Problemas de segurança na internet enfrentados pelas redes sem fio

Alunos:
Adriano Cesar Braga Borges
Fabrício Gonçalves de Azevedo
Fernando Matheus Marqus

Belo Horizonte – 08 de Novembro de 2010

1 Sumário

1. Introdução

1.1.Motivação

Seja porque você fez uma chamada usando um telefone portátil, recebeu uma mensagem no seu Pager, checou seu e-mail através de um PDA ou acessou a internet através de uma rede sem fio, você se depara com uma rede “wireless” (sem fio).

Se um usuário, aplicação ou empresa deseja tornar seus dados portáteis, móveis e acessíveis, então redes sem fio são a resposta.

Além disso, as redes sem fio se mostram muito úteis em lugares públicos: bibliotecas, hotéis, cafeteiras, instituições de ensino e aeroportos.

As redes sem fio sofrem vários problemas dado a sua transmissão através de ondas eletromagnéticas tais como interferência, falta de privacidade, instabilidade de conexão, entre outros.

Desta forma, é interessante estudar mais profundamente os problemas que assolam as redes sem fio, principalmente as redes sem fio locais, por serem as mais difundidas.

1.2.Tipos de redes sem fio

Os tipos de redes sem fio são caracterizados na tabela 1:

Tabela 1 – Tipos de Redes sem Fio caracterizadas por distância

WLANS : Wireless Local Area Networks / Redes de Locais sem Fio	Permitem os usuários de uma área local, tal como um campus de uma universidade ou uma biblioteca. Uma rede temporária pode ser formada por um pequeno número de usuários sem a necessidade de uso de um ponto de acesso (Access Point).
WPANS: Wireless Personal Area Networks/ Redes Pessoais sem Fio	As duas tecnologias existentes para WPANs são infravermelho (IR) e Bluetooth (IEEE 802.15). Elas permitem a conectividade de dispositivos pessoais com uma área de 30 pés (9,144 metros), porém os infravermelhos necessitam de estar com os feixes direcionados, diminuindo ainda mais a área de ação.
WMANS: Wireless Metropolitan Area Networks/ Redes Metropolitanas sem Fio	Essa tecnologia permite a conexão de múltiplas redes em uma rede metropolitana tal como prédios de uma cidade, sem ter a necessidade de usar cabos de cobre ou fibra ótica.
WWANS: Wireless Wide Area Networks/ Redes de Longa Distância sem Fio	Esses tipos de redes podem ser mantidas por longas distâncias, por exemplo, cidades ou países, através de sistemas de múltiplos satélites ou antenas de provedores de sinal. Esses tipos de sistemas se referem à tecnologia 2G ou

	3G.

Na tabela 2 podemos visualizar o tipo de rede e sua distância de cobertura.

Tabela 2 – Tipo de rede e distância típica de cobertura

Metros	**Rede**
0-10	Personal Area Network
0-100	Local Area Network
0-10000	Wide Area Network

As redes podem ser configuradas como redes Infra-estrutura ou Ad-Hoc. Cada tipo será explicado a seguir:

- Infra-estrutura: Consiste em um ou mais pontos de acesso sendo conectados a uma rede existente. Isto permite que dispositivos sem fio façam uso dos recursos de rede como, pro exemplo, a Internet. Os pontos de acesso são caracterizados por serem pontes de conexão entre a rede com cabos e a rede sem fio.

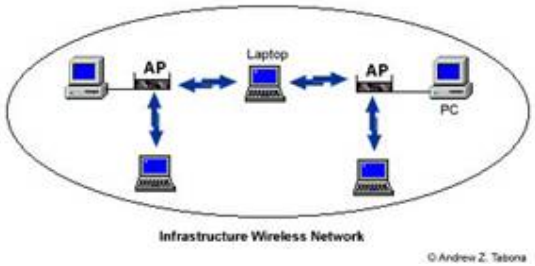

Figura 1 - Exemplo de rede sem fio com configuração Infra-estrutura

- Ad-Hoc: Os dispositivos se conectam diretamente uns aos outros.

Figura 2 - Rede sem fio com configuração Ad-Hoc

Pelo fato de redes sem fio utilizarem ondas eletromagnéticas, a privacidade pode ser comprometida, pois qualquer pessoa próxima ao ponto de acesso pode captar as informações transmitidas. Desta forma, os projetistas de redes desenvolveram várias ferramentas para aumentar a segurança dessas redes. As ferramentas de segurança serão abordadas mais adiante neste trabalho.

1.3.Família 802.11

O Padrão 802.11 surgiu nos anos 90 e foi desenvolvido pelo IEEE. Agora ele representa a principal tecnologia para redes sem fio no mundo.

Na tabela 3 estão presentes os diferentes tipos pertencentes à família 802.11.

Tabela 3 – Diversas versões do 802.11

802.11	Usa FHSS (frequency hopping spread spectrum) ou DSSS (direct sequences spread spectrum) e proporciona de 1 a 2 Mbps de largura de banda na faixa de frequência de 2,4GHz.
802.11a	Usando o OFDM (orthogonal frequency division multiplexing) proporciona até 54Mbps e funciona na faixa de frequência de 5GHz.
802.11b	Também conhecido como Wi-Fi ou 802.11 de alta frequência, utiliza DSSS e se aplica para redes sem fio locais. É mais comum em redes particulares residenciais. Proporciona largura de banda de 11 Mbps e taxa de Fall Back de 5,5, 2 e 1 Mbps.

802.11g	Proporciona uma taxa de transmissão maior que 20 Mbps. É utilizado para WLANs e funciona na frequência de 2,4GHz.
802.11n	Protocolo recente que habilita o uso de múltiplas entradas e saídas (MIMO – Multiple-In-Multiple-Out). Isso permite o aumento do desempenho e distância das redes sem fio.

1.4. Enfocando a WLAN

Uma WLAN é uma rede local sem fio, implementada como extensão ou alternativa para redes convencionais. Além de redes locais, esta tecnologia pode ser utilizada para redes de acesso à Internet, que, nestes casos, são denominadas redes WI-FI (Wireless Fidelity).

As WLANs utilizam majoritariamente sinais de RF para a transmissão de dados, minimizando a necessidade de cabos de conexão dos usuários à rede. Desta forma, uma WLAN combina comunicação de dados com mobilidade dos usuários dentro da área de cobertura da rede, que pode atingir algumas centenas de metros.

As tecnologias de redes de locais e pessoais sem fio mais conhecidas atualmente são IEEE 802.11, Bluetooth e HomeRF. O padrão IEEE 802.11 foi especialmente desenvolvido para aplicações de WLANs, enquanto que as tecnologias Bluetooth e HomeRF são utilizadas em redes pessoais WPANs.

As WLANs possibilitam altas taxas de dados a distâncias de dezenas ou até algumas centenas de metros, oferecendo todas as funcionalidades de uma rede convencional. O padrão IEEE 802.11, por exemplo, transmite dados a taxas até 11 Mbps, cobrindo uma distância nominal de 100 metros.

As WLANs têm sido usadas em campus de instituições de ensino, prédios comerciais, resorts, aeroportos, condomínios residenciais, medicina móvel no atendimento aos pacientes, transações comerciais e bancárias. Além disso, as WLANs também são

empregadas onde não é possível atravessar cabos, como por exemplo, em construções antigas ou tombadas pelo patrimônio histórico.

Dependendo da tecnologia utilizada, a transmissão de sinais RF em redes WLANs pode ser realizada em duas categorias de bandas de freqüência:

i. ISM – As Bandas ISM (Instrumentation, Scientific & Medical), compreendem três segmentos do espectro (902 a 928 MHz, 2.400 a 2.483,5 MHz e 5.725 a 5.850 MHz) reservados para uso sem a necessidade de licença.
ii. U-NII – Unlicensed National Information Infrastructure: Esta banda foi criada pelo FCC nos Estados Unidos, sem exigência de licença, para acesso à Internet, e compreende o segmento de freqüências entre 5.150 e 5.825 MHz.

A topologia de uma rede WLAN IEEE 802.11 é composta pelos seguintes elementos:

i. BSS - Basic Service Set. Corresponde a uma célula de comunicação da rede sem fio.
ii. STA - Wireless LAN Stations. São os diversos clientes da rede.
iii. AP - Access Point. É o nó que coordena a comunicação entre as STAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.
iv. DS - Distribution System. Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.
v. ESS - Extended Service Set. Conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional. Nestas condições, uma STA pode se movimentar de uma célula BSS para outra, permanecendo conectada à rede. Este processo é denominado de Roaming.

As redes WLANs podem ser configuradas tanto como Ad-Hoc ou no modo Infrastructure já explicados no item 1.2.

As WLANs utilizam os diversos padrões determinados pelo IEEE definidos na família 802.11.

As WLANs possuem as característica exibidas na tabela 4.

Tabela 4 - Características de uma WLAN

Modulação	Em um sistema de comunicação sem fio que utilize ondas de rádio, a informação a ser transmitida é modulada em uma portadora. Ou seja, ela é posicionada no espectro de frequências de modo que o mesmo meio físico possa trafegar informação de vários transmissores, desde que estes estejam utilizando uma faixa não ocupada. Por meio da modulação é possível fazer o deslocamento do espectro da informação para outra região não ocupada.

Elevada atenuação do meio físico	A potência das ondas de rádio tem um gradiente de atenuação proporcional a $1/r^3$, valor bastante elevado quando comparado com um meio de transmissão como fios de cobre. Isto limita o alcance de um transmissor. Por outro lado evita a interferência entre transmissores operando na mesma faixa de frequências.
Elevada taxas de erros	A taxa de erros média em um canal de comunicação com fios é menor que 10^{-6}. Em canais wireless, como a telefonia celular, a taxa de erros é de 10^{-3}. Esta taxa elevada exige que dispositivos de comunicação wireless possuam sistemas de deteção e correção de erros.
Interferências	Como o meio físico é compartilhado por todos os transmissores, existe o problema da interferência quando estes possuírem potência suficiente e estiverem operando na mesma região do espectro. Para evitar este problema, a utilização do espectro é regulamentada por agências governamentais (ITU, FCC, etc).
Espectro de frequências regulamentado	O espectro de frequências foi internacionalmente regulamentado e dividido em regiões com finalidades bem definidas. Por exemplo, a faixa de frequências destinadas a radiodifusão (*radio broadcasting*) AM é 600-1600 KHz e FM é 88-108 MHz. De particular interesse são as faixas ISM (*Industrial, Scientific and Medical*), que vão de 902-928 MHz, 2400-2483 MHz e 5725-6850 MHz, reservadas para transmissão de dados, e podem ser usadas sem licença para potências de transmissão menores que 1 W.
Baixa velocidade	Devido à escassez do recurso que é o espectro de frequências, as regiões reservadas para o uso em comunicação de dados são limitadas em largura de faixa. Deste modo, a informação a ser transmitida, que irá modular a portadora, não pode possuir uma frequência tal que o sinal modulado ultrapasse a região alocada a ele.

2 Desenvolvimento

2.1 Segurança de redes wireless

WLANs, assim como qualquer sistema, não são seguras por natureza. É preciso ter certas precauções e realizar configurações para que uma WLAN seja considerada realmente segura.

Sendo a comunicação feita por meio de ondas de rádio ou infravermelho como portadoras do sinal, qualquer outra estação que esteja sintonizada na faixa de frequências da transmissão recebe as informações transmitidas. Para que um mínimo de segurança exista numa WLAN, são necessários, assim, dois componentes:

- Meio de decisão de quem ou o que pode utilizar a WLAN – esse requerimento é satisfeito pelos mecanismos de **autenticação** para controle de acesso da LAN
- Meio que provê **privacidade** para informações wireless – esse requerimento é satisfeito pelos algoritmos de criptografia.

2.1.1 O Algoritmo WEP (Wired Equivalent Privacy)

O padrão de segurança das WLANs 802.11, conhecido como WEP (*Wired Equivalent Privacy*), trata-se de um algoritmo de criptografia usado por um processo de autenticação de chave compartilhada com a finalidade de autenticar usuários e criptografar dados somente sobre o segmento wireless. Ele envolve os seguintes serviços básicos de segurança:

- **Autenticação –** cujo objetivo é tentar assegurar que somente clientes pertencentes à rede poderão acessá-la através da verificação e avaliação de suas identidades.

- **Privacidade –** pretende assegurar a privacidade dos dados disponíveis na rede, isto é, avalia se os dados só poderão ser vistos por clientes que tiverem autorização.

- **Integridade –** cuja função é garantir que os dados transmitidos não sejam modificados no caminho de ida e volta entre os clientes e os pontos de acesso.

A seguir, esses itens são detalhados.

I. Autenticação

O WEP oferece dois tipos de autenticação: sistema aberto (*open system*) e chave compartilhada (*shared key*). A autenticação por sistema aberto é a opção *default* e, na verdade, funciona apenas como mecanismo de identificação, devendo ser evitado.

Se o mecanismo de criptografia não estiver habilitado, qualquer dispositivo poderá ter acesso ao ponto de acesso e, consequentemente, à rede. Se a criptografia estiver habilitada e o cliente não possuir uma chave secreta, o cliente não conseguirá transmitir mensagens através do ponto de acesso e nem recebê-las, mesmo que a estação seja autenticada.

A autenticação com base em chave compartilhada utiliza a técnica de *challenge-response*. Neste mecanismo, o ponto de acesso não é autenticado, apenas a estação. Na figura a seguir, estação sem fio está solicitando ao ponto de acesso sua autenticação. O ponto de acesso gera então um número aleatório e o envia para a estação. A estação o recebe, criptografa-o utilizando o algoritmo RC4 e o envia de volta. O ponto de acesso decripta a resposta e a compara com o número enviado. Se a comparação for positiva, o ponto de acesso envia para a estação uma mensagem confirmando o sucesso da autenticação.

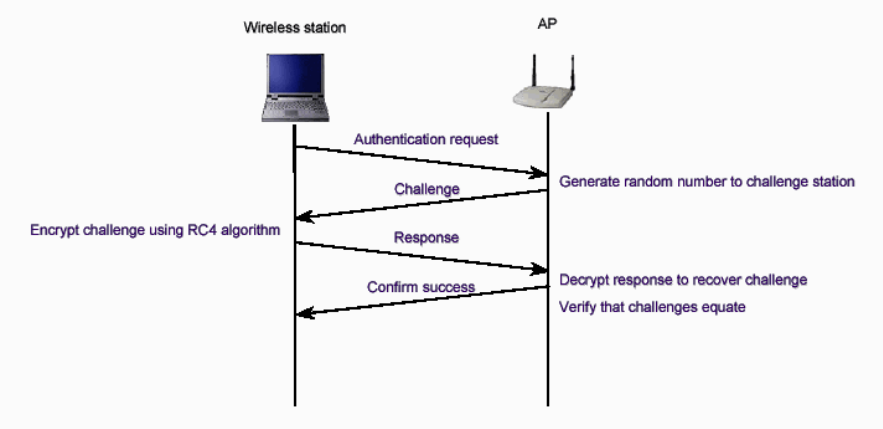

Figura 3 - Processo de autenticação WEP

A figura 10 esquematiza os processos de autenticação das WLANs 802.11.

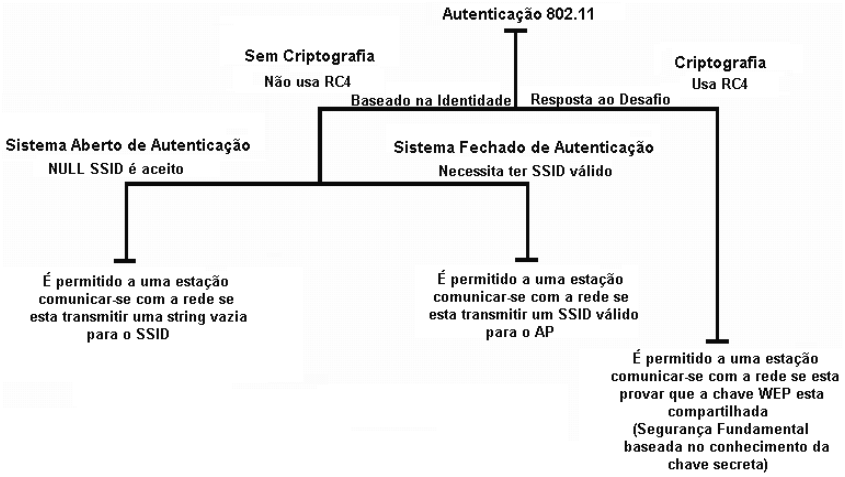

Figura 4 - Processo de autenticação das WLANs 802.11

Um grande problema deste esquema de autenticação é que o processo de *challenge-response* é vulnerável a ataques. Como é possível capturar tanto o texto cifrado como o texto original, a chave criptográfica pode ser facilmente derivada.

II. Privacidade

A implementação da privacidade é opcional. Quando habilitada, usa de técnicas de criptografia, também baseadas no algoritmo RC4, para gerar uma pseudo-seqüência de dados aleatória. Através desta técnica, o WEP pode impedir a descoberta dos dados durante a transmissão pela rede wireless.

Para que seja possível a codificação e decodificação dos quadros, é necessário que os participantes possuam a mesma chave criptográfica.

O padrão IEEE 802.11, entretanto, não especifica como deve ser a distribuição das chaves e, na prática, a maioria das instalações utiliza a mesma chave para todos os dispositivos. Isso traz problemas profundos à segurança dessas instalações, uma vez que a chave é compartilhada com vários usuários, dificultando a manutenção do segredo. Alguns administradores de rede tentam amenizar o problema não revelando a chave secreta ao usuário final, configurando, eles mesmos, os dispositivos.

Esse procedimento, entretanto, no traz a solução, pois as chaves continuam guardadas nos dispositivos remotos. A reutilização de uma única chave por vários usuários também aumenta as chances da colisão do vetor de inicialização, explicados adiante. A chance de uma colisão aleatória aumenta proporcionalmente com o número de usuários.

Além disso, uma vez que a troca de chaves requer que cada usuário reconfigure o seu dispositivo, as atualizações dos drivers controladores dos cartões de rede (NIC – Cartão de Interface de Rede) serão cada vez mais não frequentes. Na prática, a troca demorará meses ou anos para acontecer, dando mais tempo para os invasores analisarem o tráfego.

Os passos seguidos para o envio de uma mensagem são os seguintes:

1 – A estação transmissora concatena a sua chave secreta (*shared key*), de 40 a 104 bits, a um vetor de inicialização (IV) de 24 bits.

2 – O resultado serve de entrada para o algoritmo gerador de números pseudo-aleatórios (PRNG) definido pelo RC4.

3 – O PRNG gera uma seqüência de bits do mesmo tamanho do quadro MAC incluindo seu CRC.

4 - Uma operação binária XOR é executada entre o quadro MAC e a seqüência de PRNG produzindo o texto cifrado.

5 – O quadro cifrado é enviado juntamente com o IV.

6 – O receptor faz o processo inverso.

Tais etapas estão mostradas na figura a seguir.

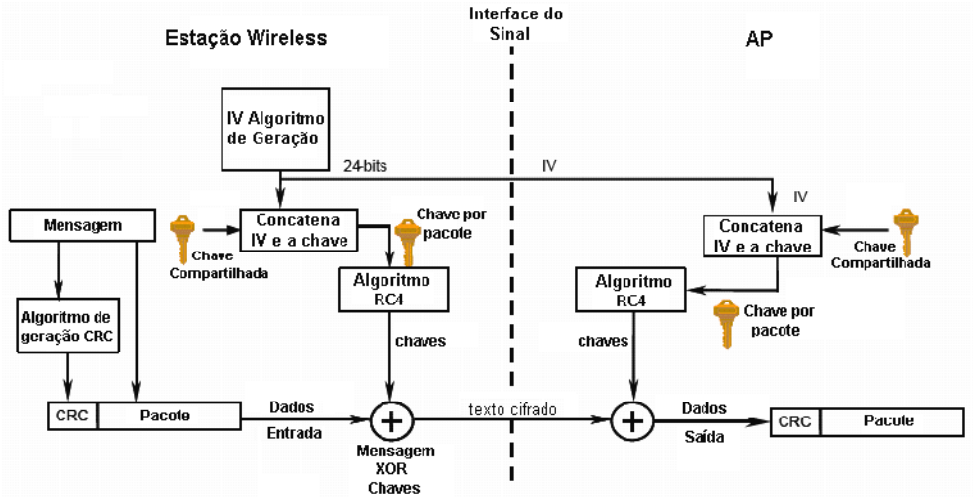

Figura 5 - Etapas para envio de mensagem em uma WLAN

Em geral, o aumento do tamanho da chave criptográfica aumenta o nível de segurança. Algumas pesquisas têm mostrado que chaves com tamanho maior que 80 bits, fazem com que a quebra do código torne-se praticamente impossível. A maioria das WLANs, entretanto, conta com chaves criptográficas de até 40 bits.

O vetor de inicialização IV no WEP tem 24 bits e, por ser muito pequeno, configura um problema da WEP. No caso extremo, esse IV é alterado a cada pacote enviado, começando no zero e indo até o valor máximo 224-1. Dessa forma, já que a chave criptográfica k é a mesma para clientes que estão se comunicando, o par (k, IV) se repete quando o IV é repetido. Essa repetição de sequência é extremamente indesejável, pois dá margem a ataques bem sucedidos e consequente descoberta de pacotes por eventuais intrusos.

III. **Integridade**

Para garantir a integridade dos dados tranmitidos entre clientes e pontos de acesso, o padrão IEEE 802.11 especifica um serviço de segurança que utiliza um simples CRC-32 (*Cyclic Redundancy Check*). Essa técnica rejeita qualquer mensagem que tenha sido alterada durante a transmissão.

O CRC é calculado em cada pacote a ser transmitido. A integridade do pacote é então criptografada utilizando uma chave RC4 para gerar o texto cifrado da mensagem. No receptor, é feita a descriptografia e, então, o CRC é recalculado na mensagem recebida. O CRC calculado é comparado com aquele da mensagem original. Caso sejam diferentes, haverá uma indicação de que a mensagem teve sua integridade violada e o receptor irá descartá-la.

A CRC-32, entretanto, é uma função linear que não possui chave. Essas duas características tornam o protocolo susceptível a dois tipos de ataques prejudiciais e indesejáveis:

- Modificação de mensagens que eventualmente tenham sido capturadas no meio do caminho sem que isso seja descoberto pelo receptor final. Isso acontece devido à linearidade da função detectora de erros e, além disso, pelo fato da função não possuir uma chave;

- Descobrir uma sequência secreta RC4 e, de posse desta, ser autenticado na rede e introduzir mensagens clandestinas nesta.

2.1.2 Outros algoritmos

Diante dos problemas verificados no WEP, foram propostas, ao longo do tempo, melhorias no sistema de segurança das WLANs, resultando em diversos métodos disponíveis para os usuários. Alguns desses métodos e suas principais características são descritos a seguir.

- **WEP2 (Wired Equivalent Privacy version 2)** – Em 2004, o IEEE propôs uma versão atualizada da WEP. É baseada no algoritmo RC4 e usa um vetor de inicialização de 128 bits, tornando-a mais robusta, mas ainda vulnerável aos ataques.

- **WPA (Wi-Fi Protected Access)** – WPA fornece encriptação através do TKIP (Temporary Key Integrity Protocol) usando o algoritmo RC4. Ele é baseado no protocolo 802.1X e melhora as fraquezas da WEP provendo melhorias como a construção e distribuição de chave por pacote, um código de integridade de mensagem e um vetor de inicialização mais poderoso. A única parte negativa é a existência da possibilidade de o hardware não suportar o WPA.

- **WPA2 (Wi-Fi Protected Access version 2)** – Baseado no padrão 802.1i, WPA2 foi lançado em 2004 e usa um método mais robusto de encriptação (AES – Advanced Encryption Standard). O AES suporta chaves de 128 bits, 192 bits e 256 bits. É compatível com WPA e usa um novo conjunto de chaves para cada sessão.

- **SSID (Service Set Identifier)** – Utiliza uma palavra-passe permitindo uma rede sem fio de ser separada em diferentes redes tendo um identificador único. Para acessar qualquer uma das redes, o computador cliente tem que ser configurado com a SSID da rede desejada. A filtragem de SSID, entretanto, não é considerada um método confiável de evitar acesso não autorizado em uma WLAN, já que O SSID é divulgado em texto puro em cada beacon que o ponto de acesso envia pela rede. Logo, não é difícil saber o SSID de uma rede usando um sniffer.

- **MAC (Media Access Control) address filtering** – Uma lista de endereços MAC pertencentes computadores clientes pode ser adicionada ao ponto de acesso e, então, só aqueles computadores terão acesso permitido. Quando o cliente faz um pedido, seu endereço MAC é comparado aos endereços da lista para permissão ou não do acesso.

Embora filtros MAC sejam uma boa medida de proteger a rede de acesso não autorizado, eles ainda são susceptíveis as seguintes invasões:

- Roubo do PC Card que está no filtro MAC do ponto de acesso.
- Utilizar um sniffer na WLAN e posteriormente clonar um endereço MAC, fazendo-se passar por aquele cliente

Filtros MAC são ótimos para redes pequenas e domésticas onde há um pequeno número de clientes. Usar WEP e filtros MAC proporciona uma solução de segurança adequada para esses ambientes, porque é muito pouco provável que um invasor gaste tempo e esforço para clonar

um endereço MAC ou mesmo tentar quebrar a chave WEP para acessar um computador ou notebook de um usuário doméstico.

- **VPN (Virtual Private Network) Link** – Talvez a forma de segurança mais confiável seria configurar uma conexão VPN na rede sem fio. VPNs usam AES e são as preferidas por gerentes de empresas.

- **802.1X** – Com o 802.1X o estágio de autenticação é feito através de um servidor RADIUS no qual as credenciais de usuário são checadas com o servidor. Quando um usuário tenta conectar pela primeira vez, ele deve informar o nome de usuário e a senha. Estes são checados com o servidor RADIUS e o acesso é garantido de acordo com o resultado. Cada usuário tem uma senha única que é mudada regularmente para oferecer maior segurança.

Quando combinado com o protoco de autenticação extensível (EAP), o 802.1x oferece um ambiente altamente seguro e flexível baseado em vários esquemas de autenticação usados hoje em dia.

EAP é um protocolo utilizado na negociação do método de autenticação e define as características do método de autenticação incluindo:

- Credencias requeridas do usuário tais como senhas, certificados, etc...
- Protocolo a ser usado (MD5, TLS, GSM, OTP, etc)
- Suporte da geração de chave e autenticação mutua.

Eis como ocorre o processo de uma autenticação 802.1x-EAP:

1. O cliente solicita a associação com o ponto de acesso
2. O ponto de acesso responde ao pedido de associação com uma requisição de identidade EAP.
3. O cliente envia uma resposta da identidade EAP para o ponto de acesso
4. A identidade EAP do cliente é encaminhada ao servidor de autenticação
5. O servidor de autenticação envia um pedido de autorização ao ponto de acesso
6. O ponto de acesso encaminha o pedido de autorização ao cliente
7. O cliente envia uma resposta da autorização EAP para o ponto de acesso
8. O ponto de acesso encaminha a resposta de autorização EAP para o servidor de autenticação
9. O servidor de autenticação envia uma mensagem EAP bem sucedida ao ponto de acesso
10. O ponto de acesso encaminha essa mensagem ao cliente e coloca a porta do cliente em modo ENCAMINHANDO.

3 Conclusões

Analisando todas os obstáculos que as WLANs têm de enfrentar para possuir bom desempenho e segurança podemos notar que muitos fatores irão ponderar para o bom funcionamento de uma WLAN.

Primeiramente, a escolha do padrão para a camada física (802.11a, 802.11b ou 802.11g) deve ser feita de forma adequada. Em cada padrão há uma definição diferente para os canais que podem ser utilizados, largura de banda e alcance. Em uma análise superficial, o 802.11a (54Mbps) oferece maior capacidade de transferência que o 802.11b (11Mbps) , com um alcance mais fraco. O padrão 802.11g tenta estender a capacidade do 802.11b para 54Mbps.

Deve-se também ajustar devidamente os canais para os pontos de acesso. O padrão 802.11b define 11 canais que se sobrepõem de forma considerável, portanto é necessário escolher canais mais separados, tanto quanto possível (por exemplo, 1, 6 e 11). No padrão 802.11a não há sobreposição e isso não se torna um problema.

A difusão das ondas de rádio deve ser bem planejada. Usuários mais distantes do ponto de acesso podem experimentar velocidades de conexão abaixo da máxima e, para evitar isso, deve-se escolher um local para o ponto de acesso e para as antenas que garanta melhor cobertura do espaço onde a rede será utilizada.

Outro problema com a difusão de ondas de rádio é a interferência de outros equipamentos externos à rede. Telefones sem fio e aparelhos de microondas costumam podem interferir significantemente na conexão em padrão 802.11b. O uso desses aparelhos no local da rede deve ser observado e, caso não possa ser evitada a interferência, pode-se optar pelo uso do padrão 802.11a a 5GHz.

Por fim, existem alguns protocolos opcionais no padrão que podem ajudar no desempenho. O protocolo RTS/CTS (*request to send / clear to send*) exige um *handshaking* entre duas estações para que estas possam enviar pacotes evitando colisões. Há também o protocolo de fragmentação, que fragmenta os quadros de dados em pequenos fragmentos, evitando a necessidade de retransmissão de um quadro inteiro em caso de erro. O tamanho do fragmento deve ser definido considerando-se que fragmentos muito pequenos acarretam maior *overhead,* enquanto fragmentos maiores implicam em retransmissão de mais dados. Esse compromisso deve ser observado na escolha do tamanho do fragmento.

Nota-se que é muito difícil disponibilizar o uso da capacidade máxima de uma WLAN, mas com experiência e estudo é possível minimizar as deficiências e obter melhor desempenho, contudo deve-se notar que, atualmente, a capacidade máxima de uma WLAN ainda é bem inferior à tecnologia atual da Ethernet.

4 4 – Referências

[1] Jim Geier. “Maximizing Wireless LAN Performance” , HTTP://www.wi-fiplanet.com/

[2]” Estudo comparativo entre redes sem fio e redes cabeadas” , http://bibdig.poliseducacional.com.br/document/?down=50

Referência: http://www.windowsnetworking.com/articles_tutorials/Introduction-Wireless-Networking-Part1.html

http://www.wirelessip.com.br/wirelessip/faqs

http://www.malima.com.br/wifi/wificomoescolhertecnologiawifi.asp

http://pt.kioskea.net/contents/wireless/wlpropa.php3

http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless032.asp

http://www.gta.ufrj.br/seminarios/semin2003_1/rmaia/802_11i.html

http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless035.asp

http://www.teleco.com.br/tutoriais/tutorialsrwireless/pagina_3.asp

http://www.windowsnetworking.com/articles_tutorials/Introduction-Wireless-Networking-Part3.html