6
Conclusão

As inúmeras vantagens proporcionadas pela WLAN contribuem para a expansão das redes sem fio IEEE 802.11 nos ambientes empresariais, governamentais e residenciais. Porém, estas redes possuem diversas vulnerabilidades decorrentes da fragilidade dos mecanismos de segurança definidos pelo IEEE na elaboração do Padrão, no tocante à autenticação, confidencialidade e integridade dos dados.

Por esse motivo, a segurança ainda é um obstáculo à ampla adoção corporativa e governamental da tecnologia WLAN. Há risco de ocorrência de interceptação e adulteração de informações confidenciais e invasão por elementos estranhos, podendo ocasionar possíveis transtornos às atividades administrativas e comerciais, além de prejuízos financeiros e à imagem da empresa/instituição.

Diversas publicações técnicas apontaram as deficiências e vulnerabilidades do mecanismo WEP, o que obrigou fabricantes e órgãos regulamentadores a desenvolverem soluções que permitissem a operação das WLAN de forma segura e confiável. Os mecanismos intrínsecos do Padrão são ineficazes, e cuja segurança proporcionada é facilmente "*quebrada"* por ferramentas de rápida obtenção na *internet*. No entanto, estes mecanismos, apesar de muito fracos, possibilitam o primeiro nível de segurança, e não devem ser desconsiderados.

A solução utilizando o Padrão IEEE 802.1x, com emprego de servidores RADIUS e de métodos seguros de transporte de credenciais, garante maior rigidez no controle de acesso e no gerenciamento das chaves secretas, com a geração e distribuição de forma confiável e segura, para criptografia do canal rádio pelo WEP.

Contudo, havia a expectativa desta solução gerar sobrecarga de pacotes para autenticação dos usuários e criptografia das mensagens, ocasionando a degradação no desempenho e comprometendo a *performanc*e da rede.

Esta dúvida foi esclarecida através da simulação em laboratório dos diversos mecanismos de segurança propiciados pelos Padrões IEEE 802.11b e IEEE 802.1x, utilizando os protocolos de aplicação FTP e HTTP.

Pelos resultados obtidos, pode-se concluir que a influência sobre a *performance* da rede quando se implementa qualquer mecanismo de segurança é pequena, sendo a degradação um pouco mais acentuada para os modelos PEAP e LEAP.

O desempenho para cada tipo de aplicação varia bastante, porém, não devido à rede sem fio, mas sim ao funcionamento dos protocolos. O tráfego FTP é fortemente influenciado pela rede sem fio, já que o *throughput* está limitado pelo mecanismo CSMA/CA de acesso ao meio, baseado no modo DCF. Por sua vez, o tráfego HTTP não é influenciado pela rede sem fio, pois o modo de operação do protocolo reduz substancialmente o desempenho, independente de se adotar ou não um modelo de segurança.

Se a empresa, instituição ou usuário residencial não estiver excessivamente preocupado com sua rede e com a integridade de deus dados, então, deve implementar, no mínimo, o WEP com 128bits, pois, como observado, não há comprometimento no desempenho da rede.

Nas aplicações corporativas e governamentais é fundamental se adotar o Padrão IEEE 802.1x, utilizando um servidor RADIUS e um dos três mecanismos: EAP-TLS, PEAP ou EAP-TTLS, em conjunto com o WEP 128bits para criptografia do canal rádio.

O EAP-TLS deve ser adotado por médias e grandes empresas/instituições que já possuem infra-estrutura de chave pública emitida por AC para clientes e servidores. Este mecanismo tem a grande vantagem do usuário não precisar de senha para acessar a rede. Porém, a exigência de certificado no cliente torna a solução onerosa, além de gerar muito esforço de administração na geração, controle e distribuição dos mesmos. Sua adoção pelo Windows facilita a implementação, principalmente no cliente.

O EAP-TTLS é uma solução para uma pequena e média empresa/instituição, pois tem o melhor desempenho quando comparado com os demais mecanismos com autenticação externa, além de não necessitar de certificado no cliente. No entanto, pelo fato do EAP-TTLS não ser suportado pelo

Windows, há necessidade de instalação de um Cliente de Autenticação (por exemplo: *SECURE W2 Client, Meetinghouse AEGIS Client ou Funk Odyssey).*

O PEAP é a melhor solução para uma pequena e média empresa/instituição, pois, apesar de apresentar o pior desempenho, tem a grande vantagem de ser suportado pelo Windows, diferentemente do EAP-TTLS, e não exigir certificado no cliente, o que facilita e reduz o custo de implementação.

O mecanismo LEAP, com autenticação baseada em senha, deve ser evitado, pois, além de ser proprietário da CISCO, sua segurança é a mais baixa dentre todos os mecanismos com autenticação externa.

Um importante parâmetro analisado neste trabalho foi o tempo médio para autenticação de um usuário. A importância reside no fato de que a primeira estratégia para reduzir ameaças à chave de criptografia WEP é garantir que as chaves de sessão do usuário sejam atualizadas periodicamente, e em intervalos de tempo inferiores ao tempo necessário para capturar o tráfego e executar as operações de força bruta. Com a reautenticação, uma nova chave de sessão é gerada para ser utilizada pelo WEP.

Desta forma, no projeto da WLAN, deverá ser considerado o tempo máximo para que ocorra uma nova autenticação. Este tempo deverá ser estimado a partir, principalmente, das características do tráfego da empresa/instituição, da quantidade de usuários e do *valor* da informação para a empresa/instituição.

Para complemento do trabalho, foi realizada a medição de desempenho com 02, 03 e 04 usuários configurados à 11Mbps.

Para operação com 02 usuários, optou-se por realizar dois experimentos: uma situação com ambos configurados à 11Mbps e outra situação com os usuários configurados em 1Mbps e 11Mbps.

A situação com os 02 clientes configurados à 1Mbps e 11Mbps é a mais comum, tendo em vista o canal rádio ser fortemente influenciado por interferências e efeitos de multipercursos causados pelos fenômenos de reflexão, difração e espalhamento.

Da análise dos resultados obtidos, conclui-se que a *performance* da rede está limitada ao *throughput* do usuário com a pior condição de propagação. Quando detecta um aumento na perda de pacotes, o cliente degrada sua taxa nominal para 5.5, 2 ou 1Mbps.

A influência sobre a *performance* da rede quando se implementa um mecanismo de segurança permanece desprezível. Desta forma, as soluções de segurança propostas continuam válidas para mais de um cliente.

Os valores de *throughput* obtidos com 02, 03 e 04 usuários estão coerentes com artigo publicado por Gilles Berger-Sabbatel, Andrzej Duda, Martin Heusse e Franck Rousseau [23].

6.1
Tecnologias Emergentes

As metas de segurança do WEP ainda possuem deficiências, que foram resolvidas parcialmente com o Padrão IEEE 802.1x:

a) ***Autenticação***: foi resolvida com o emprego do Padrão IEEE 802.1x;

b) ***Confidencialidade***: melhorou com a chave de sessão, mas ainda apresenta vulnerabilidades;

c) ***Integridade***: ainda permanece deficiente.

Portanto, ainda é necessária a adoção de soluções mais eficazes para as deficiências na ***Confidencialidade*** e na ***Integridade***.

Os mecanismos apresentados neste trabalho fazem parte de soluções propostas por fabricantes com a finalidade de melhorar a segurança e viabilizar o comércio para aplicações corporativas e governamentais. Por serem soluções em sua maioria proprietárias, não foram padronizadas por órgão regulamentadores.

A indústria, através da WECA *(Wi-Fi Ethernet Compatibility Alliance),* desenvolveu uma solução preliminar denominada WPA (*Wi-Fi Protected Access*) na tentativa de resolver as vulnerabilidades do WEP e atender ao mercado, enquanto o *Task Grup i (TGi)* não lançava o novo padrão IEEE 802.11i. O WPA pode ser considerado como um subconjunto desse padrão.

O WPA inclui um protocolo denominado TKIP (*Temporal Key Integrity Protocol)* para criptografia mais robusta do canal sem fio. Este mecanismo ainda utiliza o algoritmo RC4, porém, na montagem da chave pseudo-randômica, emprega um vetor de inicialização (IV) com 48 bits, ao invés de 24 bits, como no WEP. Isto também possibilita ampliar o tempo de vida da chave pseudo-

randômica, permitindo aumentar o tempo de reautenticação para geração de uma nova chave.

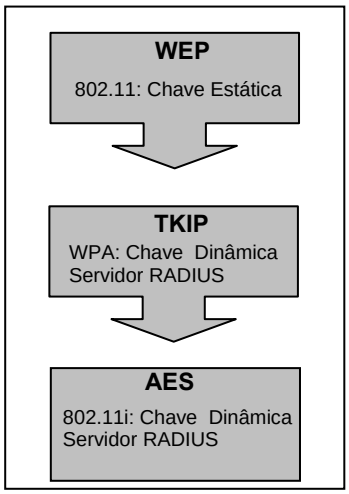

Figura 81: Evolução da Criptografia

O controle de acesso e a troca de credenciais no WPA é realizado pelo padrão IEEE 802.1x e métodos EAP. O sistema de geração e gerenciamento da chave é mais robusto (*four-way handshake*).

A integridade é garantida através da inserção de um campo MIC (*Message Integrity Check)*, calculado através de informações contidas no próprio *frame*, utilizando uma função de *Hash* conhecida como *Michael*. Além do MIC, o quadro possui um campo de seqüência SEQ, incrementado a cada frame transmitido, para evitar ataques do tipo *replay*. O AP tem a função de descartar *frames* enviados fora de ordem por um mesmo cliente

As figuras a seguir ilustram os *frames* com o WEP e com o TKIP.

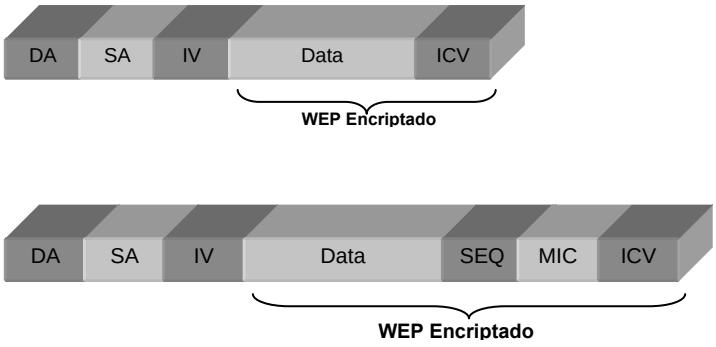

Figura 82: *Frames* no WEP e TKIP

As figuras a seguir ilustram como a chave pseudo-randômica é gerada no WEP e no TKIP.

Figura 83: Geração da chave pseudo-randômica no WEP

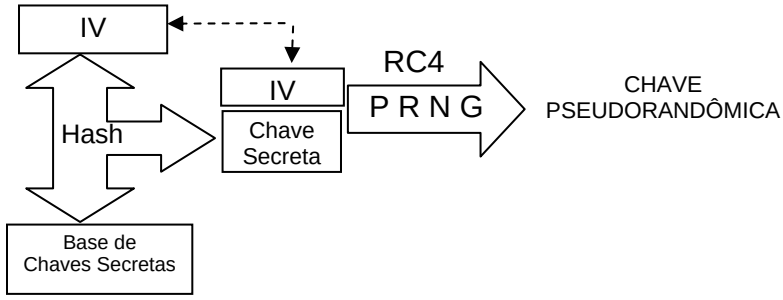

Figura 84: Geração da chave pseudo-randômica no TKIP

No ano de 2004, finalmente, o IEEE apresentou o padrão IEEE 802.11i, considerando o aproveitamento das plataformas existentes e agregando novas características com o objetivo de aumentar a segurança.

As principais características do padrão 802.11i, também conhecido como RSN (*Robust Security Network*), são:

a) ***Autenticação***: continua sendo feita mutuamente através do conjunto de padrão 802.1x e dos métodos EAP;

b) ***Confidencialidade***: adoção de mais um algoritmo de criptografia denominado AES-CCMP (*Advanced Encryption Standard – CCM Protocol*). Este algoritmo utiliza o novo padrão de criptografia AES aprovado pelo NIST (US *National Institutes of Standards and Technology*);

c) ***Integridade***: continua a ser garantida através da inserção dos campos MIC e SEQ.

6.2
Sugestões para Trabalhos Futuros

Sugestões para trabalhos futuros:

a) Análise da *performance* da rede devido ao uso conjunto dos mecanismos de autenticação externa e WPA;

b) Estudo sobre a comportamento computacional das WLAN em caso de utilização dos algoritmos TKIP e AES-CCMP.