudo sobre Criptografia e Assinatura Digital**, disponível em < www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm >, acesso em 10 de março, 2012.