Análise teórica e prática da segurança de redes sem fio na cidade de São Paulo

Wilson Leite da Silva Filho, Perito Criminal – IGP/SC

***Resumo* — Esse artigo apresenta um estudo de caso atualizado sobre a segurança de redes sem fio em importantes áreas financeiras da cidade de São Paulo. Tem como objetivo avaliar os riscos que empresas instaladas nessas áreas estão expostas devido a um possível uso inadequado dessa tecnologia.**

Para realizar essa avaliação, são abordados os principais aspectos de segurança de redes sem fio padrão IEEE 802.11, apresentados os conceitos teóricos e os dados obtidos em testes de invasão realizados em laboratório para diversas configurações de segurança das redes sem fio. Com base nos conceitos e no resultado dos testes de laboratório é possível verificar quais métodos de segurança são realmente efetivos e recomendados para a proteção da comunicação no ambiente sem fio. Uma vez verificada a periculosidade dos ataques realizados em laboratório, é possível contrapô-la aos dados colhidos em campo e com isso realizar uma avaliação dos riscos que essas empresas estão expostas devido a um possível uso inadequado da tecnologia de redes sem fio.

Além dessa análise, os dados são confrontados com um estudo prévio realizado no ano de 2004 [2]. Essa comparação permitiu visualizar, na região geográfica estudada, a evolução na utilização de redes sem fio do ano de 2004 até uma data mais recente.

***Palavras chaves*—Redes sem fio, *wireless*, 802.11, segurança.**

I. INTRODUÇÃO

Conforme a computação móvel evoluiu e os computadores ficaram menores (laptops, PDAs etc) surgiu a necessidade de associar conectividade com mobilidade. Dessa necessidade, nasceram as redes locais sem fio, que conectam os dispositivos por meio de ondas de rádio de curto e médio alcance. Para que a conectividade fosse maior e não houvesse incompatibilidade entre produtos de diversos fornecedores, o IEEE padronizou a comunicação de redes locais sem fio por meio da publicação do padrão IEEE 802.11. É nesse tipo de rede sem fio, também conhecido como Wlans, que este trabalho está focado.

O uso de redes locais sem fio pode ser uma atividade extremamente comprometedora do ponto de vista da segurança da informação ou pode ser suficientemente segura, dependendo de como a rede é configurada e de quais recursos de segurança são implementados.

A metodologia adotada nesse estudo compreende, primeiramente, em analisar as características de segurança das redes sem fio, realizando em laboratório provas de conceitos em cima dessas características, apresentando um relatório das vulnerabilidades encontradas e dos mecanismos de segurança que se mostraram eficientes em frustrar as tentativas de quebra de segurança nessas redes. Em uma segunda fase, o conhecimento adquirido será levado para fora do ambiente de laboratório, obtendo-se uma visão mais realista da segurança de redes sem fio em ambientes de produção, possibilitando, inclusive, uma comparação com um estudo prévio realizado no ano de 2004. Por motivos éticos e legais essa fase do trabalho será limitada a apenas um mapeamento de locais que possuam grande concentração de empresas, com a finalidade de ilustrar a quantidade de redes sem fio em uso e o nível de segurança empregado por essas empresas, trazendo informações para uma avaliação dos riscos que essas empresas estão expostas devido ao uso inadequado da tecnologia de redes sem fio.

II. ASPECTOS DE SEGURANÇA DAS REDES SEM FIO (802.11)

A necessidade de segurança em redes sem fio é uma questão tão ou mais importante de ser tratada quando comparamos essa necessidade com as redes com fio. A rede com fio, por sua natureza física, exige que um invasor primeiramente obtenha acesso físico a essa rede. Já na rede sem fio, a comunicação é feita via ondas de rádio, que trafegam livremente pelo ar, eliminando a necessidade de conexão física com a rede. Pode-se dizer que em uma rede sem fio todas as estações estão na mesma LAN. Posto esse fato, é importante a descrição de algumas características das redes sem fio (padrão 802.11) para a compreensão dos aspectos de segurança.

As redes sem fio são identificadas por um nome ou um número denominado SSID (*Service Set Identification*). A primeira informação que um atacante deve obter é o SSID da rede alvo.

Operando no modo com ponto de acesso (*Access Point*) uma rede sem fio envia periodicamente (100ms aproximadamente) um pacote de balizamento conhecido como *beacon*. Em algumas configurações de ponto de acesso, esse pacote contém o SSID. Um invasor pode configurar sua placa de rede sem fio para funcionar no modo monitor (*rfmon mode*), uma espécie de modo promíscuo encontrado nas placas de redes com fio. Nesse modo, basta escutar o meio com o auxilio de algum software específico de monitoração de redes sem fio para descobrir o SSID da rede. Exemplos de softwares para essa tarefa são o Kismet, Wellenreiter e o Airodump-ng.

É possível remover o SSID dos pacotes *beacon*, mas isso não adiciona muita segurança ao processo. Os pontos de acesso podem estar configurados para responderem a uma

requisição de informações sobre a rede. A estação envia um pacote de requisição de informação, não especificando o SSID no pacote. Se o ponto de acesso estiver configurado para responder a requisições do tipo "*any*", ele enviará uma resposta com o SSID da rede sem fio. Um software bastante utilizado para essa tarefa é o NetStumbler.

Seguindo nessa mesma linha, ainda é possível configurar o ponto de acesso para não responder a requisições que não especifiquem o SSID da rede. Essa também é uma configuração que acrescenta pouca segurança, já que durante o processo de associação, as estações enviam e recebem o SSID nos pacotes transmitidos. Basta voltar ao modo de monitoração passiva e aguardar que o SSID seja transmitido.

Mesmo que não haja transmissões no momento, o invasor não precisa necessariamente esperar que ela ocorra naturalmente. Existe uma técnica que permite forçar uma transmissão entre a estação cliente e o ponto de acesso. Para isso, o invasor deve enviar um pacote de desconexão para a estação cliente, forjando seu próprio endereço MAC com o endereço MAC do ponto de acesso. Como não há autenticação na estação do cliente para pacotes de controle (apenas verificação se o MAC é do ponto de acesso), o cliente encerrará a conexão e imediatamente iniciará uma nova. Essa é a oportunidade que o invasor esperava para poder obter o SSID da rede sem fio [6].

Por esses motivos, alguns esquemas de segurança baseados em criptografia foram desenvolvidos para redes locais sem fio. Entre os principais temos: protocolos WEP, WPA, WPA2 (IEEE 802.11i), autenticação por chave compartilhada e autenticação com uso de protocolos e servidores de autenticação e segurança nas camadas superiores à camada de enlace. Essas técnicas são discutidas nas seções seguintes.

A. Segurança por meio do protocolo WEP

O protocolo WEP (*Wired Equivalent Privacy*) é um protocolo de segurança que atua na camada de enlace de dados e usa recursos de criptografia para proteger a comunicação de redes 802.11. Infelizmente, o WEP possui sérios defeitos de projeto que o tornam inseguro.

O WEP utiliza uma chave secreta, compartilhada entre as partes, e o algoritmo criptográfico RC4. O algoritmo RC4 é um algoritmo de fluxo de cifras (*stream cypher*). Baseado em uma chave secreta e em um vetor de inicialização (IV), o RC4 gera um fluxo de bits. A mensagem criptografada é o resultado da operação XOR entre a mensagem em texto claro e o fluxo de bits gerados pelo RC4. Esse esquema de criptografia baseia-se no conceito do segredo perfeito por meio de chave de utilização única (*one-time pad*). A mensagem em texto claro é formada pelos dados a serem codificados mais um total de verificação (CRC-32). O pacote a ser enviado pela rede 802.11 é formado, entre outros campos, pelo vetor de inicialização (IV) não criptografado e pela mensagem criptografada pelo RC4 conforme ilustra a figura 1.

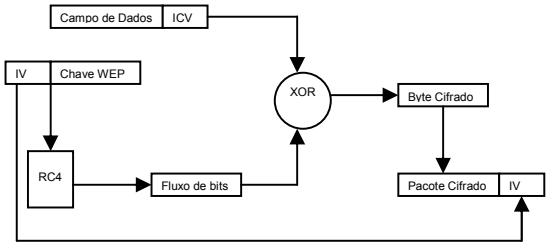

Figura 1 - Encapsulamento WEP

A segurança de um algoritmo de fluxo de chave única está baseada no fato de que determinado fluxo de chaves será usado apenas uma vez. Se o mesmo fluxo de chaves for usado mais de uma vez, a cifra pode ser quebrada de forma trivial. Tendo duas cifras que foram geradas com o mesmo fluxo de chaves, basta executar uma operação XOR entre as cifras para se eliminar a proteção da chave, resultando em uma mensagem que é o XOR das duas mensagens em texto claro. A partir daí, deve-se empregar métodos estatísticos para se obter ambas as mensagens em texto claro. Esse é um dos pontos em que o WEP falha.

Um caso prático dessa vulnerabilidade aconteceu com algumas placas de rede, que ao serem inicializadas, definiam o vetor de inicialização para o valor zero e incrementavam uma unidade ao seu valor a cada mensagem enviada. Como as placas de rede de laptops geralmente eram removidas freqüentemente, era comum que os vetores de inicialização possuíssem valores baixos. Mesmo placas que usavam um valor aleatório para o IV estavam vulneráveis, pois o tamanho do IV é de apenas 24 bits [8]. Estatisticamente, segundo o conceito do ataque de aniversário [7], após aproximadamente 5000 pacotes enviados, um deles será repetido. Com isso, um atacante deve monitorar a rede por alguns instantes para encontrar dois pacotes que utilizaram o mesmo vetor de inicialização e a mesma chave. Com essa informação, a segurança desses pacotes pode ser facilmente quebrada. Com um pouco mais de trabalho, pode-se determinar o fluxo de chaves para esse IV e montar-se um dicionário de fluxos de chaves para diversos IVs. Depois que um IV for rompido, todos os pacotes enviados com ele no futuro e no passado poderão ser totalmente decodificados e pacotes forjados poderão ser enviados.

Um outro ataque devastador ao WEP explora uma fraqueza descoberta no próprio algoritmo RC4. Em 2001, Fluhrer, Mantin e Shamir (FMS) escreveram um artigo descrevendo as vulnerabilidades no algoritmo de fluxo de chaves do RC4 quando o fluxo de chaves for gerado de um determinado modo [4]. E é justamente desse modo problemático que o WEP usa o RC4 [1].

O problema todo está no modo em que o WEP usa o vetor de inicialização em cada pacote. Quando o WEP usa o RC4 para criptografar um pacote, ele anexa o vetor de inicialização à chave secreta antes de fornecer ao RC4 essa chave. Isso significa que o atacante possui os 24 bits iniciais da chave secreta usada na criptografia de todos os pacotes. Com mais alguns cálculos baseados na saída do RC4, é possível se ter uma chance melhor do que uma chance ao acaso de se descobrir o resto da chave secreta. Se esse ataque for

executado repetitivamente, será possível descobrir a chave inteira com pouco esforço.

Esse ataque é nomeado em alguns textos da literatura como ataque estatístico contra o protocolo WEP e em outros como ataque FMS. O artigo original Fluhrer, Mantin and Shamir [4] especifica um certo padrão de vetor de inicialização que é suscetível a esse ataque. Os vetores de inicialização que seguem esse padrão foram denominados de vetores de inicialização fracos. Após a publicação desse artigo, outros padrões de vetores fracos foram encontrados, sendo que atualmente há registro de 17 padrões de vetores fracos. Algumas ferramentas que exploram esse ataque foram desenvolvidas, entre elas o airsnort e o aircrack-ng [9].

O WEP apresenta ainda algumas outras falhas de segurança. O algoritmo usado para garantir a integridade dos dados é o CRC-32. Esse algoritmo é adequado para detectar erros de transmissão em bits que tem seu valor alterado de forma aleatória devido a erros de transmissão introduzidos pelo meio físico. Mas, para uma verificação de integridade, onde os bits podem ser alterados por um atacante de maneira premeditada, esse algoritmo pode ser facilmente enganado.

Finalmente, o WEP utiliza a mesma chave secreta para criptografar os pacotes de uma mesma rede local sem fio. Esse fato facilita em muito a quebra do protocolo, já que existirá grande quantidade de dados criptografados com a mesma chave, proporcionado ao atacante uma grande quantidade de dados para criptoanálise [1].

B. Segurança por meio do protocolo WPA

Depois de ter ficado evidente a fragilidade do protocolo WEP, o IEEE e o consórcio de fornecedores de equipamentos de redes sem fio resolveram que um novo protocolo criptográfico para assegurar a comunicação nas redes sem fio precisava ser desenvolvido. O IEEE começou a trabalhar nesse novo protocolo, denominado 802.11i, que foi ratificado em 2004. Como o processo de especificação e padronização do IEEE levou um certo tempo, a indústria de redes sem fio se adiantou ao IEEE e lançou o protocolo WPA. O WPA pode ser considerado um *subset* do IEEE 802.11i e foi baseado em um rascunho do padrão IEEE 802.11i. Após a ratificação da versão final do 802.11i foi lançado o WPA2, que implementa todas as normas publicadas pelo IEEE.

Tanto o WPA como o WPA2 resolvem as falhas de segurança encontradas no WEP. O WPA introduziu um protocolo chamado TKIP (*Temporal Key Integrity Protocol*) que utiliza o protocolo criptográfico RC4 e o protocolo de verificação de integridade MIC (*Message Integrity Check*) denominado Michael. A criptografia baseada no RC4 já está presente no WEP, mantendo-se assim a compatibilidade com o hardware legado, necessitando apenas de atualizações de *firmware* e software. Já o WPA2, além do suporte ao TKIP, introduz um novo protocolo denominado CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). O CCMP usa o protocolo criptográfico AES, que não é suportado pelos dispositivos legados do WEP, necessitando assim, atualização do hardware.

O WPA resolve várias das vulnerabilidades do protocolo WEP. Primeiramente, o tamanho do campo IV é de 48 bits, o dobro do WEP, e seu valor deve ser escolhido de forma aleatória não previsível. A verificação de integridade dos dados no WEP usa o algoritmo CRC-32. No WPA a verificação de integridade do CRC-32 foi substituída pelo algoritmo muito mais robusto, Michael. O protocolo TKIP, introduzido no WPA, usa um conjunto de chaves temporais, derivadas da chave mestra e não a própria chave mestra, como faz o WEP. Além disso, o WPA executa o rechaveamento automático para derivar novas chaves temporais e mitigar o risco dos ataques estatísticos baseados nos IVs. O processo de escolha da chave temporal (PTK – *Pairwise Transient Key*) que é feita dinamicamente a partir da chave mestra (PMK – *Pairwise Master Key*) é realizado por um protocolo de autenticação de 4 vias (*4-way handshake*) [1].
Esse protocolo é ilustrado na figura 2.

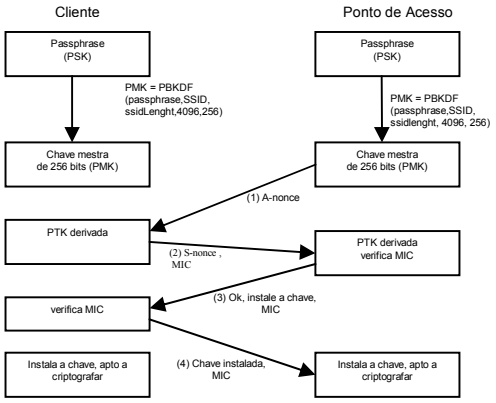

Figura 2 – Protocolo de autenticação WPA

A primeira observação a ser feita em relação a esse processo é o cálculo da chave mestra (PMK) usando a frase secreta (*passphrase*). A chave mestra é obtida submetendo-se a frase secreta a uma função de *hash* 4096 vezes. Uma vez calculada a chave mestra, o algoritmo de 4 vias de negociação de chave é usado para gerar a chave temporária (PTK). Uma chave temporária nova é criada toda vez que o cliente se conecta ao ponto de acesso e algumas vezes durante a conexão. A chave temporária é gerada em função de números aleatórios, denominados *nonces*, dos endereços MAC do cliente e do ponto de acesso. A autenticidade dos pacotes enviados é feita através do MIC recebido, que é gerado com a chave mestra. Ao receber o MIC, ele é recalculado no lado que o recebeu e comparado com o valor recebido. Se forem idênticos, o pacote é autêntico.

O WPA2 aprimora os recursos de segurança acrescentados pelo WPA, como por exemplo, o suporte ao protocolo criptográfico AES, que é mais robusto que o protocolo RC4. Até o momento, tanto o WPA quanto o WPA2 são considerados protocolos seguros para comunicação em redes locais sem fio.

III. PROVA DE CONCEITO

Como parte desse trabalho, foi montado um ambiente de rede local sem fio 802.11g e foram testadas várias configurações e diversos softwares de análise de tráfego e invasão. A rede 802.11g foi configurada sem o uso de criptografia e com o uso de criptografia por meio dos protocolos WEP, WPA, WPA2. Como esperado, pôde-se observar vulnerabilidades nas configurações sem criptografia e com criptografia WEP e verificar que com os demais protocolos de criptografia a segurança proporcionada frustra os testes de invasão realizados.

A topologia de rede usada nos testes de laboratório simula um cenário típico encontrado em redes corporativas. A rede é dividida por um roteador *firewall* em três sub-redes. A rede externa, que foi definida com o endereçamento IP 10.0.0.0/8, é a rede por meio da qual máquinas fora da corporação, consideradas desconhecidas e eventualmente hostis terão determinado acesso as redes internas. A segunda sub-rede, denominada DMZ (*Desmilitarized Zone*), recebeu o endereçamento IP 172.16.0.0/12 e é uma rede que pode ser acessada tanto pela sub-rede externa quanto pela sub-rede interna. Apenas determinado tipo de tráfego é permitido nessa rede e esse tráfego é controlado pela máquina *firewall*. A última sub-rede é a rede interna, com endereçamento IP 192.168.0.0/24. Essa rede é o ponto mais sensível da corporação. É onde estão os dados mais importantes e o ponto que deve ser mais bem protegido.

A princípio, a topologia baseada no conceito de DMZ oferece uma boa proteção, controlando todo o trafego entre as sub-redes por meio de um *firewall* centralizado. A rede interna, considerada um ponto crítico, fica isolada da rede externa, que é considerada uma rede potencialmente hostil. O conteúdo a ser oferecido para ambas as redes fica isolado na DMZ e protegido pelo *firewall*. É na DMZ que fica o servidor de páginas *Web*. O acesso direto da rede externa à rede interna é proibido pelas regras do *firewall*. Um atacante, posicionado na rede externa, teria que passar pelas regras do *firewall* para poder ter êxito em sua invasão. Esse seria um cenário típico se não existisse um ponto de acesso de rede sem fio. A rede sem fio elimina as barreiras físicas e lógicas impostas pela topologia DMZ e coloca todos que conseguirem acesso a ela na mesma sub-rede.

Com esse cenário e com as provas de conceito realizadas pretende-se mostrar que esquemas de segurança complexos podem ser burlados se a devida atenção não for dada à segurança de redes sem fio. Um atacante irá sempre tentar corromper a segurança no ponto mais frágil e a rede sem fio pode ser um ponto extremamente frágil se não estiver devidamente protegida.

O primeiro passo a ser executado na tentativa de invasão de redes sem fio é mapear essas redes e escolher um alvo a ser explorado. A ferramenta *airodump-ng* foi usada para esse mapeamento. O *airodump-ng* escuta intermitentemente em todos os canais da rede sem fio e lista as redes que puderam ser identificadas. O roteador *wireless* foi configurado para não fazer broadcast dos *beacons* com o nome (ESSID) da rede.

Mesmo sem o broadcast do ESSID, a rede alvo *labWirelessITA* pôde ser identificada. Outras redes funcionando pela vizinhança também puderam ser mapeadas.

Nos testes foram usadas duas antenas: uma de 3dbi e outra de 5dbi. A diferença entre a quantidade de redes encontradas com a antena de 5dbi foi significativa, mostrando que a escolha da antena também é uma etapa importante no processo de mapeamento e testes de redes sem fio. Todos os testes subseqüentes irão usar apenas a antena de 5dbi.

Foram selecionadas as ferramentas NetStumbler, por ser uma ferramenta muito popular no ambiente Windows e a suíte de ferramentas Aircrack-ng, por, além de oferecer bons recursos, ser uma das opções mais atuais em ambiente Linux.

O NetStumbler possui recursos interessantes como a possibilidade de integração do mapeamento com um sistema GPS. O NetStumbler é um mapeador de redes sem fio ativo. Isso significa que o seu funcionamento depende da resposta dos pontos de acesso a requisições (*probes*) enviadas pelo NetStumbler. Tais requisições são enviadas sem especificar o SSID da rede sem fio. Pontos de acesso que estiverem configurados para responder a esse tipo de requisição enviarão como resposta o seu SSID e outras informações sobre a rede sem fio. Por ser apenas um mapeador ativo, o NetStumbler não detecta redes que não respondam a requisições que não especifiquem o SSID e que não enviem pacotes *beacon* constantemente.

O NetStumbler foi a única ferramenta usada em ambiente Windows. Todas as ferramentas da suíte Aircrack-ng foram executadas em ambiente Linux. O Linux apresenta várias vantagens em relação ao Windows para testes de vulnerabilidades e *hacking* em geral. O Windows carece de ferramentas de mapeamento passivo e de *device drivers* que suportam o modo monitor das placas de rede sem fio e a injeção de pacotes pelas ferramentas de teste de vulnerabilidades. Além disso, há mais suporte da comunidade especializada em *wireless hacking* em Linux do que em Windows. Por essas razões, o Linux é o ambiente mais recomendado para a tarefa de testes de segurança em redes sem fio, ficando o Windows limitado aos testes mais simples com a ferramenta NetStumbler.

O Aircrack-ng é uma suíte de ferramentas para auditoria de redes sem fio. Por meio de suas ferramentas é possível capturar e quebrar a segurança de alguns protocolos criptográficos dessas redes. As ferramentas da suíte que foram usadas nos testes são o Airodump-ng, que é um mapeador passivo de redes sem fio, o Aircrack-ng, que é uma ferramenta capaz de quebrar pacotes protegidos pelo protocolo criptográfico WEP, uma vez que uma quantidade suficiente de pacotes seja capturada e o Aireplay-ng, que é uma ferramenta para a injeção de pacotes ARP com objetivo de aumentar o tráfego da rede e diminuir o tempo de captura de pacotes da rede sem fio.

O Aircrack-ng usa basicamente três técnicas para quebra do protocolo WEP. O primeiro método é baseado na técnica desenvolvida por Pyshkin, Tews e Weinmann (PTW). A principal vantagem da técnica PTW é que ela exige uma quantidade pequena de pacotes capturados para a quebra do protocolo. A segunda técnica é a desenvolvida por Fluhrer,

Mantin e Shamir e também por Korek, e é denominada aqui de FMS/Korek. Essa técnica incorpora vários ataques estatísticos para quebrar o protocolo WEP. A terceira e última técnica é uma combinação de dicionário de dados e força bruta. As técnicas PTW e FMS/Korek são efetivas apenas contra o protocolo WEP. Elas não surtem efeito se o protocolo criptográfico utilizado for WPA ou WPA2. Se o protocolo criptográfico utilizado for o WPA ou WPA2, apenas a técnica de dicionário de dados mais força bruta será tentada pelo Aircrack-ng [9].

A. Execução dos testes de laboratório

O mapeamento das redes sem fio e a captura dos pacotes foram feitos com a ferramenta *airdump-ng*. A rede alvo foi descoberta e seu ESSID (labWirelessITA) e o BSSID do ponto de acesso (00:1D:7E:1A:F3:E9) foram listados. Essas informações serão importantes nos testes seguintes.

Uma vez capturada uma quantidade de pacotes eles foram submetidos à ferramenta *aircrack-ng* para a tentativa de quebra do protocolo criptográfico.

Os testes para quebra de senha foram realizados em uma máquina Intel Celeron 2Ghz com 512MB de memória e os resultado dos testes estão listados na tabela a seguir.

Prot.	Tam. Chave (bits)	Quantidade tráfego monitorada	Número de chaves tentadas	Chave quebra-da	Tempo
WEP	64	250MB/280K IVs	1254	Sim	1 s
WEP	64	200MB/230K IVs	230	Sim	1 s
WEP	64	100MB/120K IVs	1497344	Não	5 min
WEP	64	50MB/58K IVs	742	Sim	1 s
WEP	64	25MB/30K IVs	435712	Não	2 min
WEP	128	1,5GB/1500K IVs	710	Sim	35 s
WEP	128	1GB/1090K IVs	1	Não	12 s
WEP	128	500MB/548K IVs	258	Não	10 s
WEP	128	250MB/27,5K IVs	684848	Não	19 min

Tabela 1 - Testes realizados para quebra da chave WEP

Os dados da tabela 1 mostram que com o número de IVs suficiente as chaves WEP podem ser quebradas rapidamente. Com um número de IVs insuficientes o processo de quebra da chave tende a falhar. Uma exceção ocorreu com a chave WEP de 64 bits e 50MB de dados transmitidos. Com um número de IVs abaixo do desejável a chave pôde ser quebrada rapidamente. Esse resultado parece estar ligado com o fator sorte, onde os ataques estatísticos de criptoanálise nos poucos IVs capturados surtiram efeito.

Deve-se observar que o aircrack-ng foi executado em sua configuração padrão. Há opções mais avançadas que poderiam resultar melhores resultados nos conjuntos de IVs que não puderam ser quebrados, mas essas opções não foram usadas nos testes.

Apesar do protocolo WEP ter sido quebrado em todos os casos, para a configuração com chave de 128 bits, por exemplo, foram necessários 1.500.000 IVs, o que corresponde a 1,5GB de tráfego de dados. Se a tentativa de quebra estiver sendo feita em uma rede com um tráfego relativamente modesto, pode-se levar um bom tempo até que se consiga capturar todos os IVs necessários. Para contornar esse inconveniente, existe um ataque denominado injeção de pacotes que permite ao atacante injetar tráfego na rede e com isso diminuir o tempo de espera para que se tenha todos os IVs necessários.

A ferramenta *aireplay-ng*, da suíte *aircrack-ng*, realiza o ataque de injeção de pacotes. O ataque de injeção de pacotes consiste em injetar pacotes ARP especiais na rede sem fio. Primeiramente o atacante deve autenticar-se no ponto de acesso. Devido às características do WEP, é possível em algumas configurações que uma estação que não possua a chave se autentique em um ponto de acesso. O *aireplay-ng* implementa as técnicas necessárias para essa autenticação, que é definida pelo *aireplay-ng* como autenticação fraudulenta (*fake authentication*). Após a autenticação, pacotes especiais ARP são injetados na rede sem fio a uma taxa de aproximadamente 500 pacotes por segundo. O ponto de acesso irá responder a esses pacotes e as respostas irão conter IVs. Esses IVs, que foram fraudulentamente solicitados, irão ser usados na quebra do protocolo WEP.

Mas, como já discutido anteriormente, a técnica de injeção de pacotes pode ser usada para agilizar o tempo de captura de pacotes. Esse processo permitiu que um pouco mais de 1.500.000 IVs fossem capturados em aproximadamente 1 hora. Com essa quantidade de IVs a chave pôde ser quebrada facilmente.

Apesar da injeção de tráfego permitir que redes protegidas com WEP de 128 bits possam ser quebradas em aproximadamente 1 hora, independente da quantidade de tráfego de pacotes legítimo da rede, essa técnica de ataque é invasiva e, portanto mais passível de ser detectada por algum software de detecção de intrusão. Além disso, a grande quantidade de tráfego injetada na rede pode criar um ataque de negação de serviço aos usuários legítimos, comportamento esse que nem sempre é desejado. Também há relatos em *sites* especializados [1] em testes de segurança de redes sem fio que a injeção de pacotes pode travar pontos de acesso de determinados fabricantes e modelos.

Em relação aos protocolos WPA e WPA2, estes se mostraram imunes a esse tipo de ataque, e devido a sua natureza de troca dinâmica de chaves e outros recursos adicionais de segurança, nenhum IV útil pôde ser capturado, conforme mostra a tabela 2.

Proto-colo	Tamanho chave	Quantidade tráfego monitorada	Número de chaves tentadas	Chave quebrada
WPA		3GB / nenhum IV	0	Não
WPA2		3GB / nenhum IV	0	Não

Tabela 2 – Resultados do monitoramento da rede com WPA e WPA2

IV. ANÁLISE DE CAMPO

A. Mapeamento das redes sem fio (Wardriving)

Wardriving é o processo de procurar nas imediações redes sem fio que apresentem alguma vulnerabilidade que possa ser explorada para dar ao atacante livre acesso à rede. Esse processo recebeu esse nome devido ao trabalho de Peter Shipley, que no ano de 2001 dirigiu seu carro pelas imediações do Vale do Silício, na Califórnia, para ver quantos pontos de acesso poderiam ser encontrados. Centenas de pontos de acesso foram encontrados naquela ocasião. Apenas a título de curiosidade, o termo *wardriving* em si, é uma alusão a um outro ataque a redes, que oferecem acesso via modem discado, chamado *wardialing*. O termo original, *wardialing*, teve sua origem no filme Jogos de Guerra, de 1986 [6].

Segundo Hurley [5], algumas ferramentas e equipamentos são necessários para atender os requisitos mínimos para praticar o *wardriving*. Os itens são: notebook, antena interna ou externa, softwares (NetStumbler, Kismet, Aircrack-ng, Network View, GPSD, *Wellenreiter, entre outros*) e opcionalmente dispositivo GPS.

Um mapeamento de redes sem fio em regiões da cidade de São Paulo foi feito no início de 2004 [2]. Nesse estudo, os autores do artigo percorreram áreas com grande concentração de empresas e monitoraram as redes sem fio dessas regiões. Com esse estudo, pôde-se chegar a um determinado número de redes sem fio detectadas e o nível de segurança delas. Pôde-se observar que a melhor segurança aplicada às redes sem fio, no âmbito da camada de enlace, foi a utilização do protocolo WEP por algumas delas.

Sabe-se, desde a época do estudo, que o protocolo WEP possui vulnerabilidades. Os testes de laboratório mostraram que esse protocolo pode ser facilmente quebrado, mesmo que não haja um fluxo de dados intenso na rede. Portanto, pode-se concluir que o cenário apresentado em 2004 é de apenas redes inseguras, já que as mais seguras estavam contando com a segurança do frágil WEP. No mesmo ano de 2004, o protocolo WPA foi ratificado pelo IEEE. A partir de então, as redes sem fio podem contar com uma opção realmente segura para sua proteção. O mapeamento realizado em nosso trabalho, quase cinco anos após o mapeamento de Cansian et al [2], mostrará a quantidade de redes que permanecem sem criptografia, as que confiam apenas no frágil WEP e as que estão realmente protegidas pelo WPA/WPA2. O novo mapeamento também mostrará o possível aumento da utilização das redes sem fio e os riscos atuais que essas redes podem apresentar.

Como discutido por Hurley [5], várias ferramentas podem ser usadas no processo de *wardriving*. Apesar de haver muitas opções, a funcionalidade de cada uma é mais ou menos a mesma. No nosso processo de *wardriving,* utilizaremos a ferramenta Airodump-ng da suíte Aircrack-ng. A Airodump-ng foi escolhida devido à familiaridade do autor com ela, já que foi a ferramenta usada nos testes de laboratório.

A estação de monitoração de redes sem fio é constituída de um carro, uma antena de 5dbi com base magnética, fixada ao teto no exterior do veículo, um notebook executando sistema operacional Linux, distribuição BackTrack3 [10], ferramenta Airodump-ng, motorista e co-piloto operando o notebook. Não dispúnhamos de aparelho GPS, mas esse detalhe não inviabilizou os testes, apenas tornou-o um pouco mais trabalhoso, devido ao fato que termos de associar os trechos monitorados aos dados obtidos de forma manual. Detalhes da configuração das ferramentas de teste e ilustrações dos procedimentos podem ser obtidos no trabalho de Florêncio, Marques e Leite [3].

O próximo ponto a definir foi a área a ser percorrida, como fazê-lo, a que horas e em quais pontos as redes seriam monitoradas. Decidimos monitorar as redes em pontos previamente definidos, em horário comercial e por um período de aproximadamente 15 minutos em cada ponto. Esse tempo foi suficiente para se obter um mapeamento geral das redes acessíveis naquela região e evitar problemas inerentes a atividades desse tipo, como, por exemplo, assaltos, suspeitas por parte da polícia, truculências do trânsito urbano e outras quaisquer.

A área escolhida para a varredura foi a mesma do estudo de Cansian et al [2]. Essa área compreende as imediações da Avenida Paulista, da Avenida Engenheiro Luís Carlos Berrine, da Avenida Brigadeiro Luís Antônio e da Avenida Juscelino Kubitschek. Essas avenidas são pontos muito conhecidos da cidade de São Paulo que concentram um grande número de empresas e têm grande importância financeira e cultural.

B. Discussão dos dados obtidos

Nesta parte do trabalho são apresentados os dados obtidos durante o processo de *wardriving* e é feita uma comparação entre esses dados e os dados do processo de *wardriving* realizado em 2004.

O *wardriving* foi realizado em um único dia, na data de 9 de setembro de 2008, em horário comercial, sendo que o processo de mapeamento de toda a área durou aproximadamente 7 horas. Os dados obtidos no estudo atual estão descritos nas tabelas 4 e 5. Os dados do estudo de 2004 estão descritos na tabela 3.

Região	Redes com WEP		Redes sem WEP (sem criptografia)		Total	
	Qtde	%	Qtde	%	Qtde	%
Av. Paulista	26	8.23	89	28.16	115	36.39
Av. Berrine	56	17.72	74	23.42	130	41.14
EixoJuscelino/ Brigadeiro	22	6.96	49	15.51	71	22.47
Total	104	32.91	212	67.09	316	100

Tabela 3 – Cenário de redes sem fio em 2004

Região	Redes c/ WEP		Redes c/ WPA		Redes c/ WPA2	
	Qde	%	Qde	%	Qde	%
Av. Paulista	589	13,96	395	9,36	132	3,13
Av. Berrine	704	16,68	520	12,33	142	3,36
Eixo Juscelino/ Brigadeiro	495	11,73	404	9,57	106	2,51
Total	1788	42,37	1319	31,26	380	9,00

Tabela 4 – Cenário de redes sem fio em 2008

Região	Redes c/ alguma criptografia (WEP+WPA+ WPA2)		Redes sem criptografia		Total	
	Qtde	%	Qtde	%	Qtde	%
Av. Paulista	1116	26,45	160	3,79	1272	30,14
Av. Berrine	1366	32,37	364	8,63	1734	41,09
Eixo Juscelino/Brigadeiro	1005	23,81	209	4,95	1214	28,77
Total	3487	82,63	733	17,37	4220	100

Tabela 5 - Cenário de redes sem fio em 2008 (continuação)

O primeiro dado a ser observado é a quantidade total de redes. Foram identificadas 4220 redes. Esse número representa um aumento de aproximadamente 13 vezes o número de redes existentes em 2004 como mostra a figura a seguir. Observa-se também que, apesar do grande aumento no número de redes, a proporção da distribuição dessas redes nas três localidades ficou próxima à de 2004, com um pequeno aumento de concentração das redes no eixo Juscelino/Brigadeiro em relação à avenida Paulista.

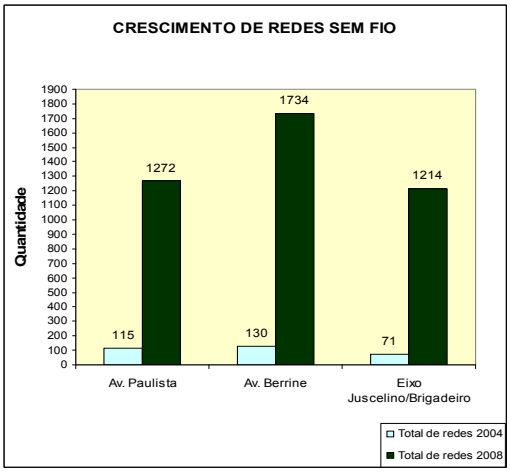

Figura 3 – Crescimento das Redes sem Fio no centro financeiro de São Paulo

Em relação à segurança, houve uma queda acentuada do número de redes sem criptografia. O número de redes sem criptografia representa atualmente 17,37% do total, contra 67,09% do ano de 2004 conforme ilustrado no gráfico da figura 5. Apesar da grande diferença, os números absolutos preocupam, pois são 733 redes totalmente abertas, contra 212 do estudo passado. Além disso, atualmente, 42,37% das redes estão protegidas pelo frágil protocolo criptográfico WEP. Isso representa 1788 redes que podem ser invadidas com as técnicas de quebra do WEP discutidas nesse artigo. As demais redes estão teoricamente seguras, sendo que 31,26% delas estão protegidas pelo robusto WPA e 9% pelo ainda mais robusto WPA2.

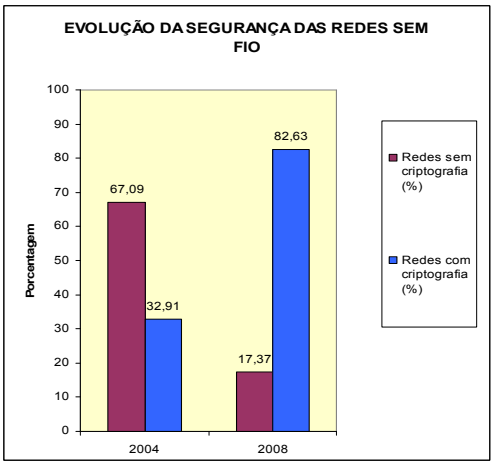

Figura 4 - Evolução da Segurança em Redes sem fio

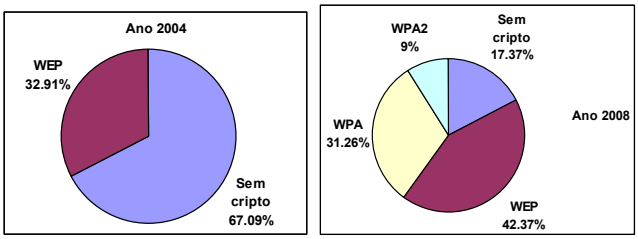

Figura 5 - Criptografia das redes sem fio

Os números mostram a grande falta de segurança no ambiente de redes sem fio dos principais pontos financeiros da cidade de São Paulo. Nada menos do que 59,74% das redes ou estão abertas ou confiam sua segurança ao protocolo WEP. Ou seja, são 2521 redes, muitas delas provavelmente contendo dados sensíveis, que podem ser invadidas com técnicas eficazes e documentadas de invasão de redes sem fio.

V. Conclusão

A questão da segurança sem fio foi explorada em três pilares: a teoria, provas de conceito realizadas em laboratório e testes práticos realizados em campo.

O primeiro pilar traz o embasamento teórico para compreensão dos testes e discute as falhas de segurança e os conceitos por detrás dessas falhas. É esse embasamento teórico que nos permitiu ter um melhor entendimento das técnicas a serem executadas em laboratório e em campo, sem o qual os testes não passariam de uma execução mecânica de procedimentos. Com os estudos dessa fase, já se mostrou evidente a fragilidade da segurança em redes sem fio que não utilizam nenhuma proteção ou baseiam sua proteção no protocolo de segurança WEP. É evidente a necessidade da implementação dos protocolos de criptografia sucessores ao frágil WEP. Os protocolos sucessores, WPA e WPA2 (802.11i), surgiram para solucionar as diversas brechas de segurança do WEP e são considerados seguros até o presente momento.

O segundo pilar do trabalho refere-se à prova de conceito realizada em laboratório. A primeira constatação dessa fase foi poder se ter idéia do grau de dificuldade de implementar os ataques existentes que foram previamente discutidos na fase anterior. Pôde-se constatar que a maior dificuldade nessa fase é configurar o software e o hardware para funcionarem de forma adequada. As ferramentas de testes e invasão de redes sem fio utilizam recursos avançados das placas de rede sem fio, como modo monitor, injeção de pacotes, entre outros. Tais recursos não estão disponíveis nas configurações padrão do sistema operacional e necessitam de controladores de dispositivo e configurações especiais. Esse desafio pôde ser superado com a ajuda de documentação encontrada na Internet e de *sites* especializados em ferramentas de segurança de redes sem fio. Dominada as técnicas de configuração desse ambiente, essa tarefa passou a ser trivial.

Uma vez configurado o ambiente, foi possível realizar diversos testes sem maiores dificuldades. Nesses testes ficou constatada a fragilidade da segurança em redes sem fio que não utilizam nenhuma proteção ou baseiam sua proteção no protocolo de segurança WEP. A facilidade com que as redes sem fio puderam ser invadidas, quando não devidamente protegidas, serve de alerta para os profissionais de segurança da informação e usuários dessas redes. Essa vulnerabilidade pode ser a porta de entrada para ataques mais elaborados e devastadores. Em contra-partida, foi possível observar também que existem técnicas eficazes de prover segurança nas redes sem fio e que essas técnicas frustraram os ataques que obtiveram sucesso em outras configurações. Os protocolos WPA e WPA2 mostraram-se resistentes aos ataques efetuados em laboratório e são altamente recomendados como um meio de prover uma segurança satisfatória.

O terceiro pilar do estudo realizado refere-se ao monitoramento das redes sem fio em campo. Com esse estudo de campo, foi possível quantificar as redes sem fio das áreas monitoradas e comparar esses dados com um estudo realizado no ano de 2004 por Cansian et al [2]. Os dados mostram um grande aumento de redes sem fio de 2004 a 2008. Apesar da porcentagem de redes sem criptografia alguma ter diminuído, mais da metade das redes sem fio dessas regiões ou estão sem criptografia ou baseiam sua segurança no frágil protocolo criptográfico WEP. Esse é um dado preocupante, já que o número de redes desprotegidas ou com uma proteção ineficiente é muito grande. É provável que exista uma grande quantidade de informações valiosas e sensíveis trafegando por essas redes inseguras.

Espera-se que estudos como este, mostrem às empresas e aos profissionais da área de tecnologia da informação o risco que seus dados estão correndo e que estes se sensibilizem e invistam na utilização de proteções mais eficazes. Em um cenário ideal, todas as redes sem fio que trafegam algum dado sensível à segurança da informação deveriam estar protegidas pelos protocolos WPA ou WPA2.

Como trabalho futuro, podemos apontar a necessidade de mais pesquisa sobre técnicas de invasão em redes protegidas pelos protocolos WPA e WPA2. Além disso, outras técnicas de proteção devem ser pesquisadas e usadas como coadjuvantes na segurança de redes sem fio. Entre essas técnicas podemos citar as ferramentas de detecção de intrusão (IDS – *Intrusion Detection System*) especializadas em detectar ataques a redes sem fio. A repetição da análise de campo de tempos em tempos também pode ser uma medida interessante para se monitorar a evolução da adoção de redes sem fio e da segurança empregadas pelos seus usuários.

REFERÊNCIAS

[1] Cache, Johnny; Liu, Vincent, "Hacking Exposed, Wireless**",** USA: 2007
[2] Cansian, Adriano Mauro; Grégio, André Ricardo Abed; de Sousa, Aleck Zander Tomé; Montes Filho, Antonio, "Uma análise crítica sobre a segurança de redes sem fio na cidade de São Paulo**"** in 1st International Conference on Cyber Crime Investigation (ICCyber'2004) – Departamento de Polícia Federal, Brasília: 2004
[3] Florêncio, Alessandre; Marques, Alessandro; Leite da Silva Filho, Wilson, "Segurança em redes sem fio IEEE 802.11 – Teoria, prova de conceito e aplicação prática", – Instituto Tecnológico de Aeronáutica – São José dos Campos: 2008
[4] Fluhrer, Scott; Mantin, Itsik and Shamir, Adi**,** "Weaknesses in the Key Scheduling Algorithm of RC4", in Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography: 2001
[5] Hurley , Chris, "WarDriving & Wireless Penetration Testing", 1st edition –USA: October: 2006
[6] Skoudis, Ed., "Counter Hack Reloaded**",** USA: 2006
[7] Stallings, William, "Criptografia e Segurança de Redes – Princípios e práticas", Tradução 4.a Edição, São Paulo: 2008
[8] Tanenbaum, Andrew S., "Redes de Computadores**"**, Tradução 4.a Edição – Rio de Janeiro: 2003
[9] D'Otreppe, Thomas, "Aircrack-ng – Main"**.** Disponível em: <http://www.aircrack-ng.org/doku.php>. Acesso em: 14 de julho de 2008.
[10] Moser, Max; Aharoni, Mati; Muenchi, J. Martin., "Backtrack"**,** Disponível em <http://www.remote-exploit.org/backtrack.html>. Acesso em: 14 de julho de 2008.

Wilson Leite da Silva Filho é graduado em informática pela Universidade Mackenzie – SP (1998), possui especialização em Análise de Sistemas por essa mesma universidade (1999), mestrado em Engenharia de Computação pelo Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT/USP, 2005) e especialização em Segurança da Informação pelo Instituto Tecnológico de Aeronáutica (ITA, 2008).

Atualmente é Perito Criminal do Instituto Geral de Perícias do Estado de Santa Catarina (IGP/SC). Já atuou como Especialista em Segurança da Informação na Companhia de Processamento de Dados do Estado de São Paulo (PRODESP) em 2008 e Analista de Software Sênior na Multinacional Norte-Americana Diebold Procomp, de 1999 a 2008.