CENTRO UNIVERSITÁRIO FEEVALE

RICARDO DALMORO BASSO

ANÁLISE DE VULNERABILIDADE DE REDE SEM FIO 802.11: UM ESTUDO DE CASO EM UM ORGÃO PÚBLICO MUNICIPAL

Novo Hamburgo, Novembro de 2008.

RICARDO DALMORO BASSO

rdbasso@gmail.com

ANÁLISE DE VULNERABILIDADE DE REDE SEM FIO 802.11: UM ESTUDO DE CASO EM UM ORGÃO PÚBLICO MUNICIPAL

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso

Professor orientador: Vandersilvio da Silva

Novo Hamburgo, Novembro 2008.

AGRADECIMENTO

Gostaria de agradecer a todos que contribuíram para a realização deste trabalho, em especial aos meus pais, por toda dedicação direcionada a minha educação e formação profissional; a minha irmã que me concedeu muito apoio; a todos os amigos que fazem parte da minha vida.

RESUMO

Devido à crescente necessidade por mobilidade houve uma vasta expansão das redes sem fio, sendo estas, tecnologias que oferecem a promessa de transferência de dados cada vez mais rápidas e de baixo custo através de ligações bastante abrangentes. Muito se tem alcançado no que se diz respeito a montar ou controlar estas redes, mas as ferramentas fundamentais que permitem a confiabilidade e a autenticidade dos dados transportados ainda não estão bem explicadas. Comunicação sem fio no que diz respeito à segurança ainda é um enorme desafio para investigação. Os protocolos conhecidos hoje no mercado e que são atualmente os mais utilizados para segurança de redes sem fio são o WEP e o WPA. Diversos problemas com estes protocolos já são conhecidos. O presente trabalho pretende aprofundar os estudos no que diz respeito a confiabilidade destes protocolos, bem como avaliar sua eficiência e a devida proteção oferecida.

Palavras-Chave: Criptografia, Segurança, *Wireless*

ABSTRACT

Due to the increasing necessity for mobility it had a vast expansion of wireless networks, being these, technologies that offer the promise of data transfer increasingly fast and low-cost connections through quite comprehensive. Much has been achieved as concerns mount or control these networks, but the basic tools that enable the trustworthiness and the authenticity of data stored has not yet clearly explained. Wireless communication in regard to security is still an enormous challenge for inquiry. The protocols known in the market today and are currently used mostly for the security of wireless networks are the WEP and WPA. Several problems with these protocols are already known.

The present paper intends to deepen the studies with respect to trustworthiness of these protocols and assess their efficiency and proper protection offered.

Key Words: Criptografia, Segurança, *Wireless*

LISTA DE FIGURAS

Figura 1: Emblema do padrão Wi-Fi. 14
Figura 2: Estrutura de rede Ad-Hoc. 15
Figura 3: Estrutura de rede Infra-Estrutura. 15
Figura 4: Exemplo de uma rede 802.11b 16
Figura 5a: Cifragem 20
Figura 5b: Decifragem 20
Figura 6: Tela principal do *Aircrack-ng* 26

LISTA DE QUADROS

Quadro 1: *Frequency Hopping World Channel Allocation* _____18

LISTA DE ABREVIATURAS E SIGLAS

AES	Encryption Standard (Padrão de Criptografia Avançada)
AP	Access Point (Ponto de Acesso)
ARP	Address Resolution Protocol (Protocolo de Resolução de Endereços)
BSS	Basic Service Set (Conjunto de Serviços Básicos)
CRC-32	Cyclic Redundance Check 32 (Checagem de Redundância Cíclica 32)
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuração de Servidor Dinâmico)
DoS	Denial of Service (Negação de Serviço)
DSSS	Direct Sequence Spread Spectrum (Espalhamento Espectral em Seqüência Direta)
EAP	Extensible Authentication Protocol (Protocolo de Autenticação para o acesso a rede)
ESS	Extended Service Set (Conjunto de Serviços Estendido)
ESSID	Extended Service Set Identifier (Identificador da rede)
FHSS	Frequency – Hopping Spread Spectrum
GPS	Global Positioning System (Sistema de Posicionamento Global)
HTML	HyperText Markup Language (Língua de Marcação de Hipertexto)
HTTP	HyperText Transfers Protocol (Protocolo de Transferência de Hipertexto)
IDS	Intrusion Detection System (Sistema de Detecção de Intruso)
IEEE	Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Elétricos e Eletrônicos)
ICV	Integrity Check Value
IP	Internet Protocol (Protocolo Internet)
IV	Initialization Vector (Vetor de inicialização)
LAN	Local Area Network (Rede de Computadores Local)

LLC	Logical Link Control (Controle Lógico de Enlace)
MAC	Media Access Control (Controle de Acesso ao Meio)
PC	Personal Computer (Computador Pessoal)
QoS	Quality of Service (Qualidade de Serviço)
RC4	Rivest Cipher Version 4
SSID	Service Set Identifier
TCP	Transmission Control Protocol (Protocolo de Controlo de Transmissão)
TKIP	Temporal Key Integrity Protocol (Protocolo Temporal de Integridade de Chave)
USB	Universal Serial BUS
VPN	Virtual Private Network (Rede Privada Virtual)
WAN	Wide Area Network (Rede Remota de Computadores)
WEP	Wired Equivalency Privacy (Privacidade Equivalente ao sistema com cabo)
Wi-Fi	Wireless Fidelity (Fidelidade Sem Fio)
WIRELESS	Sem Fio
WLAN	Wireless Local Area Network (Redes Locais Sem Fio)
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WWW	World Wide Web (Rede de Alcance Mundial)
WWAN	Wide Area Network (Rede de longa Distância sem fio)

SUMÁRIO

INTRODUÇÃO 11

1 REDES WI-FI 14
1.1 Conceito 14
1.2 Topologia 14
1.2.1 Ad hoc 15
1.2.2 Infra-Estrutura 15
1.3 Principais Padrões 16
1.3.1 Padrão 802.11b 16
1.3.2 Padrão 802.11a 16
1.3.3 Padrão 802.11g 17
1.3.4 Padrão 802.11i 17
1.4 Freqüências 17
1.4.1 *Frequency-Hopping Spread Spectrum* 17
1.4.2 *Direct Sequence Spread Spectrum* 18
1.4.3 *Orthogonal Frequency Division Multiplexing/Modulation* 18

2 PROTOCOLOS DE SEGURANÇA 19
2.1 WEP 19
2.2 WPA 21
2.3 WPA2 22

3 ANÁLISE DE VULNERABILIDADES 23
3.1 Vulnerabilidades dos Protocolos 23
3.1.1 Vulnerabilidades do Protocolo WEP 23
3.1.2 Vulnerabilidades do Protocolo WPA 24
3.1.3 Vulnerabilidades do Protocolo WPA2 24
3.2 Ferramentas 24
3.2.1 *Kismet* 24
3.2.2 *Aircrack* 25
3.2.3 *WireShark* 26
3.2.4 *Wellenreiter* 26
3.2.5 *Airodump-ng* 27
3.2.6 *Ettercap* 27
3.2.7 *WEPCrack* 27
3.3 Métodos 28
3.3.1 Ataque dicionário 28
3.3.2 Ataque DoS. 28
3.3.3 Ataque *Men-in-the-Middle* 29
3.3.4 Ataque *eavesdropping* 29
3.3.5 *Wardriving* 29

CONCLUSÃO **31**
BIBLIOGRAFIA **33**

INTRODUÇÃO

Com o avanço da comunicação nos últimos anos, a todo o momento, estão surgindo novas tecnologias de redes wireless, visando a atender as necessidades dos usuários com a melhor qualidade de transferência e segurança possíveis. Ao longo do tempo muito se evoluiu até chegar às redes de computadores da atualidade. As empresas e universidades estão apostando cada vez mais nesta tecnologia considerada revolucionária.

O crescimento da tecnologia *wireless* em ambientes empresariais vem acontecendo de maneira rápida. Em 2007, segundo o Instituto Gartner, o uso desta modalidade de redes aumentaria cerca de 64% nas organizações. Entre os participantes da pesquisa 44% citaram que a mobilidade iria alavancar a produtividade. Apesar do aumento do numero de adeptos as redes sem fio, 70% dos entrevistados relataram que não utilizam nenhum tipo de proteção contra invasores. Logo, a segurança torna-se o maior motivo de preocupação. http://www.silicon.com/

Quando o autor deste estudo ingressou em seu curso superior no ano de 2001, pouco se falava em conexões sem fio, tão pouco poderia prever a vasta expansão destes ambientes. Atualmente encontramos pontos de acesso *wireless* nos mais variados espaços sociais, desde o Aeroporto Internacional, até as praças públicas. O baixo custo e a qualidade do sinal oferecido tornam-se um grande atrativo para disseminar esta tecnologia.

Atualmente o autor atua profissionalmente em uma Prefeitura Municipal do interior do Estado, onde muito se fala em cidade digital - a qual é compreendida por uma conexão de alta velocidade que chega a um ponto, via link de uma operadora de telefonia, e se distribui no município por uma rede sem fio a lugares como escolas, postos de saúde e órgão da administração municipal. Diversos tipos de informações trafegam diariamente por essas redes, transmitindo desde dados confidenciais como folha de pagamento dos colaboradores e prontuários médicos, como simples arquivos de e-mail.

Estas redes sem fio, de fácil montagem e simples configuração, levantam uma dúvida quando se pensa em sigilo dos dados trafegados. O mercado atual disponibiliza diversos modelos de equipamentos, de diversos fabricantes. Todos estes, tendo como seus protocolos padrões de segurança WEP e WPA.

Redes *wireless* podem usar criptografia para proteger o tráfego entre a estação cliente e a base. Este ponto de acesso pode ser configurado para usar uma chave autenticadora que é armazenada e transmitida quando o cliente tenta se conectar. A maioria esmagadora das redes sem fio utiliza como protocolo de segurança o WEP, que suas falhas já são conhecidas e com algumas descobertas recentes permitiram que passassem de horas para minutos o tempo levado para sua quebra.

> Existem várias ferramentas desenvolvidas para descobrir chaves WEP, com maior ou menor grau de eficiência. Utilizam, em geral, uma combinação de força bruta, ataques baseados em dicionário e exploração de vulnerabilidades conhecidas. Por outro lado, chaves simples são mais fáceis de ser quebradas, independentemente da eficácia da ferramenta, e chaves-padrão não necessitam sequer de ferramentas para isso. (RUFINO, 2005 p.101)

Tendo em vista estes já divulgados problemas de segurança, o protocolo WEP caiu em descrédito. Antes do fechamento do padrão 802.11i o wi-fi Alliance liberou o protocolo WPA. Diversas mudanças e avanços foram incorporados a este novo protocolo, além de possuir diversos modelos que são moldáveis as necessidades do ambiente.

> Grande parte do problema de sigilo existente no WEP diz respeito aos mecanismos de criptografia utilizados. Para solucionar esses problemas, o WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. Porém, dados a diversidade e os ambientes onde uma rede sem fio pode existir (ambientes domésticos, pequenos escritórios, pequenas e grandes indústrias etc.), pensou-se ser razoável que o WPA tivesse também diferentes modelos de segurança para ter melhor aderência às diferentes necessidades. (RUFINO, 2005 p.35)

Embora o protocolo WPA seja mais seguro que seu antecessor WEP, algumas vulnerabilidades de seu método já são conhecidas nos dias de hoje, e estão reportadas em artigos e sites de busca na internet. É muito importante para seus adeptos, que sejam conhecidas estas informações para que possam se precaver em caso de qualquer tentativa de invasão. Entretanto até onde os dados criptografados por estas ferramentas estão realmente seguros? È possível garantir a integridade destas informações?

Motivado por estas indagações, este presente projeto de pesquisa será constituído de um estudo nos protocolos WEP e WPA, descrevendo suas vulnerabilidades e fazendo um comparativo entre eles. Além deste estudo pretende-se, efetuar uma tentativa de invasão ou

simples quebra de criptografia com ferramentas adequadas, na rede já existente no ambiente *wireless* da cidade digital.

1 REDES WI-FI

Neste capitulo será feito uma introdução as redes *wireless*, será apresentada as topologias disponíveis para a rede sem fio, alem de serem descritos os principais padrões do protocolo 802.11.

1.1 Conceito

As redes denominadas Wi-Fi (*Wireless Fidelity*) são uma alternativa para as redes convencionais com cabos, proporcionando as mesmas funcionalidades, mas de forma mais flexível. Essas redes seguem um padrão desenvolvido pelo IEEE (*Institute of Electrical and Eletronics Eginners*) conhecido como 802.11 (e seus sub padrões), que foi homologado no ano de 1997. Um dispositivo Wi-Fi pode ser reconhecido pelo símbolo característico apresentado na figura 1.

Figura 1: Emblema do padrão Wi-Fi.

1.2 Topologia

Em uma rede 802.11 podemos destacar dois tipos de estruturas; a chamada *Basic Service Set* – BSS, que nada mais é que um conjunto de dispositivos sem fio, comunicando entre si. Essa comunicação pode ser feita diretamente entre as estações ou através de um ponto de acesso (AP – *Access Point*).

Outro tipo de estrutura seria a *Extended Service Set* – ESS, que são vários BSS conectados entre si, através de AP. Utilizando esse modo, os AP devidamente interligados permitem aos seus usuários se movimentar de uma BBS para outra sem perder o sinal.

1.2.1 Ad hoc

Essas redes conhecidas por *Independent Basic Service Set* (IBSS) utilizam como métodos a conexão entre si de dispositivos, sem a necessidade de usar um ponto de acesso para interligá-las. O maior problema enfrentado pelos adeptos é não ter controle de acesso e segurança das informações que estão sendo trafegadas, devido a não possui um equipamento que tenha este propósito na rede. A figura 2 mostra um cenário Ad-Hoc

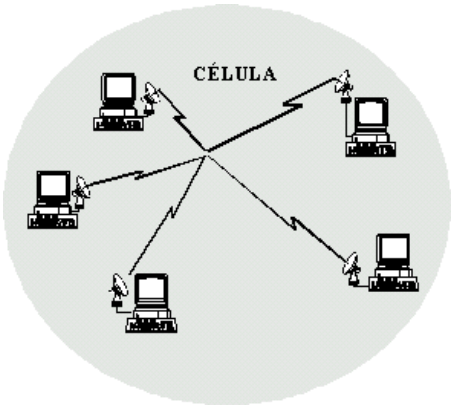

Figura 2: Estrutura de rede Ad-Hoc.
Fonte: http://www.wirelessbrasil.org

1.2.2 Infra-Estrutura

Conhecidas como *Infraestruture Basic* Service Set (*Infraestruture* BSS), essas redes utilizam-se de pontos de acesso para interligar as estações podendo também usar os AP para fazer comunicação entre de rede sem fio e uma rede tradicional com cabos. Adeptos a esse modo têm como grande vantagem uma maior segurança através de criptografia dos dados e filtragem de dispositivos por IP ou MAC. A figura 3 mostra um ambiente infra-estrutura.

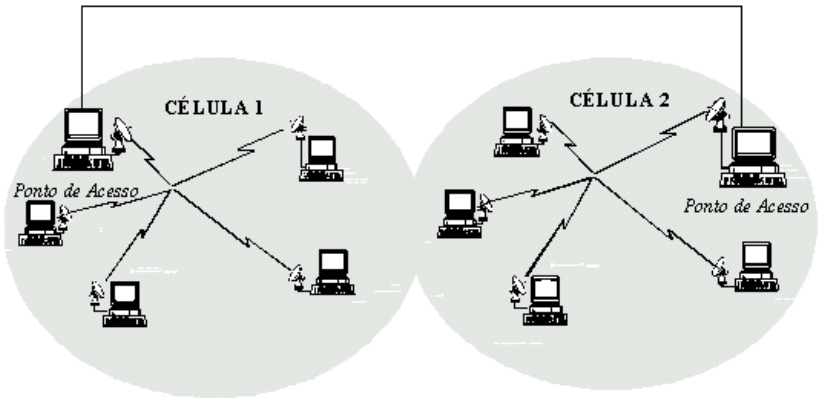

Figura 3: Estrutura de rede Infra-Estrutura.
Fonte: http://www.wirelessbrasil.org

1.3 Principais Padrões

As Wi-fi IEEE 802.11, foram umas das maiores novidades tecnológicas dos últimos anos. Esse sucesso todo é visível através do crescente numero de pontos de acesso nos mais variados lugares e com a maioria dos computadores portáteis novos já saírem de fabrica com os dispositivos IEEE 802.11. Serão citados abaixo os principais padrões para as redes 802.11.

1.3.1 Padrão 802.11b

Padrão para redes Wi-Fi que alcança uma velocidade de 11Mbps padronizada pelo IEEE, utiliza a freqüência de 2.4 GHz para trafegar informações e suporta até 32 usuários por ponto de acesso. Seus aspectos positivos seriam o baixo custo para implantação e a largura de banda gratuita, o inconveniente deste padrão seria a alta interferência gerada tanto na transmissão quanto na recepção devido a freqüência utilizada 2.4 GHz é equivalente a dos telefones móveis e dispositivos *Bluetooth*. Abaixo na figura 4 temos um exemplo de uma rede que utiliza o protocolo 802.11b

Figura 4: Exemplo de uma rede 802.11b
Fonte: http://www.babooforum.com.br

1.3.2 Padrão 802.11a

Esse padrão alcança velocidade de 54 Mbps dentro dos padrões e até 108 Mbps por fabricantes não padronizados. Suporta até 64 usuários por ponto de acesso e opera na freqüência de 5 GHz. As principais vantagens seriam a velocidade proporcionada e a ausência de interferências. Sua maior desvantagem seria a incompatibilidade com os padrões 802.11b e 802.11g quando se fala em *Access Point*.

1.3.3 Padrão 802.11g

Padrão de tem base a compatibilidade com os dispositivos 802.11b, sua velocidade é de 54 Mbps e utiliza a freqüência de 2.4 GHz. Possui as mesmas vantagens e desvantagens principais do 802.11b. Aceita para autenticação o WEP estática e também o WPA com criptografia dinâmica.

1.3.4 Padrão 802.11i

Foi criado para aperfeiçoar a segurança do protocolo 802.11, fazendo assim uma avaliação no protocolos de segurança: *Wired Equivalent Protocol* (WEP), *Temporal Key Integrity Protocol* (TKIP) *Advanced Encryption Standard* (AES) e IEEE 802.1x para autenticação e segurança. Todo o trabalho em cima do 802.11i vem sendo feito para integrar o AES com a subcamada MAC, para melhorar a segurança das informações trafegadas na rede sem fio, já que o padrão utilizado pelo WEP e WPA, o RC4 não possui a robustez necessária para garanti-la.

1.4 Freqüências

Segundo Earle (2006) as redes Wi-Fi utilizam três sistema de transmissão de rádio de espalhamento de espectro diferentes, denominados FHSS (*Frequency-Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Sprectrum*) e OFDM (*Orthogonal Frequenciy Division MUltiplexing/Modulation*).

As redes Wi-Fi trabalham em freqüências que sua utilização não depende de autorização. No Brasil a freqüência mais utilizada por adeptos das redes sem fio opera em 2.4 GHz.

1.4.1 *Frequency-Hopping Spread Spectrum*

FHSS é uma técnica de espelhamento que faz uso de um salto de freqüência, utilizando uma determinada freqüência por um período de transmissão e uma diferente durante outra. Essa característica da FHSS faz com que perca um pouco seu desempenho mas oferece uma vantagem que seria a transmissão menos sujeita a interferências visto que a freqüência utilizada muda constantemente.

Quadro 1: *Frequency Hopping World Channel Allocation*

País	Canal	Frequencia (GHz)	Tamanho do Canal (MHz)
Estados Unidos	2 a 79	2.402 – 2.479	26
Canadá	2 a 79	2.402 – 2.479	26
Inglaterra	2 a 79	2.402 – 2.479	26
França	48 a 82	2.448 – 2.482	27
Espanhe	47 a 73	2.473 – 2.495	35
Japão	73 a 95	2.473 – 2.495	23

Fone: EARLE(2006, p54)

1.4.2 *Direct Sequence Spread Spectrum*

A técnica de DSSS é um esquema de modulação que gera um padrão de bits redundante a cada bit transmitido. Segundo Rufino (2005, p.19): “Utilizado no padrão 802.11b, o DSSS utiliza uma técnica denominada code chips, que consiste em separar cada bit de dados em 11 subbits, que são enviados de forma redundante por um mesmo canal em diferentes freqüências, e a banda 2,4 GHz é dividida em três canais”. O DSSS tem melhor performance que o FHSS, devido a utilizar mais canais durante a transmissão dos dados, porem tem maior chance de sofrer algum tipo de interferência.

1.4.3 *Orthogonal Frequency Division Multiplexing/Modulation*

Está técnica de modulação de freqüência baseia-se na idéia de multiplexação por divisão de freqüências, onde envia diversos sinais em diverentes freqüências. O OFDM consegue dividir uma transmissão em diversos sinais, assim utilizando uma menor ocupação espectral. Está forma é a mais eficiente é utilizada tanto em redes sem fio quanto em redes cabeadas.

2 PROTOCOLOS DE SEGURANÇA

Segundo Soares (2005, p.448): “segurança são procedimentos para minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos, onde vulnerabilidade é qualquer fraqueza que pode ser explorada para violar um sistema ou as informações que ele contém”.

Neste capítulo serão abordados separadamente os mecanismos de segurança disponíveis para redes Wi-Fi. O objetivo principal é conceituar e descrever os protocolos, bem como suas características e funcionalidades.

2.1 WEP

O protocolo WEP (*Wired Equivalent Privacy*) é bastante utilizado por adeptos a redes Wi-Fi, para impedir que seja possível ler os dados transmitidos, e para evitar que intrusos tenham acesso à rede sem fio.

Este protocolo possui três serviços básicos:

- Confidencialidade: Através de uma chave secreta que cada estação de trabalho possui, este serviço que é opcional nos dispositivos permite que somente pessoas autorizadas tenham acesso as informações trafegadas;
- Integridade: Garante que o receptor receberá as informações corretas, sem modificações ou perda de dados;
- Autenticidade: Este serviço permite um alto padrão de segurança, para evitar que dispositivos não autorizados tenham acesso a rede.

O algoritmo utilizado para fazer a criptografia dos dados é o RC4, projetado por Ron Rivest, em 1987. Este algoritmo é de fluxo, ou seja, faz a criptografia dos dados a medida em que são transmitidos, aumentando assim sua performance. O código deste algoritmo foi mantido em segredo até ser postado na internet em 2001.

A segurança dos dados do protocolo WEP é composta por dois métodos: chave estática, que deve ser a mesma em todos os dispositivos de rede alem de possuir um componente dinâmico, que juntos formam a chave criptográfica. Segundo Rufino (2005, p.36): “WEP é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas”.

Um vetor de inicialização (IV – *Initialization Vector*) de 24 bits é utilizado junto a chave secreta de 40 ou 104 bits para gerar as informações criptografadas. Este vetor IV é enviado junto à mensagem cifrada, formando uma chave de 64 ou 128 bits pra que o receptor possa reverter o processo de criptografia. O IV também permite uma variação da chave estática em 24 bits, tornado diferenciado o resultado de mensagens idênticas. O esquema do funcionamento do WEP é apresentado abaixo sendo 5a esquema de cifragem e 5b decifragem.

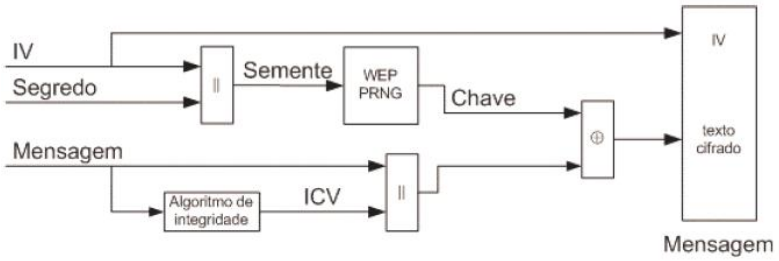

Figura 5a: Cifragem

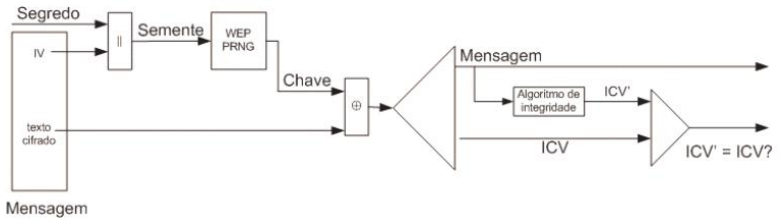

Figura 5b: Decifragem

Para que o protocolo WEP possa proporcionar segurança, a sua chave nunca deve ser reutilizada. Isto é muito imprescindível, pois quando se esgotarem o numero de possíveis IVs, a chave secreta deverá ser modificada. O motivo deste fato vem da possibilidade de um atacante obter uma chave (não a semente, mas a chave utilizada nas operações XOR) e com ela obter os dados cifrados com a mesma chave em outro momento.

Além disso, para tratar da integridade dos dados o WEP utiliza CRC-3213 (*Cyclic Redundance Check 32*), para calcular o *checksum* da mensagem, que é adicionado no quadro,

para garantir que a mensagem não foi alterada durante a transmissão. Dessa forma, o receptor recalcula o *checksum* para garantir a total integridade dos dados.

2.2 WPA

O WPA (*Wi-Fi Protected Access*) surgiu devido à necessidade de aumentar o nível de segurança nas redes sem fios, resolvendo alguns dos principais problemas do WEP. Criado em 2003, através de um conjunto de membros da *Wi-Fi Alliance* e de membros do IEEE, o propósito principal deste protocolo é a mudança constante da chave de encriptação dificultando a invasão ou descoberta da chave.

Este protocolo resolve a questão dos cabeçalhos fracos do WEP, que são chamados de vetores de inicialização (IV), e oferece uma forma de garantir a integridade das mensagens transmitidas pelo MIC (*Message Integrity Code*) usando TKIP (*Temporal Key Integrity Protocol)* para melhorar a criptografia de dados.

O WPA é compatível com o padrão de redes sem fio 802.11i e realiza melhorias em encriptação de dados e autenticação do usuário, porém para efetuar migração requer um upgrade de software. Ele pode ser utilizado numa rede híbrida que tenha WEP instalado. Segundo Rufino (2005, p.35): “Várias mudanças e avanços foram incorporados a esse protocolo, porém a maior parte deles exige a inclusão de outros elementos à infra-estrutura”.

Esse protocolo atua em duas áreas distintas:

• Primeira área - Onde visa substituir completamente o WEP. Essa primeira área trata da cifração dos dados, que tem por objetivo garantir a privacidade das informações que são trafegadas

• Segunda área - Foca a autenticação do usuário (área não coberta pelo WEP), utilizando os padrões 802.1x e EAP. (RUFINO, 2005)

É obrigatória no WPA a autenticação 802.1x; no padrão 802.11 era opcional. Essa autenticação é uma combinação de sistema aberto e autenticação 802.1x que possui duas etapas: a primeira é realizada pela autenticação de sistema aberto e indica ao usuário da rede sem fio que ele pode enviar quadros para a base e a segunda fase utiliza o 802.1x para realizar a autenticação do usuário.

Outro método de autenticação que o protocolo disponibiliza para ambientes domésticos onde não existe um servidor, é o chamado PSK (*Pre-Shared Key*), que possibilita ao usuário digitar manualmente suas chaves e senhas

Mesmo o WPA possuindo características de segurança superior ao protocolo WEP, ainda têm vulnerabilidades já conhecidas e reportadas, exigindo assim dos adeptos um conhecimento dessas técnicas para tentar minimizar ao máximo os estragos.

2.3 WPA2

O protocolo WAP corrigiu diversos problemas do WEP, mas seu desempenho foi prejudicado em termos de estabilidade, com isso, surgiu o WPA2 com a promessa de ser a solução definitiva de estabilidade e segurança para as redes sem fio. Sua principal mudança em relação ao seu antecessor WAP é o método criptográfico utilizado.

O WAP2 utiliza o AES (*Advanced Encryptation Standart*) junto com o TKIP com chave de 256 bits, um método mais poderoso que o WAP que utilizava o TKIP com o RC4. O AES permite ser utilizada chave de 128, 192 e 256 bits, o padrão no WPA2 é 256 bits, sendo assim, uma ferramenta muito poderosa de criptografia. Utilizando o AES surgiu a necessidade de novo hardware para processamento criptográfico, devido a isso, os dispositivos WP2 tem um co-processamento para realizar os cálculos criptográficos.

3 ANÁLISE DE VULNERABILIDADES

Neste capitulo serão tratadas às vulnerabilidades do protocolo 802.11, apresentando características que por sua vez podem causar riscos a rede sem fio. Também será feito um estudo sobre ferramentas e métodos para exploração dos pontos fracos de segurança.

3.1 Vulnerabilidades dos Protocolos

Diversas vulnerabilidades dos protocolos de segurança WEP e WPA já foram descobertas e reportadas. Esses problemas precisam ser conhecidos pelos administradores de redes para assim poder minimizar os prejuízos que podem ser ocasionados devido a essas falhas.

3.1.1 Vulnerabilidades do Protocolo WEP

O protocolo de segurança de redes sem fio WEP possui diversas vulnerabilidades, entre os principais já reportados destaca-se o fato de utilizar uma chave única e estática que deve ser compartilhada entre todos os dispositivos de rede. Em ambientes de pequeno porte (pequenos escritórios ou uso doméstico), o compartilhamento dessas chaves não chega ser um grande problema, mas em ambientes maiores ou em lugares que precisam de grande mobilidade o processo fica bem dispendioso.

Outra questão seria o algoritmo de criptografia utilizado RC4, que mesmo fazendo um processamento e devolvendo mensagens diferentes da original, permite que sejam identificadas essas informações através de seu tamanho. Segundo Rufino (2005, p.60): “Ao utilizar uma técnica de equivalência numérica, o RC4 recebe um byte que realiza um processamento e gera como saída também um byte, só que diferente do original. Essa função permite identificar quantos bytes tem a mensagem original, já que a informação gerada terá o mesmo número de bytes que a original”.

O vetor de inicialização VI foi criado para evitar que quando uma mensagem é cifrada com uma chave fixa idêntica a anterior tenha o mesmo resultado. Seu grande problema seria transmitir mensagens em puro texto, que é facilmente capturado por um software, deixando as informações disponíveis para qualquer intruso montar um ataque. O WEP também permite que seja reutilizado o VI, permitindo assim decifrar dados. A integridade (*Integrity Check Value*) sendo baseada em CRC32 permite que seja alterada a mensagem e o ICV sem que as estações de trabalho que utilizam a rede percebam.

3.1.2 Vulnerabilidades do Protocolo WPA

Mesmo possuindo características de segurança superiores as do WEP, ainda assim possui vulnerabilidades já conhecidas. A principal seria o ataque de força bruta ou dicionário, onde o intruso testa diversas senhas ou simples palavras em seqüência. As chaves utilizadas que possuem menos de 20 caracteres são mais susceptíveis a ataques. Segundo Rufino (2005,p.62) “É muito comum fabricantes usarem senhas pequenas (de 8 a 10 posições) imaginando que o administrador irá modificá-las quando colocar o equipamento em produção, porém isso não ocorre na prática, o que torna redes mesmo com WPA tão ou mais vulneráveis que redes que utilizam WEP.”

3.1.3 Vulnerabilidades do Protocolo WPA2

Conforme foi visto anteriormente o WPA2 possui um bom mecanismo de segurança. Os dispositivos que disponibilizam o WPA2 ainda não são amplamente utilizados, assim poucas vulnerabilidades são conhecidas o que proporciona uma maior sensação de proteção para quem o utiliza.

3.2 Ferramentas

Será feito uma conceituação de algumas das ferramentas mais utilizadas para analise de pacotes em redes sem fio. Os softwares descritos têm características tanto de ataque quanto de monitoramento preventivo da Wi-Fi.

3.2.1 *Kismet*

URL: http://www.kismetwireless.net

Esse sniffer é um detector de redes sem fio e um sistema de descoberta de intrusão. Desenvolvido em plataforma opensource trabalha com as redes 802.11b, 802.11a, e 802.11g,

possui em seu conjunto um grande numero de opções. Segundo Rufino (2005, p.80): “Por ser uma das ferramentas com maior velocidade de atualizações e adição de novas funcionalidades, o Kismet pode ser utilizado para vários fins, todos relacionados a redes sem fio. Possui poucos competidores em relação à quantidade de funcionalidades, número de chipsets suportados entre outras características.”

Esse software tem a característica de monitorar diversas origens diferentes. Foi projetado com a estrutura cliente-servidor e pode ter como base um único cliente para diversos servidores espalhados. Os pacotes capturados podem ser salvos em diversos formatos diferentes, também tem por padrão armazenar todas as redes encontradas durante a pesquisa.

Entre suas funcionalidades o sniffer pode mostrar em um estudo de trafego, quando o ultimo pacote foi recebido, alem da qualidade do sinal durante a transmissão dos dados. Também consegue fazer relações dos clientes de uma determinada rede, com seus devidos IP, que podem ser descobertos através de requisições ARP, UDP e TCP. Esse software é considerado pelas pesquisas feitas um dos melhores opensources da atualidade.

3.2.2 *Aircrack*

URL: http://www.aircrack-ng.org

Esse software é uma ferramenta para análise de trafego em redes sem fio, sua plataforma permite rodar tanto em Linux como em Windows. Tem como sua função descobrir ou recuperar chaves WEP e WPA-PSK de redes 802.11 a partir de dados capturados de qualquer ambiente Wi-Fi. *Aircrack* é na verdade um conjunto de ferramentas, entre elas estão: *Airodump* e *Wzcook*.

Seu novo modelo conhecido como Aircrack-ng já implementa o padrão FMS de ataque em conjunto como inúmeras otimizações como o *KereK*, alem dos novos PTW tornando assim o ataque muito mais rápido se comparado a outras ferramentas. Para utilização completa deste programa é necessário a captura de alguns dados de uma rede sem fio. Esta coleta de trafego poder ser executada por qualquer dispositivo wireless capaz de entrar um modo RFMON. Abaixo na figura 6 podemos visualizar a tela do *Aircrack-ng*.

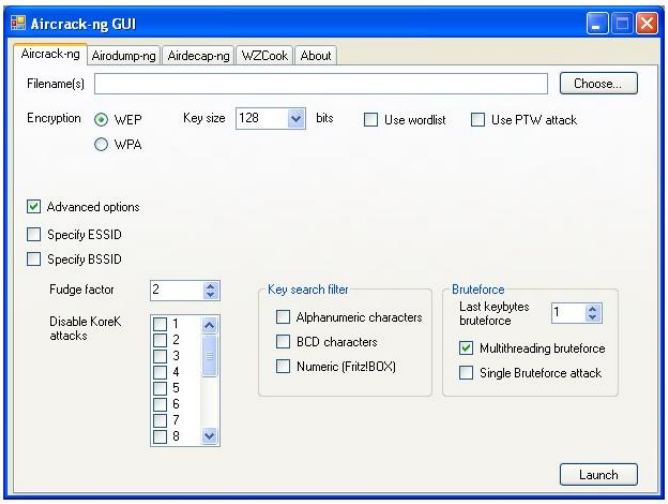

Figura 6: Tela principal do *Aircrack-ng*
Fonte: http://www.vivasemfio.com

3.2.3 *WireShark*

URL: www.wireshark.org

Mais conhecido como *ethereal* por adeptos, essa é a mais nova versão deste analisador de trafego de redes. Esse programa verifica pacotes transmitidos pelas interfaces de comunicação do PC e tem como objetivo detectar problemas de rede, conexões suspeitas, auxiliar no desenvolvimento de aplicações entre outras.

Wireshark também conhecido por tubarão dos fios é uma ferramenta totalmente livre, é muito utilizada por usuários de Linux. São inúmeras as funcionalidades desta ferramenta entre filtros e muitas informações, o utilizador consegue ter um controle total sobre os dados que são transmitidos na rede em diferentes protocolos.

3.2.4 *Wellenreiter*

URL: http://www.wellenreiter.net

O software *Wellenreiter* é uma ferramenta para monitorar e localizar redes sem fio. Possui uma excelente interface gráfica que permite a fácil visualização dos dados disponibilizados pelo programa. As informações trafegadas na rede como: canal de comunicação, marca do AP, criptografia utilizada entre outras; são passíveis de identificação utilizando esse programa. Alem disso a ferramenta registra todo o trafego da rede analisada.

Entre as funcionalidades do *sniffer Wellenreiter* está à capacidade de fazer um ataque de força bruta nos SSID, fazendo assim com que pacotes sejam enviados de maneira que o software fique oculto enquanto observa as informações solicitadas.

3.2.5 *Airodump-ng*

URL: http://www.aircrack-ng.org

A ferramenta *Airodump-ng* tem como sua função principal à captura de pacotes trafegados da rede sem fio. Normalmente esse software é utilizado em conjunto com o aircrack-ng, pois necessita de programa adequado para decifrar os dados capturados. Consegue capturar os quadros do vetor de inicialização IV do WEP, alem de criar um arquivo de texto contendo detalhes de todos os *Access Points* e clientes vistos.

3.2.6 *Ettercap*

URL: http://ettercap.sourceforge.net

Esta ferramenta pode ser considerada um canivete suíço, pois é um aplicativo com inúmeras funções. Trabalho explorando largamente o protocolo ARP e pode realizar vários ataques diferentes. Como envia um ARP *REQUEST* para o IP da LAN, não consegue executar suas funções oculto.

Entre as funções que o *Ettercap* possui estão: Permitir a colocação de caracteres em uma conexão estabelecida; Permite filtrar os pacotes trafegados na rede, alterando ou descartando; Permite a realização de *scanning* passivo da LAN; Permite a verificação de existência de outros *poisoner*s na rede.

3.2.7 *WEPCrack*

URL: http://sourceforge.net/projects/wepcrack/

Este programa explora a vulnerabilidade encontrada no protocolo de segurança WEP no começo do ano 2001. Funciona em qualquer sistema que possua suporte aos scripts Perl. Quem utilizar o *WEPCrack* normalmente são pessoas mal intencionadas que coletam informações essenciais da rede como por exemplo a BSSID, para programar ataques futuros a rede sem fio.

3.3 Métodos

Como já percebemos, sempre haverá um novo protocolo de segurança para tentar fazer as redes sem fio mais confiáveis. O problema é que junto com esses novos protocolos também vão surgindo técnicas para quebrá-los, abaixo será feito um estudo de métodos já utilizados para tal fim.

3.3.1 Ataque dicionário

Nesta forma especifica de ataque, os responsáveis pela tentativa de intrusão utilizam um *sniffer* para capturar o trafego em transito de uma determinada rede sem fio entre uma estação de trabalho e um ponto de acesso. Com isso, fazem uso de uma ferramenta adequada para adivinhar senhas. Já existem sites na internet que possuem uma lista de palavras excelentes para o ataque dicionário, normalmente estas listas não têm palavras repetidas o que ajuda muito na hora de utilizá-la. Uma delas está disponível em: ftp://ftp.se.kde.org/pub/security/tools/net/Openwall/wordlists/

Segundo Rufino (2005, p.62): “No caso do WPA, senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque.” Em redes que utilizam o protocolo WPA basta capturar quatro pacotes específicos de dados para tentar descobrir as senhas, enquanto no WEP é necessário pegar uma quantia grande de trafego. Uma maneira para tentar fugir destes ataques seria utilizando senha de um tamanho considerável e misturando caracteres com números, outra forma seria utilizando servidor de autenticação.

3.3.2 Ataque DoS.

Ataque *Denail of Sercice* (DoS – Negativa de Serviço) é um método onde o usuário perde o acesso ao servidor, e enquanto tenta resolver o problema apresentado o hacker que já está conectado a sua rede aproveita para copiar as informações direto da base principal. Este problema afeta principalmente as redes Wi-Fi que operam em banda de 2.4 GHz e com velocidade baixa, menos de 20 Mbps.

Os ataques podem ser efetuados de qualquer lugar dentro da cobertura da rede sem fio, durante um ataque o dispositivo se mantém de maneira que o canal fica sempre ocupado o que impede a transmissão de informações na Wi-Fi. Segundo Duarte (2003, p.41): “enviando as requisições de dissociação em períodos curto de tempo o DoS é concretizado. Isso, pois os clientes não conseguiriam permanecer conecta por muito tempo”.

Hoje em dia possuímos diversos equipamentos que operam na mesma freqüência 2.4 GHz que os protocolos 802.11b e 802.11g, entre eles estão o forno de microondas e o telefone sem fio, estes produtos podem ajudar nos ataques de negativa de serviço.

3.3.3 Ataque *Men-in-the-Middle*

O ataque *Men-in-the-Middle* (MITM) é um método no qual o hacker invade o sistema e fica alojado entre o usuário e o servidor conseguindo comprometer a comunicação sem que nenhuma das partes perceba. Normalmente o atacante fica no meio da transmissão entre dois pontos, dessa forma podendo ler, inserir e modificar os dados, qualquer informação que o usuário tiver acesso o atacante também terá.

Este ataque possui dois tipos de classificação: *full-duplex* que é quando o *hacker* consegue interceptar ambos os sentidos da comunicação e *half-duplex* que consiste na interceptação de um sentido somente, deixando o outro trafegar de forma normal. Além disso, o *hacker* durante o ataque pode ter uma posição transparente que seria ficar invisível enquanto é realizada a transmissão ou servir de proxy se expondo as entidades.

3.3.4 Ataque *eavesdropping*

Esse método de ataque também conhecido por *Sniffing*, consiste na analise de trafego entre cliente e servidor. Todas as informações trafegadas são monitoradas para utilizadas posteriormente para propósitos diversos. Com o uso de ferramentas de *sniffing* na rede, pode-se facilmente fazer uma leitura dos dados trafegados, alem de ter acesso aos pacotes, mesmo que sendo encriptados podem ser decifrados dependendo do algoritmo utilizado.

Um das formas para tentar minimizar o problema de *eavesdropping*, é usar VPN dificultando assim a escuta das informações, pois é possível analisar o trafego da rede sem fio pelo responsável.

3.3.5 *Wardriving*

Neste método de ataque, são utilizados dispositivos para encontrar todas as redes que estão dentro do raio de atuação do equipamento de monitoração. Um dos principais objetivos deste tipo de ataque é mapear todos os pontos detectados com o auxilio de um GPS.

> "WarDriving é o ato de mover-se ao redor de uma específica área e mapear a população de pontos de acesso wireless para um propósito estatístico. Estas estatísticas são então utilizadas para elevar a atenção sobre problemas de segurança

> associados a estes tipos de rede (tipicamente wireless)."(HURLEY, Chris et al, 2004, p.12).

O *WarDiving* na verdade pode ser considerado um método que aulixia quem necessita buscar redes Wi-Fi, alem de possibilitar acesso a essas redes de fio pesquisadas. Sem previa autorização dos proprietários da rede não é possível acessar nenhum tipo de recurso dos pontos de acesso.

CONCLUSÃO

Este projeto de pesquisa teve como prioridade apresentar os mecanismos de segurança das redes sem fio. Também foram abordadas ferramentas e métodos para tentar quebrar a proteção oferecida por estes dispositivos. A necessidade de aprofundamento bibliográfico em diversas áreas referentes das Wi-Fi proporcionou um bom conhecimento sobre o assunto.

A falta de segurança é considerada a maior preocupação existente para quem implanta Wi-Fi, mesmo com a existência dos protocolos, são conhecidos diversos métodos para quebrá-los e por em risco os dados trafegados na rede. É imprescindível que as pessoas que utilizam as redes sem fio, sejam informadas das vulnerabilidades existentes neste métodos de segurança para poder minimizar os problemas que podem ser causados.

O padrão mais utilizado pelas redes o 802.11b, tem muitos problemas referentes a segurança devido ao seu principal protocolo o WEP. As vulnerabilidades do WEP são facilmente exploradas com uma ferramenta adequada, desta forma comprometendo a segurança nas redes que o utilizam. Gradativamente os adeptos estão substituindo o WEP por outro padrão mais eficiente como o WPA.

Normalmente quem utiliza as ferramentas que exploram as vulnerabilidades da rede sem fio, são pessoas mal intencionadas e com um bom conhecimento da tecnologia. Hoje em dia o que beneficia os interessados nestes programas, é a facilidade com que estes softwares são encontrados na rede mundial de computadores, aumentando ainda mais as inseguranças das redes, alem dos problemas e vulnerabilidades apresentados pelos protocolos serem de domínio público e estarem disponíveis na internet.

Ao longo do estudo, foi possível entender que a maior parte dos ataques acontecem por descuido ou falta de conhecimento dos utilizadores das redes sem fio. A falta de atenção

do usuário, também permite que utilizando técnicas especiais o atacante induza-o a fazer ações que permita roubar informações sigilosas

.

BIBLIOGRAFIA

DUARTE, Luiz Otávio. **Análise das Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Trabalho de Conclusão de Curso. São José do Rio Preto: UNESP, 55p.

EARLE, Aaron E. **Wireless Security Handbook**. United States of America: Auerbach Publications, 2006. 354p.

IEE, Institute of Electrical and Electronics Engineers. **IEE Standards**. Disponível em <http://www.ieee.org/standards> Acesso em: outubro de 2008

PRODANOV, Cleber Cristiano. **Manual de metodologia científica.** 3.ed. Novo Hamburgo: Feevale, 2006. 77 p.

ROSS, John. **Wi-Fi – Instale, configure e use redes wireless (sem fio)**. Rio de Janeiro: Alta Books, 2003. 246p.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**. 2.ed. São Paulo: Novatec, 2005. 224p.

SILVA, Lino Sarlo da. **Virtual Private Network.** São Paulo: Novatec, 2002.

SOARES, Alcenir Barbosa, **Analise de qualidade de serviço VPN – Redes Privadas Virtuais – Utilizando redes sem fio**. Minas Gerais: 2004, 69p. Monografia (Graduação em Sistemas de Informação) – Faculdade de Ciências Aplicadas de Minas, UNIMINAS, 2004.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Elsevier, 2003

TORRES, Gabriel. **Redes de Computadores Curso Completo**. Rio de Janeiro: Axcel Books, 2001. 664p.

WI-FI Alliance. **Wi-Fi standards**. Disponível em <http://www.wi-fi.org > Acesso em: Setembro de 2007.