Uso das Chaves Individuais e Sistema de Autenticação Remota na Segurança de Redes *Wireless*

Bruno D´avila Fernandes*
CCEI – Urcamp Bagé, RS
bruno@urcamp.edu.br

Cristiano Cachapuz e Lima**, Abner Guedes**
CCEI – Urcamp Bagé, RS

Resumo*— Este trabalho trata de explanar a respeito das funcionalidades de uma rede sem fio que utiliza radiofrequência em sua comunicação, abordando protocolos de segurança wireless, que são: controle por MAC (*Media Access Control*), WEP (*Wired Encriptation Protocol*), WPA (*Wi-Fi Protected Access*), WPA2 (*Wi-Fi Protected Access 2*), tendo implantação dentro da empresa Alternet (Provedor de Internet via rádio em Bagé/RS). Este tipo de rede, ratificado pelo IEEE (*Institute of Eletrical and Eletronic Engineers*), utiliza o padrão 802.11, este padrão possui variações: 802.11b, 802.11a, 802.11g, 802.11n. Testes de vulnerabilidade foram realizados através do controle por MAC e os protocolos: WEP, WPA, WPA2, também de desempenho da velocidade de transferência de arquivos, assim como testes de autenticação no servidor freeRADIUS, (PPPoE (*Point-to-Point Protocol over Ethernet*)). Será demonstrado um dos vários métodos de segurança existentes, por exemplo, protocolo criptográfico WPA2, junto com o servidor RADIUS (*Remote Authentication Dial-In User Server*) e MySQL. Com este método a chave de autenticação ficará dentro do servidor MySQL juntamente com o RADIUS, assim assegurando a autenticidade dos usuários e confiabilidade das informações. Este tipo de rede, quando a sua segurança é bem configurada, é uma excelente opção a ser implantada, pois sua configuração é simples, o que justifica o aumento de usuários para melhor difusão desta tecnologia.

I. INTRODUÇÃO

Este artigo trata de apresentar as funcionalidades de uma rede sem fio que utiliza radio frequência em sua comunicação, abordando protocolos de segurança como WEP, WPA e WPA2 e controle por MAC, além de testes de transferências entre ambos [2].

A utilização da criptografia WPA implantada no Mikrotik utilizando uma única senha de acesso padrão, é uma vulnerabilidade ocasionada pelo administrador da rede, sendo possível que algum hacker mal-intencionado descubra a senha, podendo danificar vários rádios (clientes do Mikrotik), observando esta falha foi realizado um estudo e implantado na Alternet (provedor de Internet via rádio, Bagé/RS) a criptografia WPA2 junto com o servidor RADIUS (gerando uma conexão PPPoE), sendo assim cada cliente terá um login e password individual, eliminando a falha cita anteriormente, proporcionando uma maior segurança e integridade dos dados dos clientes no acesso à Internet neste provedor.

A metodologia que foi adotada no presente trabalho, bem como as principais etapas que envolvem os métodos e os procedimentos que foram utilizados, como segue abaixo:

- Realizar um comparativo de velocidade, sem a utilização de criptografia, usando somente o SSID (*Service Set Identifier*) do AP e os protocolos IEEE 802.11: WEP, WPA e WPA2;
- Executar alguns testes de vulnerabilidade aos demais protocolos e documentar os resultados;
- Implantar as técnicas de aplicação de segurança escolhida;
- Configurar o servidor RADIUS (PPPoE) para autenticação com o WPA2;
- Realizar testes de autenticação na comunicação dos clientes com o servidor RADIUS.

II. REVISÃO DE LITERATURA

A. *Redes sem fio*

Há mais de 100 anos atrás, Marconi inventor do rádio, demonstrava a curvatura da Terra pelo uso das ondas de rádio. Hoje em dia estas mesmas ondas nos propiciam mobilidade em um mundo cada vez mais sem distâncias. Na realidade as ondas de rádios já estavam presentes há algum tempo ao redor do mundo, mais foi através do aperfeiçoamento constante desta tecnologia que se pode chegar ao que hoje é definido como wireless. A palavra Wireless já vem sendo usada há algum tempo quando se refere a revolução tecnológica na área da comunicação [5].

A comunicação Wireless esta presente há um bom tempo no cotidiano. São exemplos de conexão sem fio; Bluetooth, InfraRed, WiMAX, telefones sem fio, entre outros. Uma outra tecnologia nova que desponta é a UltraWideband, que permite a transmissão de grande quantidade de dados sobre distâncias curtas mesmo contornando paredes. Existe no momento uma disputa pela definição deste protocolo entre Texas Instruments e Intel de um lado, e Motorola do outro. [5]

Padrão IEEE 802.11, possui variações, que para cada uma delas, existe uma determinada configuração: 802.11a (54Mbps a 5Ghz); 802.11b (11Mbps a 2,4Ghz); 802.11g (54Mbps a 2,4Ghz); e 802.11n (65Mbps a 600Mbps, freqüência de 2.4Ghz ou 5Ghz) [2].

Os protocolos utilizados para fazer a segurança destes padrões são: o WEP, que foi criado em 1999 por um grupo de voluntários membros da IEEE, que não eram especialistas em segurança, por isso o WEP veio com algumas falhas conhecidas, ele utiliza o algoritmo RC4 para fazer a criptografia dos dados. O WPA foi criado em 2003 para ser uma solução temporária, enquanto o grupo 802.11i desenvolvia um novo protocolo de alta segurança, o WPA e basicamente uma copia do WEP (rodando no

*Acadêmico do Curso de Sistemas de Informação da Universidade da Região da Campanha, Bagé, RS
** Professores do Centro de Ciências da Economia e Informática da Urcamp, Bagé, RS

mesmo hardware) e utiliza o RC4 com o TKIP para fazer a criptografia dos dados.[2]

Finalmente em 2004 o grupo 802.11i finaliza o protocolo denominado WPA2, sendo muito mais seguro ele utiliza o algoritmo AES o mesmo que era usado pelo governo do EUA, junto com o TKIP, esse protocolo necessita de co-processadores por exigir muito mais processamento que os protocolos anteriores.[2]

B. KISMET

O kismet é um analisador de rede (um sniffer), que pode identificar várias informações do Access Point. Ele pode ser usado tanto para observar as redes vizinhas e canais congestionados. É uma ferramenta de código-aberto, ele oferece um conjunto completo de testes de segurança, que pode ser usado tanto para verificar a segurança da sua própria rede, quanto invadir redes mal configuradas. As informações que ele consegue obter são: o número de redes sem fio, o número total de pacotes capturados pelas redes, os tipos de criptografias ou a ausência dela, o número de pacotes irreconhecíveis, o número de pacotes descartados e o tempo decorrido, quantos clientes estão conectados e seus respectivos MACs. [4].

Ele atua de forma passiva, ativando a placa sem fio em modo de monitoramento, mesmo os pontos que estão configurados para não mostrar o SSID e o tipo de criptografia são detectados, provando sua eficiência. O principal obstáculo para usar o Kismet é que ele é compatível com um número relativamente pequeno de placas, basicamente, apenas modelos baseados nos chips Orinoco, Prism, Intel IPW 2100, Atheros e Aironet. O Kismet funcionará com qualquer placa wireless que suporte o modo raw monitoring [4].

Na figura 1, pode-se observar que o Network list mostra os possíveis modos de monitoramento; neste estudo será utilizado o modo channel (as redes sem fio que estão sem segurança fica destacadas em amarelo.

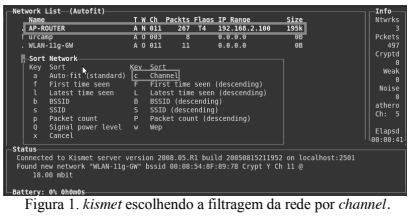

Figura 1. *kismet* escolhendo a filtragem da rede por *channel*.

1) RADIUS

O Radius é um servidor AAA (*authentication*, *authorization and accounting*) consolidado no mercado como uma solução robusta para diversos serviços de autenticação. Desenvolvido no início da década de 90, e sendo continuamente incrementado, o RADIUS ainda consegue satisfazer os requisitos das tecnologias emergentes, mas toda está adaptabilidade acaba gerando alguns problemas. No decorrer deste trabalho, serão explicados os conceitos principais que envolvem o RADIUS, o seu funcionamento e suas áreas de aplicação, os métodos de autenticação por ele providos, assim como suas deficiências, além disso, será abordado, o ainda não consolidado DIAMETER, que propõe algumas mudanças no atual RADIUS, para aumentar o grau de segurança e superar algumas limitações do mesmo [1].

III. EXPERIMENTOS

A. Teste de transferência

A figura 2 mostra o diagrama utilizado para processo de testes de transferência, foi utilizado um arquivo de 4MB, através de uma distribuição Ubuntu10.04 para outra distribuição Ubuntu10.04, por meio de dois rádios AProuter (em *bridge*) utilizando comando time scp; para tal teste de desempenho foi escolhido um arquivo que é uma música em MP3, onde foram feitas 7 transferências com cada protocolo IEEE 802.11, tais como: none (sem criptografia), WEP, WPA, WPA2.

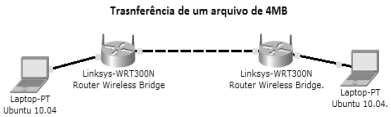

Figura 2. Rede de teste de transferência

A figura 3 apresenta o gráfico da latência e a tabulação dos dados colhidos nos testes de transferência com os protocolos IEEE 802.11, bem como o teste sem criptografia (*none*), onde foi calculada a média destes dados, buscando comparar a velocidade de transferência entre os mesmos, não sendo relevante neste momento o aspecto segurança, este experimento foi realizado para mostrar se existe alguma diferença de velocidade entre os protocolos de segurança, além do teste sem criptográfica com propósito de comparação de velocidade. Foi utilizado comando *time scp* para fazer a transferência de um arquivo de 4MB, este processo foi realizado sete vezes com: *none*, WEP, WPA, WPA2.

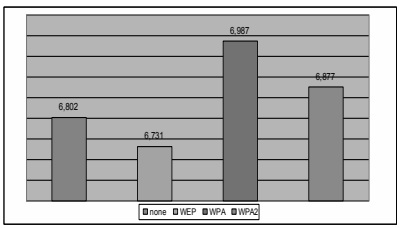

Figura 3. Média de velocidade de transferência dos protocolos.

IV. RESULTADOS

Foram feitos testes de transferência entre dois micros com Linux Ubuntu 10.04 para testar se havia alguma

diferença de desempenho entre os protocolos apresentados. Os resultados provaram que o método sem criptografia e o que usa WEP são praticamente iguais, já o método WPA provou ser o menos estável, com variações. Já o WPA2 provou ser o protocolo mais seguro e com mais estabilidade de conexão (ao que se refere ao tempo de transmissão e oscilação de pacotes). Ao realizar os procedimentos para a quebra do protocolo WEP, obtendo-se sucesso. Já no método WPA e WPA2, só pelo método "Dicionário", ou seja, tentativa e erro. Assim, entende-se que a melhor criptografia ser implementada nesta situação seria a criptografia WPA2+Servidor RADIUS (PPPoE).

O *Aircrack*-ng - é a principal coleção de ferramentas para o trabalho. Possui diversas ferramentas voltadas para ataques a redes sem fio IEEE 802.11.[3]

O Aircrack-ng foi utilizado porque contém todas as ferramentas necessárias para a realização de ataques ao WEP, sendo a ferramenta que realiza a quebra mais rapidamente, ele também altera a placa de rede sem fio para o modo *monitor* e faz obtenção dos pacotes até a realização do ataque. [3]

As principais ferramentas utilizadas foram:

- ***airmon-ng*** Altera uma placa de rede sem fio para o modo promíscuo (*monitor*);
- ***airodump-ng*** O *sniffer* de pacotes, faz a captura de pacotes os salva em um determinado arquivo .CAP;
- ***aireplay-ng*** O injetor de pacotes, para realizar ataques ativos para gerar tráfico;
- ***aircrack-ng*** Levando o nome do pacote, é o *cracker* que implementa os ataques descritos, pode funcionar em modo *on-line* (simultaneamente à captura) ou *off-line* (com um arquivo de captura salvo de outro momento).

A figura 4 mostra o *Aircrack-ng* e a chave devidamente descriptografada, pode-se observar que ele realmente quebra a chave WEP de *128bits*, o tempo para a quebra depende da quantidade de dados capturados, neste caso levou aproximadamente 5 minutos.

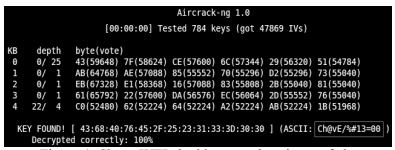

Figura 4. Chave WEP devidamente descriptografada.

coWPAtty - Está aplicação é usada para ações de ataque chamadas "*brute force*", para descobrir a chave WPA e WPA2. Ela simplesmente descarrega milhares de combinações alfanuméricas de um arquivo dicionário tentando que algumas coincidam e permitam a autenticação, para isso ela precisa que uma certa quantidade de dados sejam coletados para que possa tentar descobrir a chave.[6]

Na figura 5 pode-se observar que o *coWPAtty* encontrou a chave em seu dicionário.

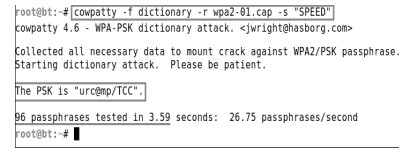

Figura 5. coWPAtty rodando, chave WPA2 encontrada.

A. Teste de logs no servidor freeRADIUS

A figura 6 mostra o teste de *logs* no servidor RADIUS, pode-se observar que todos os *logins* criados obtiveram sucesso.

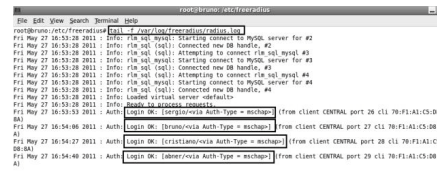

Figura 6. *logs* dos usuários no *free*RADIUS

V. CONCLUSÃO

De acordo com os métodos acima relatados neste artigo, em que foram aplicados testes para avaliar as vulnerabilidades relacionadas aos protocolos de segurança 802.11, controle por MAC e RADIUS. È importante enfatizar que todos os testes realizados obtiveram sucesso, no que tange a quebra ou acesso a conexão de redes *wireless*. Para a execução de tais testes, foram utilizadas as distribuições Linux baseadas em Debian: Ubuntu 10.04, BackTrack 5, Ubuntu Server 11.04. Além disso, foi necessário fazer o uso de ferramentas para filtragem e captura de dados/pacotes, tais como, o Aircrack-ng e o coWPAtty. Ainda podemos observar que todas estas etapas de configuração levam a uma possível implantação de um servidor RADIUS, no qual se pode integrar como um dos métodos de segurança relatados neste artigo. Outro aspecto que se deve destacar é que o WPA2 ainda é a melhor criptografia a ser aplicada. Assim um sistema de segurança que aplique um servidor RADIUS e o protocolo WPA2 torna-se um método misto mais seguro atualmente, prova disso, que tal pratica esta sendo usada por grande parte dos provedores de acesso a Internet, por exemplo, a OI, GVT e operadoras VOIP, entre outras.

Verificou-se que no presente artigo, o método de segurança de controle por MAC apresentou as seguintes vulnerabilidades: o controle por MAC é uma segurança relativamente fraca, pois utilizando o Kismet foi possível verificar todos os dados do AP, por exemplo, os MACs dos clientes conectados, o tipo de criptografia, quantos clientes estão conectados, o IP de cada MAC, o canal e o BSSID. Através destas informações pode-se clonar o MAC e se passar por um determinado cliente. Contudo, o controle por MAC é uma boa alternativa, ao invés de usar somente o SSID do AP, entretanto, se for utilizado em

conjunto com uma criptografia do tipo WPA2, seria um método muito mais seguro.

Na criptografia WEP, com a utilização do aircrack-ng foi demonstrado a grande vulnerabilidade deste protocolo, que pode ser realmente quebrado com um ataque de força bruta em poucos minutos, contudo, a WEP foi a 1° criptografia criada em 1999 e foi uma criptografia segura por algum tempo, uma vantagem é que ela utiliza menos processamento, a transferência de arquivos e mais rápida que os demais protocolos apresentados abaixo, sendo uma opção ainda melhor do que só utilizar controle por MAC.

No WPA já foram feitos outros tipos de ataques, devido à vantagem de que ele não pode ser quebrado utilizando força bruta, entretanto, a grande vulnerabilidade deste protocolo é o ataque por dicionário (tentativa e erro), foi utilizado para o ataque o aircrack-ng junto com o coWPAtty (usado para ataques de dicionário) foi demonstrado que se caso o dicionário usado não tiver a chave certa, não conseguirá obter a chave. Já se o dicionário tiver a chave, ele descobrirá em segundos. Contudo, o WPA é uma criptografia segura se for utilizada uma chave complexa. Para se proteger deste tipo de ataque, o ideal é que seja utilizada uma chave com, no mínimo, 20 caracteres alfanuméricos.

Com o WPA2 foi realizado, praticamente, o mesmo processo utilizado para descobrir a chave WPA, tendo como a grande vulnerabilidade o ataque por dicionário. Este protocolo tem um ponto negativo, necessita-se de um processador mais robusto, pelo fato de um maior processamento requerido para executar algoritmos mais complexos. Este protocolo é o mais seguro atualmente, pode-se configurar uma chave de até 64 caracteres alfanuméricos e quanto maior a chave mais processamento será necessário, sendo ratificado em 2004 pela IEEE ele veio para substituir o WPA e suas vulnerabilidades, sendo o protocolo mais estável até o momento.

E finalmente uma das maiores referências em segurança: o RADIUS, este tipo de segurança quando bem implementada torna a rede muito segura, neste trabalho foi utilizado o freeRADIUS para a implantação na empresa Alternet (provedor de Internet em Bagé/RS), para fazer as autenticações *wireless*, utilizando o Mikrotik como *Access Point* - PPPoE, ou seja, o cliente manda a solicitação com login e *password* para o Mikrotik que redireciona para o servidor freeRADIUS na Alternet, que irá checar na base de dados do Mysql se este usuário existe, se sim, irá permitir o acesso desse cliente a Internet.

Ao encerrar este artigo, conclui-se, então que a melhor segurança atualmente em redes sem fio é a utilização da criptografia WPA2, servidor RADIUS junto com um banco de dados para o armazenamento dos dados dos clientes (*login*, *password*, *IP address* e *netmask*)

Referências

[1] CARVALHO, Hugo Eiji Tibana. RADIUS. Trabalho Desenvolvido Para a diciplina de Redes de Computadores, UFRJ, 2008.

[2] GIMENES, Eder Coral. Segurança de Redes Wireless. Monografia apresentada ao Curso Tecnólogo em Informática com ênfase em Gestão de Negócios. FATEC: Mauá, SP, 2005.

[3] MITSUYA, Yuko. Usando Kismet e Aircrack-ng para explorar vulnerabilidades em Redes Sem Fio. Monografia apresentada na Universidade do Pará Santarém, PA, 2009.

[4] Kismet. Disponível em: <http://www.hardware.com.br/termos/kismet> Acesso em: 9 jun.2011.

[5] O que é wireless, História da wireless. Disponível em: <http://ensite.com.br/index-3.html >. Acesso em: 3 jun. 2011.

[6] Wireless - Como driblar a segurança. Disponível em: <http://pplware.sapo.pt/windows/software/wireless-como-driblar-a-seguranca/>. Acesso em: 4 jun. 2011.