Considerações sobre Segurança em Redes Sem Fio

André Peres[1], Raul Fernando Weber[2]
[1] ULBRA - Universidade Luterana do Brasil
Faculdade de Informática
peres@ulbra.tche.br
[2] UFRGS - Universidade Federal do Rio Grande do Sul
Pós-Graduação em Computação
weber@inf.ufrgs.br

Resumo
O presente trabalho apresenta uma descrição da forma de funcionamento dos dispositivos sem fio padrão IEEE 802.11, focando especificamente as características envolvendo a segurança neste tipo de ambiente. São descritos os mecanismos de segurança deste padrão e as fraquezas do protocolo de segurança WEP – *Wired Equivalent Pivacy* atualmente utilizado. Também são apresentadas algumas propostas de aprimoramento da segurança da comunicação entre dispositivos sem fio, as quais são, atualmente, fontes de estudo.

Palavras-chave: Segurança de redes, IEEE 802.11, *wireless*, WEP, criptografia.

1 Introdução

As redes de computadores sem fio estão se tornando uma realidade para um grande conjunto de instituições e empresas. Estas redes permitem uma série de novas funcionalidades para troca de informações, tais como a facilidade de mobilidade de dispositivos e flexibilidade de conexões. As novas tecnologias de redes prometem o aumento da produtividade com custos relativamente baixos.

A mobilidade permite que dispositivos sendo transportados dentro da instituição possam permanecer conectados, sem perda de acesso aos sistemas e dados da rede. A flexibilidade que este ambiente proporciona diz respeito à facilidade dos dispositivos de acessar a rede sem a necessidade de uma estrutura física de fios.

Atualmente são definidos três padrões de troca de informações sem fios, sendo:

- redes WLAN (*Wireless Local Area Networks*) definidas pelo padrão IEEE 802.11 [1];
- redes WPAN (*Wireless Personal Area Networks*) definidas pelo padrão *Bluetooth*, atualmente incorporado no padrão IEEE 802.15 [2][3];
- redes WMAN (*Broadband Wireless Metropolitan Area Networks*), definidas pelo padrão IEEE 802.16.

No padrão IEEE 802.11, é especificada a forma de ligação física e de enlace de redes locais sem fio, com o objetivo de fornecer uma alternativa às atuais conexões utilizando cabos. Já no padrão IEEE 802.15, é apresentada uma nova forma de conexão local centrada no usuário, onde os dispositivos próximos a ele (aproximadamente 10m) estarão conectados e compartilhando recursos. O padrão IEEE 802.16 especifica conexões para redes metropolitanas sem fio.

A forma de conexão e de compartilhamento é estabelecida de acordo com a arquitetura adotada, sendo definidas as arquiteturas de: redes *ad hoc*; redes de infra-estrutura básica; e redes de infra-estrutura.

As redes *ad hoc*, ou IBSS (*Independent Basic Service Set*), são compostas por estações independentes, sendo criadas de maneira espontânea por estes dispositivos. Este tipo de rede se caracteriza pela topologia altamente variável, existência por um período de tempo determinado e baixa abrangência.

As redes de infra-estrutura básica, ou BSS (*Basic Service Set*), são formadas por um conjunto de estações sem fio, controladas por um dispositivo coordenador denominado AP (*Access Ponit*). Todas as mensagens são enviadas ao AP que as repassa aos destinatários. O AP funciona com o mesmo princípio de um equipamento concentrador (*hub*) para o ambiente sem fio; e operando como uma ponte (*bridge*) entre o ambiente sem fio e a rede com fios.

As redes de infra-estrutura são também denominadas ESS (*Extended Service Set*). Estas redes são a união de diversas redes BSS conectadas através de outra rede (como uma rede *ethernet*, por exemplo). A estrutura deste tipo de rede é composta por um conjunto de APs interconectados, permitindo que um dispositivo migre entre dois pontos de acesso da rede. As estações vêem a rede como um elemento único.

O presente artigo propõe-se a analisar e apresentar os aspectos relativos à forma de segurança atualmente utilizada por redes sem fio IEEE 802.11, suas falhas e algumas propostas de solução.

2 Aspectos de Segurança em Redes sem Fio

A utilização de uma rede sem fios implica em alguns aspectos especiais em relação à segurança, quando defrontada com uma rede com fios. As redes que utilizam fios para interconexão dos computadores possuem características de segurança física inexistentes em redes sem fio, tais como:

- limites físicos definidos - as redes sem fio tornam impossível o controle da abrangência do sinal que está sendo transmitido. Um atacante pode aproveitar esta característica para, de fora dos limites físicos de uma empresa (em uma rua próxima ou no estacionamento da própria empresa, por exemplo) acessar os dados da rede;
- meio controlável - em uma rede sem fio, é impossível a utilização de dispositivos de controle do meio como, por exemplo, comutadores (*switches*). Em uma rede com fios, é possível excluir uma determinada sala, simplesmente não fornecendo nenhum ponto para acesso à rede;
- controle de acesso físico - ao utilizar fios para a comunicação, apenas os dispositivo que possuem acesso a este recurso podem utilizar a rede. Em redes sem fio, não existe controle físico de dispositivos acessando a rede. Isto garante que, ao utilizar fios, somente os dispositivos fisicamente localizados dentro da empresa tem acesso à rede.

Para que uma rede sem fios possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados.

Os limites da abrangência das redes são definidos pelos dispositivos de ponto de acesso AP, podendo variar entre dezenas a centenas de metros. Esses limites são dependentes da potência do dispositivo AP e das antenas utilizadas pelas estações que desejam acesso.

É importante salientar que a segurança que deve ser adicionada encontra-se no nível de enlace de dados. Isto se deve ao fato de que os aplicativos e protocolos de níveis superiores foram desenvolvidos contando com a segurança física disponível nas redes com fios. O nível de enlace das redes sem fio deve, então, prover características de segurança que compatibilizem estes dois tipos de conexão, e possibilitem a execução de aplicativos sem riscos.

A segurança a nível de enlace que deveria garantir a compatibilidade entre conexões com e sem fios foi prevista no padrão IEEE 802.11 através do protocolo WEP (*Wired Equivalent Privacy*). Este protocolo provou-se ineficiente em uma série de estudos [3], [4], [5], [6] e [7] e, atualmente encontra-se em fase de reformulação por um grupo especial da IEEE, o grupo IEEE 802.11i [8].

3 Redes IEEE 802.11

As redes locais sem fio WLAN estão especificadas no padrão da IEEE (*Institute of Electrical and Electronics Engeneers*) como IEEE 802.11 [1]. O padrão IEEE 802.11b, utilizado como foco neste artigo, opera utilizando freqüências entre 2.4GHz a 2.5GHz ISM (*Industrial, Scientific, and Medical*) com DSSS (*Direct Sequence Spread Specrtum*). Possuem a taxa de transferência de 11Mbps.

Para identificar as fraquezas nas implementações atuais, é necessária uma análise nos princípios de segurança existentes no padrão das redes sem fio. Serão apresentadas as características de autenticação de dispositivos, ou seja, da garantia de que uma determinada informação veio de um equipamento autorizado, e de privacidade, que garante a confidencialidade de informações trocadas entre os dispositivos.

3.1 Autenticação no IEEE 802.11

O padrão IEEE 802.11 define duas formas de autenticação: *open system* e *shared key*. Independentemente da forma escolhida, toda autenticação deve ser realizada entre pares de estações, nunca havendo comunicação *multicast.* Em sistemas BSS as estações devem se autenticar e realizar a troca de informações através do *Access Point* [1]. As formas de autenticação previstas definem:

- Autenticação *Open System* - é o sistema de autenticação padrão sendo que, neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo.
- Autenticação *Shared key* - nesta autenticação, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP.

A autenticação do tipo *Open System* foi desenvolvida focando redes que não necessitam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção. Também aconselha-se que estas redes permaneçam separadas da rede interna por um *firewall* (a semelhança de uma zona desmilitarizada – DMZ).

A autenticação *Shared Key* utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos. Um segredo é utilizado como semente para o algoritmo de criptografia do WEP na cifragem dos quadros. A forma de obter esta autenticação é a seguinte:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudo-randômicas.
3. A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
4. O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

3.2 Privacidade de dados no IEEE 802.11

Para cifrar a mensagem de autenticação e todos os outros pacotes que serão trocados entre as estações, utiliza-se o protocolo WEP. O protocolo WEP foi desenvolvido originalmente por um conjunto de fabricantes de *hardware* com o intuito de evitar a ocorrência de falhas na privacidade dos dados trafegando em uma rede sem fio. Estas falhas são ocasionadas por agentes maliciosos portando dispositivos para escuta não autorizada de informações, ou enviando dados sem autorização para a rede. É um protocolo de criptografia baseado no uso de chaves criptográficas trocadas entre pares de estações. De acordo com a IEEE [1], o protocolo WEP possui as seguintes características:

- é razoavelmente robusto - devido à necessidade de grande esforço computacional para descoberta da chave secreta;
- é capaz de autossincronização - como o meio físico possui grandes taxas de perda de mensagens, a cada nova mensagem existe uma sincronização entre as entidades e a escolha de uma nova chave criptográfica (o segredo permanece o mesmo, enquanto a chave é alterada). Se não houver nova sincronização, a perda de uma mensagem acarreta na impossibilidade de decifragem das subsequentes, tendo em vista o funcionamento do algoritmo de cifragem;
- é eficiente - pode ser implementado tanto em *hardware* como em *software*;
- pode ser exportado dos Estados Unidos - devido à política de exportação de sistemas criptográficos norte-americana na época em que foi desenvolvido, cuidados foram tomados para que esse governo aprovasse a exportação de equipamentos que utilizassem este protocolo;
- a sua utilização é opcional.

Para melhor identificar o método de criptografia utilizado pelas redes sem fio, torna-se necessária a apresentação do modo de funcionamento do algoritmo criptográfico RC4, criado em 1987 [9].

O algoritmo RC4 funciona como um algoritmo de fluxo, ou seja, é utilizado para enviar um conjunto de bits cifrados em um fluxo contínuo. Neste tipo de algoritmo, não se pode esperar o acúmulo de um certo número de bits para transmitir. É classificado como sendo de chave simétrica, ou seja, a chave de cifragem é a mesma de decifragem.

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 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.

A figura 1 apresenta o código KSA - Key Scheduling Algorithm, utilizado para permutar o vetor S, e o código PRNG para gerar os números pseudo-aleatórios. Sendo: *K*: segredo compartilhado; *N*: número de posições do vetor *S*, *l*: tamanho da chave *K* (em bytes).

O protocolo WEP funciona utilizando o gerador de números PRNG, do RC4. A semente para geração da

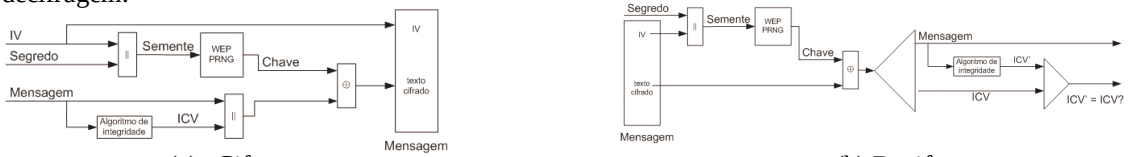
chave é uma combinação do segredo compartilhado com um vetor aleatório de 24 bits chamado IV (*Initialization Vector*). Para cada quadro, o protocolo WEP deve selecionar um IV diferente, permitindo que a chave secreta permaneça a mesma, enquanto a semente é alterada, mantendo o sincronismo.
Como o destinatário da mensagem deve criar a chave de decifragem a partir da mesma semente, o remetente envia o IV escolhido sem criptografia com o quadro. Desta forma, o destinatário pode unir o segredo compartilhado com o IV escolhido e utilizar estas informações como semente no PRNG.

```
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 1 – algoritmos KSA e PRNG

Para verificar que os dados não foram alterados durante a comunicação, é utilizado um algoritmo redundante do tipo CRC-32 (*Cyclic Redundancy Check*) denominado ICV - *Integrity Check Value*.
O esquema do funcionamento do WEP é apresentado na figura 2, sendo (a) esquema de cifragem e (b) decifragem.



(a) Cifragem (b) Decifragem

Figura 2 – protocolo WEP cifragem e decifragem

Para que o WEP possa prover segurança, uma chave nunca deve ser reutilizada. Isto é muito importante, pois no momento em que o número de possíveis IVs for esgotado, o segredo deverá ser modificado.
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.
Os aspectos sobre os possíveis ataques ao protocolo WEP e redes sem fios serão discutidos no item 4 deste artigo.

4 Possíveis ataques e fragilidades de segurança do IEEE 802.11

Os ataques mais comuns em redes sem fio referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviço. Estes ataques possuem graus de dificuldade dependentes das características de implantação da rede.

4.1 Redes *Open System*

A principal preocupação em relação à segurança em redes sem fio diz respeito a forma de funcionamento padrão destas redes ser do tipo *Open System*. Isto significa que um usuário desavisado, ao instalar a rede pela primeira vez, possibilita acesso a todos os dados da rede sem proteção alguma. Todos os sistemas computacionais em execução nesta rede que não possuem criptografia estarão disponíveis a qualquer dispositivo dentro da área de abrangência do AP.
Os usuários que optam por este tipo de sistema, não possuem qualquer forma de confidencialidade, nem de autenticação de dispositivos, tendo como problemas imediatos:

1. Ataque passivo para captura legível de informações da rede

É possível a um atacante obter todas as informações que trafegam na rede sem criptografia. Entre os diversos programas que não utilizam qualquer forma de cifragem estão as aplicações de *e-mail*, *telnet* e *ftp*, disponibilizando nomes de usuários e senhas. O atacante não interfere no funcionamento da rede e, nos casos das redes sem fio, pode facilmente mascarar-se sem ser detectado.

2. Ataque ativo durante a comunicação

Um atacante pode fazer-se passar por um AP da rede. Com isto, os dispositivos passam a confiar informações sensíveis diretamente ao atacante. Como não existe autenticação, não existe forma de se garantir que o AP com quem um dispositivo está associado é realmente um equipamento autorizado. Este ataque é conhecido como "*man-in-the-middle*".
O atacante deve alterar o funcionamento normal da rede para conseguir passar-se por um dispositivo

válido (ataque de *spoof* inicial para realizar o *man-in-the-middle*).
Também á possível que um atacante simplesmente autentique seu dispositivo móvel na rede através de um AP. A partir deste momento, conforme as permissões da rede, terá o mesmo acesso que um usuário autorizado.

4.2 Redes *Shared Key* com WEP

Nas redes que utilizam a autenticação *Shared Key* juntamente com o protocolo de segurança WEP, os mesmos ataques podem ser realizados, aumentando-se a complexidade, como é apresentado adiante.
Tendo em vista o mecanismo de cifragem do WEP, se um atacante altera um bit do texto cifrado, este mesmo bit será alterado na mensagem original. Ou seja, o atacante consegue alterar um bit específico na mensagem cifrada, mesmo sem conhecer seu conteúdo, o segredo compartilhado, ou a chave.
As técnicas utilizadas para tentar evitar estes tipos de ataque são a utilização de IVs para impedir a repetição da chave; e o campo de verificação de integridade (que realiza o cálculo de CRC-32).
A utilização de diferentes IVs não impede a repetição de chaves, pois o seu pequeno tamanho (24 bits) acarreta em repetições. Por exemplo, em uma rede onde o AP envia pacotes de 1500 bytes a 11 Mbps ocorrerão repetições a cada: $(1500*8)*(2^{24})/(11*10^6) \cong 18000$ segundos, ou seja, a cada 5 horas [10].
Com estas repetições é possível que o atacante realize operações de análise estatística dos quadros cifrados com a mesma chave.
Já a utilização de CRC-32 falha por ser linear, ou seja, é possível identificar os bits do CRC que devem ser alterados caso deseje-se alterar um bit específico da mensagem. O atacante pode alterar o bit que desejar da mensagem e recalcular o CRC para que seja aceito [10].
Os ataques mais comuns em redes que utilizam o WEP, apresentados no trabalho [10] são os ataques estatísticos, de injeção de tráfego, redirecionamento de mensagens e construção de tabelas de decifragem.

4.2.1 Ataques Estatísticos

Os ataques estatístico são ataques passivos, onde o objetivo é descobrir o significado de textos cifrados. Uma forma de realizar este tipo de ataque é a de obter uma série de pacotes cifrados com a mesma chave. Ao calcular o resultado de operações de XOR entre as mensagens cifradas com a mesma chave, tem-se o XOR entre os textos originais.
Com este resultado, é possível inferir dados a respeito das mensagens, incluindo campos conhecidos, como cabeçalhos IP, ou tentar deduzir o conteúdo de uma das mensagens. Ao obter um dado de uma mensagem, obtém-se o conteúdo de todas as mensagem cifradas com a mesma chave. O ataque perde complexidade conforme um número maior de mensagens é capturado. Uma forma de otimizar este ataque é através da inserção de dados na rede, tornando o ataque ativo.
Ao inserir conteúdo conhecido na rede (como um *e-mail*, por exemplo), o atacante possui o conhecimento do texto original, o texto cifrado e o IV utilizado para a cifragem. Com isto é possível obter o conteúdo de qualquer mensagem cifrada com o mesmo IV.
Quanto maior o número de dispositivos sem fio conectados na rede, maior a probabilidade de colisões de IVs e, consequentemente, maior o número de mensagem decifradas pelo atacante.

4.2.2 Ataques de injeção de tráfego

Supondo-se que o atacante possua conhecimento completo do conteúdo de uma mensagem cifrada. Basta que construa uma nova mensagem, calcule o novo CRC e altere os bits da mensagem original (dados e CRC) para que seja aceita pelo AP. Este ataque segue a lógica de que $RC4(X) \oplus X \oplus Y = RC4(Y)$.
Caso o atacante não possua o conhecimento completo do texto, mesmo assim poderá alterar partes deste texto (inserindo comandos maliciosos em uma sessão *telnet*, por exemplo) e alterar os bits correspondentes nos dados e CRC. Com este tipo de ataque, é possível inserir dados na rede aproveitando pacotes enviados por dispositivos já autenticados.
Tendo conhecimento desta fraqueza, alguns novos modelos de cálculo de integridade não lineares estão sendo propostos como, por exemplo, o MIC – *Message Integrity Check*. Este algoritmo utiliza um cálculo de resumo (*hash*) entre a semente, endereço MAC origem, MAC destino e dados. Qualquer alteração em um destes dados afetará o resultado do MIC.

4.2.3 Ataques de redirecionamento de mensagens

Possuindo conhecimento sobre os cabeçalhos dos pacotes, o atacante pode alterar informações como endereço de destino e fazer com que um pacote seja direcionado para internet. Ao direcionar o pacote a um endereço IP destino em uma máquina a qual possui controle, o atacante faz com que o AP decifre a mensagem antes de enviá-la.

Na máquina destino, o atacante recupera o texto original, enquanto monitorando a rede sem fio obtém a mesma mensagem cifrada. Assim, além de obter o conteúdo da mensagem, o atacante toma conhecimento de mais uma chave gerada a partir de um IV.

4.2.4 Construção de tabelas de decifragem

O pequeno número de IVs possibilita que um atacante, realizando um conjunto de ataques à rede, possa montar uma tabela contendo uma série (ou todas) as chaves utilizadas com os respectivos IVs. Uma vez construída esta tabela, é possível decifrar todas as mensagens que possuem as chaves com IVs conhecidos.

4.2.5 Obtenção do segredo compartilhado

O próprio algoritmo RC4 ao ser utilizado nas redes sem fio apresenta fraquezas. O trabalho [11] apresenta os resultados de uma pesquisa sobre fraquezas na escolha de chaves para o algoritmo RC4 utilizado nas redes sem fio. Estas fraquezas dizem respeito a um grande número de chaves fracas geradas pelo WEP, e pela possibilidade de descobrir bits da chave a partir da análise/conhecimento dos primeiros bits da mensagem (pelo fato do IEEE 802.11 utilizar os dados encapsulados pelo LLC – *Logical Link Control* os primeiros bits dos quadros são sempre os mesmos). A partir dos resultados obtidos em [11] foram desenvolvidos uma série de programas como o AirSnort [12], os quais conseguem obter o segredo compartilhado entre as estações através da análise do tráfego da rede. Ao obter o segredo compartilhado, a privacidade da rede fica completamente vulnerável.

5 Propostas de solução/ aprimoramento da segurança

Alguns modelos propõem técnicas para acréscimo de segurança nas redes sem fio. Estes modelos estão atualmente em fase de análise, sendo os que possuem maior destaque: utilização de mecanismos de proteção nas camadas superiores; e utilização do padrão IEEE 802.1x para autenticação de dispositivos.

5.1 Mecanismos de proteção nas camadas superiores

Uma possível solução para a comunicação em redes sem fio é a de utilizar segurança nas camadas acima do enlace. Dentre estas soluções, a mais natural é a utilização do *IPSec* (ou outro algoritmo robusto de criptografia) em conjunto com redes VPN - *Virtual Private Networks*.

O protocolo *IPSec* possui como objetivo prover um meio de comunicação seguro fim-a-fim em redes IP. Este protocolo opera entre os níveis de rede e transporte, cifrando os dados do transporte, e fornecendo o resultado ao nível de rede. Operando desta maneira não são necessárias alterações no nível de rede (IP), permitindo que os dados sejam transportados (roteados) nas redes atuais. O *IPSec* garante mecanismos para privacidade e autenticidade dos dados transportados.

As redes VPN são construídas através de dispositivos que possuem algoritmos como o *IPSec* implementado. Um exemplo da utilização de redes VPN em um ambiente sem fio é descrito na figura 3.

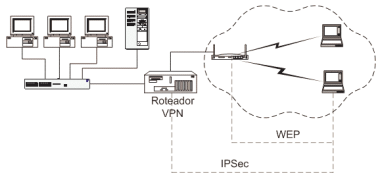


Figura 3 – rede WLAN com VPN/IPSec

Para que a rede sem fio utilize VPN é necessário que todos os dispositivos sem fio (com exceção do AP) suportem VPN, e que exista um equipamento na fronteira da rede interna que faça a decifragem dos dados para a rede interna.

As informações dos níveis abaixo do nível de rede não são cifradas pelo *IPSec*. Isto significa que um atacante pode obter informações do nível de enlace para obter acesso à rede sem fios. Esta solução impede apenas que o atacante recupere os dados de uma comunicação (acima do nível de rede) de forma legível. Também chama-se atenção ao impacto deste tipo de solução no desempenho da rede e a necessidade de poder de processamento do roteador VPN de acordo com o número de túneis criados.

5.2 Padrão IEEE 802.1x

O padrão IEEE 802.1x especifica um mecanismo para autenticação de dispositivos e/ou usuários através da utilização de variações do protocolo EAP - *Extensible Authentication Protocol* [13]. O protocolo EAP, na sua definição, permite a utilização de uma grande variedade de mecanismos de autenticação. A forma de funcionamento deste protocolo é baseada na troca de mensagens do tipo texto-desafio.

A união do padrão EAP com a utilização do protocolo TLS - *Transport Layer Security*, gerou a proposta

de protocolo PEAP [14] para utilização com o padrão IEEE 802.1x, da seguinte maneira [15]:

1. A estação notifica o AP que deseja autenticar-se, e envia uma lista de algoritmos criptográficos suportados por ela;
2. O AP repassa esta mensagem para uma estação autenticadora localizada na rede da instituição. Esta estação é chamada *back-end server*. Nota-se que o AP não dá acesso para a rede ao dispositivo enquanto este não for autenticado;
3. O *back-end server* responde (através do AP) com um identificador de seção, uma lista de algoritmos criptográficos selecionados e uma chave pública.
4. A estação gera o segredo compartilhado, e cifra esta informação utilizando a chave pública do *back-end server*;
5. O *back-end server* envia para a estação uma mensagem cifrada com o segredo, finalizando a autenticação.

Como o EAP permite diferentes tipos de autenticação, alguns fabricantes adotam modelos diferentes do citado. A CISCO, por exemplo, no trabalho [16] propõe a utilização de autenticação mútua entre rede e dispositivo. O *back-end-server* poderá ser, por exemplo, um servidor RADIUS - *Remote Access Dial-In User Service*.

Após a troca inicial de chave pública e segredo, as estações podem trocar qualquer informação que desejarem como, por exemplo, dados para autenticação do usuário ou renovar o segredo compartilhado pelo WEP.

O padrão também especifica que todos os APs devem estar conectados ao mesmo *back-end-server*. Com isto, ao migrar entre dois APs, uma estação mantém a mesma chave de seção, simplesmente informando ao novo AP o identificador da seção que está utilizando.

Neste protocolo, não existe forma de verificar se a chave pública realmente pertence ao *back-end server*, devido a falta de uma entidade de certificação que assine esta chave. O padrão autentica a estação na rede, mas não garante a autenticação da rede para a estação. É possível que um atacante apresente-se como o AP para um dispositivo. Este dispositivo tentará se autenticar com o *back-end server* enviando seus dados diretamente para o atacante. Quando isto acontecer, o atacante se porta como um equipamento requisitando autenticação para o AP real, como demonstra a figura 4 (a). Desta forma, todo o tráfego da seção passará pelo atacante.

No momento de estabelecer a seção TLS, o atacante fornece uma chave de seção para o *back-end server* e cria outra seção com o dispositivo alvo, efetuando um ataque do tipo "*man-in-the-middle*". Este mesmo ataque pode ser efetuado em protocolos de autenticação mútua sem autoridade certificadora.

Outro problema presente neste protocolo é a possibilidade de seqüestro de seção como mostra a figura 4(b). Um atacante pode (1) enviar para uma estação já autenticada uma mensagem de desautenticação, fazendo-se passar pelo *back-end-server*. Desta forma, o alvo é desassociado (2), enquanto o back-end server mantém internamente o estado do dispositivo como conectado. Basta ao atacante assumir a identidade (endereço MAC) do alvo para se associar à rede (3). Este ataque só é possível graças a falta de autenticação presente nos quadros da rede sem fio [17].

(a) *man-in-the-middle* (b) *hijack*

Figura 4 – ataques *man-in-the-middle* e *hijack*

Este tipo de mensagem também pode causar um ataque de negação de serviço, desassociando as estações e impedindo a troca de mensagens.

Algumas alternativas para aprimorar o protocolo IEEE 802.1x são apresentadas no documento [17].

6 Conclusões

Tecnicamente, as redes sem fio apresentam uma série de vulnerabilidades que tem origem na concepção do padrão. A melhor forma de garantir um acréscimo de segurança neste tipo de ambiente, até a atualização do padrão, é através de políticas e procedimentos de segurança específicos para esta nova tecnologia. Uma política específica para redes sem fio envolve, no mínimo:

- a configuração cuidadosa dos equipamentos utilizados;
- limitar os equipamentos que podem acessar a rede, dificultando a operação de atacantes;

- caso a instituição necessite confidencialidade nos dados das camadas superiores, utilizar equipamentos específicos para este fim, como roteadores VPN;
- caso a instituição necessite de autenticação a nível de usuário e/ou dispositivo, deve utilizar autenticação e distribuição de chaves de seção através do padrão IEEE 802.1x (a troca de chaves públicas deve ser feita de maneira segura, tentando evitar ataques);
- manter registros das atividades na rede e sistemas de identificação de intrusão;
- em redes onde as informações internas da instituição são confidenciais, os pontos de acesso de dispositivos sem fio deve ser considerados como pontos de acesso público.

Infelizmente estes procedimentos acarretam na queda de desempenho da rede, e maior consumo de energia dos dispositivos sem fio alimentados por baterias. Este fato é uma barreira na utilização destas medidas de segurança e também interfere na análise de possíveis padrões de segurança que possam vir a ser adotados.

Mesmo em casos onde os custos da utilização de mecanismos de segurança extras são válidos, sabe-se que são possíveis ataques bem sucedidos em redes sem fios. Os mecanismos existentes atualmente são contornáveis com relativa facilidade por um atacante motivado.

O padrão IEEE 802.11 está, durante a escrita deste artigo, passando por uma análise dos aspectos relacionados à segurança, realizado por um grupo especial denominado IEEE 802.11i [8]. Este grupo será o responsável pelo acréscimo de mecanismos de segurança que aprimorem o padrão atual.

Sabe-se, no entanto que diversos dispositivos estão em uso atualmente e deverão ser atualizados quando a nova versão do protocolo de segurança WEP for finalizada.

7 Bibliografia

[1] IEEE 802.11. Part 11: **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. Disponível por www em: http://standards.ieee.org/getieee802/802.11.htm. l999.

[2] IEEE 802.15. **Wireless MAC and PHY Specifications for Wireless Personal Area Networks (WPANs)**. Disponível por www em: http://ieee802.org/15/, 2002.

[3] OWEN, Les; Karygiannis, Tom. **Special Publication 800-48: DRAFT - Wireless Network Security 802.11, Bluetooth, and Handheld Devices**. Disponível por www em: http://csrc.nist.gov/ publications/drafts.html, 2002.

[4] ARBAUGHT, William A; et al. **Your 802.11 Wireless Network has No Clothes**. Department of Computer Science - University of Maryland. Disponível por www em: http://www.cs.umd.edu/~waa/wireless.pdf

[5] KABARA, Joseph; et al. **Information Assurance in Wireless Networks**. Department of Information Science and Telecomunications - University of Pittsburgh.

[6] CHICKINSKY, Alan. **Wireless LAN Security Threads**. IEEE P802.11, doc: IEEE802.11-01/258. Disponível por www em: http://grouper.ieee.org/groups/802/ 11/Documents /DocumentsHolder/1-258.zip. Maio 2001.

[7] WALKER, Jesse R. **Unsafe at any key size; An analysis of the WEP encapsulation**. Intel Corporation, Oregon, 2000. Disponível por www em: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

[8] IEEE 802.11i. **The Working Group for LAN Standards**. Disponível por www em: http://ieee802.org/11/.

[9] SCHNEIER, Bruce. **Applied Cryptography. Second Edition: protocols, algorithms, and source code in C**. John Wiley & Sons Inc. 1996.

[10] BORISOV, Nikita; et al. **Security of the WEP algorithm**. Disponível por www em: http://www.isaac.cs.berkeley.edu/ isaac/wep-faq.html

[11] FLUHRER, Scott; et al. **Weaknesses in the Key Scheduling Algorithm of RC4**. Cisco Systems Inc. Disponível por www em: http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

[12] **AIRSNORT**. Disponível por www em: http://airsnort.shmoo.com/

[13] BLUNK, L; Vollbrecht, J. **PPP Extensible Authentication Protocolo (EAP)**. Merit Network, Inc. RFC Standard 2284. Disponível por www em: http://ietf.org/rfc/rfc2284.txt

[14] ANDERSSON, H; Josefsson, S. **Protected EAP Protocol (PEAP)**. RSA Security Inc; CISCO; Microsoft Inc. Internet-draft. Fevereiro 2002. Disponível por www em: http://ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-02.txt.

[15] RSA Security. **Improving Wireless LAN Authentication – A Description of the Authentication in 802.1x Standard**. RSA Security Inc. Disponível por www em: http://www.rsasecurity.com/go/ slides2001Q4/wirelesslive/WirelessLANAuthentication2.pdf

[16] CONVERY, Sean; Miller Darrin. **SAFE: Wireless LAN Security in Depth**. CISCO. Disponível por www em: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

[17] MISHRA, Arunesh; Arbaugh, William. **An Initial Security Analysis of the IEEE 802.1X Standard**. University of Maryland. Disponível por www em: http://www.cs.umd.edu/~waa/1x.pdf