Análise Crítica da Implementação da Cifra RC4 no Protocolo WEP

Palma, S.M. *Member, IEEE* and A. Pereira

***Abstract*— It is nine years since the first serious problems of the Protocol WEP (Wired Equivalent Privacy) were identified by cryptanalysts. This security protocol for wireless networks using the algorithm of RC4 stream cipher, and these problems are due to poor implementation of such a protocol. In this paper we analyze the mistakes made in the design of WEP that prevent you from achieve your goal. For this we introduce the operation, and major vulnerabilities of the RC4 stream cipher and its impacts on security of WEP. In order to contextualize the application of cryptographic systems in real security systems, also introduce notions of IEEE 802.11 wireless networking and security best practices that should be taken to secure environments tor before the vulnerable WEP.**

Keywords— WEP, RC4, IEEE 802.11, wireless networkting, Wireless Security, cryptanalysts, vulnerabilities.

I. Introdução

O uso de tecnologias de redes de computadores sem fio IEEE 802.11, também conhecidas como redes wireless, redes Wi-Fi (Wireless Fidelity) ou simplemente WLANs (Wireless Local Area Network) vem ser tonando cada vez mais popular nos últimos anos. Observa-se atualmente uma grande presença deste tipo de rede, seja em ambientes domésticos, instituições, universidades, empresas ou outros.

Neste contexto de grande utilização, a preocupação com a segurança da informação destes sistemas se torna fundamental. É muito importante, portanto, que estas redes atendam aos seguintes atributos:

- Confidencialidade: limita o acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- Integridade: garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição);
- Disponibilidade: garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

O protocolo WEP (Wired Equivalent Privacy), definido pelo padrão IEEE 802.11b, visa contemplar os dois primeiros atributos citados acima: confidencialidade e integridade. Uma vez definido, em 1999, este protocolo passou a ser largamente utilizado em redes sem fio e logo se tornou um padrão de fato. Em 2001, contudo, Fluhrer et al. [1] descobriram fraquezas no algoritmo RC4 (usado pelo WEP para prover criptografia) e afirmaram que estas poderiam tornar o WEP vulnerável, sem contudo implementar um ataque. No ano seguinte, (2002) Rubin et al. [2] implementaram tal ataque e colocaram em cheque a segurança do protocolo WEP. Na mesma época outros autores implementaram o ataques semelhantes e chegaram ao mesmo resultado. Nos anos seguintes surgiram ainda outros ataques ao protocolo, tais como [3], [4], [5] e [6].

Este trabalho é dividido da seguinte forma: na Seção 2 é apresentado os conceitos básicos do funcionamento das redes sem fio. Na Seção 3 é apresentada a Cifra RC4 e as fraquezas descobertas em [1]. Na Seção 4 são expostos os aspectos que tornam a implementação do WEP insegura. Algumas considerações finais serão apresentadas na Seção V.

II. Redes Sem Fio

As redes sem fio IEEE 802.11, que também são conhecidas como redes Wi-Fi (Wireless Fidelity) ou wireless, foram uma das grandes novidades tecnológicas dos últimos anos. Atualmente, são o padrão de facto em conectividade sem fio para redes locais. Como prova desse sucesso pode-se citar o crescente número de redes instaladas e o fato de a maioria dos computadores portáteis novos já saírem de fábrica equipados com interfaces IEEE 802.11 [7].

Uma rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos (sejam eles telefônicos, coaxiais ou ópticos), por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho.

Sua classificação é baseada na área de abrangência: redes pessoais ou curta distância (WPAN - Wireless Personal Area Network), redes locais (WLAN - Wireless Local Area Network), redes metropolitanas (WMAN - Wireless Metropolitan Area Network) e redes geograficamente distribuídas ou de longa distância (WWAN - Wireless Wide Area Network) [8].

A arquitetura de uma rede sem-fio é composta pelos seguintes elementos:

- Ponto de acesso (AP -Access point): elemento centralizador responsável pela comunicação entre os dispositivos móveis da rede. Em geral este se conecta a uma rede cabeada, caso no qual atua também como um ponto de acesso para outra rede.
- Dispositivos Móveis: são aqueles que usam a radio frequência para manter uma comunicação com outros dispositivos sem fio.

Uma rede sem-fio pode ser montada usando uma das seguintes topologias:

- Ad Hoc: rede sem nenhum elemento centralizador. Nesta topologia os nós da rede comunicam-se diretamente entre si ou são roteados por outros nós para chegar ao seu destino. Esta topologia está ilustrada na Figura 1.
- Infra-estruturada: rede onde um elemento centralizador (AP) é responsável pela comunicação entre os nós

clientes. Esta topologia está ilustrada na Figura 2.

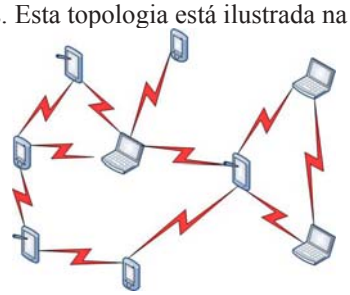

Figura 1. Rede Ad Hoc IEEE 802.-11 [1].

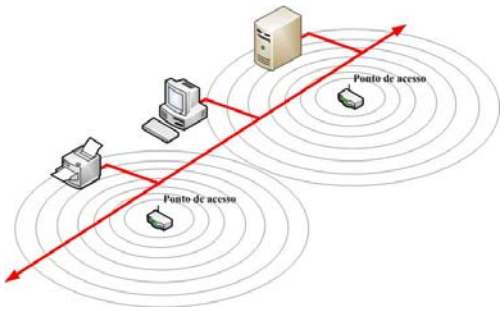

Figura 2. Configuração por Infra-estrutura da LAN 802.11 [2].

A. *IEEE 802.11*

O padrão IEEE 802.11 descreve os protocolos da camada de enlace sem fio para redes Wi-Fi. Trata-se de um conjunto de padrões descritos e algumas em projeto [9].

Para o presente trabalho, estamos particularmente interessados nos seguintes protocolos:

- **IEEE 802.11b:** desenvolvido pelo IEEE LAN/MAN Standards Committee, al canҫa uma velocidade de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes não padronizados. Opera na frequência de 2.4 GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz, mesma frequência utilizada por telefones sem-fio, fornos de micro-ondas e dispositivos Bluetooth. Os aspectos positivos são o baixo preço dos seus dispositivos e o uso de uma faixa de frequências não licenciada (de uso gratuito). O 802.11b é amplamente utilizado por provedores de Internet sem fio. Este padrão o foi o primeiro a introduzio o protocolo de segurança Wired Equivalent Privacy (WEP), com o objetivo de prover confidencialidade e integridade aos dados transmitidos através da rede [7]
- **IEEE 802.11i:2004:** Criado para definir e aperfeiçoar os serviços de segurança de redes sem fio além do protocolo WEP. Mantém o protocolo WEP para fins de compatibilidade com equipamentos mais antigos, porém alerta para o fato de que tal protocolo está defasado e não deve mais ser utilizado.

O principal benefício do projeto do padrão 802.11i é sua extensibilidade. Caso uma falha seja descoberta em alguma técnica de criptografia utilizada, o padrão permite facilmente a adição de uma nova técnica sem a substituição do hardware [10].

B. *Protocolos de segurança em redes sem-fio*

Redes sem-fio IEEE 802.11 dispõem de diferentes protocolos de segurança. Abaixo estão relacionados os três mais importantes:

- WEP (Wired Equivalent Privacy): foi o primeiro protocolo de segurança adotado e ainda é muito utilizado nos dias atuais. Utiliza a cifra RC4 com chave compartilhada de 40 ou 104 bits para criptografar os pacotes, a fim de garantir confidencialidade aos dados de cada usuário. Além disso, utiliza o algorítmo CRC-32 (uma função de detecção e recuperação de erros de transmissão) com objetivo de conferir integridade aos pacotes [11].
- WPA (Wi-Fi Protected Access): desenvolvido para corrigir as fraquezas do Sistema WEP, também chamado de TKIP (Temporal Key Integrity Protocol). O WPA surgiu em 2003, como fruto de um esforço conjunto de membros da Wi-Fi Aliance e de membros do IEEE, empenhados em aumentar o nível de segurança das redes 802.11, combatendo algumas das vulnerabilidades do WEP. [12]. As principais diferências com relação ao WEP são as seguintes:
  - ❖ Troca dinâmica de chaves (TKIP).
  - ❖ Uso de vetores de inicialição (IV) maiores que no Protocolo WEP.
  - ❖ Melhoria na estratégia de integridade da informação.
- WPA2 (Wi-Fi Protected Access 2): é o protocolo de segurança atual em redes 802.11 e é certificado pelo padrão IEEE 802.11i. Usa o algoritmo AES (Advanced Encription Standard) para cifrar os pacotes da camada de enlace.

III. CIFRA RC4

Cifras de fluxo são cifras que criptografam o texto claro (*Plaintext*) de maneira contínua, bit a bit, byte a byte ou unidades dados maiores por vez, conforme decisão de projeto [13]. A Figura 3 representa um diagrama representativo da estrutura de cifra de fluxo, em esta estrutura a chave é ingressada para um Gerador Pseudo-aleatórios por byte que produz um fluxo de 8 bits que são aparentemente aleatórios. A saída do gerador (*keystream*) é combinada byte por byte com o Plaintext utilizando a operação exclusiva XOR e obtendo o fluxo de byte de Texto Cifrado C.

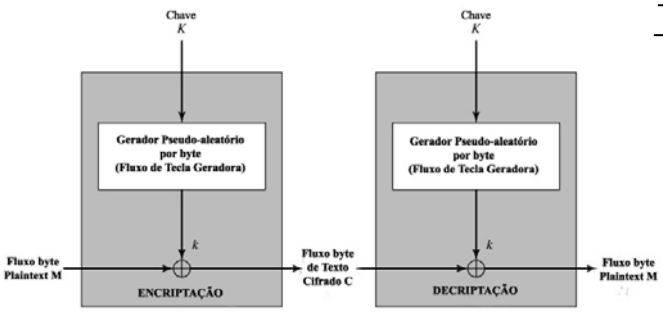

Figura 3. Diagrama de cifras de fluxo [13].

O Algoritmo RC4 é uma cifra de fluxo com tamanho de chave variado e orientada a byte. Foi desenvolvida em 1987 por Ron Rivest para a empresa RSA Security[1]. Esta cifra foi mantida como segredo comercial por esta empresa, e se tornou muito utilizada em diversas aplicações comerciais, tais como *Internet Explorer, Netscape, Adobe Acrobat*, dentre outros. Dentre os produtos que usam atualmente a cifra RC4 pode-se citar os protocolos SSL/TLS (Secure Sockets Layer / Transport Layer Security), WEP (Wired Equivalent Privacy) e WPA[2] (WiFi Protected Access).

Dentre os fatores determinantes para o sucesso do RC4 pode-se citar a simplicidade do código e o alto desempenho das operações de criptografia e descriptografia.

Em 1994, contudo, o algoritmo do RC4 foi publicado anônimamente em uma lista de discussão sobre criptografia, a Cipherpunks. A partir deste momento começaram a surgir diversos ataques criptoanáliticos sobre o algoritmo e sobre protocolos criptográficos que o utilizam. Na Seção III.B serão apresentados alguns destes ataques.

A. Funcionamento

O algoritmo RC4 é dividido em duas partes: KSA (The Key Scheduling Algorithm) e PRGA (Pseudo-Random Generation Algorithm).

O KSA consiste em inicializar um vetor S de 256 byes como uma permutação de todos os números de 8 bits (0 a 255). Essa permutação é condicionada a chave K utilizada no algoritmo. O tamanho da chave pode variar de 1 a 256 bytes [13], porém os valores de 40 a 256 são os mais comumente utilizados [1]. O Algoritmo 1 apresenta o pseudo-código desta etapa.

```
Algorithm 1 KSA(K)
  for i = 0 ... N − 1 do
    S[i] = i
    T [i] = K[i mod keylen]
  end for
  j=0
  for i = 0 ... N − 1 do
    j = (j + S[i] + T [i]) mod 256
    swap(S[i], S[j])
  end for
```

```
Algorithm 2 PRGA(K)
  i=0
  j=0
  while true do
    i = (i + 1) mod 256
    j = (j + S[i]) mod 256
    swap(S[i], S[j])
    t = (S[i] + S[j]) mod 256
    k = S[t]
  end while
```

A segunda etapa do algoritmo, PRGA, consiste em gerar um fluxo de bytes comtendo números pseudo aleatórios[3], que será utilizado para fazer a operação XOR com o fluxo de bytes do texto claro para produzir o texto cifrado, conforme ilustrado na Figura 3. O Algoritmo 2 apresenta o pseudo código desta etapa e a Figura 4 apresenta uma visão geral do processo.

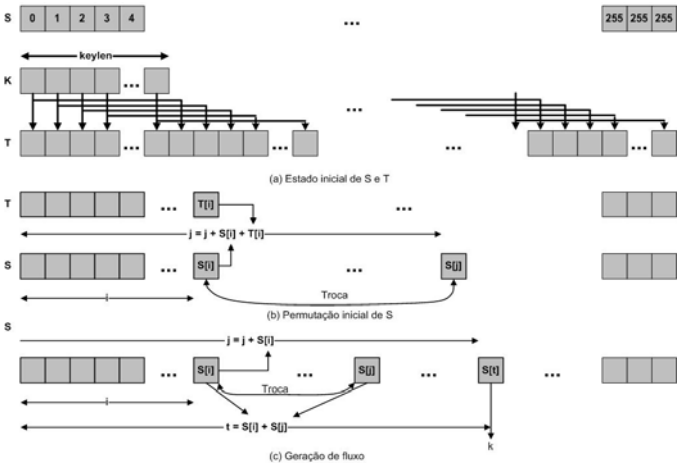

Figura 4. Estrutura do RC4 [13].

Em aplicações reais, costuma-se utilizar chaves de seção, de forma que uma mesma chave não seja utilizada para criptografar sequencias muito longas de bytes (keylen). Em protocolos de rede, por exemplo, pode se utilizar uma chave diferente por cada pacote. Em particular, existe um modo de operação do RC4 que consiste em compor a chave. Neste modo de operação a chave que será entregue ao algoritmo RC4 é uma concatenação da chave K com um vetor de inicialização (Initialization Vector - IV). Na Seção III.B será mostrado que este modo de operação pode ser explorado por um atacante na tentativa de recuperar a chave K. Apresenta-se ainda na Seção IV.A que este modo de operação é explorado na tentativa de recuperar a chave do protocolo WEP.

B. Vulnerabilidades

Desde a divulgação pública do algoritmo na lista Cipherpunks,em 1994, começaram a surgir ataques criptoanalíticos contra o RC4, porém, o primeiro ataque significativo surgiu em 2001, quando Fluhrer, Martin e Shamir

[1] http://www.rsa.com/

[2] A versão 2 deste protocolo, o WPA2, não utiliza a cifra RC4.

[3] Um fluxo pseudo-aleatório é aquele que é imprevisível sem o conhecimento da chave de entrada [13].

demonstraram [1][4] que o protocolo RC4 possuia vulnerabilidades em seu algoritmo de agendamento de chaves (KSA) e que seriam possíveis ataques práticos a protocolos de segurança que utilizassem esta cifra, tal como o WEP, sem contudo implementar tais ataques. Em 2002 [2] implementou o ataque proposto por Shamir e colocou em cheque a segurança do protocolo WEP. Na mesma época outros autores implementaram o ataque de Shamir e chegaram ao mesmo resultado.

Nos anos seguintes, surgiram mais ataques práticos sobre contra a cifra RC4. Em 2004 um cracker usando o pseudônimo de KoreK publicou em uma lista de discussão[5] 16 correlações entre os l primeiros bytes da chave do RC4 e os dois primeiros bytes do fluxo pseudo-aleatório gerado pela cifra RC4. Em 2006 Adreas Klein publicou dois novos ataques. O primeiro demonstrando uma nova correlação entre os primeiros bytes da sequência pseudo-aleatória e que não mais requer a existência de uma forma especial do vetor S (tais como as condições resolvidas de ataque FMS), o que permitiu uma grande diminuição no número de IV necessários para um ataque efetivo. O segundo ataque dispensa a necessidade dos primeiros bytes do fluxo pseudo-aleatório. Este ataque pode ser particulamente útil em aplicações que descartam os primeiros 256 bytes do fluxo pseudo-aleatório (conforme recomendado em [14]), porém não é muito útil no contexto do WEP, uma vez que, em tal protocolo, dispõe-se dos primeros bytes do fluxo. Nota-se que este segundo ataque possui uma complexidade computacional maior que os ataques anteriores.

Data a sua importância prática e histórica, detalhamos um pouco mais o funcionamento do ataque FSM abaixo.

Ataque de FMS Em [1], Fluhrer et. al demonstraram que a função KSA(K) (apresentada no Algoritmo 1) do RC4 é vulnerável, possuindo duas fraquezas significativas:

- Existência de uma larga classe de chaves consideradas fracas, onde uma pequena porção dos bits da chave determinam um grande número de bits da pertumação inicial S.
- Fraqueza do Vetor e inicialização (IV weakness): se um atacante conhecer parte da chave (IV), ele é capaz de rederivar a parte secreta da chave analizando o byte inicial do fluxo de byte de saída do RC4 com (relativo) pouco esforço.

A segunda fraqueza citada acima (Fraquesa do IV) é particularmente interessante neste trabalho pois pode ser explorada em um ataque real ao protolo WEP. Segundo FMS, o primeiro byte do fluxo pseudo-aleatorio de bytes depende apenas de três valores da permutação inicial S (saida do KSA), sendo igual ao valor Z da Figura 5.

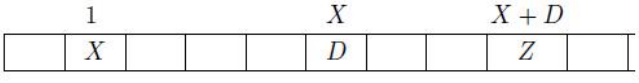

Figura 5. Permutação inicial S (Saída do Algoritmo KSA) [1].

Alguns IV colocam o algoritmo KSA em um estado que permite a obtenção de informação da chave, este estado é chamando por FMS de resolved condition (condição resolvida). Uma condição resolvida é caracterizada quando em algum momento do KSA temos um valor i >= 1, X, Y onde X é Si [1] e Y é X + S i[X] (ou seja, X + D). Quando tem-se um condição resolvida, tem-se uma probabilidade de aproximadamente 5% de que os valores S[1], S[X] e S[Y] não participarão de mais nenhuma troca futura. Nesse caso o valor do primeiro byte do fluxo pseudo-aleatório será determinado pelos valores Si[1], Si[X] e Si[Y]. Nos outros 95% dos casos a condição resolvida é perdida e nada pode-se dizer sobre o primeiro byte do fluxo.

A equação para este primeiro byte nestes 5% de casos resolvidos será S[Y] (ou S[S[1] + S[S[1]]]). Nestes casos, portanto, obtemos alguma informação da chave. Se olharmos para um grande número de casos resolvidos encontraremos uma direção para os bytes corretos da chave[5].

C. *Implementações seguras*

Apesar das vulnerabilidades apresentadas na Seção anterior, o protocolo RC4 ainda pode ser considerado seguro se utilizado de maneira correta, através de uma implementação segura. Um bom exemplo de que isto é possível é o TLS [15] (Transport Layer Security).

A razão para a segurança do TLS[6] é que ele pré-processa a chave criptográfica e o IV através do uso de funções de hash seguras (MD5, SHA ou outras), resutando em chaves completamente diferentes e não relacionadas entre as seções de comunicação.

Uma recomendação para o uso seguro do RC4 (feita pela criadora do protocolo, a empresa RSA Security) é de que os primeiros 256 bytes do fluxo pseudo-aleatório gerado pelo RC4 devem ser descartados, como forma de evitar as fraquesas do algoritmo KSA. Segundo o documento [14], os ataques apresentados contra a cifra RC4 atuam apenas sobre o algoritmo KSA, e poderiam ser "remediados" (através de técnicas de hashing, tal como faz o TLS), mas o coração do protolo, o gerador de fluxo pseudo-aleatórios, continua seguro e eficiente, e não é vulnerável, atualmente, a nenhum tipo de ataque. Por essa razão "o RC4 provavelmente continuará a ser o algoritmo de escolha de muitas aplicações".

Segundo a RSA Security Inc, aplicações que utilizam o RC4 devem ser revisadas para ver se seguem as recomendações acima, e projetistas de protocolos que utilizem o RC4 não devem se preocupar com novos ataques enquanto seguirem estas recomendações.

IV. PROTOCOLO WEP

Conforme introduzido anteriormente, o protocolo WEP é um protocolo de segurança que foi introduzido no padrão de redes sem fio 802.11a e que ainda é mantido (por questões de compatibilidade) no padrão 802.11i. Seu uso, contudo, não é recomendado uma vez que é publicamente reconhecido que o protocolo não atinge os seus objetivos, os quais são descritos em [12] e são autenticação, confidencialidade e integridade.

Para suportar o primeiro objetivo, o WEP dispõe de dois

[4] Neste artigo o trabalho de Fluhrer, Martin e Shamir será referenciado como Ataque(s) FMS.

[5] Seção 7.1 de [1] mostra os passos detalhados para obtenção de informação da chave.

[6] RFC 4246 especifica que o protocolo TLS deve utilizar um algoritmo de criptografia simétrica, podendo ser o RC4, DES, ou outros.

métodos de autenticação [11]: Sistema Aberto e Chave Compartilhada:

- Sistema Aberto O cliente não tem que se identificar com o Ponto de Aceso durante a autenticação. Assim, qualquer cliente, independente da chave WEP, pode solicitar acesso a rede. Depois da autenticação e a associação, o sistema WEP pode ser usado para cifrar os pacotes de dados. A segurança reside no fato de que, se o cliente não conhecer a chave ele não será capaz de enviar e receber as mensagens da rede (que são cifradas).
- Chave compartilhada Este método divide-se em quatro etapas (Figura 6):
    - o A estação cliente envia um pedido de autenticação ao ponto de acesso.
    - o O ponto de acesso responde com um texto modelo.
    - o O cliente tem que cifrar o texto modelo usando a chave WEP conhecida, e reenviá-lo ao ponto de acesso.
    - o O ponto de acesso decifra o texto codificado e o compara com o texto modelo que foi enviado. Se a comparação for verdadeira, o ponto de aceso envia uma confirmação de autenticação.

A confidencialidade do protolo é obtida através da criptografia. Para isso utilizase a cifra RC4 com chaves de tamanho 40 ou 104 bits combinadas com um vetor de inicialização (Initialization Vector - IV) de 24 bits, resultando portanto, em um tamanho de chave efetiva de 64 ou 128 bits respectivamente.

O algotirmo WEP funciona conformes os passos listados abaixo. A Figura 7 ilustra tal algoritmo.

1. Calcula-se o valor de verificação de integridade (Integrity Check Value - ICV) do texto claro usando o algorítmo CRC-32 (Cyclic redundancy check) e o concatena com o texto claro.
2. Gera-se uma chave de pacote contatenando-se um IV selecionado com a chave secreta.
3. A chave de pacote é utilizada do Gerador de números Pseudo-aleatórios (PseudoRandom Number Generator - PRNG), o qual gera um fluxo de bytes pseudo-aleatórios. Note que o PRNG é na verdade a cifra RC4.
4. A sequencia pseudo-aleatória e o texto claro concatenado com o ICV passam por uma função XOR, resultando no texto criptografado
5. Transmite-se IV conjuntamente com o texto criptografado.

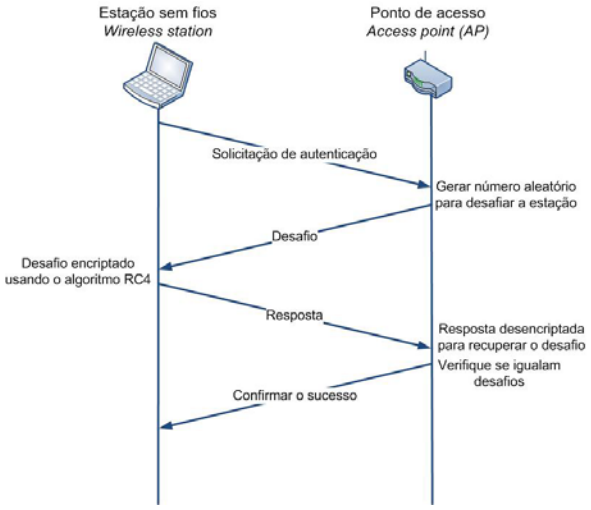

Figura 6. Autenticação por chave compartilhada.

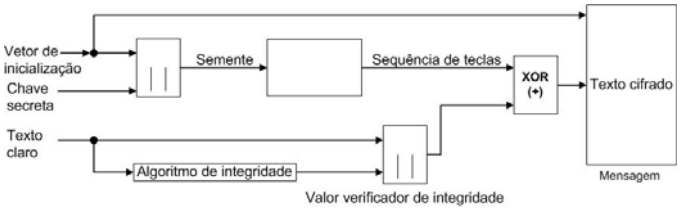

Figura 7. Funcionamento do Protocolo WEP [16].

O receptor deve gerar o mesmo fluxo de bytes pseudo-aleatórios utilizando a chave conhecida e o IV recebido em texto claro junto com a mensagem cifrada e então fazer uma nova operação XOR do fluxo de bytes com o texto cifrado para recuperar o texto claro.

A. Vulnerabilidades

O protocolo WEP possui uma série de vulnerabilidades que o tornaram incapaz de atingir os seus objetivos de confidencialidade e integridade de mensagens, por isso o seu uso não é mais recomendado. Contudo, ainda observa-se um grande número de redes rodando este protocolo. Em [16] são apresentados os principais problemas do protocolo WEP.

Um destes problemas é o fato do IV ser muito curto (24 bytes) e chave permanecer estática, o que resulta em fluxos pseudo-aleatórios da cifra RC4 parecidos e até mesmo repetidos. Se um atacante coletar vários quadros com o mesmo IV, ele pode recuperar valores compartilhados entre estes quadros, tais como o fluxo pseudo-aleatório ou até mesmo a chave (ataques baseados na propriedade de que o XOR de dois valores criptografados com o mesmo fluxo pseudo-aleatório cancela o valor do fluxo). Uma vez que o atacante tenha dois textos cifrados que tenham usado o mesmo IV, vários tipos de ataque podem ser aplicados para recuperar-se o texto claro. Em uma rede de 11 Mbps com alto tráfego, o espaço de IVs se esgota em aproximadamente 5 horas [17].

Outro problema importante do protocolo WEP é o seu fraco gerenciamento de chaves. O protocolo definido pelo padrão 802.11 não como a distribuição de chaves deve ser feita. Note que sem uma gerência apropiada das chaves, as redes tendem a utilizar chaves fracas por um longo período. É uma tarefa grande e tediosa mudar a chave de uma rede WEP, uma vez

que requer a reconfiguração manual de cada nó da rede, por isso os administradores tendem a não fazê-la, resultando no uso da mesma chave por um período de meses, ou mesmo anos. Note que este problema favorece o cenário de um atacante que deseje explorar o problema do espaço de IVs ser curto, citado anteriormente.

Contudo, o mais sério problema deste protocolo reside na má implementação da cifra RC4, a qual permite que o protocolo WEP seja vulnerável aos ataques apresentados na Seção III.B, os quais permitem a recuperação da chave, significando que o protocolo pode ser totalmente quebrado.

Estes três problemas citados mostram que este protocolo não atende o seu requisito de confidencialidade. Porém, nada foi dito sobre a integridade que o WEP afirma oferecer. Conforme explicado na Seção anterior, o WEP oferece um campo chamado ICV (Integrity Check Value - Valor de Checagem de Integridade), o qual é usado para que o receptor da mensagem possa conferir a sua integridate. Este campo é computado usando o protocolo CRC-32 (Cyclic redundancy check - Verificação cíclica de redundância), um algoritmo linear muito utilizado para detecção e correção de erro em transmissões de dados sob canais ruidosos. Trata-se de um excelente algorítmo para detecção e correção de erros, mas é uma péssima escolha para uma função de algoritmos de hash: por ser uma função linear, um atacante pode facilmente alterar bits da mensagem criptografada e calcular o novo valor do campo ICV.

B. Ataque prático

Com o objetivo de comprovar a fraqueza do WEP, montamos um ataque prático contra uma rede 802.11 rodando WEP de 104 bits.

Escolhendo os equipamentos Foi utilizado um roteador wireless Linksys WRTP54G (AP), com firmware Versão 3.1.17, um computador Dell Studio 1737 (D1) com sistema operacional Windows Vista Professional e um computador Dell Latitude D410 (D2) com sistema operacional GNU/Linux, distribuição Backtrack 3[7].

Montando o ataque O AP foi configurado para utilizar o protocolo WEP com chave de 104 bits e o computador D1 foi configurado como cliente válido. Deixamos, portanto, D1 conectado ao ponto de acesso e gerando tráfego. O tráfego gerado foi um simples download de arquivos grandes na Internet. O computador D2, por sua vez foi configurado para ficar ouvindo o tráfego e, reinjetando pacotes de requisição ARP gerados por D1 na rede como forma de agilizar a obtenção da quantidade de IVs necessária. Note que tratou-se de um ataque ativo, uma vez que o atacante D2 enviou pacotes para a rede. Este ataque poderia, contudo, ter sido passivo, porém isto implicaria em uma demanda de tempo maiorpara a obtenção dos IVs.

Em D2, três ferramentas foram utilizadas: Airodump, Aireplay e Aircrack. Sendo a primeira o sniffer de rede responsável pela captura dos pacotes, a segunda a ferramenta responsável para injeção de requisições ARP na rede e terceira a ferramenta de criptoanálise que roda o ataque PTW [6], o qual consiste em uma combinação dos ataques FMS e KoreK apresentados na Seção III.B e técnicas de força bruta.

O ataque Em primeiro lugar lista-se as redes sem fio disponíveis a fim de obter-se o endereço MAC de AP. Em seguida inicializa-se a ferramenta Airodump em D2 e obtem-se o código MAC do cliente D1. Esta ferramenta escreve todo o tráfego capturado em um arquivo chamado dumpfile. Os comando abaixo são utilizado para estes fins:

```
bt sdb1 # iwlist eth0 scan
bt sdb1 # airodump-ng --channel 7 --bssid 00:18:39:B7:32:77 \\
        -w dumpfile rtap0
```

Uma vez conhecidos os MACs do AP e do cliente “alvo”, e estamos capturando todo o tráfego da rede, inicia-se a parte ativa do ataque: a reinjeção de pacotes ARP do cliente alvo. Para isso configuramos a placa de rede sem fio de D2 com o mesmo endereço MAC de D1 e, em seguina, iniciamos a reinjeção com o comando Aireplay:

```
bt sdb1 # ifconfig eth0 hw ether 00:14:22:FD:C6:AD
bt sdb1 # aireplay-ng --arpreplay -b 00:18:39:B7:32:77 \\
          -h 00:14:22:FD:C6:AD -i rtap0 eth0
```

Por último inicializamos a ferramenta Aircrack, a qual aplica o ataque PTW sobre os pacotes que estão sendo escritos no arquivo dumpfile.

```
bt sdb1 # aircrack-ng -z -b 00:18:39:B7:32:77 dumpfile.cap
```

Resultados Após cerca de cinco minutos de captura de tráfego, tinhamos a nossa disposição 80015 IVs, número suficiente para que a ferramenta Aircrack utilizando o Ataque PTW conseguisse recuperar a chave de 104 bits. Portanto, obtivemos sucesso após cerca de cinco minutos de ataque ativo.

V. 5. CONCLUSÕES

Este trabalho demonstrou um atáque criptoanálitico prático contra a implementação WEP da cifra de Fluxo RC4.

As diversas vulnerabilidades existentes na implementação do protocolo WEP deixam claro que o seu uso deve ser descontinuado. O incremento do tamanho da chave do protocolo WEP não impacta significativamente na sua segurança, uma vez que os ataques práticos contra este algorítmo são criptoanalíticos e não de força bruta.

O uso da Cifra RC4 em ambientes de produção, contudo, ainda é aceitável, uma vez que o núcleo do algoritmo não é vulnerável a nenhum tipo de ataque prático. Nota-se que com uma implementação cuidadosa esta cifra ainda pode ser utilizada de maneira segura, apesar de tais implementações implicarem em perda de desempenho e simplicidade de implementação.

REFERENCIAS

[1] S. Fluhrer, I. Martin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” Lecture Notes in Computer Science, no. Volume 2259/2001, 2001.

[2] A. Stubblefield, J. Ioannidis, and A. Rubin, “Using the Fluhrer, Mantin, and Shamir attack to break WEP,” Proceedings of the 2002 Network and Distributed Systems, 2002.

[3] A. Klein, “Attacks on the RC4 stream cipher,” Designs, Codes and Cryptography, no. Volume 48, Number 3, 2006.

[7] http://www.remote-exploit.org/backtrack.html

[4] E. Tews, R. Weinmann, and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds,” Lecture Notes in Computer Science, no. Volume 4867/2008, 2008.
[5] KoreK, “Next generation of WEP attacks?.” [Online; acessado em 15 de junho de 2009].
[6] E. Tews and M. Beck, “Practical attacks against WEP and WPA,” Proceedings of the second ACM conference on Wireless network, 2009.
[7] IEEE, “International Standard ISO/iec 8802-11: 1999(e) part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.” [On-line; acessado em 10 de junho de 2009].
[8] J. F. Kurose and K. W. Ross, Rede de computadores e a Internet, Uma abordagem top-down. Pearson Addison Wesley, 2006.
[9] IEEE, “Offical IEEE 802.11 Working group Project Timelines.” [Online; acessado em 12 de junho de 2009].
[10] T. e. a. CHOC, “Wireless local area network (wlan) security - the 802.11i solution,” 2004.
[11] A. Internet Security, Applications and Cryptography, “Security of the wep algorithm,” 2001.
[12] M. Borsc and H. Shinde, “Wireless security & privacy,” pp. 424–428, Jan. 2005.
[13] W. Stallings, Criptografia e segurança de redes. Princípios e práticas, ch. 6. Pearson Prentice Hall, 2006.
[14] RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4. [On-line; acessado em 8 de junho de 2009].
[15] T. D. e E. Rescorla, “The Transport Layer Security (TLS) Protocol.” RFC 4346, Apr. 2006.
[16] Zhao and C. Shoniregun, “Critical Review of Unsecured WEP,” pp. 368–374, July, 2007.
[17] e. D. W. N. Borisov, I. Goldberg, “Intercepting mobile comunications: The insecurity of 802.11,” Proceeding of the 7th annual international conference on mobile computing and network, 2001.

Marcelo Invert Palma Salas Possui graduação em Ingenieria de Sistemas - Escuela Militar de Ingenieria (2005). Conhecimentos em SAP R/3 e DBA Oracle 9i. Fundador e Past President do Capítulo Professional IEEE Computer Society - Seção Bolivia. Encargado dos Ramos Estudiantes na Bolivia para o IEEE. Trabalho na "Superintendencia de Telecomunicaciones"na Bolivia, Price Water House Coopers e Antalis Bolivia - GMS Chile. Profesor e Conselho de Departamanto de Sistemas na "Escuela Militar de Ingeniería". Atualmente é bolsista da Universidade Estadual de Campinas. Encarregado de Atividades Estudianties para a IEEE Região 9 Latinoamérica.

André Augusto da Silva Pereira Possui graduação em Engenharia de Computação pela Universidade Federal do Pará (2008). Atualmente é aluno de Mestrado da Universidade Estadual de Campinas (UNICAMP). Tem experiência na área de Ciência da Computação, com ênfase em Administração e Segurança de Sistemas Computacionais.