

Segurança em Redes Sem Fio



Uma rede cabeada pode, por natureza, ser acessada apenas por quem tem acesso físico aos cabos. Isso garante uma certa segurança, já que para obter acesso à rede, um intruso precisaria ter acesso ao local. Nas redes wireless, por outro lado, o sinal é simplesmente irradiado em todas as direções, de forma que qualquer um, usando um PC com uma antena suficientemente sensível, pode captar o sinal da rede e, se nenhuma precaução for tomada, ganhar acesso a ela.

A maioria dos pontos de acesso utilizam antenas de 2 ou 2.2 dBi e as placas wireless utilizam, em geral, antenas ainda menos sensíveis. O alcance divulgado pelos fabricantes é calculado com base no uso das antenas padrão. Entretanto, é possível captar o sinal de muito mais longe utilizando antenas de alto ganho, sobretudo antenas direcionais, que concentram o sinal em uma faixa bastante estreita. Existe até uma velha receita que circula pela Internet de como fazer uma antena caseira razoável usando um tubo de batata Pringles. Não é brincadeira: o tubo é forrado de papel alumínio e tem um formato adequado para concentrar o sinal gerado pela antena.

Usando uma antena apropriada, o sinal de um ponto de acesso colocado perto da janela pode ser captado de 1, 2 ou até mesmo 3 quilômetros de distância em cenários onde não existam obstáculos importantes pelo caminho. Caímos, então, em um outro problema. Você simplesmente não tem como controlar o alcance do sinal da rede. Qualquer vizinho próximo, com uma antena de alto ganho (ou um tubo de batata), pode conseguir captar o sinal da sua rede e se conectar a ela, tendo acesso à sua conexão com a web, além de arquivos e outros recursos que você tenha compartilhado entre os micros da rede.

Surgiram então os sistemas de encriptação, que visam garantir a confidencialidade dos dados. Eles não fazem nada para impedir que intrusos captem o sinal da rede, mas embaralham os dados de forma que eles não façam sentido sem a chave de descriptação apropriada.

WEP

O primeiro passo foi o WEP, abreviação de "Wired-Equivalent Privacy", que, como o nome sugere, trazia como promessa um nível de segurança equivalente ao das redes cabeadas, o que logo se revelou falso.

Existem dois padrões WEP: de 64 e de 128 bits. Os primeiros pontos de acesso e placas 802.11b suportavam apenas o padrão de 64 bits, mas logo o suporte ao WEP de 128 bits virou norma. Muitos fabricantes adicionaram extensões proprietárias que permitiam utilizar chaves de 256 bits, mas apenas entre produtos do mesmo fabricante.

O grande problema é que o WEP é baseado no uso de vetores de inicialização que, combinados com outras vulnerabilidades, tornam as chaves muito fáceis de quebrar, usando ferramentas largamente disponíveis, como o aircrack. As chaves de 128 bits são tão fáceis de quebrar quanto as de 64 bits, os bits extra apenas tornam o processo um pouco mais demorado, fazendo com que sejam necessários 10 minutos para quebrar a chave de encriptação da sua rede ao invés de 30 segundos, por exemplo.

Usar o WEP em uma rede atual é como fechar a porta de casa com um arame. Ele pode dar uma certa sensação de segurança, mas um invasor só teria o trabalho de desenrolá-lo para entrar. Usar o WEP de 128 bits equivale a dar mais voltas no arame: apenas torna o processo um pouco mais demorado. Se você ainda usa equipamentos antigos, que estão limitados à encriptação via WEP, é recomendável substituí-los assim que possível.

WPA e WPA2

Em resposta às múltiplas vulnerabilidades do WEP, a Wi-Fi Alliance passou a trabalhar no desenvolvimento do padrão **802.11i**, que diferentemente do 802.11b, 802.11a, 801.11g e 802.11n não é um novo padrão de rede, mas sim um padrão de segurança, destinado a ser implantado nos demais padrões.

Como uma medida emergencial até que fosse possível completar o padrão, foi criado o WPA (Wired Protected Access), um padrão de transição, destinado a substituir o WEP sem demandar mudanças no hardware dos pontos de acesso e nas placas antigas. O WPA foi criado em 2003 e praticamente todos os equipamentos fabricados desde então oferecem suporte a ele. Como não são necessárias mudanças no hardware, um grande número de equipamentos antigos podem ganhar suporte através de atualizações de firmware.

O WPA abandonou o uso dos vetores de inicialização e do uso da chave fixa, que eram os dois grandes pontos fracos do WEP. No lugar disso, passou a ser usado o sistema TKIP (Temporal Key Integrity Protocol) onde a chave de encriptação é trocada periodicamente e a chave definida na configuração da rede (a passphrase) é usada apenas para fazer a conexão inicial.

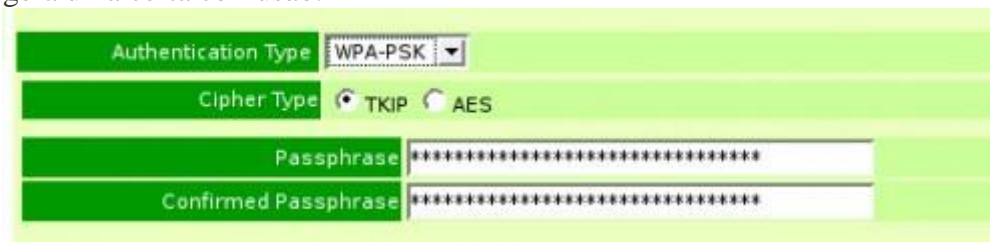
Combinando o uso do TKIP com outras melhorias, o WPA se tornou um sistema relativamente seguro, que não possui brechas óbvias de segurança. É ainda possível quebrar chaves fáceis ou com poucos caracteres usando programas que realizam ataques de força bruta, mas chaves com 20 caracteres ou mais são inviáveis de se quebrar, devido ao enorme tempo que seria necessário para testar todas as combinações

possíveis. Hoje em dia, o WPA é o absoluto mínimo em termos de segurança que você deve pensar utilizar.

Além do padrão WPA original, de 2003, temos também o WPA2, que corresponde à versão finalizada do 802.11i, ratificado em 2004. A principal diferença entre os dois é que o WPA original utiliza algoritmo RC4 (o mesmo sistema de encriptação usado no WEP) e garante a segurança da conexão através da troca periódica da chave de encriptação (utilizando o TKIP), enquanto o WPA2 utiliza o AES, um sistema de encriptação mais seguro e também mais pesado.

O AES é o sistema de criptografia bastante seguro, baseado no uso de chaves com de 128 a 256 bits. Ele é usado pelo governo dos EUA, de forma que, mesmo que alguém descobrisse uma falha no algoritmo, que pudesse permitir um ataque bem-sucedido, teria sistemas muito mais interessantes para invadir do que sua parca rede.

Os equipamentos atuais suportam ambos os padrões, de forma que você pode escolher qual usar ao configurar o ponto de acesso. Em muitos casos, as opções são renomeadas para "TKIP" (que corresponde ao WPA original) e "AES" (WPA2), o que gera uma certa confusão:

A screenshot of a wireless network configuration interface. It features a green header bar. Below it, there are four rows of configuration options. The first row is labeled 'Authentication Type' and has a dropdown menu set to 'WPA-PSK'. The second row is labeled 'Cipher Type' and has two radio buttons: 'TKIP' (which is selected) and 'AES'. The third row is labeled 'Passphrase' and has a text input field filled with asterisks. The fourth row is labeled 'Confirmed Passphrase' and also has a text input field filled with asterisks.

Usar o AES garante uma maior segurança, o problema é que ele exige mais processamento, o que pode ser um problema no caso dos pontos de acesso mais baratos, que utilizam controladores de baixo desempenho. Muitos pontos de acesso e algumas placas antigas simplesmente não suportam o WPA2 (nem mesmo com uma atualização de firmware) por não terem recursos ou poder de processamento suficiente.

Existem também casos onde o desempenho da rede é mais baixo ao utilizar o WPA2 (pois apesar do firmware oferecer suporte ao algoritmo, o controlador usado no ponto de acesso não possui potência para criptografar os dados na velocidade permitida pela rede) e também casos de clientes com placas antigas, ou com ferramentas de configuração de rede que não suportam o AES e por isso não conseguem se conectar à rede, embora na grande maioria dos casos tudo funcione sem maiores problemas.

Tanto ao usar o TKIP quanto ao usar o AES, é importante definir uma boa passphrase, com pelo menos 20 caracteres e o uso de caracteres aleatórios (em vez da simples combinação de duas ou três palavras, o que torna a chave muito mais fácil de adivinhar). A passphrase é uma espécie de senha que garante o acesso à rede. Como em outras situações, de nada adianta um sistema complexo de criptografia se as senhas usadas são fáceis de adivinhar.

A passphrase é apenas uma chave de acesso, que permite que o cliente ganhe acesso à rede. Sempre que um cliente se conecta, é criado um túnel seguro entre ele e o ponto de acesso, através do qual os dados são transferidos. Com isso, mesmo que alguma pessoa mal intencionada saiba a passphrase, ela poderá apenas se conectar à

rede, sem contudo ter como snifar a conexão com o objetivo de roubar senhas e outras informações, como é possível em redes abertas ou em redes com o WEP.

Com isso, mesmo que você esteja implantando uma rede de acesso público (como em uma lanchonete ou café, por exemplo) é muito mais recomendável ativar o uso do TKIP ou do AES e colar uma placa com a passphrase na parede do que deixar a rede aberta. Não apenas isso ajuda a evitar o uso por parte de freeloaders ocasionais (só quem realmente entrar no estabelecimento e ver a placa vai ter a passphrase) mas garante a privacidade dos clientes, evitando que clientes mal intencionados possam capturar o tráfego da rede.

Enquanto escrevo, por exemplo, redes Wi-Fi abertas são a forma mais comum de hackear contas do Facebook, já que como o site ainda não usa https ou outra forma de encriptação para os logins, basta capturar o tráfego da rede por algum tempo para ter acesso a todos os logins e senhas de usuários do Facebook (bem como de outros sites que também não utilizem https) que utilizaram a rede dentro daquele espaço de tempo. Existem softwares para o Android, como o FaceNiff, que automatiza o processo, permitindo fazer tudo discretamente com um simples smartphone com o Android.

WPA-Personal e WPA-Enterprise

A versão "doméstica" do WPA, onde é utilizada uma chave de autenticação, é chamada de **WPA Personal** (ou **WPA-PSK**, onde PSK é abreviação de "Pre-Shared Key", ou "chave previamente compartilhada"). Além dela, temos o **WPA-Enterprise** (ou **WPA-RADIUS**), onde é utilizada uma estrutura mais complexa, onde o ponto de acesso é ligado a um servidor RADIUS, que controla a autenticação.

A sigla "RADIUS" é o acrônimo de "Remote Authentication Dial In User Service". Apesar do nome intimidador, o RADIUS nada mais é do que um protocolo de autenticação de rede, que é utilizado por diversos outros serviços. Justamente por isso, ele acabou sendo escolhido para uso no WPA-Enterprise.

O servidor RADIUS pode ser tanto uma máquina Linux (com o FreeRADIUS) quanto um servidor Windows, cujo endereço é indicado na configuração do ponto de acesso. No caso do AP do screenshot abaixo, a opção de usar o WPA-Enterprise foi renomeada para apenas "WPA" e a opção de usar o WPA-Personal aparece como WPA-PSK:

The screenshot shows a configuration interface for a wireless access point. At the top, 'Authentication Type' is set to 'WPA' and 'Cipher Type' is set to 'AES'. Below this, under the '802.1X' section, there are fields for 'RADIUS Server 1' (IP: 192.168.1.252, Port: 1812, Shared Secret: masked) and 'RADIUS Server 2 (Optional)' (IP: 0.0.0.0, Port: 0, Shared Secret: masked).

Authentication Type		WPA
Cipher Type		<input type="radio"/> TKIP <input checked="" type="radio"/> AES
802.1X		
RADIUS Server 1	IP	192.168.1.252
	Port	1812
	Shared Secret	*****
RADIUS Server 2 (Optional)	IP	0.0.0.0
	Port	0
	Shared Secret	

Exemplo de configuração para utilizar o WPA-Enterprise, com um servidor RADIUS

Nessa configuração, o ponto de acesso passa a ser chamado de "autenticador" e passa a retransmitir os pedidos de conexão para o servidor de autenticação ligado a ele. O servidor verifica as credenciais dos clientes e dá a ordem para que o ponto de acesso libere ou não o acesso. O mais comum é que a autenticação seja feita pela combinação de uma passphrase e de um certificado digital, que pode ser tanto armazenado no próprio HD (menos seguro) quanto em algum dispositivo externo, como um pendrive ou um smartcard. Quando o cliente se conecta, é criado um túnel encriptado entre ele e o servidor, garantindo a segurança dos dados transmitidos.

Os nomes "WPA-Personal", "WPA-PSK" e "WPA-Enterprise" dizem respeito ao funcionamento do sistema de autenticação, enquanto o "WPA" e o "WPA2" dizem respeito ao algoritmo de encriptação usado (RC4 ou AES). Tanto as redes que utilizam o WPA-PSK quanto as que utilizam o WPA-Enterprise podem utilizar tanto o WPA quanto o WPA2, de acordo com os equipamentos usados e a configuração.

Fonte: <http://www.hardware.com.br/guias/redes-wireless/seguranca.html>