Vulnerabilidades em Redes Wireless

Raimundo Pereira da Cunha Neto
Professor de Sistemas de Informação da FAETE, Av. Dr. Nicanor Barreto, 4381 – Teresina-PI – 64.053-355 – Fone: (86) 3231-4020 – netocunha@faete.edu.br

Resumo: *As redes de computadores se tornam cada vez mais presente na sociedade atual, devido ao grande poder de informação que a Internet nos proporciona. Aliada a esse crescimento, as redes sem fios passou a ser melhor opção para corporações e usuários domésticos, devido a sua facilidade de implementação e aos baixos custos de seus equipamentos. No entanto, as transmissões sem fios possuem enormes riscos, pelo seu meio de propagação é o ar, o que facilita a qualquer invasor que estiver dentro do campo de atuação.*

Palavras-chave: *Redes, Wireless, Ataque, Vulnerabilidade***.**

Abstract: *The computers networks become ever more present on actual society because of the great power of the information provided by Internet. Allied to this growth, the wireless network has become the best option to corporations and home users, because of the easy way of implementation and the low costs of the equipments. However, the wireless transmissions have a lot of risks in consequence to the spreading channel: the air, what make it easier to any attacker that is within the scope the wireless network.*

Key-Words: *Network, Wireless, Attack, Vulnerability***.**

1. Introdução

As transformações mundiais ocorrem muitas vezes sem nos darmos conta, quando percebemos estamos totalmente envolvidos pelo avanço tecnológico. O ser humano busca sempre o crescimento e a sua superação, o que nos levou a uma sociedade, que a todo momento quer se qualificar e esta sempre informada, ocasionando um avanço da informática, onde percebemos desta a evolução dos hardwares, quanto dos softwares, facilitando a difusão da tecnologia entre todas as classes. Esta sociedade, que podemos caracterizar como a "Sociedade da Informação", fez com que a Internet passasse a ser uma das grandes meios de informação, através de muitos mecanismo como portal de noticias, fórum, chat, blog, entre outros. Mas não só a informação era suficiente para estes usuário, faltava a disponibilidade de acesso em todos os lugares, começa então a evolução das redes de computadores. Dentre os grandes avanços destacamos a redes sem fios, que pela praticidade, tem se difundido em diversos setores. Sem necessidade de maiores conhecimentos, o usuário pode implementar sua rede sem fio, ou até mesmo conectar a redes abertas. O baixo custo nos equipamentos de informática, faz com que, maior número de pessoas possam adquiri-los, aliada as vantagens dos serviços virtuais, observamos o crescimento de usuários em aeroportos, shopping, universidades, entre outros locais. Sendo as transmissão sem fio um meio não guiado e propagado pelo ar, verificamos assim um campo de transmissão pelo ponto de acesso, onde as informações são trocadas a todo instante. Devido a esse fator estamos exposto a ataques pelas grandes fragilidades, principalmente quando não utilizamos nenhum meio de segurança, o que ocorre na maioria das vezes.

2. Redes Sem Fios

As Redes sem Fios trabalham utilizando o mesmo principio das redes cabeadas, no entanto, diferem quanto ao meio de transmissão não serem guiados. Este tipo de rede converte pacotes de dados em onda de rádio ou infravermelho e os envia para outros dispositivos.

A sua principal vantagem é fato de dispensar o uso de cabos e a mobilidade, sendo o essencial para ambientes onde a passagem de cabos se torna inviável. A utilização de um ponto de acesso(AP) muitas vezes se faz necessário, pois este faz em o papel de concentrador nas redes de topologia de Infra-estrutura, sendo dispensado na redes de topologia Ad-Hoc, que funciona sem o ponto central.

Figura 01 – Uso de AP em redes sem fios

O IEEE – Instituute of Eletricical and Eletronics Engineers constituiu um grupo chamado de Wireless Local - Area Networks Standard Working Group, com a finalidade de criar padrões para redes sem fio, definindo um nível físico para redes onde as transmissões são realizadas na freqüência de rádio ou infravermelho, e um protocolo de controle de acesso ao meio, o DFWMAC (Distributed Foundation Wireless MAC). Esse padrão foi denominado de Projeto IEEE 802.11. Atualmente o padrão 802.11 conta com alguns sub-padrões, sendo os principais descritos abaixo:

- 802.11b: permite 11 Mbps de velocidade de transmissão máxima;
- 802.11a: definido após o 802.11b, busca resolver problemas existentes anteriormente, possui velocidade máxima de 54Mbps;
- 802.11g: permite que equipamentos dos padrões b e g, possam operar mesma faixa, tendo como velocidade máxima 54Mbps, sendo que alguns fabricantes não padronizados trabalham em 108Mbps.

Na grande maioria das redes são usado um ponto central, que recebe o sinal de acesso a Internet e os envia para o restante da rede, como acontece nos provedores, que o repetem aos seus clientes, como mostra a figura abaixo.

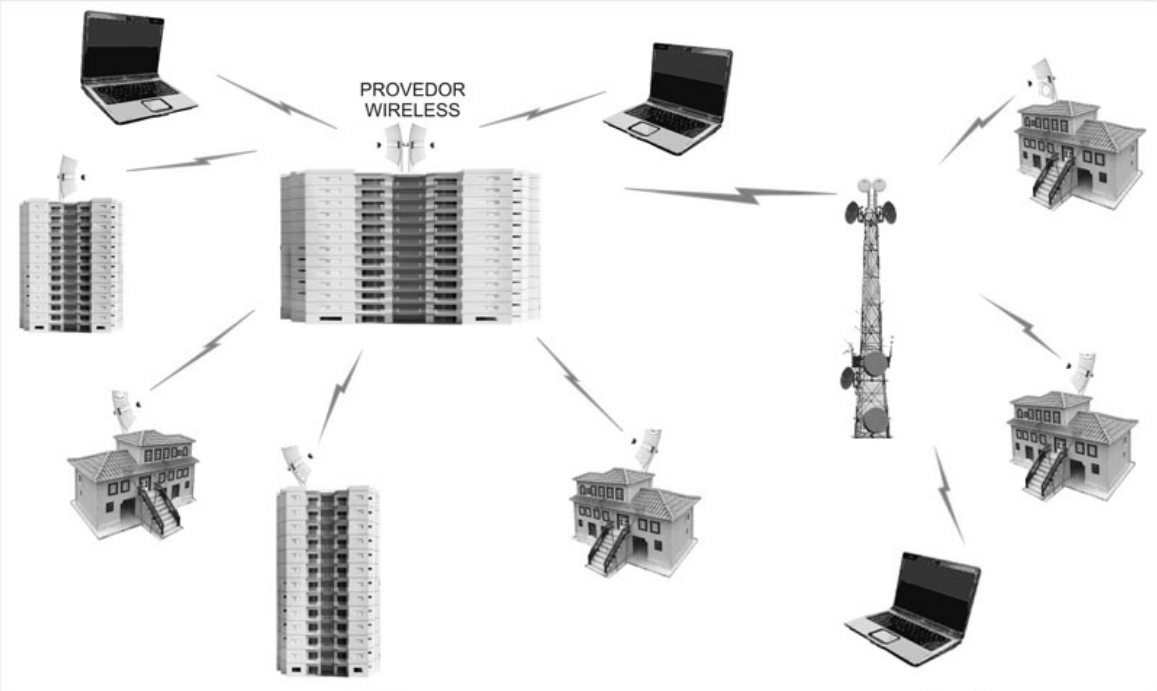

Figura 02 – Transmissão sem fio, usada pelos provedores de acesso a rádio

2.1. Classificação das Redes Sem Fios

Quando falamos sobre a distância que as redes sem fio possuem podemos classificar quanto ao alcance em:

- WPAN (Wireless Pessoal Area Network): Este tipo de rede é utilizada para interligação de equipamentos em uma área pequena, para evitar a utilização de cabos. Podemos também dizer que é uma rede sem fio pessoal.
- WLAN (Wireless Local Area Network): É uma rede local sem fios com conectividade com a Internet, geralmente utilizada em escritórios, faculdades, aeroportos, shopping, entre outros locais.
- WWAN(Wireless Wide Area Network): Nesta encontramos as redes sem fios de grandes extensões, ou seja, de área geográfica de dimensões maiores, como um país, ou mesmo o mundo inteiro.
- WMAN(Wireless Metropolitan Area Network): As redes metropolitanas sem fios, são utilizadas para a conexão de uma cidade, ou até mesmo em áreas um pouco menores como universidades.

3. Vulnerabilidades

As fragilidades das redes de computadores, tanto as redes cabeadas como as redes sem fios, são enormes, muitas são as formas de vulnerabilidades nesta tecnologia, dentre elas temos algumas formas de ataques descritos abaixo:

- Wardriving;
- Captura de tráfego de dados

- Ação Maliciosa
- DoS

3.1.Wardriving

Este técnica de ataque é realizada através do mapeamento dos pontos de acesso das redes sem fios, a fim de entrar na campo de transmissão, geralmente são feito com uso de um veículo para movimentação usando GPS, para detecção da área de abrangência, como demonstrado na figura abaixo. Através do rastreamento o invasor verifica as fragilidades existente, como o uso de protocolo de segurança, senhas de acesso, entre outros meios. Alguns softwares podem ser testados para esta técnica, como é o caso do NetStumbler, software livre muito popular, trabalha como sistema operacional o Windows.

Figura 03 – Utilização da Técnica de Wardriving

3.2.Captura de tráfego de dados

A transmissão de sinal são enviados por ondas, onde são propagadas pelo ar, sendo criado uma área de conexão, quando não são usado cifradas, tanto sinal, quanto as informações que trafegam dentro desta rede podem ser capturados por um invasor. Neste caso podem ser usados softwares específicos para esta ação maliciosa, por exemplo o kismet, que rastreia e captura as informações trafegadas. Esta é uma técnica bastante simples de ser usada pois o software utilizado não necessariamente comunica-se com a rede. Podemos observar muitos pontos onde não há segurança no trafego destas redes, como em faculdades.

Figura 04 – Captura de Tráfego de Dados por Espião

3.3.Associação Maliciosa

Este tipo de ação ocorre quando pessoas mal intencionadas usam técnicas para se passarem pelo ponto de acesso original. Desta forma toda transmissão dos usuários passarão por este AP pirata, o pirata terá toda e qualquer informação trafega, podendo ai, verificar senhas de email, contas de bancos, ou até mesmo roubar dados empresariais. A técnica é realizada com a utilização de um software de conexão, a partir deste momento o AP pirata responderá a qualquer requisição do usuário.

3.4.DoS

O DoS (Denail of Service ou negação de serviço) torna algum recurso ou serviço indisponível. Este tipo de ataque muitas vezes se torna uma vulnerabilidade bem simples, quando não se há intenção de realizá-la. Alguns equipamentos que transmitem onda como é o caso dos aparelhos de micro-onda, telefone sem fio, ou até mesmo AP bem próximos, podem neutralizar um serviço de transmissão de redes sem fios, fazendo com que este pare de enviar sinal. São cuidados como esse que muitos administradores de redes não se preocupam, pois parecem sem muito simples, mas em muitos casos podem parar grande parte dos serviços. Não apenas sem intenção como também, por pessoas mal intencionadas, este ataque pode acontecer, principalmente quanto piratas querem parar um serviço de transmissão.

5. Conclusão

De acordo com a análise realizada, observamos que a transmissão sem fio traz muitos benefícios e facilidades, principalmente pela comodidade e fácil instalação, mas apesar de tudo, temos uma tecnologia ainda em fase de construção, onde novos padrões tem sido desenvolvidos com a finalidade de correções de padrões anteriores.

Muitas são as vulnerabilidades encontradas em transmissão sem fio, principalmente

por seu campo de propagação ser o ar. Ferramentas são utilizadas por parte de invasores em busca de roubar informações, que encontram usuários sem grande conhecimentos, utilizando em seus acessos senhas de bancos, e-mail, sistemas de informação, entre outros mecanismos de trabalho.

O desconhecimento por parte dos usuários, que muitas vezes não consultam sobre a segurança do acesso utilizado, tem tornado um dos pontos fortes as vulnerabilidades, há necessidade de uma política de segurança para os provedores de acesso, além da não utilização de certos serviços em locais públicos se faz necessário para este usuário não ficar totalmente exposto.

6. Referências Bibliográficas

RUFINO, NELSON MURILO DE O. (2005) *Segurança em Redes sem Fio.* Ed. Novatec. 2ª. Edição, São Paulo-SP.

TANENBAUM, ANDREW S. (2003) "Redes de Computadores". 4. ed. Rio de Janeiro, Campus.

DUARTE, LUIZ OTAVIO. (2008) "*Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio802.11x*." www.acmesecurity.org/hp_ng/files/testes_monografias/ acmemonografia-Wireless-2003-LOD.pdf, Agosto/2008.

NETSTUMBLER.COM.(2008) www.netstumbler.com, Setembro/2008.