UNIPAC - UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS
FACULDADE DE CIÊNCIA DA COMPUTAÇÃO E COMUNICAÇÃO SOCIAL

CURSO DE CIÊNCIA DA COMPUTAÇÃO

S É R G I O P E R E I R A

SEGURANÇA EM REDES DE COMPUTADORES SEM FIO

BARBACENA
DEZEMBRO DE 2004

S É R G I O P E R E I R A

SEGURANÇA EM REDES DE COMPUTADORES SEM FIO

Trabalho de conclusão de curso apresentado à Universidade Presidente Antônio Carlos como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

ORIENTADOR: Prof. Luis Augusto Mattos Mendes

BARBACENA
DEZEMBRO DE 2004

S É R G I O P E R E I R A

SEGURANÇA EM REDES DE COMPUTADORES SEM FIO

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Aprovada em _____/_____/_____

BANCA EXAMINADORA

_____

Prof. Luis Augusto Matos Mendes (Orientador)
Universidade Presidente Antônio Carlos

_____

Prof. Ms Gustavo Campos Menezes (Membro Examinador)
Universidade Presidente Antônio Carlos

_____

Prof. Eduardo Macedo Bhering (Membro Examinador)
Universidade Presidente Antônio Carlos

Dedico este a minha querida Avó, que me ensinou que todas as coisas na vida são conquistadas com esforço e dedicação.
Dedico este estudo a todos os amigos que surgiram nestes quatro anos e que com certeza permanecerão para toda a vida.

Agradeço a Deus por todas as oportunidades que tive em minha vida e por sempre estar junto de mim.
A minha família pelo carinho e apoio incondicional.
Aos amigos Alisson. (Pepe), Ednardo (Narigudo) e Henrique (Pretinho) pelos trabalhos desenvolvidos em conjunto.
Aos amigos Alisson (Cadernal), Fausto (Bob) e Leandro (Mr. Beem) pela amizade e companheirismo ao longo dos anos de convivência.
A todos os colegas de sala e de ônibus que sempre contribuíram com sugestões e criticas.
Aos amigos da Gerdau Açominas em especial ao Isaias pelos conselhos, apoio e sugestões.
Ao professor Luís Augusto pela orientação neste trabalho, ensinamentos e amizade.
Aos demais amigos que direta ou indiretamente me ajudaram.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AP	*Access Point*
BSA	*Basic Service Area*
BSS	*Basic Service Set*
DSSS	*Direct Sequence Spread Spectrum*
ESA	*Extended Service Area*
ESS	*Extended Service Set*
FHSS	*Frequency Hopping Spread Spectrum*
FTP	*File Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
ICV	*Integrity Check Value*
IDEA	*International Data Encryption Algorithm*
IEEE	*Institute of Electrical and Electronics Engineers*
IPSec	*Internet Protocol Security*
IV	*Initialization Vector*
MAC	*Médium Access Control*
MIC	*Message Integrity Code*
PKI	*Public Key Infrastructure*
SSID	*Service Set Identifier*
VPN	*Virtual Private Network*
WEP	*Wired Equivalency Privacy*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WLAN	*Wireless Local Area Network*
WPA	*Wi-Fi Protected Access*
WTLS	*Wireless Trasnport Layer Security*

SUMÁRIO

.

CAPÍTULO 1 - INTRODUÇÃO

Pela facilidade de instalação e grande flexibilidade que oferece aos usuários. As redes sem fio ocupam um lugar de destaque no mercado tecnológico atual. As instituições descobriram que, através das redes sem fio, são capazes de gerar uma maior mobilidade para seus empregados e com isso, alcançar um retorno mais rápido dos investimentos. Isso alavancou as pesquisas no setor.

Apesar de todas as vantagens que as redes sem fio oferecem, existe a questão da segurança, que ainda preocupa os usuários dessas redes.

O trabalho Segurança em redes sem fio de computadores estuda os conceitos de mobilidade e comunicação sem fio analisando as redes *Wireless* suas vulnerabilidades e técnicas de ataque mais comuns utilizadas na atualidade.

Este estudo está dividido em três etapas importantes: No segundo capitulo é descrito a conceituação teórica sobre mobilidade e funcionamento das redes sem fio e seus respectivos padrões.

No terceiro capitulo é realizado um estudo sobre a questão da segurança nas redes *Wireless* abordando a fundamentação teórica sobre criptografia, autenticação destas redes.

No quarto capitulo é feito um estudo sobre o perfil e comportamento dos intrusos diante de uma rede sem fio, bem como uma analise das principais vulnerabilidades e dos principais ataques a redes sem fio.

CAPITULO 2 – COMUNICAÇÃO SEM FIO

Desde os primórdios da civilização, o homem já manifestava a vontade de se comunicar à distância sem utilizar-se dos fios. Com os avanços tecnológicos essa vontade passa a ser uma realidade.

Evoluímos dos sinais de fumaça dos primitivos para as redes sem fios (*Wireless network*).

2.1 – REDES SEM FIO

Muitas pessoas já têm e outros milhares terão acesso aos dispositivos móveis e as tecnologias de comunicação sem fio, tornando-se usuários móveis, comunicando-se entre si e acessando vários recursos de informação utilizando computadores portáteis, assistentes digitais pessoais, equipamentos de rádio e celular.

Vários profissionais de diferentes segmentos da sociedade descobriram as vantagens da computação móvel. Em ambientes de negócios, faz-se necessária à

disponibilidade das informações corporativas todo o tempo, fazendo com que as aplicações desenvolvidas para as estações de trabalho móveis não parem por falta de dados.

2.2 – MOBILIDADE

A palavra de ordem para os fabricantes de equipamentos móveis é mobilidade, aproveitar e garantir esse padrão aos produtos é dotá-los com tecnologia *Wireless* para possibilitar a conexão com os sistemas remotos.

As *Wireless* não têm o propósito de substituir as redes guiadas, e sim amplia-las. A mobilidade dos equipamentos portáteis oferece as empresas à oportunidade de compartilhar dados entre redes, com e sem fios, dinamizando a comunicação dos usuários.

As redes locais sem fio constituem-se como uma alternativa às redes convencionais guiadas, fornecendo as mesmas funcionalidades, mas de forma flexível, de fácil configuração e com boa conectividade em áreas prediais ou de campus. Para isso, é preciso que haja uma infra-estrutura capaz de compartilhar dados e informações de forma simples, dinâmica e segura.

2.3 – A TECNOLOGIA *WIRELESS*

Uma *Wireless* é uma extensão de uma rede local convencional guiada, seu funcionamento não é complicado.

Em um ponto central e estratégico, se fixa uma antena, à qual se conecta a rede local, esta antena converte os dados recebidos em onda de rádio ou infravermelho e os envia para outros dispositivos sem fio ou para um ponto de acesso que serve como uma conexão para uma LAN guiada. Como mostra a figura 01.

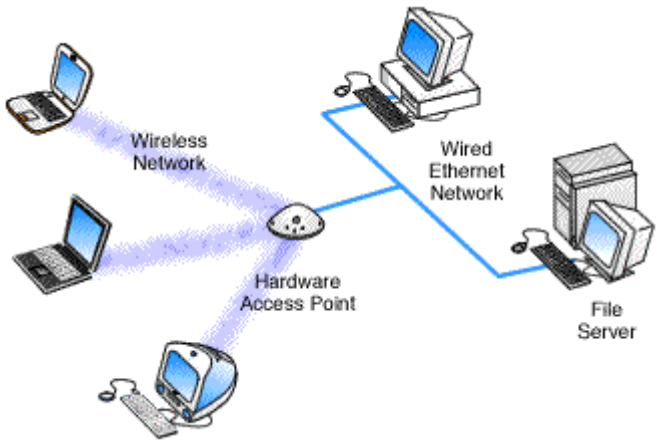


Figura 01: Conexão de uma rede sem fio com uma convencional guiada

Fonte: ARTHAS, 2004

As placas utilizadas nessas instalações (antena-computador) são baseadas no padrão IEEE 802.11b e tem entre outros objetivos apresentar robustez com relação a interferências, oferecer privacidade e controle de acesso ao meio.

As redes sem fios são versáteis e vem ganhado força no mercado. A aprovação do padrão IEEE 802.11, em 1997 e o barateamento dos equipamentos para WLAN (*Wireless Local Área Network*), contribuíram para a expansão da tecnologia *Wireless*.

2.4 – PADRÕES DE MERCADO

O IEEE (*Institute of Electrical and Electronics Engineers*) definiu como padrão para as redes *Wireless* o modelo IEEE 802.11.

Desde o primeiro protocolo IEEE 802.11 aprovado em 1997, ainda houve várias tentativas em melhorar o protocolo. Na introdução dos protocolos, primeiro veio o 802-11, sendo seguido pelo 802.11b. A seguir veio IEEE 802.11a que fornece até cinco vezes a capacidade de largura de banda do 802.11b e depois a IEEE 802.11g que utiliza a mesma faixa de freqüência do IEEE 802.11b atual. Cada um destes grupos tem como objetivo acelerar o protocolo IEEE 802.11, tornando-o globalmente acessível, não sendo necessário reinventar a camada física deste.

2.5 DIFERENÇAS ENTRE PROTOCOLOS

Quando se discute a configuração de uma WLAN existem alguns padrões que devem ser considerados:

2.5.1 IEEE 802.11b

A camada física do 802.11b utiliza espalhamento espectral por seqüência direta que usa transmissão aberta de rede opera na freqüência de 2.400 a 2.4835 GHZ no total de 11Mbps, em ambientes abertos (~450 metros) os fechados (~50 metros). Esta taxa pode ser reduzida a 5,5Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando paredes, interferência, etc.

Dentro do conceito de WLAN tem-se o conhecido Wi-fi (*Wireless Fidely*) que nada mais é do que um nome comercial para o padrão de rede *Wireless* chamado de 802.11b, utilizado em aplicações *indoor*.

A velocidade das redes 802.11b é de 11Mbps, comparável à das redes *Ethernet* de 10Mbps, mas muito atrás das redes de 100Mbps. Estes 11Mbps não são adequados para redes com tráfego muito pesado, mas são mais do que suficientes para compartilhar o acesso a *Web*, trocar pequenos arquivos, jogar games multiplayer, etc.

Conforme a potência e qualidade do sinal se degrada, o ponto de acesso pode diminuir a velocidade de transmissão a fim de melhorar a confiabilidade da transmissão. A velocidade pode cair para 5.5 Mbps, 2 Mbps ou chegar a apenas 1 Mbps por segundo antes do sinal se perder completamente. Algumas placas e pontos de acesso são capazes de negociar velocidades ainda mais baixas possibilitando a conexão à distância ainda maiores. Nestes casos extremos o acesso à rede pode se parecer mais com uma conexão via modem do que via rede local.

Figura 02 – Exemplo de uma rede 802.11b

Fonte: ARTHAS, 2004

2.5.2 IEEE 802.11a

O 802.11b utiliza a freqüência de 2.4 GHZ, a mesma utilizada por outros padrões de rede sem fio e pelos microondas, todos potenciais causadores de interferência. O 802.11a por sua vez utiliza a freqüência de 5GHZ, onde a interferência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo respectivamente 54 Mbps.

A velocidade real das redes 802.11a pode chegar 54 Mbps, quase 5 vezes mais rápido que no 802.11b. Permitindo que mais pontos de acesso sejam utilizados no mesmo ambiente, sem ocorrer perda de desempenho.

Este padrão é mais caro, por isso os primeiros produtos foram destinados ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas.

2.5.3 IEEE 802.11g

Este é um padrão recentemente aprovado pelo IEEE, capaz de transmitir dados a 54 Mbps, assim como o 802.11a. A novidade é que este padrão utiliza a mesma faixa de freqüência do 802.11b (2.4GHZ), e mantém a compatibilidade com esse padrão.

O 802.11g usa o que o 802.11a e o 802.11b possuem de melhor, ou seja, a modulação do 802.11a, o OFDM, e a faixa de freqüência do 802.11b, funcionará de modo

similar ao 802.11a, mas na faixa de 2,4GHZ possibilitando também todas as suas configurações de velocidades.

Tabela 01 - Resumo das taxas de transmissão do 802.11

		802.11b @2.4GHz		802.11g @2,4GHz		802.11a @5.2GHz	
Rate. Mbps	**Single/Multi Carrier**	**Mandatory**	**Optional**	**Mandatory**	**Optional**	**Mandatory**	**Optional**
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	PFDM	
9	Multi			OFDM,CCK-OFDM			OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM,CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM,CCK-OFDM		OFDM
48	Multi				OFDM,CCK-OFDM		OFDM
54	Multi				OFDM,CCK-OFDM		OFDM

Fonte: AMADEI, 2003

2.6 ARQUITETURA DE REDES SEM FIO

O Padrão de arquitetura utilizado pelo IEEE 802.11 é baseado na divisão da área coberta pela rede em células. Essas células são denominadas de BSA (*Basic Service Area*). O tamanho da BSA (célula) depende das características do ambiente e da potência dos transmissores/ receptores usados nas estações.

Também faz parte da arquitetura das *Wireless*:

- BSS (*Basic Servic Set*): Representa um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA;
- AP (*Access Poit*): estações responsáveis pela captura e transmissões de sinais; sistema de distribuição infra-estrutura de comunicação que interliga múltiplas BSS para permitir a construção de redes cobrindo áreas maiores que uma célula;
- ESS (*Extended Service Set*): Representa um conjunto de estações formado pela união de vários BSS conectados por um sistema de distribuição;
- ESA (*Extended Service Area*): Interligação de vários BSS pelo sistema de distribuição através dos APS.

Embora os elementos que fazem parte da arquitetura sem fio possibilitar a constituição de uma rede abrangendo áreas maiores do que o ambiente local, o projeto do IEEE 802-11 limita o padrão IEEE 802-11 às redes locais, com ou sem infra-estrutura.

Na rede WLAN sem infra-estrutura (Ad Hoc), as estações se comunicam numa mesma célula, sem a necessidade de estações especiais para estabelecer comunicações. Numa rede local com infra-estrutura, é necessário a interconexão de múltiplos BSSs, formando um ESS. Nesse caso, a infra-estrutura é representada pelos APs, e pelo sistema de distribuição que faz a interligação desses APs. (Arthas, 2003)

O ponto de acesso é elemento fundamental na arquitetura de rede local sem fio, desempenhando as seguintes funções:

- Autenticação: associação e reasociação garantem a conexão dos dispositivos móveis mesmo que esta saia da sua célula de origem.

- Gerenciamento de potência: Trabalho para economizar energia dos dispositivos móveis.

- Sincronização: garante que as estações conectas ao mesmo *Acesss Point* sejam sincronizadas por um relógio comum.

CAPITULO 3 -SEGURANCA EM REDES SEM FIO

É grande a propagação de empresas que optam por redes *Wireless* ao invés de redes cabeadas. A agência de pesquisa *Gartner Inc.* prevê que, em 2010, cerca de 80% dos principais processos de negócios irão depender do compartilhamento de informações em tempo real entre funcionários móveis. (Symantec, 2004)

Este fato se dá pela flexibilidade e mobilidade, pois se permite a conexão em rede através de ondas de rádio presentes no ar. Mas o que de deve levar em consideração é a segurança, porque apesar da grande facilidade, ela é também muito vulnerável.

Devem-se analisar os riscos e traçar uma política de segurança para garantir confidencialidade, autenticidade e integridade das informações.

A rede *Wireless* utiliza padrões de funcionamento da IEEE, uma organização sem fins lucrativos composta por profissionais de engenharia, computação e eletrônica de 150 países.

A rede sem fio é alvo de muitos ataques, *hackers* estão atentos para roubar dados privados, como senhas de banco, números de cartões de crédito ou até mesmo alterar mensagens e reenviá-las para o seu destino comprometendo assim, a integridade da mensagem.

Para garantir a segurança é necessário ações combinadas, pois prevenções como antivírus apenas não é recomendado para se proteger dados. Métodos diferentes como *firewall*, antivírus, autenticação, criptografia e prevenção de intrusos, agem em conjunto no sentido de bloquear com eficácia as ameaças as quais a *Wireless* está exposta.

Várias tecnologias de segurança são utilizadas, entre elas a VPN (*Virtual Private Network*), que é uma rede privada construída sobre infra-estrutura da rede, que cria túneis de proteção onde às informações são criptografadas na sua origem e são interpretadas apenas no seu destino. Dessa forma os dados que são transmitidos, se capturados não podem ser decifrados.

A VPN pode ser feita de dois arranjos. A figura 03 ilustra o primeiro arranjo. Ao conectar-se com uma rede, se institui um túnel com a rede remota.

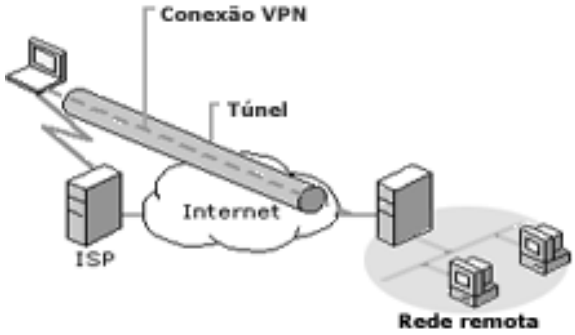


Figura 03: Conexão VPN de um simples *Host*

Fonte: SANTOS VPN, 2004

No segundo arranjo, forma-se um túnel entre duas redes que se interligam, como ilustrados na figura 04.

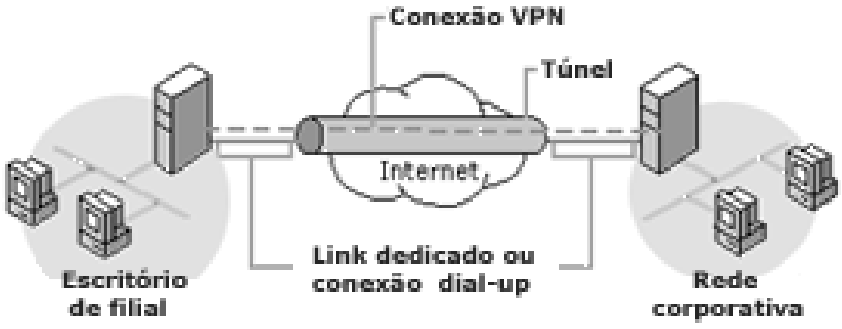


Figura 04: Conexão VPN entre duas redes interligadas

Fonte: SANTOS VPN, 2004

A rede VPN faz uso de vários protocolos, entre eles o IPSec (*Internet Protocol Security*). Tal protocolo permite a conexão e a criptografia entre os *hosts* da rede privada.

O IPSec é baseado em criptografias unificadas, o que dificulta a decodificação no caso de um ataque e assegura maior confidencialidade. Ë necessário também proteção de firewall nas duas pontas.

Sempre que preciso pode-se alterar o SSID (*Service Set Identifier*) como medida de segurança. O SSID é um código usado como senha para o login na rede e permite conexão entre a base e os clientes na rede 802.11.

O WEP (*Wired Equivalency Privacy*) é um algoritmo que usa um sistema de criptografia RC4 da RSA. Quando há transmissão de dados, a chave secreta de 40 ou 104 bits se une a um IV (*Initialization Vector*) de 24 bits para constituir a chave de 64 ou 128 bits.

O WEP deve ser apontado apenas como mais um método de segurança, pois apresenta diversos problemas.

3.1 CRIPTOGRAFIA EM REDES SEM FIO

A criptografia é uma técnica utilizada na computação para armazenar e transportar informações na rede. Faz uso de chaves para abrir e fechar dados criptografados.

Existem dois métodos de trabalho com chaves criptográficas:

Criptografia de chave simétrica: modo usado para aplicações limitadas onde remetente e destinatário se preparam para o uso da chave, deve-se conhecer a chave, pois

quando a mensagem criptografada é recebida apenas à pessoa que contem a chave pode abri-la na caixa de entrada. Este é o modo tradicional e não é recomendado para conexões inseguras.

O IDEA (*International Data Encryption Algorithm*) é um tipo de algoritmo de chave simétrica. Onde a soma da mensagem mais chave gera uma mensagem criptografada, após a geração, ela é enviada através da rede, e ao chegar ao lado oposto, ela é descriptografada através da chave que está no destino (SANTOS). Conforme ilustrado na Figura 05.

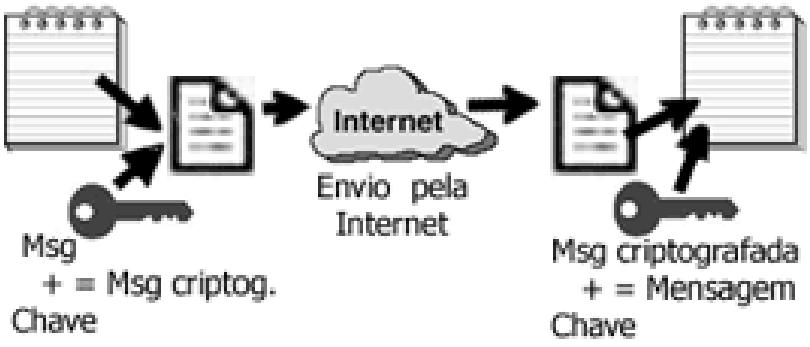
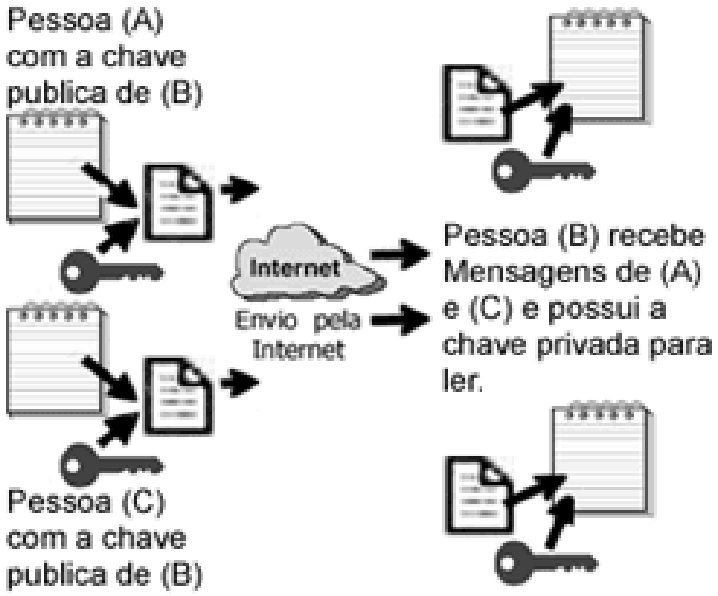


Figura 05: Funcionamento do IDEA

Fonte: SANTOS, 2004

Criptografia de Chave Assimétrica: Modo onde se deve usar duas chaves uma para criptografar e outra para descriptografar. Uma chave fica disponível e outra em sigilo, sendo assim a garantia do segredo da mensagem está na chave privada. O algoritmo que a chave usa é o RSA. Seu funcionamento é ilustrado na Figura 06.

Figura 06: Funcionamento do RSA



Fonte: SANTOS, 2004

Pessoas diferentes (A e C) e com chaves públicas, utilizam a chave de uma outra pessoa (B) para escrever a mensagem. A mesma é enviada pela internet e a pessoa (B) recebe a mensagem (A e C) e usa uma chave privada para descriptografar.

3.2 WEP

Como já foi dito o WEP é um algoritmo usado para criptografar dados na rede, empregando confidencialidade para os clientes é um mecanismo para privacidade de dados que usa a criptografia avançada. O WEP também usa a função CRC-32 para revelar erros. Ao fazer o "*checksum*" de uma mensagem enviada gera o ICV (*Integrity Check Value*) que deve ser comparado pelo destinatário, garantindo que a mensagem não foi corrompida ou alterada.

O WEP tem a função de prevenir o reconhecimento dos dados e invasão por intrusos, é um sistema de segurança de nível médio onde se torna necessário possuir segurança adicional.

Dizem os especialistas que a sua estrutura pode ser facilmente invadida através do controle das chaves, através da monitoração passiva do fluxo de dados por um certo período, ou ainda através da inserção de textos puros combinados com tentativas de vetores possíveis, os quais são limitados a 24 bits de tamanho e que podem assim ajudar a deduzir a chave, que, aliás, é um segredo compartilhado que nunca muda. (WolrdTelecom, 2004)

Um novo algoritmo foi lançado, o WPA (*Wi-Fi Protected Access*) um WEP melhorado com mais eficiência nos recursos de segurança.

Criado para implementar a segurança e acabar com as vulnerabilidades da WEP, o WPA é um protocolo usado para entrega de informações e serviços, incluindo suporte para encriptação, para equipamentos utilizados na comunicação de redes *Wireless*. Para quem tem o WEP instalado e quer fazer uso da WPA, basta atualizar o software.

Um dos benefícios é que ao utilizar a chave temporária (TKIP) torna possível a criação de chaves por pacotes o que melhora a criptografia de dados, e inclui uma função captadora de erros, um VI de 48 bits e um modo de distribuição de chaves.

Outro beneficio é a autenticação central que faz a autenticação dos usuários antes de acessarem a rede.

O funcionamento do protocolo acontece da seguinte maneira: o WTLS (*Wireless Trasnport Layer Security*) faz a encriptação da estação ate o *gateway* WAP e a encriptação desse ponto ate o servidor *Web* é feito pelo SSL.

O problema é que a informação nesse caso deve ser encriptada no *gateway* WAP, depois volta a ser encriptada usando WTLS antes de ser enviada ao dispositivo WAP de maneira que no *gateway* WAP, neste momento a informação que é puro texto, fica temporariamente desprotegida. Deve-se evitar que a informação fique desprotegida em qualquer ponto de transmissão da rede *Wireless*.

3.2.1 PROBLEMAS DO WEP

A chave secreta usada numa rede é a mesma para todas as estações o que muda é o VI que deve ser diferente para cada pacote, eliminando a repetição de seqüência RC4, pois gera ataques por intrusos e ate descoberta de pacotes.

É necessário que a chave secreta seja trocada constantemente para aumentar a segurança da rede. Porem a troca é manual o que torna o processo de troca impraticável quando essa rede é utilizada por muitos clientes.

A CRC.32 que tem a função de revelar erros não contem chave, sendo assim fica possível modificar uma mensagem , no meio do caminho sem que seja descoberto pelo destinatário.

É possível descobrir a seqüência RC4 e ser autenticado na rede, podendo inclusive enviar mensagens clandestinas, isso porque a função não possui uma chave.

Outro ponto é que 80% das redes sem fio não usam mecanismos básicos de segurança, por que os mesmos vêm desabilitados.

3.3 IEEE 802.11i

Grupo de trabalho que está definindo novo padrão de segurança para prevenir vulnerabilidades da *Wireless*, com soluções para WLAN como a 802.11a e 802.11g. Sua função é resolver problemas ligados a confidencialidade e integridade, substituindo o protocolo WEP. (MAIA, 2003)

3.4 TKIP (*Temporal Key Integrity Protocol*)

Criado pela IEEE para excluir problemas apresentados pela WEP, proporcionando maior segurança e compatibilidade.

O MIC (*Message Integrity Code*) tem a finalidade de impedir ataques do tipo bit-flipping, é ele quem garante a integridade no TKIP.

O MIC é um campo do frame 802.11i, calculado a partir de diversas informações contidas no próprio frame, como, por exemplo, os endereços MAC de origem e destino. (MAIA, 2003).

3.5 CONFIGURAÇÃO

Existem alguns tipos de configurações de WLAN, basta analisar a que melhor atende as suas necessidades ou da sua empresa.

- Rede Ad Hoc: Do latim “apenas para esse propósito”, rede onde há outras sem infra-estrutura de cabo cria-se uma rede “on the fly” através da configuração dos nós onde os dispositivos fazem parte da rede apenas no período da comunicação, conforme apresentado na Figura 07.

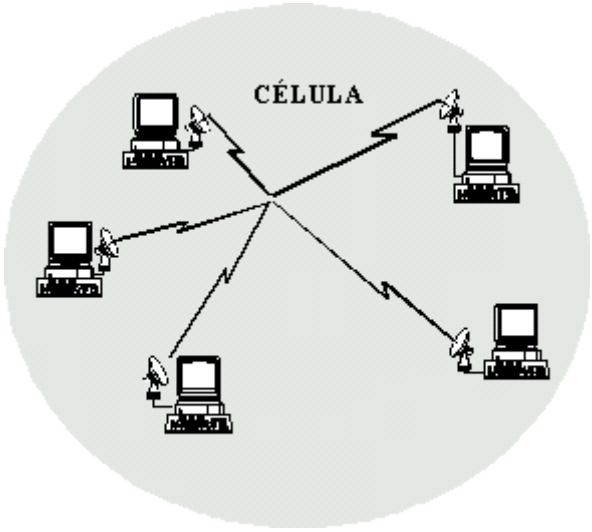


Figura 07: Rede *Wireless* Ad Hoc

Fonte: GARCIA, 2004

- Rede de Infra-estrutura: Modo mais utilizado, nas WLANS, permite que os clientes se comuniquem com a rede guiada através de um AP, funcionando como um cliente de rede Poe cabo BSS é especificação usada para este tipo de rede. Pontos de conexão – deve-se configurar o componente com a tecnologia WI-FI para se conectar a produtos e serviços da LAN sem fio grátis ou pago, conforme apresentado na Figura 08.

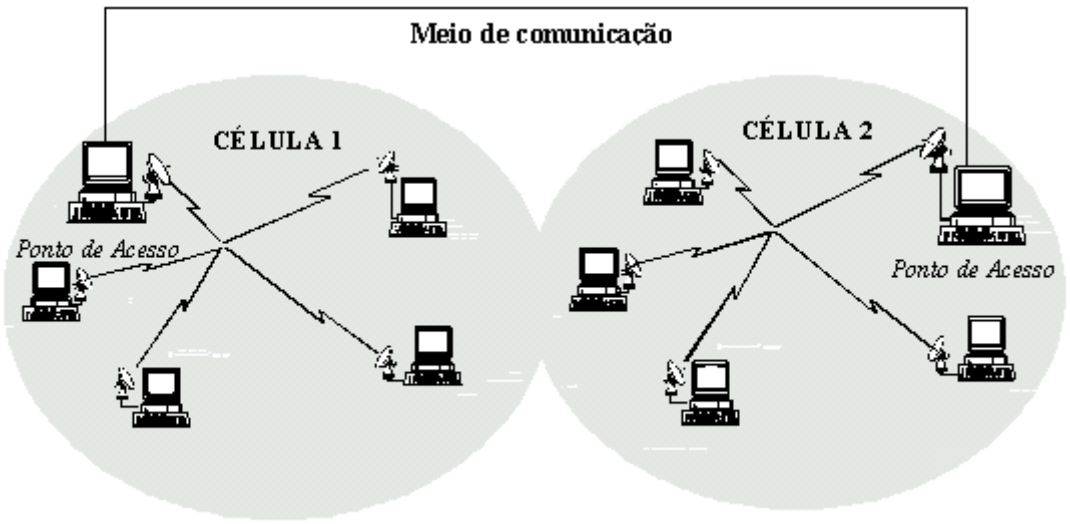


Figura 08: Rede *Wireless* de Infra Estrutura

Fonte: GARCIA, 2004

- Rede Infra estruturada: também conhecido como ESS (*Extend Service Set*) permite que o cliente mude seu AP e continue conectado através Aps de redes distintas (BSS DS), criando uma única rede, conforme apresentado na Figura 09.

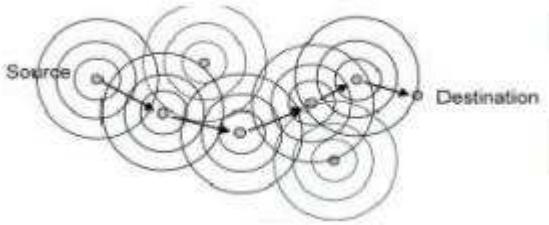


Figura 09: Rede *Wireless* Infra estruturada

Fonte: ARTHAS, 2003

3.6 *ACCESS POINT*

São pontos que permitem o acesso de clientes na rede *Wireless* a redes locais cabeadas.

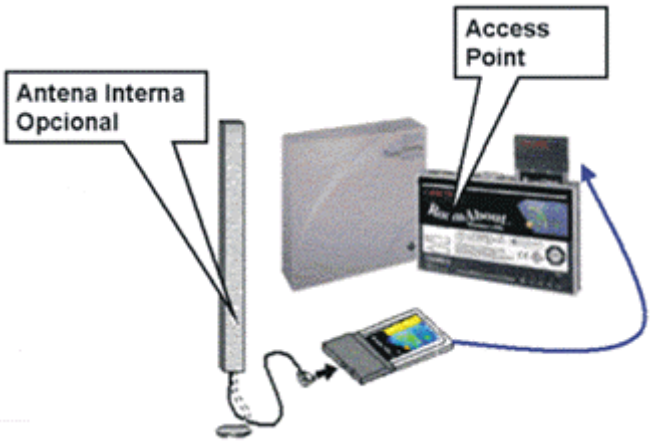
Wireless precisa de um acess point quando se quer conectar *notebooks* ou computadores de mesa a rede com fios.

A grande vantagem é que a capacidade de alcance da rede local sem fio é aumentada para quase o dobro, quando comparado à rede simples (ad-hoc).

Permite que as estações operem em velocidade máxima, direcionando todos os dados da rede, ou seja, é usado como fiscalizador de tráfego.

Admite o compartilhamento de internet ao utilizá-lo como ligação central com o mundo externo, , conforme apresentado na Figura 10.

Figura 10: AP (A*cess Point*)



Fonte: GARCIA, 2003

3.7 AUTENTICAÇÃO

Tecnologias disponíveis para rede *Wireless* têm seu controle de acesso através da autenticação, que pode ser de dois tipos:

- *Open System*: Pode-se acessar a rede através de qualquer estação. Quando o mecanismo de criptografia estiver habilitado, se a estação não possuir a chave secreta não se consegue transmitir nem receber dados pelo AP, mesmo que estação seja autenticada. Quando estiver desabilitado, qualquer estação poderá acessar o AP.

- *Shared Key*: Apenas os clientes são autenticados no AP através de chaves WEP que são compartilhadas. O problema está no caso de furto de alguma estação, caso isso aconteça as chaves devem ser trocadas. A chave compartilhada usa a técnica *challenge-response*. A figura abaixo mostra seu funcionamento.

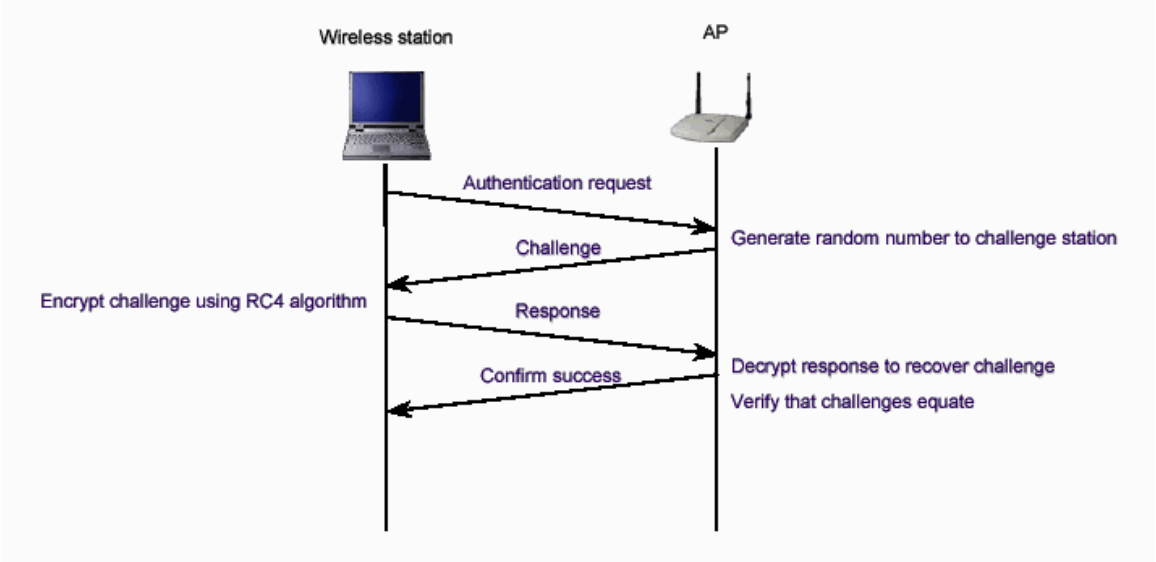


Figura 11: Autenticação *shared key*

Fonte: GARCIA, 2003

Na figura 11 a estação sem fio (*Wireless station*) está solicitando ao AP sua autenticação (*authentication request*). O AP gera um numero aleatório (*challenge*) e o envia para a estação. A estação recebe o numero, criptografa-o utilizando o algoritmo RC4 e o envia de volta (*response*). O AP decripta a resposta e a compara com o numero enviado. Se a comparação for positiva, o AP envia para a estação um mensagem confirmando o sucesso da autenticação. (Garcia, 2003)

4. INSEGURANÇA NO AR

O acesso de intrusos aos computadores, sejam eles de uso pessoal, empresarial e outros, sem apoderar-se do HD, é possível graças ao uso das redes. Essa intromissão ao banco de dados de outros usuários que utilizam esse tipo de serviço, tem motivos e objetivos diferentes, que variam de acordo com o tipo de intruso.

O que tem de mais importante nessas intromissões são as conseqüências que isso podem trazer para as pessoas que usufruem desta tecnologia. Alguns exemplos são: a clonagem dos números de cartão de crédito para vendê-los, as visitas ao correio eletrônico alheio, os desvios de dinheiro de uma conta bancária e principalmente a insegurança gerada aos indivíduos que permanecem por muito tempo on-line.

4.1 INTRUSOS

No mundo físico, um intruso poderia ser descrito como uma pessoa que sem autorização tenta invadir a sua casa, seja arrombando uma porta ou janela ou pulando o muro. Com o objetivo de roubar alguns de seus pertences ou espionar sua vida íntima.

No mundo computacional, um intruso pode ser descrito como um indivíduo que tenta acessar um sistema sem possuir permissão para isso. Este pode apresentar objetivos distintos como:

- Acessar o correio eletrônico de outras pessoas;
- Roubar dados;
- Descobrir as estratégias empresárias dos concorrente;
- Vingar-se de instituições;
- Descobrir e clonar números de cartões de crédito;
- Espionar segredos militares de inimigos; Etc.

Para atingirem seus objetivos os intrusos apresentam basicamente quatro comportamentos distintos com relação a origem e destino das mensagens:

- Interrupção: Tenta interromper o fluxo de dados, deixando o destino sem receber informações, conforme apresentado na Figura 12.

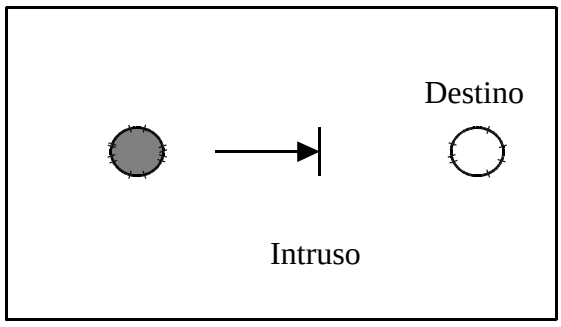


Figura 12: Comportamento de interrupção.

- Interceptação: Tenta apenas tomar conhecimento do fluxo de dados que trafega em uma conexão, conforme apresentado na Figura 13.

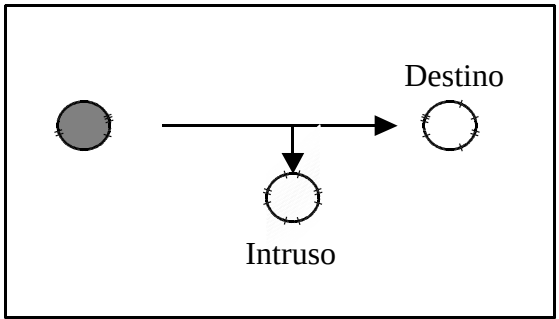


Figura 13: Comportamento de interceptação.

Modificação: Tenta interceptar os dados e modificá-los antes que estes cheguem ao destino, conforme apresentado na Figura 14.

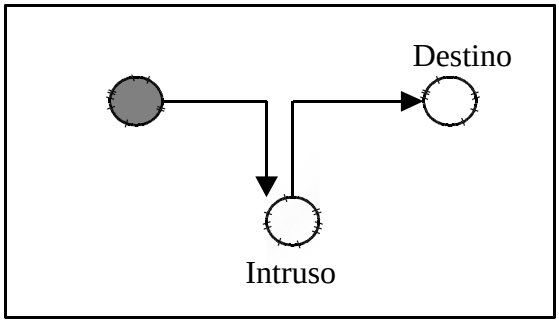


Figura 14: Comportamento de modificação.

- Fabricação: Tem como objetivo fabricar dados e enviá-los ao destino como se fosse uma origem válida, conforme apresentado na Figura 15.

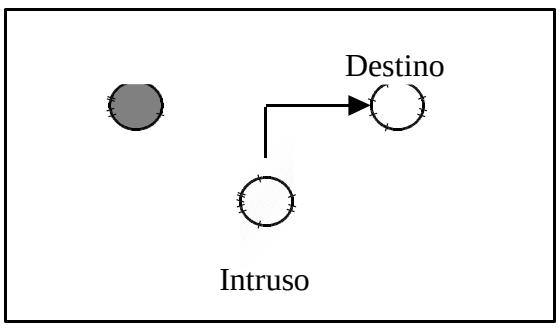


Figura 15: Comportamento de fabricação.

E assim o que seria o conforto da tecnologia moderna se torna um motivo irritabilidade e um desgaste para o usuário que deverá então procurar novas formas de segurança para que tenha atendida as suas expectativas com relação ao serviço de rede.

4.2 VULNERABILIDADE DAS REDES SEM FIO

O protocolo 802.11 apresenta pouca vulnerabilidade, mais no entanto podem causar enormes problemas. A principal vulnerabilidade encontrada diz respeito ao WEP que utiliza o algoritmo RC4 para a criptografia, gerando um grande problema com relação a confiabilidade, uma vez que o RC4 utiliza uma nova chave a cada frame enviado. Esta chave é formada por uma palavra chave formada por 40 ou 104 bits, e por uma parte variável (IV) formado por 24 bits.

O problema está justamente no IV que pode se repetir em pouco tempo comprometendo a chave como um todo.

A vulnerabilidade das redes sem fio podem ser definidas como sendo os pontos frágeis, aos quais um intruso pode explorar para conseguir acesso a rede. Estas se dividem em:

4.2.1 AS FALHAS NOS MÉTODOS DE AUTENTICAÇÃO

De acordo com o IEEE 802.11b é através dos métodos de autenticação criptografados ou não que uma conexão pode ser estabelecida.

Access Points, beacons, broadcasts e os SSIDs dão informações sobre os canais a serem usados e identificam uma rede disponível para o acesso. E a isso consideramos um método de autenticação não criptografado aberto. Esse AP, que permite a conexão entre LAN e *Wireless*, dá margem para que o SSID seja descoberto por qualquer dispositivo.

O método não criptografado fechado exige apenas a seqüência correta de caracteres do SSID para o acesso à rede. Mas esses são métodos arcaicos e muito vulneráveis.

No método criptografado o cliente não tem a segurança de que está estabelecendo uma comunicação com um AP autorizado porque as chaves compartilhadas, WEP pré-definidas, autenticam o cliente no AP, mas não autentica o AP para o cliente. As mensagens sempre são criptografadas com uma chave diferente, porém a mesma chave usada pra criptografar pode descriptografar, já que utiliza um algoritmo RC4 que é simétrico.

Para que as chaves WEP sempre sejam diferentes são inseridos nela elementos adicionais conhecidos como *Stream Cipher*. E são esses elementos que dificultam o uso desse algoritmo nas redes sem fio devido ao tamanho das chaves e do vetor de iniciação.

4.2.2 A VULNERABILIDADE DE ALGUNS DISPOSITIVOS

A maioria dos equipamentos vem com os mecanismos básicos de segurança desabilitados. Isso normalmente ocorre devido à complexidade de configuração de sistemas operacionais e aplicativos.

Mesmo quando estão habilitados é importante que as chaves WEP e a senha utilizada não sejam as mesmas que acompanham a configuração padrão dos equipamentos.

Porque o sistema é frágil e permite que através de uma simples busca na internet, o intruso consiga os dados para realizar a invasão.

A utilização de APs não autorizados é um fator que aumenta a vulnerabilidade das redes sem fio, porque durante uma conexão todos os canais, sejam eles o canal atual, o anterior ou posterior, recebem os *Beacon frames* através de APs. Estes vão fazer a sincronia, sinalização e envio de informações sobre a rede sem fio que está sendo utilizada. Muitas desses *frames* serão indicadores de *rogue access points*, ou seja, indicam o grampeamento dos pontos de acesso.

4.3 FATORES QUE CONTRIBUEM PARA A INVASÃO

Existem os riscos externos ou internos caracterizados por ataques diretos ou não, respectivamente. Esses ataques são possíveis devido a exposição das vulnerabilidades dos dispositivos aos intrusos.

A não autorização à instalação e a falta de conhecimento técnico sobre as WLANs, faz com que elas sejam instaladas de maneira incorreta e que não alcancem o seu desempenho esperado. E como conseqüência disso, os usuários que não respeitam a política de segurança terão expostos o seu SSID ao enviá-los em *broadcast* e sem o uso da criptografia. Essas são as chamadas *Rogue* WLANs, que permite que os dados sejam expostos sem que o invasor exerça um ataque direto para adquiri-las.

O uso correto das configurações de segurança dos sistemas de redes sem fios é uma das melhores maneiras de prevenir a invasão.

A falta de esclarecimento aos clientes sobre o uso de configurações de segurança e à área de cobertura faz, com que os usuários tenham as suas redes expostas a ataques externos, agravando o problema que diz respeito a associação de um dispositivo a outro.

Essas associações podem ocorrer quando o sinal de um usuário invade uma área de abrangência de outro e então dados deste podem se associar ao banco de dados daquele.

O dispositivo atuando em modo ad hoc também facilita essa associação de dispositivos uma vez que em suas redes não é preciso a confirmação de um AP para que seja estabelecida a comunicação.

Outra forma de associação é a criação de uma ESS, que nada mais é que a associação de APs.

Muitas pessoas não sabem da existência do dispositivo de segurança e quando sabem a maioria não tem conhecimento suficiente de como usá-lo. Como cada vez mais o sistema *Wireless* está fazendo parte dos computadores pessoais e empresariais, devido ao menor custo, a associação acidental pode tornar-se cada vez mais freqüente.

O uso de VPNs nas WLANs não é suficiente para impedir as invasões, porque usuário experiente ao invés de atacar a VPN pode simplesmente realizar o ataque a métodos de autenticação dos dispositivos de rede sem fio que são mais vulneráveis. Sendo assim, as WLANs que utilizam VPN tem uma configuração insegura.

O uso de VPNs permite que o tráfego seja analisado e por isso minimizam os ataques. Mas ainda não é um dispositivo completamente seguro já que a identificação do atacante é complicada, graças ao uso de recursos do sistema *Wireless*. Onde o atacante não precisa estar ligado ou associado fisicamente ao dispositivo que vai interceptar para analisar e

capturar todos os dados. Essa é a grande dificuldade de saber como impedir este tipo de ataque e introdução de vulnerabilidade, que é conhecida como *Espionage* e *Eavesdropping*.

Através de todas as técnicas descritas anteriormente o invasor pode conseguir um IP válido e um endereço MAC válido e a partir daí alterar o seu próprio MAC e IP acessando com os dados da vítima.

Conhecer o SSID e ter um método de autenticação aberto não é mais o suficiente para estar conectando a WLAN, pois esta na maioria das vezes consegue filtrar os usuários por endereços MAC (*Médium Access Control*).

4.4 INVASÃO ÀS REDES SEM FIO

O ataque a redes não começou com o aparecimento das WLANs. Os ataques a redes sem fio seguem, em grande maioria, o mesmo padrão de ataque feitos as redes guiadas. Somente alguns tipos de ataque sofreram modificações para serem disparados e obter melhores resultados.

A maioria dos invasores busca ganhar acesso ou comprometer a rede guiada, mas sem prejudicar a rede sem fio.

Como as redes guiadas são as mais antigas elas já desenvolveram sistemas de defesas mais avançados. Um exemplo disso é o uso do *firewall.*

O *firewall* é um dispositivo que tenta diminuir ao máximo uma invasão. Ele pode analisa a conexão a procura de um hacker, quando uma tentativa de invasão é detectada

ele bloqueia a conexão, informa ao usuário sobre o problema antes que a invasão seja estabelecida e pode bloquear portas vulneráveis.

Os principais ataques à redes sem fio na atualidade são:

ASSOCIAÇÃO MALICIOSA: Ocorre quando o atacante consegue tantas informações quanto necessárias para poder configurar um *access point* e iluda o sistema fazendo que este pense estar conectando a uma rede sem fio real.

ARP *POISONING*: Este ataque, também conhecido como ataque de envenenamento ao protocolo de resolução de endereço (ARP), só pode ser executado se o atacante estiver conectado à mesma rede da vítima. Limitando-se a redes conectadas por *hubs*, *switches a bridges* (Duarte, 2003).

MAC *SPOOFING*: Algumas instituições enviam lista de acesso para os dispositivos autorizados a acessar a rede sem fio. Mas como os dispositivos para redes sem fio permitam alterar o seu endereço físico. O atacante altera seu endereço MAC pelo cliente que possui permissão para acessar a rede (Duarte, 2003).

D.O.S (*DENIAL OF SERVICE*): Como as redes sem fio, a maioria trabalha na rádio freqüência de 2,4 GHz, que é a mesma utilizada por

inúmeros aparelhos eletrodomésticos o atacante pode usufruir desta particularidade para disparar o ataque de D.O.S que como o nome mesmo indica possui o objetivo de tornar o sistema ou recurso indisponível, o que pode causar uma grande incômodo para os usuários da rede.

ATAQUE DE VIGILÂNCIA: Consiste basicamente em o atacante percorrer a instituição localizando a posição da instalação de dispositivos *Wireless*, para posteriormente poder tentar invadir a rede através destes dispositivos, ou até mesmo resetar ou até mesmo roubar estes dispositivos.

***WARDRIVING*:** É a atividade de dirigir um veículo pela cidade com a finalidade de procurar redes *Wireless* desprotegidas. Utiliza para tal um notebook, uma placa Ethernet, e algum tipo de antena (que pode ser construída até mesmo com uma lata de batatas fritas). O atacante pode através da técnica *Wardriving* identificar redes indefesas o que facilita o ataque. Os praticantes consideram a atividade legítima.

***WARCHALKING*:** É a prática de escrever através de símbolos específicos em paradas ou em calçadas informações sobre as redes *Wireless*, facilitando a invasão por outros atacantes. Alguns símbolos são descritos abaixo:

Open Node: Rede vulnerável, conforme apresentado na Figura 16.

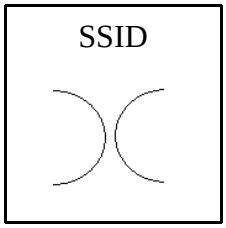


Figura 16: *Open Node*

Closed Node: Rede fechada, conforme apresentado na Figura 17.

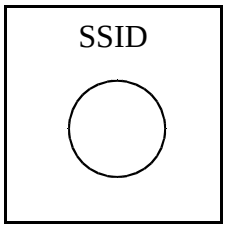


Figura 17: *Closed Node*

WEP *Node*: Informa que a rede *Wireless* utiliza o padrão de segurança WEP, conforme apresentado na Figura 18.

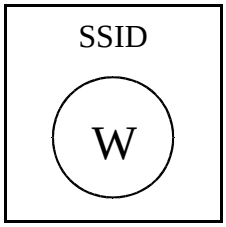


Figura 18: WEP *Node*

Em cima de cada símbolo temos o SSID, que funciona como uma senha de login a rede.

CONCLUSÃO

As redes sem fio, já foram aceitas pelos usuários que vêem grande vantagens em utilizar a computação móvel, seja no ambiente corporativo ou mesmo em suas residências.

Os problemas que envolvem a segurança existentes hoje podem ser minimizados alterando simplesmente a configuração padrão dos equipamentos. O que torna a invasão às redes *Wireless*, por intrusos com pouco conhecimento e falta de dispositivos tecnológicos sofisticados quase impossível.

Com a elaboração de novos padrões que visam aumentar a segurança, este problema tende a ser definitivamente corrigido, transformando a invasão a redes *Wireless* em um grande desafio para os intrusos.

A computação móvel esta realizando uma revolução no atual estágio de desenvolvimento da computação pessoal, já podemos contar com dispositivos voltados para os mais diversos fins. Isso faz com que os fabricantes de soluções invistam pesada cifras neste segmento, que se torna muito atrativo para os profissionais que queiram desenvolver-se nesta área.

BIBLIOGRAFIAS

ARTHAS, Kael, **Tutorial: Redes *Wireless***, *Net* 2003, Disponível em <www.babooforum.com.br/idealbb/view.asp?mode=viewtopic&topicID=269602&num=20&pageNo=1> Acesso em 03 de dez. 2004.

DUARTE, Luiz Otávio. Trabalho Monográfico - Universidade Estadual Paulista Júlio de Mesquita Filho, unesp. *Net* 2003, Disponível em www.acmesecurity.org/hp_ng/files/testes_monografias/acme-monografia-*Wireless*-2003-LOD.pdf. Acesso em 23/03/2004.

GARCIA, Luis Guilherme Uzeda, **REDES 802.11 (Camada de Enlace)**, *Net* 2003, disponível em www.gta.ufrj.br/grad/01_2/802-mac/R802_11.htm , Acesso em 03/12/2004.

It*Web*, **Wi-Fi na sua vida**, *Net* 2004, disponível em www.it*Web*.com.br/solutions/telecom/*Wireless*/artigo.asp?id=39740, Acesso em 03/12/2004.

Jornal Log*Web*, **RF: um mercado em crescimento**, *Net* 2003, Disponível em www.cdcbrasil.com.br. Acesso em 03/12/2004.

AMODEI JUNIOR, Aurelio. **Esquemas de Modulação do IEEE 802.11**, *Net* 2003, disponível em www.gta.ufrj.br/seminarios/semin2003_1/aurelio/indice.htm , Acesso em 03/12/2004.

LIMA, Leonilde Antonieta T. de, **FUNCIONAMENTO E REDES SEM FIO**, *Net* 2004, Disponível em http://www.dimap.ufrn.br/~gold/funcionamento.htm#inicio. Acesso em 03/12/2004.

MAIA, Roberto. **Segurança em Redes *Wireless* 802.11i**, *Net* 2004, Universidade Federal do Rio de Janeiro disponível em www.gta.ufrj.br/~rmaia/802_11i.html#a1. Acesso em 08/04/2004.

MARINHO, Edemar, **Mobilidade Corporativa - Problemas e Soluções**, *Net* 2004, Disponível em www.hbtec.com.br/portal/modules.php?name=News&file=article&sid=4, Acesso em 03/12/2004.

MARTINS, Marcelo, **Protegendo as redes *Wireless* 802.11b – Write paper,** *Net* 2003, Modulo Security disponível em www.modulo.com.br/index.jsp. Acesso em 23/08/2004.

MATEUS, Geraldo Robson, LOUREIRO, Antonio Alfredo F., Introdução à Introdução à Computação Móvel, 11a Escola de Computação, COPPE/Sistemas, NCE/UFRJ, 1998, disponível em http://www.dcc.ufmg.br/~loureiro/cm/docs/cm_livro_1e.pdf Acesso em 03/12/04.

MODULO SECURITY. Disponível em www.modulosecurity.com.br. Acesso 03/12/2004.

PORTAL INDEPENDENTE DE TELECOMUNICAÇÕES. Disponível em www.*Wireless*brasil.org. Acesso em 03/12/2004.

SANTOS VPN, Luiz Carlos dos, **Como funciona a VPN?**, *Net* 2004, disponível em www.clubedasredes.eti.br/rede0004.htm, Acesso em 03/12/2004.

SANTOS, Luiz Carlos, **Como funciona a Criptografia?**, *Net* 2003, disponível em www.clubedasredes.eti.br/rede0009.htm , Acesso em 03/12/2004.

SILVA, Adailton J. S. **As Tecnologias de Redes *Wireless*** - Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa 15 de maio de 1998, volume 2, número 5 disponível em www.rnp.br/newsgen/9805/*Wireless*.html#ng-ieee. Acesso em 20/08/2004

SYMANTEC, **Evolução das pragas virtuais expõe redes sem fio**, *Net* 2004, disponível em www.noticias.uol.com.br/mundodigital/proteja/symantec/corporativa/ult2595u12.jhtm, Acesso em 03/12/2004.

Symantec, Evolução das pragas virtuais expõe redes sem fio, publicado em 27/10/2004, disponível em www.noticias.uol.com.br/mundodigital/proteja/symantec/ corporativa/ult2595u12.jhtm, Acesso em 03/12/2004

WMLClub, **SEGURANÇA EM WAP**, *Net* 2004, disponível em www.br.wmlclub.com/noticias/2001-03-08-3.htm , Acesso em 03/12/2004.

WordTelecon, **Como criar uma WLAN inviolável**, *Net* 2003, disponível em http://worldtelecom.uol.com.br/AdPortalV3/adCmsDocumentoList.aspx, Acesso em 03/12/2004.