SAFETY ASSESSMENT IN WIRELESS NETWORKS

Márcio Aurélio Ribeiro Moreira (PITÁGORAS – Faculdades Pitágoras, MG, Brasil) - marcio.moreira@pitagoras.com.br
Jairo Rodrigues de Araújo (PITÁGORAS – Faculdades Pitágoras, MG, Brasil) - jairoinf16@yahoo.com.br
Rogério Mendes Ferreira (UNIPAC – Universidade Presidente Antônio Carlos, MG, Brasil) - rogerio@websec.com.br
Flamaryon Guerin (UNITRI – Centro Universitário do Triângulo, MG, Brasil) - flamaryon@unitri.edu.br

This paper presents the basic workings of wireless networks in terms of security protocols and configuration modes, assesses the security level of WEP, WPA and WPA2 protocols, considering the PSK authentication mechanism and AES or TKIP encryption algorithms, assesses the most recent attacks to the vulnerabilities of these protocols, presents several invasion tests, detailing one of them and finally presents the recommended settings to resist to theses attacks and vulnerabilities assessed. The studies and penetration tests lead to the conclusion that WEP, WPA and TKIP are insecure and only one configuration with WPA2, using PSK with AES-encrypted is currently recommended.

Keywords: WLAN, WEP, WPA, WPA2, TKIP, PSK and AES.

AVALIAÇÃO DE SEGURANÇA EM REDES SEM FIO

Este artigo apresenta o funcionamento básico de redes sem fio em termos de protocolos de segurança e modos de configuração; faz uma avaliação do nível de segurança dos protocolos WEP, WPA e WPA2, considerando o mecanismo de autenticação PSK e os algoritmos de criptografia TKIP e AES; avalia os ataques mais recentes às vulnerabilidades destes protocolos; apresenta vários testes de invasão, detalhando bem um deles; finalmente apresenta as configurações recomendadas para resistir às vulnerabilidades e ataques avaliados. Os estudos e os testes de invasão levam à conclusão que o WEP, o WPA e o TKIP são inseguros e, somente uma configuração com o WPA2 com o PSK sendo criptografado pelo AES é recomendada atualmente.

Palavras-chave: WLAN, WEP, WPA, WPA2, TKIP, PSK e AES.

1. Introdução

A mobilidade é uma tendência inevitável que está presente no dia á dia da sociedade, ou seja, o uso das redes sem fio (wireless) é cada vez mais comum. A crescente popularidade da computação móvel, da telefonia celular e a internet, abriram ainda mais, as possibilidades para a criação de novas tecnologias e, em conseqüência, novos serviços e produtos. Dispositivos móveis, como notebooks e PDAs (*Personal Digital Assistents*) constituem um dos segmentos de mais rápido crescimento da indústria de informática. Além dos desktops que usam a tecnologia wireless por conveniência, ou seja, evitar cabos. Muitos usuários desses computadores possuem máquinas de desktop no escritório e querem se manter conectados a essa base mesmo quando estão em casa ou no trânsito (SILVA, 2005).

Tendo em vista que é impossível ter uma conexão por fios em automóveis e aviões, existe um grande interesse no uso de redes sem fio. Considerando esse interesse no cenário atual, é indiscutível a importância da segurança da informação. O aumento do número de aplicações, a distribuição dessas aplicações através do uso maciço de redes de computadores e o número crescente de ataques a esses sistemas retratam essa preocupação e justifica o esforço em pesquisas voltadas a essa área. Novos mecanismos, técnicas mais eficientes e normas internacionais para a gestão da segurança da informação são constantemente desenvolvidas, incentivados por organismos governamentais e empresas preocupadas com o atual estágio de fragilidade da maioria das instalações computacionais (MOREIRA & MENDES, 2008).

Pessoas mal intencionadas podem usar o canal onde trafegam informações simples para atacar os dados mais relevantes, ou seja, é muito importante que estes canais onde trafegam dados relevantes ou não estejam bem protegidos, pois se existir uma vulnerabilidade ela servirá para atacar qualquer tipo de dado ou recurso (SILVA, 2005).

Os objetivos deste trabalho são mostrar o funcionamento de uma rede sem fio (wireless), avaliar os protocolos de segurança existentes atualmente, verificar as principais vulnerabilidades, testar os principais ataques e apresentar as melhores configurações de segurança disponíveis atualmente para as redes sem fio.

2. As Redes Sem Fio

As redes sem fio são chamadas *Wireless LAN* (*Local Area Network*) ou simplesmente WLAN. As WLANs foram definidas no padrão IEEE 802.11b, também chamado de Wi-Fi (*Wireless Fidelity*), é um padrão que foi desenvolvido pelo IEEE (*Institute of Electrical and Electronics Engineers*), uma organização internacional que desenvolve padrões para centenas de tecnologias eletrônicas e elétricas. Dentre os seus diversos comitês pode-se destacar o 802.3, que desenvolve padrões para redes baseadas no padrão Ethernet (muito difundido e utilizado nas redes locais), o 802.15 que desenvolve padrões para redes PAN (*Personal Área Network*), e o 802.11 que desenvolve padrões para WLAN (SILVA, 2005).

Uma topologia clássica de uma WLAN é mostrada na Figura 1. Nela há um Ponto de Acesso da WLAN ligado à rede da empresa (LAN), a qual dá acesso à Internet e às aplicações da empresa. Na WLAN são mostrados os vários tipos de equipamentos que

podem se ligar a uma WLAN, dentre eles: notebooks e estações de trabalho, *Tablets PCs, Smartphone, PDAs*, impressoras, etc.

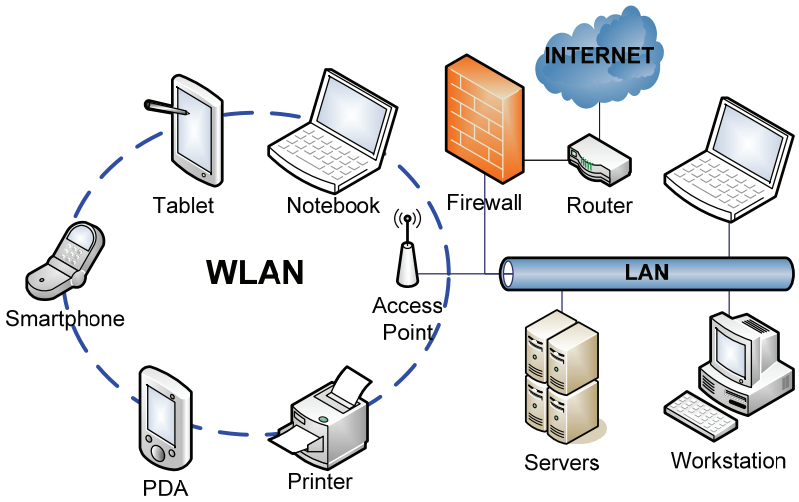

Figura 1: Uma topologia de uma rede sem fio (WLAN) do tipo BSS

3. Modos de Configuração

A forma como e feito a comunicação e o compartilhamento de uma rede wireless, conforme Oliveira (2003) é definida de acordo com a arquitetura adotada. São três os modos de configuração de uma rede sem fio, para garantir o controle e gerenciamento da rede: modo infraestrutura básica, modo infraestrutura e modo ponto a ponto (*ad hoc*).

3.1. Modo Infraestrutura Básica (BSS)

Este é o modo de comunicação mais encontrado, ele utiliza concentradores de acesso denominados Ponto de Acesso (*AP: Access Point*), que são fixos e podem ou não conectar uma rede sem fio a redes convencionais. O Ponto de Acesso é o responsável pela conexão entre as estações móveis e é utilizado também para autenticação na rede, gerência e controle de fluxo de dados. O termo mais comum para este tipo de rede é BSS (*Basic Service Set*), que é um grupo de estações comunicando entre si através de um Ponto de Acesso comum.

No modo infra-estrutura básica cada cliente da rede sem fio se comunica diretamente com o Ponto de Acesso, que faz parte do sistema de distribuição. A Figura 1 ilustra uma WLAN com um Ponto de Acesso para a realização de comunicação e transmissão de dados. Neste caso o Ponto de Acesso não apenas fornece a comunicação com a rede convencional como também serve de intermédio de tráfego entre os clientes sem fio. Dessa forma, qualquer pedido de comunicação entre estações contidas na BSS deve passar pelo AP. No modo BSS a rede terá tantos pontos quantos couber no AP disponibilizado para ela.

3.2. Modo Infraestrutura (ESS)

O modo infraestrutura são redes ESS (*Extended Service Set*), que na verdade é a união de diversas redes BSS conectadas através de outra rede, por exemplo, uma rede

Ethernet, como mostrado na Figura 2. A estrutura deste tipo de rede, normalmente é composta por um conjunto de APs interconectados, o que permite a "migração" de um dispositivo (um notebook, por exemplo) entre os dois Pontos de Acesso da rede. É importante ressaltar que para as estações esse processo é totalmente transparente, logo a rede é vista como um único elemento. No modo infraestrutura, o número máximo de nós que a rede sem fio pode chegar é de até 2048.

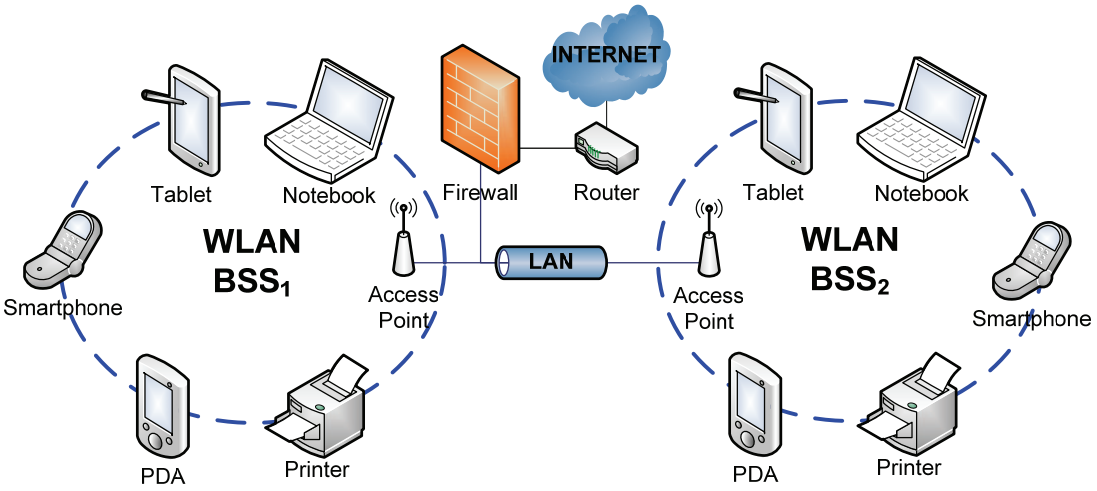

Figura 2: Uma WLAN do tipo ESS

3.3. Modo Ponto a Ponto (*ad hoc*)

O modo Ponto a Ponto (*ad hoc*) também é conhecido como IBSS (*Independent Basic Service Set*). Nesse modo de comunicação, os clientes da rede sem fio comunicam-se diretamente entre si, sem a necessidade de um concentrador. Todas as estações possuem um mesmo BSSID (*Basic Service Set Identifier*), que corresponde a um identificador da célula sem fio. A operação numa rede nesse modo de comunicação é extremamente fácil, mas a área de cobertura é reduzida, sendo necessário que a área de cobertura de uma estação alcance a outra para que haja comunicação. A Figura 3 ilustra a comunicação entre os dispositivos de uma mesma célula de comunicação sem fio, onde não existe nenhum AP. No modo *Ad Hoc*, o número máximo de estações é de 256.

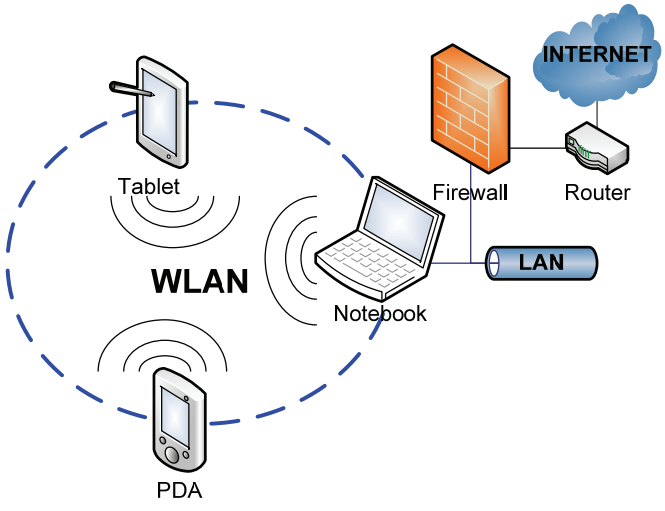

Figura 3: Uma WLAN Ponto a Ponto (*ad hoc*)

No caso de uma rede wireless configurada no modo *ad hoc*, é necessário configurar um cliente sem fio inicial que assuma parte das responsabilidades de um AP, como a emissão de *beacons* (mensagens de alerta) do nome da rede sem fio *ad hoc* para outros clientes da rede sem fio.

4. Protocolos de Configuração de Redes Sem Fio

Esta seção não tem a pretensão de fazer uma descrição completa dos padrões de redes sem fio, descritos pelo IEEE ((*Institute of Electrical and Electronics Engineers*), para esta finalidade favor consultar o próprio IEEE (www.ieee.org ou www.ieee.org.br) ou ainda Silva (2005) ou Oliveira (2003). O propósito desta seção é apresentar os principais protocolos de segurança utilizados nas redes sem fio.

4.1. WEP

O WEP (*Wired Equivalent Privacy* ou privacidade equivalente a cabeada) foi o primeiro protocolo de segurança, definido no padrão de redes 802.11 com o propósito de prover confidencialidade (somente usuários autorizados devem ver os dados), integridade (o dado gerado na origem não pode ser alterado durante a transmissão) e autenticação (os usuários devem confirmar suas identidades). Para atingir estes objetivos foi utilizado um sistema criptográfico baseado no RC4 (*Rivest Cipher 4*) utilizando chaves de 40 a 128 bits.

Uma boa descrição do RC4 pode ser obtida em Stallings (1999), de forma bem simples o algoritmo funciona com uma chave secreta (compartilhada entre o cliente e a estação-base) a qual é concatenada a um vetor inicializado. Esta chave forma a semente do gerador de números pseudo-aleatórios PRNG (*Pseudo Random Number Generator)* definido no RC4.

Apesar de ser relativamente rápido, o RC4 e o WEP apresentam falhas de segurança descritas por Obermayr (2003) e Berghel & Uecker (2004). Dentre as principais podem ser destacadas: compartilhamento de chaves, reutilização do vetor inicializado e autenticação de somente um dos lados da rede. As chaves utilizadas pelo protocolo WEP podem ser facilmente quebradas após a captura de alguns pacotes por um software analisador de tráfego. Logo, mesmo com as melhores recomendações para este protocolo, incluindo o uso de um servidor de autenticação RADIUS (*Remote Authentication Dial In User Service*), ele ainda permanece inseguro. Entretanto, se não for possível nenhum outro, o WEP é melhor que nada, pois sem criptografia, o tráfego da rede sem fio pode ser inspecionado, alterado ou mesmo forjado.

4.2. WPA

O WPA (*Wi-Fi Protected Access*) é um protocolo de criptografia para redes sem fio baseado no grupo de trabalho IEEE 802.11i, que fundamentou o protocolo num algoritmo de cifragem (codificação) mais robusto, o TKIP (*Temporal Key Integrity Protocol*) ou o AES (*Advanced Encryption Standard*). O TKIP permite a geração aleatória de chaves e, para maior segurança, oferece a possibilidade de alterar a chave de codificação várias vezes por segundo.

O funcionamento do WPA baseia se na instalação de um servidor de autenticação, na maioria das vezes um servidor RADIUS, permitindo identificar os usuários na rede e definir os seus níveis de acesso. Esta versão é chamada da WPA Enterprise e está definida no padrão 802.1x. No entanto, pequenas redes podem ser instaladas com uma versão restrita do WPA, chamada WPA *Personal* ou WPA-PSK (*Pre-Shared Key*). Neste caso, a PSK é armazenada no Ponto de Acesso e nos clientes da rede e é utilizada no primeiro contato entre ambos. Para definição da PSK, o WPA permite utilizar uma "frase secreta" que é convertida na PSK por um algoritmo condensador do WPA.

O WPA foi concebido inicialmente como uma melhoria do WEP. Além das melhorias introduzidas pelo TKIP, destacam-se o melhoramento na concatenação de chaves, verificação da integridade das mensagens MIC (*Message Integrity Check*), melhorias no vetor de inicialização e um mecanismo de atualização de chaves a cada sessão ou um conjunto de pacotes trafegados.

Apesar de todas as melhorias, o WPA também possui vulnerabilidades, como as descritas por Beck & Tews (2008), no artigo "*Practical attacks against WEP and WPA*", onde eles mostram algumas vulnerabilidades, propõem um ataque e demonstram que o WPA não pode ser considerado completamente seguro.

4.3. WPA2

O WPA2 (*Wi-Fi Protected Access 2*) utiliza o AES (*Advanced Encryption Standard*), um algoritmo padrão de criptografia avançado que permite um nível equivalente de segurança a seus antecessores (como o DES - *Data Encryption Standard*) com chaves menores (MOREIRA, FERREIRA & BORGES, 2009). O WPA2, corresponde à versão finalizada do 802.11i, a principal diferença entre ele, o WPA e o WEP é o uso de um algoritmo de criptografia mais robusto, o AES, o que requer um processamento adicional dos equipamentos, isto pode tornar o padrão incompatível com velhos dispositivos de hardware, contudo o WPA2 é o padrão mais confiável na atualidade. Outra vantagem do AES é que ele permite a descoberta de uma chave inicial de criptografia de difusão Ponto a Ponto exclusiva para cada autenticação.

Alguns fabricantes de equipamentos para redes sem fio, para oferecer ainda mais segurança, podem oferecer o WPA2 com o TKIP ou PSK, neste caso prefira o PSK. Além disto, os equipamentos também permitem a integração com servidores RADIUS para autenticação de usuários. São comuns também a oferta de extensões para versões corporativas como o EAP (*Extensible Authentication Protocol*) com as variantes TLS (*Transport Layer Security*), TTLS (*Tunneled Transport Layer Security*), MD5 (*Message-Digest algorithm 5*), IKEv2 (*Internet Key Exchange*), FAST (*Flexible Authentication via Secure Tunneling*), SIM (*Subscriber Identity Module*), etc. Para estes casos é necessário consultar o manual do fabricante do equipamento e buscar a melhor recomendação.

O ataque mais comum ao WPA2 está relacionado ao uso do TKIP ou PSK, pois é ataque de dicionário, cujo propósito é identificar a chave de segurança compartilhada entre os nós da rede. Por conta disto recomenda-se o uso do AES. Se isto não for possível, não utilize senhas padrões ou senhas fáceis. Outro ataque ao WPA2 chamado "Hole 196" foi proposto em Julho de 2010, onde um usuário autenticado pode tentar se passar por outra

pessoa da rede, ou seja, fazer um ataque do homem do meio (man-in-the-middle). Mesmo neste caso, conforme análises nos artigos Motorola (2010), GHKSAR (2010) e AirTigh (2010), o AES é apontado como única forma capaz de evitar este ataque.

A Figura 4 apresenta um resumo das pesquisas sobre avaliação dos protocolos utilizados em redes sem fio, considerando os mecanismos de autenticação e de criptografia utilizados pelos protocolos WEP, WPA e WPA2. Pelo estudo realizado somente o WPA2, com PSK, utilizando o AES como mecanismo de criptografia apresenta o melhor nível de segurança.

Características		Nível de Segurança dos Protocolos		
Autenticação	**Criptografia**	**WEP**	**WPA**	**WPA2**
Nenhuma	Nenhuma	Baixo	n/a	n/a
	TKIP	n/a	Baixo	Baixo
	AES	n/a	Médio	Médio
PSK	Nenhuma	n/a	n/a	n/a
	TKIP	n/a	Baixo	Médio
	AES	n/a	Médio	Alto

Figura 4: Resumo da pesquisa de protocolos de segurança de WLAN

5. Ataque Contra uma Rede Sem Fio com WEP ou WPA

O teste de ataque deste trabalho foi feito num ambiente Linux, mas existem versões das ferramentas utilizadas para o ambiente Windows. O teste de invasão foi feito utilizando informações disponíveis em Boileau (2006) e Morimoto (2006). No teste foi feito um ataque de dicionário. As ferramentas utilizadas suportam ataque de força bruta, no caso do WEP este ataque é relativamente rápido, já no caso do WPA este ataque demora um pouco mais, entretanto é eficaz.

Para o teste precisamos instalar o pacote **Aircrack-ng**, sucessor do Aircrack, que contém as ferramentas que utilizaremos. Ele está disponível para download em www.aircrack-ng.org. Para funcionar, ele precisa que o *driver* da placa wireless suporte o modo monitor, que é suportado por padrão em um número cada vez menor de placas. Na maioria dos casos, você vai precisar primeiro modificar os *drivers* da placa, baixando e instalando um *patch* e o *driver* modificado, este passo é fundamental, se a sua placa não conseguir operar no modo monitoramento não terá como executar o teste.

Para aplicar o teste, comece usando o **Kismet**, disponível para download em www.kismetwireless.net, para descobrir o SSID (*Service Set IDentifier*, identificador definido para o serviço ou nome da rede) e o canal utilizado pela rede que deseja testar, além do endereço MAC (*Media Access Control*) do Ponto de Acesso e o endereço MAC de pelo menos um cliente que esteja conectado a ele. Se você está testando sua própria rede, basta checar as informações na configuração do Ponto de Acesso.

O passo seguinte é usar o **Airmon-ng** (parte do Aircrack-ng) para capturar o processo de autenticação de um dos clientes da rede. Ele é baseado no uso de um "*four-way handshake*", onde uma série de quatro pacotes é utilizada para negociar uma chave

criptográfica entre o cliente e o Ponto de Acesso, que é então usada para criptografar o processo de autenticação.

Naturalmente, capturar esta seqüência de pacotes não permite descobrir a senha da rede, mas oferece a possibilidade de executar o ataque de força bruta, testando várias possibilidades até descobrir a chave correta. Comece colocando a placa wireless em modo monitor, com o seguinte comando:

 # airmon-ng start eth1

No caso das placas com chipset Atheros, é necessário desativar a interface "ath0″ e recriá-la em modo monitor, usando os comandos:

 # airmon-ng stop ath0
 # airmon-ng start wifi0

O passo seguinte é capturar o processo de autenticação de um dos clientes. Isto é feito abrindo dois terminais. O primeiro será usado para rodar o **Airodump-ng** (parte do Aircrack-ng) que captura as transmissões, e o segundo para rodar o **Aireplay-ng** (parte do Aircrack-ng), que desconecta um cliente ativo da rede obrigando-o a se reconectar ao Ponto de Acesso, de forma que os pacotes possam ser capturados.

No primeiro terminal, ative o Airodump-ng, especificando o nome e onde será gravado o arquivo com os pacotes capturados ("logwlan.cap" no diretório corrente no exemplo), o canal usado pelo ponto de acesso e a interface, com o comando:

 # airodump-ng -w logwlan –channel 2 ath0

Utilizando o Aireplay (parte do Aircack-ng), no outro terminal, rode o comando abaixo. Este comando especifica o endereço MAC do Ponto de Acesso (após o "-a") e o endereço MAC do cliente que será desconectado (após o "-c").

 # aireplay-ng –deauth 1 -a xx:xx:xx:xx:xx:xx -c yy:yy:yy:yy:yy:yy

Este comando faz com que seu PC envie um pacote falsificado ao Ponto de Acesso, simulando o processo de desconexão do cliente especificado. Enganado pelo pacote, o Ponto de Acesso desconecta o cliente, o que faz com que ele se re-autentique em seguida, um processo executado de forma automática pela maioria dos sistemas operacionais que devem estar rodando no cliente. Com isso, o processo de autenticação será gravado pela captura iniciada no outro terminal. Por uma questão de sigilo, o endereço MAC acima teve seus dígitos substituídos por "xx" e "yy".

Para realizar o ataque baseado em dicionário, é necessário utilizar um arquivo de texto, contendo uma lista das palavras que serão testadas. Existem diversos arquivos de dicionários em vários idiomas disponíveis na Internet, basta fazer uma busca por "*wordlists*". O dicionário utilizado neste teste foi conseguido na Internet e foi salvo com o nome "dic.txt". Com o dicionário disponível, use o comando abaixo para testar as combinações (palavras existentes no dicionário), especificando o SSID (descoberto com o Kismet) da rede (no exemplo o SSID foi substituindo por idssid por segurança), o arquivo

do dicionário e o arquivo com a captura dos pacotes (gerado pelo Airmon-ng, "logwlan.cap" no teste).

$ aircrack-ng -e idssid -w dict.txt logwlan.cap

A tela resultante do teste realizado está mostrada na Figura 5. A chave utilizada no PSK foi "*dictionary*", encontrada pelo Aircrack-ng e exibida após o texto "*Key Found*". Para cada palavra no dicionário (dic.txt), o Aircrack tenta decifrar os pacotes armazenados no arquivo de log (logwlan.cap). Se algumas informações padrões (fixas) forem legíveis (encontradas) em determinadas partes do pacote de rede armazenada, a palavra utilizada é a senha utilizada e, portanto, está quebrada a segurança do protocolo utilizado. Uma vez descoberta a senha, basta configurar o protocolo da placa de rede sem fio de sua máquina e passar a acessar a rede como se você fosse um usuário legítimo dela.

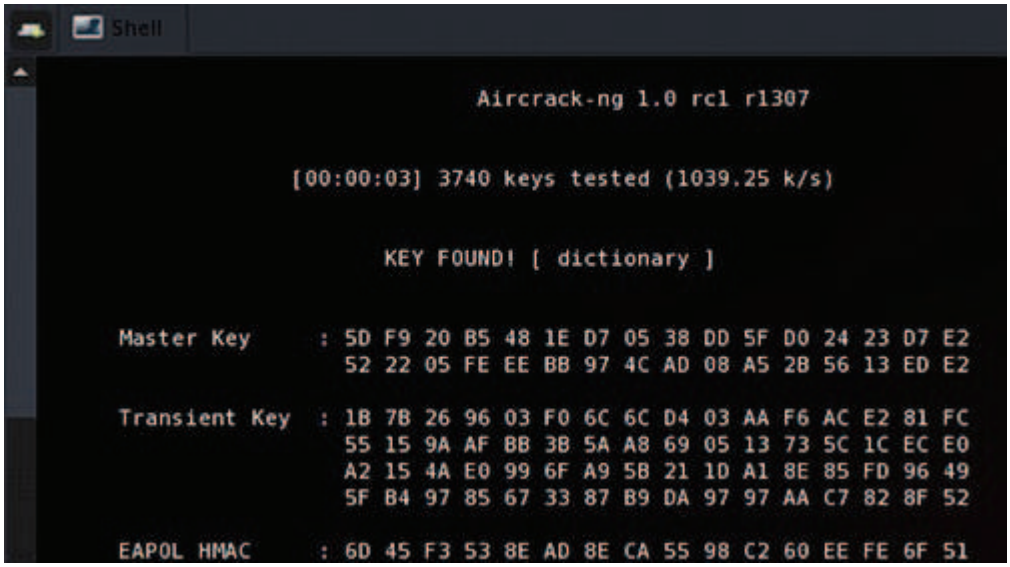

Figura 5: Ataque de dicionário ao WPA-PSK usando o Aircrack-ng

Até encontrar a senha o ataque não acessa o Ponto de Acesso para testar cada palavra do dicionário de ataque. Ele testa os pacotes armazenados, isto torna o processo mais rápido e evita os softwares de detecção de intrusos disponíveis em algumas redes. Mesmo assim, dependendo do tamanho do dicionário e da complexidade da senha utilizada, o ataque pode demorar um bom tempo. Uma máquina de 1.4 GHz consegue testar 100 palavras do dicionário por segundo, ou seja, 360 mil palavras por hora ou 8,64 milhões por dia. Parece muito? Nem tanto, utilizando uma senha forte de 5 caracteres (40 bits) contendo letras maiúsculas e minúsculas, números e caracteres especiais, ou seja, considerando 96 possibilidades em cada caractere; no pior caso, um ataque de força bruta poderia levar até 3 anos. Por isto o ataque de dicionário é preferível. Por outro lado, se o ataque de força bruta for dividido entre 100 máquinas *dual core* de 1.4 GHz, que podem ser obtidas através de um ataque de máquinas zumbis, o mesmo ataque pode ter sucesso em até 5 dias.

Fazendo um teste de invasão similar numa rede com o protocolo WEP, foi mostrada uma tela semelhante à exibida na Figura 6. Note que neste caso a chave utilizada foi "BK?(P" ("42:4B:3F:28:50" em hexadecimal), esta é uma chave de 5 caracteres, ou seja, 40 bits.

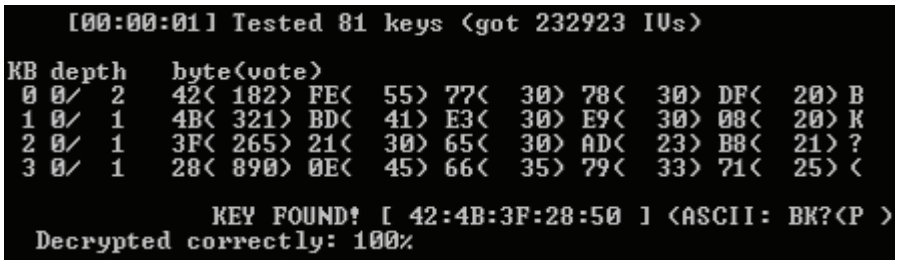

Figura 6: Ataque de dicionário ao WEP usando o Aircrack-ng

Configurando a rede com o WPA2-PSK criptografado pelo AES, um novo teste de invasão fracassou. Outros testes foram feitos com redes encontradas ao redor do prédio. Nestes testes 2 redes configuradas com o WEP foram quebradas, 1 rede configurada com o WPA-TKIP foi quebrada, já em outras 2 redes configuradas com o WPA2-PSK e AES os testes fracassaram.

6. Configurando um Ponto de Acesso

Para exemplificar a configuração de um Ponto de Acesso, foi utilizado um AP TP-Link TL-WR542G, um equipamento comum no mercado brasileiro. Caso o equipamento a ser utilizado seja novo, para iniciar a configuração, siga os procedimentos descritos no manual do fabricante. No caso do TP-Link, na barra de endereço do *browser*, acesse o endereço http://192.168.1.1. No primeiro acesso, será necessária a autenticação, os valores originais de fábrica são usuário "*admin*" e senha "*admin*". O endereço IP e as credenciais de acesso mudam de fabricante para fabricante. Por segurança, estes valores devem ser alterados o mais rápido possível. Em seguida, clique na opção "*Wireless Settings*", na área de links do lado esquerdo da tela. Será exibida uma tela semelhante à mostrada na Figura 7. Com os conhecimentos disponíveis até o momento, a figura mostra a melhor configuração possível para uma rede simples (BSS).

A título de exemplo, para o nome da rede sem fio foi colocado a palavra "teste" no campo SSID. Altere o nome da rede e não utilize nomes comuns, tais como: casa, rede, minha rede, etc.

Modifique a região para o país a qual vive. Isto é importante para adequar a faixa de frequência de transmissão e recepção do aparelho. Será dado um aviso que esta alteração só entrará em vigor após a reinicialização do equipamento.

Existem disponíveis para uso 14 canais dentro da freqüência de 2,4 GHz (padrão dos equipamentos de rede sem fio). Se você tiver vários AP, o indicado é a utilização dos canais o mais distante possível uns dos outros para minimizar a interferência de um canal em outro. Sendo assim, se for utilizar um AP no canal 1, utilize outro no canal 6 e o último no canal 11, por exemplo. Se o sinal do equipamento estiver fraco, teste outros canais. Isto pode ser causado por interferências de outros equipamentos sem fio na mesma faixa de freqüência, tais como: telefones sem fio, caixas de som sem fio, outras redes sem fio nas proximidades, etc.

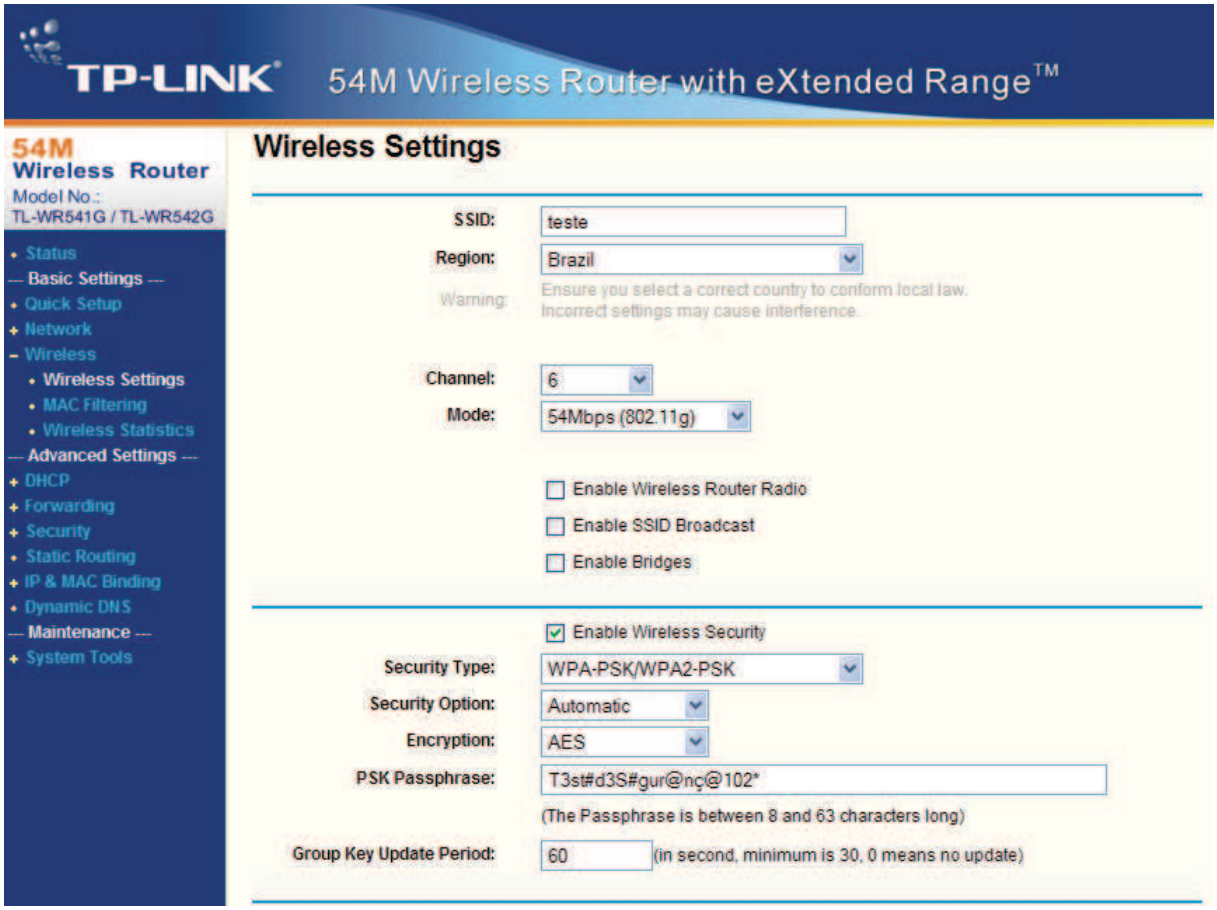

Figura 7: Tela de configuração de um Ponto de Acesso

O modo determina qual será o padrão 802.11 utilizado. O padrão é 802.11g, que é o recomendado devido sua compatibilidade com o padrão 802.11b, sua velocidade mais elevada e o suporte ao WPA2-PSK com o uso do AES.

A opção "*Enable Wireless Router Radio*" caso esteja marcada irá implicar na possibilidade do usuário configurar o Ponto de Acesso utilizando a própria rede sem fio, o que constitui em um risco. Recomenda-se não utilizar este recurso.

Marcar a opção "*Enable SSID Broadcast*" irá habilitar a divulgação do nome da rede (SSID) permitindo que qualquer pessoa possa descobrir sua rede e tentar se conectar. É uma boa política manter esta opção desmarcada, a não ser que você queira tornar pública a sua rede. Este ponto é bem importante, pois é bom dificultar ao máximo o trabalho de um atacante. Por outro lado, numa *lan-house* ou num cybercafé, o usuário precisa ter o máximo de facilidade de conexão possível.

A opção "*Enable Bridges*" deve ser marcada se for usar o AP como ponte, quando você precisar que um AP repasse as conexões para outro. Isto é utilizado para ampliar a cobertura da rede utilizando AP como repetidores. Um AP deverá ser eleito como o principal, deve estar conectado na rede local (LAN) e dar saída para a Internet, neste caso, ele atuará como gateway para os demais. Utilizando o modo ponte, recomenda-se cadastrar em todos os AP da rede o endereço MAC de todos os outros.

A opção "*Enable Wireless Security*" irá possibilitar que possamos tornar nossa rede mais segura. Habilitando esta opção irão surgir as opções que iremos dar maior foco. Estando desmarcada esta opção, o tráfego em sua rede sem fio será em texto plano, ou seja, sem nenhum mecanismo de criptografia ou de segurança.

Em "*Security Type*" selecione a melhor alternativa possível, neste caso, WPA-PSK/WPA2-PSK. Neste tipo, o aparelho permite o uso do WPA ou WPA2 com o PSK.

Em "*Security Option*" selecione WPA2-PSK, isto fará com que os equipamentos da rede se comuniquem com este protocolo. Deixando no modo automático, o AP irá identificar se o cliente usa o WPA-PSK ou WPA2-PSK.

Em "*Encryption*", como visto nas seções anteriores deste artigo, você deve obrigatoriamente definir o AES, caso contrário a segurança de sua rede estará comprometida. O TP-Link permite o uso do TKIP ou a colocação em automático, para que ele defina o valor para cada cliente que se conectar na rede. Neste caso, force todos os equipamentos de sua rede sem fio a utilizarem o AES.

Em "*PSK passphrase*" você deve colocar a senha que será compartilhada por todos que utilizarão sua rede. Esta senha pode ter de 8 a 63 caracteres (64 a 504 bits). Para criar uma senha forte, foi utilizada a frase "TestedeSegurança102*", onde o "e" foi trocado por "3" e "#" alternadamente, e o "a" por "@", foi utilizado ainda, maiúscula na primeira letra de teste e segurança. Além disto a senha usa números (3 e 102) e caracteres especiais (# e *). Estas pequenas mudanças aliadas ao tamanho da senha, a tornam mais forte, ou seja, mais resistente aos ataques de dicionário e força bruta. Isto é o recomendado para redes domésticas, para redes corporativas recomenda-se o uso de um servidor RADIUS.

O campo "*Group Key Update Period*" identifica de quanto em quanto tempo as chaves de seção AES deverão ser trocadas. Caso o valor seja zero a chave será estática. O valor mínimo é de 30 segundos, quanto menor este valor mais segurança a rede terá. Recomenda-se 60 segundos, que dá uma boa segurança e não onera tanto o processamento. Você pode utilizar tempos maiores, mas não deixe o valor zero. Para finalizar, salve as configurações, configure um cliente e teste a rede.

7. Conclusão

O trabalho apresentou o funcionamento básico das redes sem fio em termos de modos de configuração e protocolos; avaliou as principais vulnerabilidades e concluiu que o protocolo WEP e WPA, com TKIP ou PSK, são inseguros; identificou que o protocolo WPA2 com o PSK criptografado com o AES é a melhor recomendação de configuração no momento. Também foram pesquisados os ataques mais recentes às redes sem fio. Nestes casos as recomendações encontradas apontam para a permanência, pelo menos por enquanto, do WPA2-PSK com AES.

No trabalho foram feitos vários testes de invasão, um deles em uma rede utilizando o WPA com PSK sem o uso do AES, o teste foi bem sucedido. O teste foi repetido para uma rede com o protocolo WEP e também teve sucesso. Outros testes foram feitos e tiveram sucesso com redes WEP e WPA-TKIP. Já testes feitos em outras duas redes

configuradas com o WPA2-PSK, criptografadas com o AES, falharam. Estes testes demonstram que as inferências identificadas nas pesquisas estavam corretas.

Por fim, o trabalho mostrou detalhadamente como configurar um Ponto de Acesso, típico do mercado, com as melhores recomendações de segurança identificadas durante as pesquisas e os testes feitos para este trabalho.

7. Referências Bibliográficas:

AIRTIGH. ***WPA2 Hole196 Vulnerability***. Vulnerability presented at Black Hat Arsenal (July, 29, 2010) & Defcon 18 (July, 31, 2010). AirTight Networks. Disponível em: www.airtightnetworks.com/WPA2-Hole196. Acessado em 19/1/2011.

BECK, M. & TEWS, E. ***Practical attacks against WEP and WPA***. 2008. Germany. Disponível em: http://dl.aircrack-ng.org/breakingwepandwpa.pdf. Acessado em: 18/1/2011.

BERGHEL, H. & UECKER, J. ***Wireless Infidelity II: Airjacking.*** *Assessing the extent of the security risks involved in wireless networking technology by considering three possible scenarios demonstrating vulnerabilities*. On Digital Village - Communications of the ACM. Vol. 47, No. 12. December 2004. Disponível em: www.berghel.net/col-edit/digital_village/dec-04/dv_12-04.pdf. Acessado em: 18/1/2011.

BOILEAU, A. ***Wireless Networks: Success, Failure & Insecurity***. In Security-Assessment.com Breakfast Briefing, September 2006. Disponível em: http://www.security-assessment.com/files/presentations/SA_Sydney_BB_Wireless_06_AB.pdf. Acessado em: 19/1/2011.

GHKSAR. The Government of the Hong Kong Special Administrative Region. ***Wireless Networking Security***. Dec 2010. Acessado em: 19/1/2010. Disponível em: www.infosec.gov.hk/english/technical/files/wireless.pdf.

MOREIRA, M., & MENDES, R. ***ITIL na Gestão da Segurança da Informação***. 2008. 5º CONTECSI Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação (pp. 3009-3029). São Paulo: TECSI EAC FEA USP.

MOREIRA, M., FERREIRA, R., BORGES, F. ***Algoritmo de Assinatura Digital por Curvas Elípticas ECDSA (Elliptic Curve Digital Signature Algorithm)***. In: 6 CONTECSI International Conference on Information Systems and Technology Management, 2009, São Paulo. Anais do 6o CONTECSI. São Paulo: TECSI - FEA USP, 2009. v. 2009. p. 261-261.

MORIMOTO, C. ***Segurança em redes Wireless***. Publicado no Guia do Hardware em 22/8/2006. Disponível em: www.guiadohardware.net/tutoriais/entendendo-quebrando-seguranca-redes-wireless/pagina4.html. Acessado em: 19/1/2011.

MOTOROLA. Understanding the WPA2 “Hole196” Attack - Vulnerabilities & Motorola WLAN Countermeasures. 2010. Technical Brief for Airdefense. Disponível em:

www.airdefense.net/whitepapers/UnderstandingWPAWPA2Hole196Attack_TB_0810_chv4.pdf. Acessado em 19/1/2011.

OBERMAYR, T. ***Analysis of 802.11b WEP Vulnerabilities in Wireless Access Points and Bridges***. 2003. University of Applied Sciences. Graz, Austria. Disponível em: http://www.obit.at/AirSnort-03-obermayr.pdf. Acessado em: 18/1/2011.

OLIVEIRA, Nelson J. M. ***Análise Tecno-económica de Serviços Móveis Sem Fio***. 2003. Departamento de Electrónica e Telecomunicações. Universidade de Aveiro. Disponível em: http://gsbl.det.ua.pt/gsbl/Documentos/Relatorios/An%E1lise%20Tecno-Econ%F3mica%20de%20Servi%E7os%20M%F3veis%20e%20Sem%20Fios.pdf. Acessado em: 17/1/2011.

SILVA, Gilson Marques. ***Segurança em Redes Locais Sem Fio***. 2005. Dissertação de Mestrado em Ciência da Computação - Universidade Federal de Uberlândia.

STALLINGS, W. ***Cryptography and Network Security: Principles and Practice***. 1999. Prentice Hall.