Análise de Vulnerabilidade em Rede Sem Fio 802.11x

Giancarlo Cardoso Vecchia, Luís Augusto Mattos Mendes

Universidade Presidente Antônio Carlos (UNIPAC)
Rodovia MG 338, Km 12 – Colônia Rodrigo Silva – 36.200-000 – Barbacena – MG – Brasil

gian@ufsj.edu.br, luisaugustomendes@yahoo.com.br

Resumo. A tecnologia *wireless*, ou seja, o padrão 802.11 para redes sem fio, tem sido amplamente utilizado em ambientes domésticos e corporativos com a finalidade de economia em infra-estrutura de cabeamento. Este sistema também permite maior mobilidade e flexibilidade para redes locais e em contrapartida exige algumas preocupações adicionais em segurança que são inerentes a um meio de comunicação sem fio. Este artigo tem como finalidade uma analise das vulnerabilidades e os ataques conhecidos neste sistema, bem como trazer alternativas de segurança ao sistema.

Palavra Chave : *WEP, WPA, Segurança de redes, criptografia*

1. Introdução

As redes sem fio, mais conhecida como ***Wireless*** ou ***Wi-Fi***, são redes locais que operam sem fio e estão se tornando, a cada dia, mais populares. Este sistema tem como pontos fortes a grande mobilidade, a praticidade, a utilização tanto em ambientes domésticos como em ambientes corporativos e o baixo custo em se tratando da inexistência de sistemas cabeados. O ponto fraco nesta nova tecnologia é a segurança, pois o meio de transmissão deste sistema está no ar. É factível o rastreamento e roubo de dados. Neste cenário, é necessário entender as características e particularidades das redes sem fio, permitindo um esclarecimento das vulnerabilidades do sistema e a aplicação de recursos que possibilitarão seu uso com maior segurança. Neste artigo foram utilizados softwares compatíveis com a plataforma Windows, que irão explorar estas vulnerabilidades.

2. Conceitos

Nesta seção, iremos abordar as tecnologias relacionadas ao padrão 802.11, conhecidas como *wireless* ou *wi-fi*. Serão discutidos os fundamentos, a forma de transmissão, as características, os padrões, a estrutura e os protocolos de uma rede sem fio.

As redes sem fio utilizam o ar como meio de transmissão de dados. Por este motivo, vários fatores interferem no sinal transmitido por um AP (*Access Point*), sendo necessária à criação de protocolos específicos que garantam a consistência e segurança dos dados. "*Fatores externos ocasionam muito mais interferência nas redes sem fio que as redes convencionais.*" [1]

2.1. Meios de transmissão

Os sinais transmitidos pelo *wireless* são chamados de radiofreqüência. Este sinal pode alcançar alguns centímetros ou vários quilômetros, pois a distância percorrida pelo mesmo está diretamente ligada à freqüência. Quanto maior a freqüência, menor será o alcance do sinal.

"*Uma faixa é, em geral, subdividida em freqüências menores, para permitir a transmissão em paralelo de sinais diferentes em cada uma delas,*" [1] chamadas de canais.

2.1.1. Bandas Públicas

De acordo com a agência governamental que regulamenta a utilização das radiofreqüências, ANATEL (Agência Nacional de Telecomunicação), existem, pelo menos, três freqüências disponíveis para uso de redes sem fio. Estas faixas de freqüência são:

- 902 – 928 MHz;
- 2,4 – 2,483 GHz;
- 5,150 – 5,825 GHz.

A faixa de freqüência de 2,4 GHz a 2,5 GHz é utilizada pela maioria dos equipamentos que provê acesso por uma rede sem fio. A faixa de 5,725 a 5,825 é estritamente para uso militar, o que restringe a comercialização de produtos que a utilizam.

2.1.2. Bandas Licenciadas

A utilização de faixas de radiofreqüência pode ser controlada, pela ANATEL, com o objetivo de destinar, a prestadores de serviços, uma faixa com menos interferência e que atinja uma distância maior em seu sinal. Isto acontece, por exemplo, com o WiMAX (*Wordwide Interoperability for Microwave Access*). Este sistema utiliza uma faixa de freqüência que vai de 3,5 a 5,8 GHz.

2.2. Características

Nos sistemas de redes sem fio, alguns conceitos foram adaptados das redes cabeadas e outros são restritos a tecnologia das redes sem fio. Em virtude das características especiais das redes sem fio, a maioria dos padrões foi criada para satisfazer as exigências desta nova tecnologia. Vejamos os principais conceitos que vieram das redes cabeadas e os inerentes ao sistema de redes sem fio.

2.2.1. *BEACON*

Os AP’s, para facilitarem a vida dos clientes, enviam sinais informando sobre a sua existência. Estes sinais são conhecidos por *BEACON FRAMES*, ou seja, informações enviadas gratuitamente pelos AP’s para orientar os clientes . Pode-se entender o *BEACON FRAME* como sendo um “quadro de anúncio”. Várias informações importantes preenchem o *BEACON FRAME*, entre elas: sincronizador de tempo, taxas suportadas e a mais importante, a informação do ESSID (*Extended Service Set Identifier*).

2.2.2. *Extended Service Set Identifier* (ESSID)

O ESSID é um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede sem fio. Cada fabricante utiliza um valor default para os seus dispositivos de rede. Em redes sem fio, o concentrador ou AP deve conhecer todos os clientes que desejam conexão enviando sinais com o identificador que é detectado pelos equipamentos clientes que por sua vez fazem um pedido de conexão.

2.2.3. Meios Compartilhado

Nas redes *Ethernet* cabeadas, através das chamadas redes distribuídas, recursos e informações são compartilhados entre todas as estações. Analogamente as redes *Ethernet* cabeadas, em redes sem fio o meio é compartilhado entre todas as estações que fazem parte de um mesmo AP. O tráfego fica visível para todas as estações participantes da rede sendo possível à captura não originado em si ou que lhe é destinado. Vejamos então as arquiteturas lógicas disponíveis para sistemas de redes sem fio.

2.2.3.a. *Ad-Hoc*

Utilizando uma rede *Ad-Hoc*, os clientes sem fio comunicam-se diretamente sem a utilização de um AP. Essa rede pode ser chamada também de *peer-to-peer* (ponto a ponto). Quando se trabalha em uma rede no modo *Ad-Hoc* os clientes desta rede formam um IBSS (*Independent Basic Service Set*) que consiste em pelo menos duas estações que se comunicam.

2.2.3.b. Infra-estrutura

Utilizando uma rede em modo Infra-estrutura, o AP cobre certa área e é responsável pela autenticação das estações e vários AP's podem ser utilizados na mesma rede sem fio. Através do *BEACON* vindo do AP, a estação escolhe uma rede das disponíveis e inicia o processo de autenticação com o AP. Uma vez que a estação e o AP se autenticaram o processo de associação é iniciado, permitindo que troquem informações e funcionalidades. Um simples AP que suporta um ou mais clientes sem fio é chamado de BSS (*Basic Service Set*) e múltiplos AP's em uma mesma rede lógica é chamada de DS (*Distribution Systems*). *"Uma ESS (Extended Service Set) é constituída por dois ou mais AP's conectados na mesma rede cabeada que pertencem ao mesmo segmento lógico (subnet), separado por um roteador."* [3]

2.4. Padrões

Os padrões aplicados em redes sem fio são formulados pelo IEEE (*Institute of Electrial and Electronics Engineers* - Instituto de Engenharia Elétrica e Eletrônica), que através de um grupo de trabalho definiu o padrão 802.11 que agrega uma série de normas para definir como deve ser feita a comunicação entre um usuário e um AP e entre usuário e usuário. As características principais das variações feitas ao longo do tempo são mostradas na Tabela 1.

Padrões	Freqüência	Taxa de Transmissão	Número de Usuários	Técnicas de Modulação
802.11b	2,4 Ghz	1 a 11 Mbps	32	DSSS
802.11a	5 Ghz	6 a 54 Mbps modo normal e 108 modo turbo[1]	64	OFDM
802.11g	2,4 Ghz	1 a 54 Mbps modo normal e 108 modo turbo[1]	255	DSSS, OFDM e MIMO
802.1n	2,4 Ghz	Até 500 Mbps[2]	255	DSSS, OFDM e MIMO

Tabela 1. Características principais do padrão 802.11

De acordo com a Tabela 1, DSSS (*Direct Sequence Spread Spectrum*) "*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 de 2,4 Ghz é dividida em três canais*" [1]; OFDM (*Orthogonal Frequency Division Multiplexing/Modulation*) que utiliza multi-portadora, como forma de transmissão, com a idéia básica de divisão de um sinal digital com uma alta taxa de bits, em um esquema de baixa taxa de bits e transmissão paralela e

[1] No modo turbo o AP pode chegar a taxas de transmissão de 108 Mbps que corresponde a duas vezes a velocidade nominal de 54 Mbps.

[2] Taxa de transmissão estimada

MIMO (*Multiple Input, Multiple Output*) que trabalha com várias antenas, o que permite enviar diversos pacotes de dados simultaneamente.

2.4.1. Padrão 802.11i

Em junho de 2004 foi confirmado o padrão 802.11i como responsável por ditar as técnicas de autenticação e privacidade para sistemas de redes sem fio. Neste padrão se determina os protocolos e algoritmos utilizados para implementar a segurança.

2.5. Estrutura de camadas do padrão 802.11

O padrão 802.11 utiliza como base a camada de referência OSI. O posicionamento dos protocolos dentro da camada física e de enlace utilizadas na camada de referência OSI corresponde neste padrão a PHY para a camada física, e MAC (*Medium Access Control*) com LLC (*Logical Link Control*) para a camada de enlace (Figura 1).

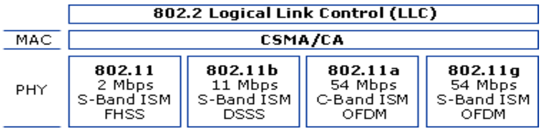

Figura 1. Camada Física e Enlace do padrão 802.11 [3]

2.5.1. Camada Física – PHY

Na camada física o 802.11 define uma série de padrões de transmissão e codificação para a comunicação sem fio com funções de: codificar e decodificar os sinais, gerar e remover parâmetros de sincronização, receber e transmitir os sinais e incluir as especificações do meio de transmissão.

2.5.2. Camada de Enlace – MAC e LLC

Na camada de enlace o 802.11 define duas camadas separadas, o MAC (*Medium Access Control*) e o LLC (*Logical Link Control*). A camada MAC tem como função reunir e abrir os dados de um pacote com endereços e campos de detecção de erro e controlar o acesso ao meio de transmissão. A camada LLC provê interface para camadas superiores e executa o controle de fluxo e erro de pacotes.

3. Segurança e Criptografia

Nesta seção, iremos abordar de forma conceitual, os mecanismos utilizados pelas redes sem fio que estabelecem a segurança do transporte de dados, dando ênfase para as características e funcionalidades destes mecanismos.

3.1. Criptografia

A palavra Criptografia vem das palavras em grego *Kriptos* (escondido, oculto) e *Grapho* (grafia, escrita), portanto é a ciência de escrever em códigos “um texto” claro (inteligível) em “um texto” cifrado (ininteligível). O objetivo da Criptografia é o provimento da privacidade das comunicações sensíveis e têm como objeto de estudo os processos de Encriptação e Decriptação. Encriptação é a transformação de um texto em uma forma que torna impossível a sua leitura sem o apropriado conhecimento com o propósito de assegurar a privacidade; por outro lado, a Decriptação e a transformação de um texto encriptado novamente em um texto na forma inteligível.

Nas transmissões de informações em redes sem fio exigem que os dados possam ser verificados quanto a sua integridade e origem e quanto a sua autenticidade.

A solução tradicional para garantir segurança e autenticidade de mensagens sujeita ao ataque, sempre envolveram técnicas de escrita criptografadas. As formas de criptografar as mensagens são sistemas criptográficos simétricos e sistemas criptográficos assimétricos.

3.1.1. Sistemas Criptográficos Simétricos

Os sistemas criptográficos simétricos utilizam um método de cifragem tradicional onde a chave de cifragem é a mesma da chave de decifragem. Em um sistema criptográfico simétrico, o princípio de reconhecimento da mensagem é descrito por: *"Se uma entidade pode cifrar corretamente uma mensagem utilizando uma chave que o verificador acredita ser conhecida apenas pela entidade com a identidade reclamada, este ato constitui prova suficiente de identidade"*.[5]

3.1.2 Sistemas Criptográficos Assimétricos

Os sistemas criptográficos assimétricos utilizam um método de cifragem onde às chaves de cifragem e decifragem são distintas. O originador do sinal usa uma chave privada para realizar a cifragem da mensagem, e publica uma chave pública correspondente a sua chave privada. O princípio básico de sistemas criptográficos assimétricos é: *"Se uma entidade pode assinar corretamente uma mensagem utilizando a chave privada da identidade reclamada, então esse ato constitui prova suficiente de autenticidade"* [5].

3.2 WEP (*Wired Equivalent Privacy*)

Nas redes 802.11 o tráfego pode ser criptografado através da utilização do protocolo *WEP* (*Wired Equivalent Privacy*). *"Uma chave WEP é uma chave de criptografia que provê a privacidade dos dados transmitidos entre um cliente e o AP criptografando os dados"* [3] utilizando algoritmo simétrico. *"O IEEE 802.11 especificou o WEP como sendo um simples protocolo de criptografia. Contudo, esse protocolo usa um stream para criptografia RC4 simétrica."* [3] O RC4 emprega uma chave secreta de 40 ou 104 bits que é compartilhada entre os clientes e o AP da rede. Durante a transmissão do pacote um vetor de inicialização de 24 bits é escolhido randomicamente e é anexado a chave WEP para formar a chave de 64 ou 128 bits. (Figura 3)

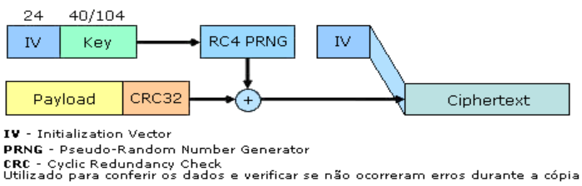

Figura 3. Formação do texto cifrado utilizando WEP [3]

3.3 WPA (*WI-FI Protected Access*)

O WPA é um subconjunto do padrão IEEE 802.11i criado pela WECA (*Wireless Ethernet Compatibility Alliance*), organização sem fins lucrativos formada em 1999, com o objetivo de certificar a interoperabilidades de produtos WLAN e neste caso, prover melhor segurança para redes sem fio. O WPA utiliza um protocolo de encriptação de chave, o TKIP (*Temporal Key Integrity Protocol*), mais avançada que a utilizada no sistema WEP e funciona em conjunto com o protocolo 802.1x. O 802.1x foi projetado para trabalhar em qualquer tipo de rede e define bem três papéis: um cliente (chamado de solicitante), um AP (chamado de autenticador) e um servidor de banco de dados (onde estão registrados os clientes). *"No 802.11 a autenticação 802.1x é opcional. Já quando se utiliza o WPA, a autenticação 802.1x é exigida. A autenticação WPA é uma combinação de sistemas abertos e 802.1x e utiliza as seguintes fases:*

- *a primeira fase usa uma autenticação de sistema aberto para indicar a um cliente sem fio que pode enviar quadro para o AP;*
- *a segunda fase usa o 802.1x para executar a autenticação em nível de usuário."*[3]

Basicamente, o processo de encriptação no WPA funciona da seguinte maneira:

- o dispositivo começa com uma chave-base secreta de 128 bits chamada de TK (*Temporal Key*);
- a TK é combinada com a TA (*Transmitter Address*), o endereço MAC do transmissor criando a chave TTAK (*Temporal and Transmitter Address Key*);
- a TTAK é então combinada com o vetor de inicialização (de 24 bits e não previsível) para criar as chaves que variam a cada pacote.

4. Análise dos Algoritmos Usados em Redes Sem Fio 802.11x

As redes sem fio utilizam-se de algoritmos que provêem ou tentam prover a segurança dos dados transmitidos. Nesta seção iremos abordar os algoritmos utilizados pelos sistemas de criptografia WEP e WPA.

4.1. Algoritmo RC4

O algoritmo RC4 foi desenvolvido em 1987 por Ron Rivest para a empresa *RSA Data Security Inc*, líder mundial em algoritmos de segurança. Durante sete anos foi um segredo comercial e, em 1994, foi introduzida numa lista de discussão dedicada à criptografia como um código equivalente e tem como principal característica o uso de um array que quando é utilizado tem os seus valores permutados e misturados com a chave. A chave pode ter tamanho de 256 bytes ou seja 2048 bits. Portanto, é um algoritmo de fluxo que envia um conjunto de bits cifrados em fluxo contínuo, classificado com sendo um sistema criptográfico simétrico.

"*O RC4 cria bytes pseudo-aleatórios a partir de uma semente de tamanho variável. Estes bytes formam a chave de criptografia que será utilizada para encriptar uma mensagem, através de operações XOR bit a bit. Ao receber esta mensagem cifrada, o destinatário deve executar o algoritmo da mesma maneira (realizando XOR bit a bit com a mesma chave), recuperando a mensagem.*

Por exemplo: seja uma chave composta pela seqüência de bits: k1 k2 k3 ... o dispositivo origem realiza, então, operações $\oplus$ (XOR) entre um texto: p1 p2 p3 ... e esta chave, gerando uma seqüência de bits de texto cifrado: c1 c2 c3 ... onde ci = pi $\oplus$ ki, para i=1, 2 , 3, ... O destinatário, ao receber os bits cifrados c1 c2 c3 ... realiza novamente a operação de XOR com a chave, recuperando o texto p1 p2 p3 ... sendo pi = ci $\oplus$ ki, para i=1, 2, 3, ...

A criação da chave RC4 funciona da seguinte maneira:

- *o RC4 recebe uma semente K de n bits (entre 1 e 2048). A partir desta semente, cria um vetor S de 256 bytes. Este vetor tem suas posições permutadas, de acordo com o valor da semente;*
- *com o vetor formado, o algoritmo utiliza seus dados para criar uma seqüência de números pseudo-aleatórios para criptografar a mensagem. Conforme a mensagem vai sendo enviada, o vetor S tem seu conteúdo alterado*." [6]

Os algoritmos KSA (*Key Scheduling Algorithm*) e PRNG são utilizados para permutar o vetor S e gerar os números pseudo-aleatórios. (Figura 4)

Utilizando-se do WEP como sistema de criptografia, um outro algoritmo é usado com o objetivo de verificar se os dados não foram alterados durante a comunicação. Este algoritmo redundante chamado de CRC-32 (*Ciclic Redundancy Check*) é um código detector de erros; um tipo de função *hash* que gera um valor expresso em poucos bits em função de um bloco maior de dados.

```
KSA (K)
inicialização:

   para i=0.. N-1
      S[i]=i
   j=0

permutação:

   para i=0.. N-1
      j=j+S[i]+K[i mod l]
      inverte (S[i], S[j])
```

```
PRNG (K)
inicialização:

   i = 0
   j = 0

loop de geração da chave:

   i = i + 1
   j = j + S[i]
   inverte (S[i], S[j])
   saída ch = S[S[i]+S[j]]
```

Figura 4. Algoritmos KSA e PRNG [6]

4.2. Algoritmo AES - Rijndael

O NIST (*National Institute of Standards and Tecnology*), a pedido do governo americano, lançou um processo de seleção que definiria um novo algoritmo de chave simétrica e tinha como objetivo a proteção de informações do governo federal. Este novo algoritmo, chamado de AES (*Advanced Encryption Standard* – Padrão de Criptografia Avançado), substituiria o DES (*Data Encryption Standard* – Padrão de Criptografia de Dados), que havia sido quebrado. *"Três anos e meio após o início do concurso, o NIST chega à escolha do vencedor: Rijndael. O nome é uma fusão de Vincent Rijmen e Joan Daemen, os dois belgas criadores do algoritmo. Segundo o NIST, ele combina as características de segurança, desempenho, facilidade de implementação e flexibilidade. O Rijndael apresenta alta resistência a ataques como "power attack" e "timing attack" e exige pouca memória, o que o torna adequado para operar em ambientes restritos como "smart cards", PDAs e telefones celulares."*[7]

O algoritmo *Rijndael* é constituído de uma cifra de blocos baseado em uma rede de permutação em blocos de 128, 160, 192, 224, e 256 bits e chaves de 128, 160, 192, 224, e 256 bits. Os blocos consistem de matrizes de 4x4 bytes (blocos de *Rijndael* com mais de 128 bits usam matrizes maiores). As chaves de cada iteração são calculadas em operações de campo finito (a maioria das operações dentro desse algoritmo são feitas dessa forma). Cada iteração (com exceção da última) consiste em 4 etapas, primeiro cada byte da matriz é substituído em uma *S-Box*[3], então cada linha da matriz é deslocada N posições, em seguida as colunas são substituídas numa operação de campo finito (com exceção da última iteração) e então é aplicada a chave da iteração a matriz resultante. Este processo é repetido 10, 12 e 14 vezes dependendo do tamanho da chave utilizada (128, 192, 256). Não existem ataques efetivos conhecidos contra o AES; em 2002 um ataque teórico conhecido como "*XLT attack*" foi proposto por Nicolas Courtois, porém estudos posteriores não reproduziram os termos de Courtois, ataques "*XLT*" são considerados especulativos e nunca foram reproduzidos. Em Abril de 2005 Daniel J. Bernstein propôs um ataque chamado "*cached timing*", que devido à falta de praticidade de reprodução (foram usados 200 milhões de "*chosen plaintexts*") foi considerado impraticável. O governo americano considera AES como utilizável em proteção de dados considerados secretos.

5. Análise das Vulnerabilidades em Redes Sem Fio 802.11x

Nos dois sistemas de criptografia utilizados em redes sem fio, problemas administrativos e técnicos tornam estes sistemas vulneráveis a ataques. Nesta seção, iremos abordar estas vulnerabilidades.

5.1. Vulnerabilidade do protocolo WEP

O protocolo WEP caiu em descrédito quando foram publicadas maneiras de quebrar seu algoritmo. Recentemente, um artigo escrito por ErikTews, Ralf-Philipp Weinmann e

[3] S-Box é uma matriz calculada através de passos chamados de *rounds*

Abdrei Pyshkin da Universidade de Tecnologia de *Darmstadt*, demonstra esta vulnerabilidade, e foi resumida assim: “*Nós demonstramos uma agressão rápida no protocolo WEP que está apto para recuperar uma chave WEP de 104-bit usando menos do que 40.000 pacotes com a probabilidade de êxito de 50%. Para obter um sucesso de 95% em todos os casos 85000 pacotes são necessários. O IV* (vetor de inicialização) *destes pacotes podem ser escolhidos aleatoriamente. Este é um progresso no número de pacotes exigidos em ordem de grandeza aos métodos conhecidos para a recuperação de chave sobre ataque ao WEP. Em uma rede 802.11g, o número de pacotes desejados podem ser alcançados por re-introdução em menos do que 1 minuto.”* [8]

Vamos então dar uma noção com é feita a encriptação e decriptação dos dados em uma rede sem fio com o protocolo WEP.

Sabemos que o WEP trabalha com uma chave secreta k, compartilhada entre as partes envolvidas na comunicação, e usada na encriptação dos dados. Esse processo é dividido em 3 fases distintas:

- ***checksumming*** → possuímos a mensagem M a ser transmitida, e calculamos o seu CRC (*Cyclic Redundancy Check*) c(M). Concatenamos ambas e obtemos o texto-plano P = [M, c(M)]. (Figura 5)

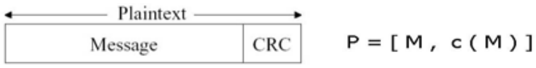

Figura 5. Diagrama Checksumming [6]

- **encriptação** → P é encriptado usando o algoritmo de encriptação RC4. É escolhido um vetor de inicialização v e, com base nele e na chave k, é gerada uma seqüência de *bytes* pseudo-aleatória, a qual chamará de *keystream* (RC4(v, k)). O próximo passo é fazer um XOR (ou exclusivo) de RC4 com P, obtendo o texto encriptado. (Figura 6)

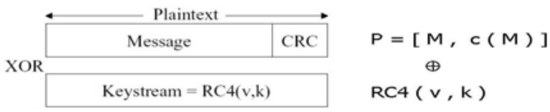

Figura 6. Diagrama Encriptação [6]

- **transmissão** → finalmente é transmitido C juntamente com o vetor v.(Figura 7)

Figura 7. Diagrama Transmissão [6]

Na recepção, o receptor faz o processo inverso:

- com base em v (enviado junto de C) e em k (que ele já possui), é calculado o RC4.
- é feito um XOR de RC4 com C:

$$\begin{aligned} P' &= C \oplus RC4(v,k) \\ &= P \oplus RC4(v,k) \oplus RC4(v,k) \\ &= P \end{aligned}$$

- é calculado o *checksum* na forma [M´, c(M´)]. Se ele for igual a c(M), então M´= M

O cenário com o transmissor e receptor é demonstrado na Figura 8.

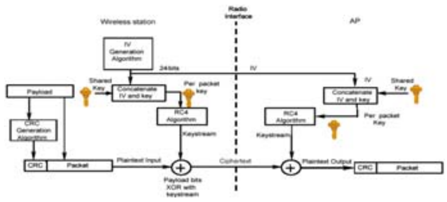

Figura 8. Diagrama com Transmissor e Receptor[6]

O objetivo da segurança do WEP é confidencialidade, integridade e controle de acesso baseado na dificuldade de descobrir a chave secreta por meio de força bruta.

5.1.1. Reutilização da *KeyStream*

A encriptação de duas mensagens com o mesmo vetor de inicialização pode revelar informações sobre ambas as mensagens. Por exemplo:

$C1 = P1 \oplus RC4(v,k)$ e $C2 = P2 \oplus RC4(v,k)$

$C1 \oplus C2 = [P1 \oplus RC4(v,k)] \oplus [P2 \oplus RC4(v,k)]$

$C1 \oplus C2 = P1 \oplus RC4(v,k) \oplus P2 \oplus RC4(v,k)$

$C1 \oplus C2 = P1 \oplus P2 \oplus RC4(v,k) \oplus RC4(v,k)$

$C1 \oplus C2 = P1 \oplus P2$

Então, conhecendo o XOR de C1 e C2, conhecemos o XOR de P1 e P2.

Isto pode levar ao ataque mais óbvio, que é: se P1 é conhecido, P2 também o será.

Existem duas condições requeridas para ataques em que a reutilização da RC4 é explorada como falha:

- disponibilidade de textos encriptados com a mesma RC4
- conhecimento parcial de alguns dos P´s

Na tentativa de prevenir ataques, o WEP usa um vetor de inicialização diferente por pacote. Como a RC4 é gerado a partir de k e de v, cada pacote recebe uma *keystream* diferente.

Contudo, v é enviado na parte não encriptada dos dados transmitidos. Assim, ele está disponível tanto para os receptores quanto para malfeitores.

Existem vários exemplos de reutilização da RC4, alguns são citados abaixo:

- v é público → uma causa potencial de reutilização da RC4. Como a chave k raramente é mudada, a reutilização de v acarreta na reutilização de uma RC4. Como v é pública, o malfeitor pode muito bem descobrir a RC4 e reutilizá-la em futuros ataques.
- v muda a cada pacote de acordo com o padrão WEP, contudo, nada mais é especificado sobre como é feita a seleção de v´s. Algumas placas PCMCIA retornam o valor de v para zero quando são reinicializadas (ou seja, toda vez que são inseridas num *laptop*). Se isso ocorrer frequentemente, *keystreams* correspondentes a baixos valores de v têm uma maior probabilidade de reutilização.
- v tem 24 *bits* → um cálculo simples demonstra que um AP trabalhando com pacotes de 1500 *bytes* numa taxa média de 5 Mbps vão exaurir todos os valores possíveis de v em menos de um dia.

5.2. Vulnerabilidade do protocolo WPA

Em relação ao WPA, é sabido que este protocolo tem "*características de segurança superiores às do WEP, ainda assim apresenta algumas vulnerabilidades*"[6] e que devem ser mostradas para que a segurança proposta possa acontecer.

"*A despeito desta vulnerabilidade não ser especifica do protocolo WPA, este também está sujeito a ataques de força bruta ou dicionário, onde o atacante testa senhas* *em seqüências e/ou em palavras comuns (dicionário). No caso do WPA, senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque*”[6] e é muito “*comum fabricantes usarem senhas pequenas (de 08 a 10 posições) imaginando que o administrador irá modificá-las*”[6], porém isso não acontece na prática, o que torna redes mesmo com WPA tão ou mais vulneráveis que redes que utilizam WEP.

Não há até o momento ferramentas publicamente disponíveis que promovam ataques de força bruta e/ou dicionário para ataque ao WPA utilizando a plataforma Windows. São conhecidas ferramentas na plataforma Linux como o WEP Crack e o WPA-supplicant e para a plataforma MacOS X existe o KisMAC.

“*Mesmo com as melhorias verificadas no WPA, há vários pontos vulneráveis no processo, independentemente do método utilizado (chaves previamente compartilhadas ou modo infra-estrututa), verificam-se problemas no armazenamento das chaves, tanto nos clientes quanto nos servidores/concentradores, que podem comprometer a segurança de redes que utilizam WPA.*”[6]

6. Técnicas e ferramentas de ataque

Ao longo desta seção serão mostradas as várias técnicas de ataque e as ferramentas utilizadas para comprovar a insegurança do sistema mostrada na seção 5.

6.1. Ataques as Redes Sem Fio

Alguns ataques às redes sem fio ocorrem da mesma forma que nas redes cabeadas, assim como outros novos tipos que foram introduzidos. Pela natureza das redes sem fio, o AP precisa anunciar a existência da rede, de modo que os clientes possam se conectar e usufruir de todos os serviços e recursos fornecidos. Para isso, *beacons* são enviados periodicamente, facilitando a descoberta de uma rede sem fio, inclusive por pessoas mal-intencionadas.

6.1.1. Associação Maliciosa

A associação maliciosa ocorre quando um atacante simula um AP, iludindo outro sistema de maneira que este acredite estar se conectando em uma rede sem fio real. Com o auxílio de um software, como o HostAP, o atacante é capaz de enganar um sistema, mostrando um dispositivo de rede padrão como um AP

6.1.2. ARP *Poisoning*

O ataque de envenenamento do protocolo de resolução de endereços (ARP – *Address Resolution Protocol*) ocorre na camada de enlace de dados e só pode ser disparado quando o atacante está conectado na mesma rede local da vítima. Este ataque limita-se às redes conectadas por *hubs*, *switches* e *bridges*, excluindo as redes conectadas por roteadores e *gateways*.

O ataque de ARP *Poisoning* já era conhecido na rede cabeada. No entanto, a forma de concepção dos APs e a implicação da arquitetura de rede gerada pelo AP fazem com que esta rede seja particularmente vulnerável a esta forma de ataque.

6.1.3. MAC *Spoofing*

Para as redes onde os APs utilizam o endereço MAC para o controle dos usuários autorizados, a conexão pode ser invadida por este tipo de ataque. Um atacante mal intencionado pode capturar um endereço MAC válido de um cliente e trocar seu endereço pelo do cliente. No Windows esta modificação é trivial, conforme mostrado na figura 9. De posse de tal endereço, o atacante poderá utilizar a rede e todos os seus recursos.

Figura 9. Janela de configuração do endereço MAC de uma placa de rede

6.1.4. Negação de Serviço

Este tipo de ataque, conhecido como DoS (*Denial of Service*), procura tornar algum recurso ou serviço indisponível. Um determinado atacante pode disparar um ataque de negação de serviço de várias maneiras, podendo ser disparados de qualquer lugar dentro da área de cobertura da rede sem fio.

Como as redes do padrão 802.11b/g trabalham com a freqüência de 2.4 GHz, também utilizada por fornos microondas, aparelhos de monitoramento de crianças e recentemente por telefones sem fio, os ataques de negativa de serviço são facilitados com a inserção de ruídos emitidos por estes aparelhos.

No entanto, existem ataques mais sofisticado, como por exemplo, um atacante se passando por um AP com o mesmo ESSID e endereço MAC de um outro AP válido inundando, assim, a rede com pedidos de dissociação. Estes pedidos fazem com que os clientes sejam obrigados a se desassociarem e se reassociarem.

Enviando as requisições de dissociação em períodos curtos de tempo, o DoS é concretizado. Isso acontece porque os clientes não conseguiriam permanecer conectados por muito tempo. Finalmente, outra maneira de disparar um ataque de negativa de serviço é simplesmente inundando a rede com tráfego aleatório.

6.1.5. *Wardriving*

Wardriving pode ser considerado uma forma de ataque de vigilância, tendo como objetivo encontrar fisicamente os dispositivos de redes sem fio para que estes dispositivos possam, posteriormente, ser invadidos.

Para isto, algumas ferramentas fáceis de serem encontradas na Internet são usadas para encontrar redes sem fio que estão desprotegidas. A partir disso, pode-se fazer o *logon* ou conectar-se através dessa rede à Internet, podendo monitorar o tráfego da rede e até violar suas chaves de criptografia WEP.

6.1.6. *Warchalking*

A partir da utilização de técnicas de *wardriving*, o atacante identifica os sinais de redes acessíveis e as identifica através da pichação de muros e calçadas com símbolos próprios numa tentativa de mantê-las em segredo.

A Figura 10 apresenta esses símbolos, que tem o seguinte significado:

- O símbolo com dois semicírculos, um de costas para o outro, significa uma rede acessível, ou seja, “aberta”;
- O símbolo fechado significa que, no local onde foi desenhado, encontra-se uma rede fechada;
- O terceiro símbolo, um círculo com um W dentro, significa que a rede utiliza criptografia WEP. O SSID encontra-se na arte superior e a largura da banda é mostrada abaixo dele.

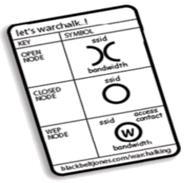

Figura 10. Símbolos de Warchalking

6.2. Ferramenta de monitoramento e mapeamento

Uma das primeiras ferramentas disponíveis para o monitoramento e mapeamento de redes sem fio em ambiente Windows foi o Netstumbler que possui características úteis como, permitir a integração com equipamentos de GPS (*Global Positioning System*) e, desta maneira, obter um mapa preciso de APs identificados. Esta ferramenta está sendo sempre atualizada com os padrões da tecnologia e aceita uma grande quantidade de dispositivos de rede. Por meio dela podemos identificar as rede, seus nomes, endereços MAC e outras informações como nível de sinal de cada rede encontrada. (Figura 11)

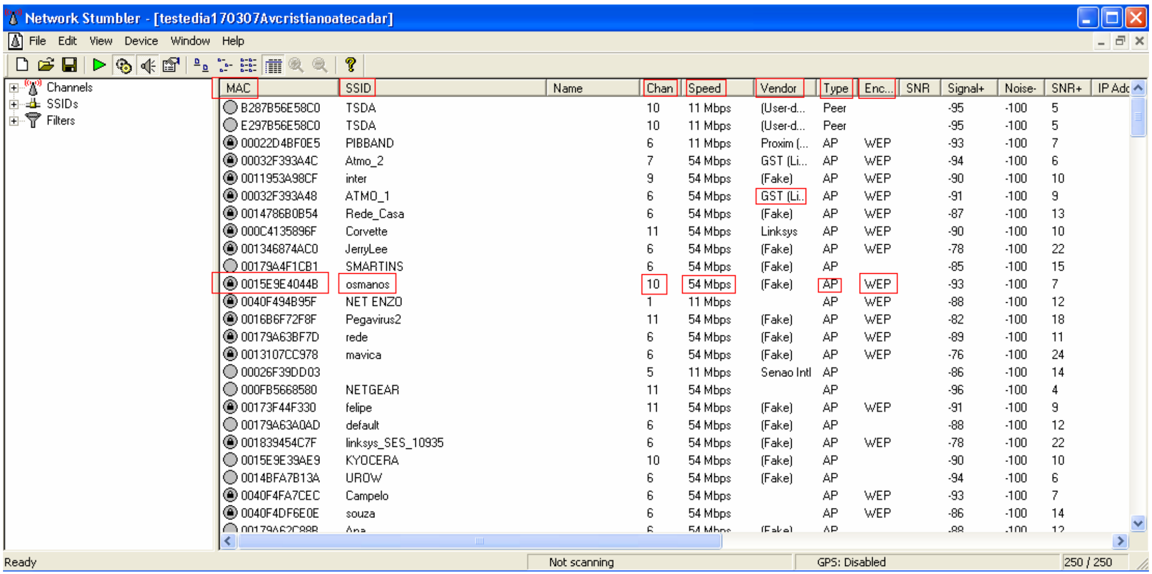

Figura 11. Netstumbler em ação

Na figura 11 é demonstrado o Netstumbler em ação, mostrando de forma bem simples o MAC do AP, o seu SSID, em qual canal se encontra este dispositivo, qual a velocidade de transmissão máxima, em alguns casos, dependendo da versão é mostrado o fabricante do AP e também qual o sistema de criptografia está sendo utilizado. Esta varredura foi efetuado em Belo Horizonte no dia 17/03/2007 da Av. Cristiano Machado à Av. Cadar onde foi detectado 238 APs e 11 host com 158 APs com protocolo WEP habilitado e 92 sem nenhum protocolo de segurança e três APs com SSID *default*.

Uma das funcionalidades exclusivas do Netstumbler é a capacidade de continuar uma análise salva anteriormente, o que permite adicionar informações acerca de redes já catalogadas e paralelamente detectarem novas formando um só conteúdo. Em contrapartida, apresenta limitações como não permitir captura de tráfego e não possuir métodos para quebra de chaves.

6.3. Ferramenta de escuta e quebra

Tecnicamente falando, sempre é possível obter informações sobre uma rede caso o tráfego passe em claro, ou seja, quando não há mecanismo de criptografia envolvido. Essa afirmação se aplica tanto a redes cabeadas como em redes sem fio, visto que as informações estão, literalmente, no ar para quem quiser capturá-las.

Neste trabalho foram utilizadas duas ferramentas que promovem a escuta e quebra de mecanismo de criptografia, o Ethereal e o CommView for WiFi.

O Ethereal é uma das mais completas ferramentas, tendo como característica principal a possibilidade de remontar uma sessão. O conceito de sessão diz respeito a pacotes relacionados entre si, com marcas de início, meio e fim bem definidos. O Ethereal possui todas as principais funcionalidades presentes em ferramentas que usam LibPcap, tais como seleção de tráfego por campos dos cabeçalhos (IP, TCP etc.), origem, destino, tipo de protocolo, porta, entre muitas outras possibilidades, e também grava e lê arquivos no formato *pcap* para manipulação posterior. Foi uma das primeiras ferramentas desta categoria a tratar pacotes específicos de redes sem fio e, sem dúvida, trata-se de uma ferramenta com enorme facilidade de evolução, capacidade de incorporar novas funcionalidades e deve, certamente, fazer parte da lista de ferramentas indispensáveis ao administradores de redes, seja ela com ou sem fio. (Figura 12)

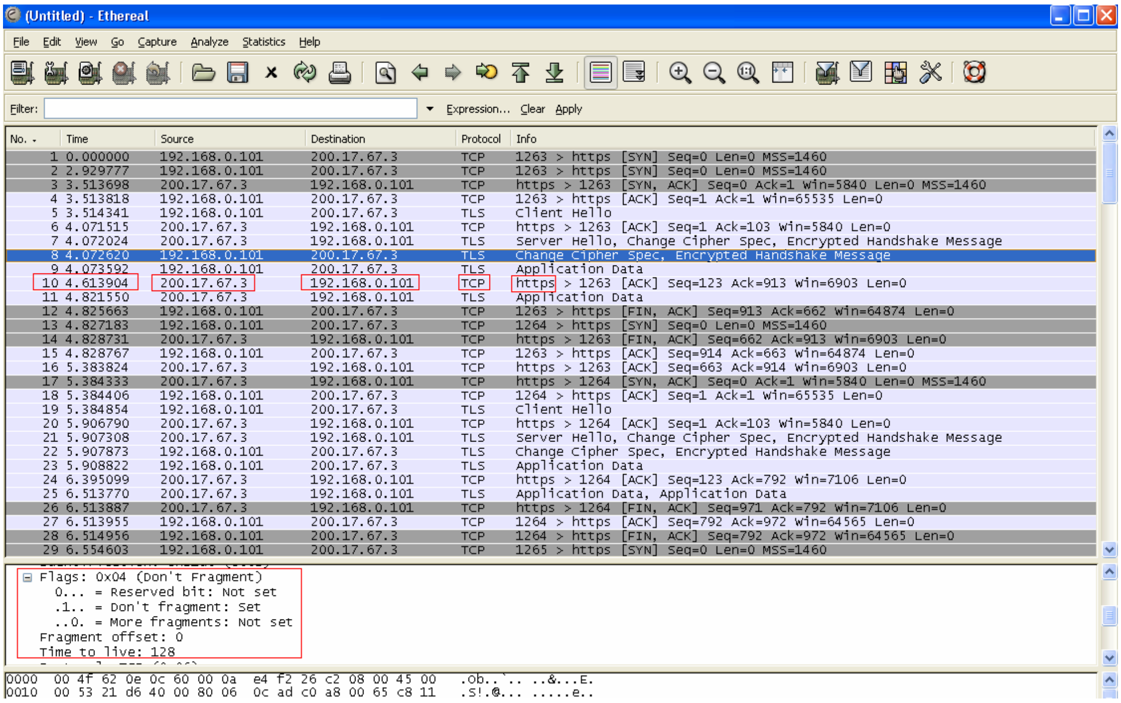

Figura 12. Ethereal em ação

Na figura 12 é demonstrado o Ethereal em ação mostrando o envio de um pacote ao IP 192.168.0.101 pelo IP 200.17.67.3 solicitando através de um https a senha de acesso ao *WEB MAIL*. Veja abaixo que os fragmentos destes pacotes são livremente mostrados.

Outro software extremamente útil é o CommView for WiFi que foi desenvolvida para capturar e analisar pacotes de informação para rede *wireless* 802.11a/b/g. Reúne informações do adaptador *wireless* e decodifica as informações analisadas. Além disso, é possível ver a lista de conexões de rede, estatísticas de IP, e examinar pacotes individuais. Os pacotes podem ser desencriptados utilizando chaves definidas pelo usuário e são decodificados em uma camada inferior. (Figura 13)

Na figura 13 é demonstrado o CommView em ação mostrando um dado criptografado que aparentemente não pode ser quebrado por completo mas é demonstrado logo abaixo parte do vetor IV utilizada na criptografia. Este software depende de um ataque ao meio onde é necessário um grande número de pacotes para a quebra da chave.

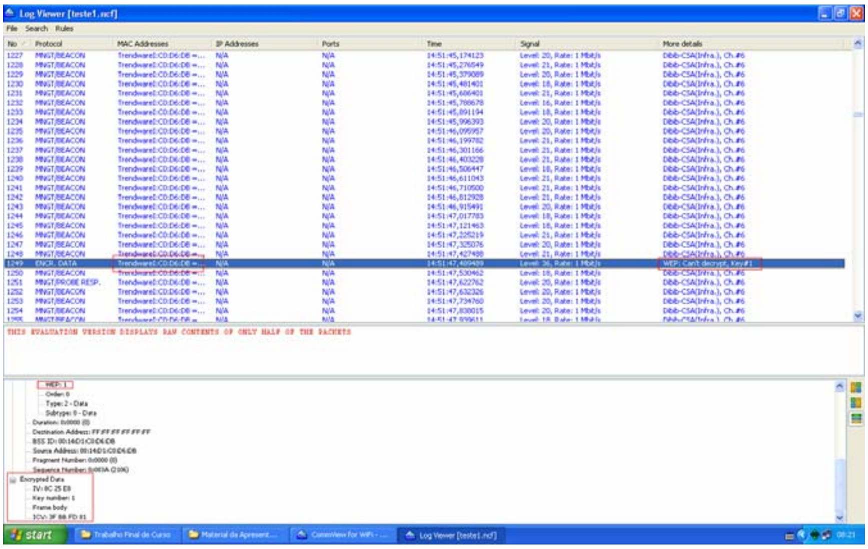

Figura 13. CommView for WiFi em ação

7. Métodos de defesa

Nesta seção, várias técnicas de proteção e configuração para aumentar a segurança nas redes *wi-fi* serão abordadas. Várias delas isoladamente não proporcionam um nível de segurança adequada, portanto devem ser combinadas para que se tornem realmente efetivas.

7.1 Configurações do AP

O acesso ao AP é um ponto crítico da infra-estrutura de um ambiente de rede. Citaremos a seguir as ações para cada caso:

- **defesa do equipamento** -> critérios de acesso físico devem ser estabelecidos no sentido de garantir a segurança e privacidade dos clientes e proteger a rede contra acesso indevido;
- **desabilitar a difusão do envio de ESSID** -> esta configuração procura dificultar ações maliciosas escondendo (ou tentando esconder) o nome da rede. Este ocultamento é uma ação típica denominada “segurança por obscuridade”;
- **modificar o nome ESSID padrão** -> também chamada de “segurança por obscuridade”, é uma medida eficaz para ao menos retardar um ataque em curso e promover as contramedidas necessárias;
- **substituir o endereço MAC** -> essa mudança no AP, quando realizada no momento da instalação, evita a identificação imediata do fabricante por parte de um possível atacante;
- **desabilitar acesso ao AP via rede sem fio** -> é uma boa prática desabilitar a opção de acesso ao AP via rede sem fio, para evitar que os pacotes com usuário e senha sejam capturados por um possível atacante;
- **ignorar clientes que enviam SSID igual a “ANY”** -> um cliente que busca qualquer AP pode ser um atacante tentando explorar o ambiente. Desativar esta possibilidade é uma prática eficaz;
- **geração de chaves** -> evite utilizar chaves simples como palavras do dicionário. Uma ferramenta bastante interessante para a geração de chaves mais difíceis de serem atacadas é a ABC Gerador de Chaves para o Windows.
- **utilizar APs com AES** -> utilize APs que possuem suporte a criptografia de dados via AES.

7.2 Configurações do Cliente

A defesa dos clientes tem duas principais vertentes a serem consideradas, uma que diz respeito à inviolabilidade de comunicação, dados e equipamentos do usuário e outra cuja preocupação é quando ao acesso indevido às configurações de segurança da rede, ou seja, evitar que um ataque bem sucedido ao equipamento do usuário revele chaves e outras informações que possibilitem, ao atacante, acesso à rede com as credenciais capturadas da máquina cliente.

Quanto ao equipamento em si, caso ocorra o roubo, todas as chaves devem ser alteradas para garantir a segurança. Quanto à comunicação, um mecanismo chamado de PSPF (*Publicly Secure Packet Forwarding*), que bloqueia o acesso de um cliente a outros ligados ao mesmo AP deve ser considerado, pois impede o ataque direto de um usuário contra o outro.

8. Considerações Finais

Este artigo trata do estudo de protocolos e de suas vulnerabilidade diante do comportamento ofensivo às redes sem fio e ao estudo das ferramentas de uso malicioso. Foi necessário um estudo em diversas áreas o que possibilitou um grande aprendizado. A insegurança mostrada nas seções anteriores existe e deve ser tratada pelos administradores de rede como prioridade. A utilização de protocolos mais robustos devem ser aplicadas, pois uma grande variedade de software são criados e modificados para testar esta “segurança”, haja visto que todas as ferramentas utilizadas neste artigo foram encontradas com facilidade na rede mundial de computadores.

Quanto às análises elas foram confirmativas, pois as vulnerabilidades já são conhecidas e testadas em laboratório.

Para trabalhos futuros sugiro uma análise do algorítmo AES e também uma análise utilizando a plataforma Linux.

Referências Bibliográficas

[1] RUFINO, Nelson Murilo de O., “*Segurança em Redes sem Fio*” , São Paulo: Novatec Editora Ltda, 2005.

[2] SOARES, Luiz Fernando G., “Redes de Computadores: das LANs, MANs e WANs às redes ATM / Luiz Fernando Gomes Soares, Guido Lemos e Sérgio Colcher. – 2. ed. Ver e ampliada. – Rio de Janeiro: Campus, 1995.

[3] Teleco – Informações em Telecomunicações – http://www.teleco.com.br (verificado em 28/04/2007), 2007.

[4] Boa Dica – http://www.boadica.com.br (verificado em 11/06/2007), 2007.

[5] Woo, Thomas Y.C e Lam, Simon S., “Authentication for Distributed Systems. IEEE Computer, Janeiro 92.

[6] PERES, André; WEBER, Raul Fernando - Considerações sobre Segurança em redes sem fio. Faculdade de Informática, Universidade Luterana do Brasil, Canoas, Rio Grande do Sul.

[7] ROSA, Rafael Antônio da Silva; FALEIROS, Antônio Cândido - Análise do Algoritmo vencedor do AES: O Rijndael, Instituto Tecnológico de Aeronáutica, São José dos Campos, São Paulo.

[8] TEWS, Erik; WEINMANN, Ralf-Philipp; PYSHKIN, Andrei - Breaking 104 bit WEP in less than 60 seconds, FB Informatik Hochschulstrasse, Darmstadt, Germany.