SEGURANÇA DE MÉTODOS DE AUTENTICAÇÃO EM REDES SEM FIO.

Paulo Eduardo Aparecido Manoel dos Santos[1], José Roberto de Almeida[1]
[1]Universidade de Uberaba - UNIUBE, Uberaba - Minas Gerais
pauloedaparecido@hotmail.com.br; jose.almeida@uniube.br

Resumo
Nos dias atuais a maioria das empresas faz o uso da tecnologia de redes sem fio, devido à mobilidade que proporcionam ao se conectar à internet em um ambiente de trabalho. A segurança quanto à utilização de redes sem fio se inicia no processo de autenticação e associação em uma rede, utilizando os métodos de autenticação de sistema aberto ou autenticação de chave compartilhada. Este artigo refere-se as falhas de segurança à infraestrutura de redes sem fio e apresenta alguns métodos de autenticação.

Palavras-chave: Redes Sem Fio. Segurança. Mobilidade.

1 Introdução

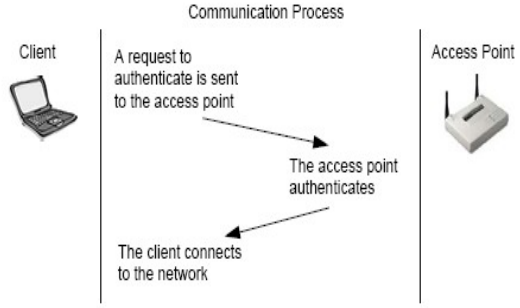
Em 1888, um físico cujo nome é Heinrich Rudolf Herz, conseguiu produzir sua primeira onda de rádio começando a descobrir uma das tecnologias mais utilizadas atualmente. Alguns anos depois após a descoberta, esta forma de ondas de rádio se tornou um meio de comunicação, abrindo o caminho para rádio, televisão e radares com a descoberta das ondas eletromagnéticas. Após a descoberta das ondas eletromagnéticas um pesquisador Italiano chamado Guglielmo Marconi Marchese, conseguiu ampliar o raio de ondas para uma distância de duas milhas. Após 1899, este mesmo pesquisador conseguiu enviar um sinal a uma distância de 9 milhas. Em 1901, uma descoberta muito importante até mesmo para a globalização, foi que Marconi conseguiu enviar sinais através do Oceano Atlântico (LIFESTYLES, 2013).

A aproximação entre comunicação móvel e internet aconteceu no fim dos anos 90, com a chegada do SMS, um serviço de celular que permite enviar mensagens curtas. As operadoras que ofereciam este serviço no Brasil estavam disponíveis em poucos estados, mas naquela época já se pensavam que, em um futuro próximo, poderiam escrever e enviar *e-mails* através do celular. Conectar um prédio ao outro tradicionalmente significava lançar cabos de dados através do solo, mas com a chegada da transmissão a rádio isto se tornou bem mais simples. Esta tecnologia se expandiu de tal forma que a maioria das pessoas possui um aparelho eletrônico que utiliza a comunicação sem fio. Mas, não se pode esquecer a segurança que deve-se ter ao utilizar as redes sem fio, pois a maioria dos crimes cibernéticos se inicia com *hackers* que tentam se conectar em redes de corporações em busca de informações valiosas em sistemas que contém dados importantes. O objetivo deste artigo é apresentar alguns métodos de autenticação que são necessários para que um dispositivo se conecte a rede com segurança em um ambiente empresarial, tais como autenticação de sistema aberto e autenticação de chave compartilhada.

2 Materiais e Métodos

Na autenticação de sistema aberto, o processo é realizado através do SSID do cliente e do *Access Point* (AP). A primeira solicitação de autenticação é realizada pelo cliente que contém um identificador, que seria o MAC de sua placa de rede. Isso é seguido de uma resposta do roteador que retorna ao dispositivo uma mensagem de êxito ou falha. A falha geralmente pode ocorrer devido ao roteador não possuir ou for excluído o endereço MAC do dispositivo nas configurações do AP. O processo é, portanto, bastante simples, conforme ilustra a Figura 1.

Figura 1: Processo de sistema aberto



Fonte: Battisti (2015)

Podemos citar também a opção de usar *Wired equivalent privacy* (WEP) que neste método não é de utilidade obrigatória para criptografar o processo, mas de acordo com a Intel (2006), WEP não é recomendado para uma WLAN segura devido às suas vulnerabilidades inerentes. Um dos principais riscos de segurança é que um *hacker* capture a forma criptografada de um quadro de resposta de autenticação, usando aplicativos de software amplamente disponíveis e usando as informações para descobrir a criptografia WEP.

Autenticação de chave compartilhada, ao contrário do método citado anteriormente, neste método se faz o uso obrigatório de WEP.

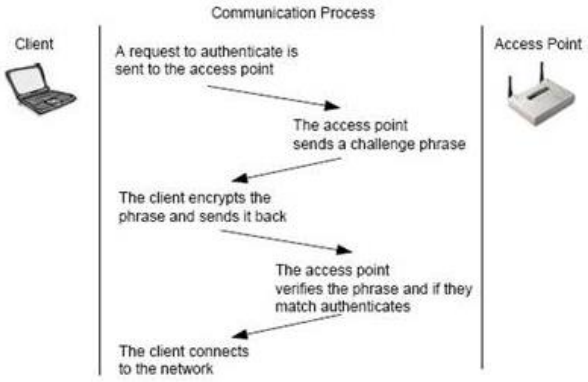
A criptografia WEP usa chaves tanto no cliente quanto no AP, e elas devem ser as mesmas para que o WEP possa operar. Essas chaves são configuradas manualmente.

O processo ocorre quando o cliente faz um pedido de associação ao AP (Esse passo é o mesmo da autenticação de sistema aberto). O AP envia uma pergunta ao cliente, sendo que essa pergunta é um texto gerado aleatoriamente e enviado ao cliente na forma de texto puro. O cliente responde a essa pergunta e a chave WEP do cliente é usada para criptografar a pergunta e, para finalizar, a mesma é enviada já codificada de volta ao AP. O AP responde a resposta do cliente. A resposta codificada enviada pelo cliente é então decodificada usando a chave WEP do AP, verificando assim se o cliente tem a mesma chave. Se a chave do cliente é a correta, o AP responderá positivamente e autenticará o cliente. Se a chave do cliente não for a correta, o AP responderá negativamente e não autenticará o cliente. (BATTISTI, 2015).

O processo de chave compartilhada é mais complexo, porém não significa que seja mais seguro (INTEL, 2006).

A Figura 2 representa o processo de chave compartilhada.

Figura 2: Processo de chave compartilhada.



Fonte: Battisti (2015)

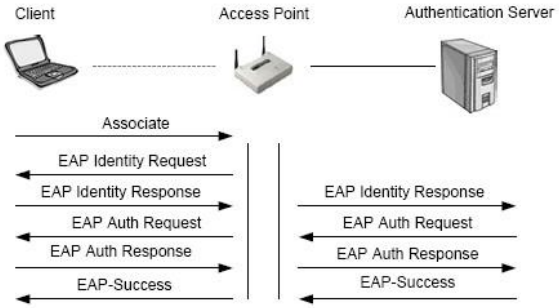
O padrão de autenticação 802.1x é mais utilizado em organizações, pois não se trata apenas de uma autenticação no roteador, mas se faz necessário a utilização de um servidor de autenticação para que a mesma seja configurada.

Tipicamente a autenticação dos usuários é realizada usando um servidor RADIUS e algum tipo de base de dados de usuários para validação dos mesmos. O novo padrão 802.1i, também conhecido como WPA, inclui suporte a 802.1x, EAP, AAA, autenticação mútua e geração de chave, e nenhum desses foi incluído no padrão original 802.11 (BATTISTI, 2015).

No modelo 802.1x padrão, a autenticação depende de três partes importantes, ou seja, requisitante (cliente), o autenticador (AP) e o servidor de autenticação (RADIUS).

A Figura 3 exemplifica basicamente este processo de autenticação.

Figura 3: Processo de autenticação RADIUS



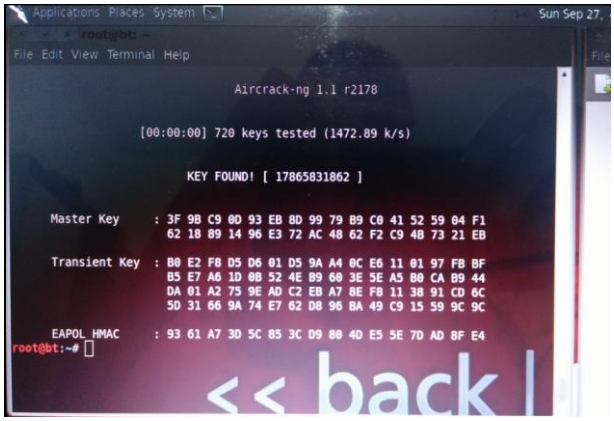
Fonte: Battisti (2015)

A apresentação de Peres (2012), diz que o AP serve como um NAS (*Network Access Server*), a comunicação ocorre entre o cliente e o servidor RADIUS, em que este último informa ao AP o resultado da autenticação.

3 Resultados

Para iniciar os testes de quebra de senhas criptografadas, foi necessária a instalação de uma distribuição *Linux* cujo nome é *BackTrack*, sendo que a versão utilizada nos testes foi a *BackTack 5 R3*. Este sistema operacional (SO) é gratuito e executado através de um CD/DVD ou USB. Trata-se de um SO baseado no *Debian*, focado apenas para testes de segurança e testes de penetração, utilizado por *hackers* e analistas de segurança, sendo executado através de um CD/DVD, dispositivos removíveis USB, máquinas virtuais ou simplesmente através do *Hard Disk*. Com o SO em execução, utilizou-se uma ferramenta chamada *AirCrack* que por padrão já está atribuída a esta distribuição *Linux*. Esta poderosa ferramenta pode ser também instalada separadamente na distribuição *Ubuntu* 14.0. Em geral, o programa realiza uma comunicação com o AP, envia pacotes para o mesmo equipamento e salva estes pacotes em um arquivo. Se faz necessário baixar um arquivo com extensão ".txt", que tem a função de ser uma espécie de dicionário para o *AirCrack*. Este arquivo pode ser facilmente encontrado na internet e baixado livremente. O *AirCrack* valida linha por linha e as *strings* dessas linhas são enviadas para o AP e validadas suas autenticidades. Ao encontrar uma linha válida, o *AirCrack* apresenta a mensagem conforme ilustra a Figura 4.

Figura 4: Quebra de senha *AirCrack*



Fonte: Elaborado pelo autor.

A quebra de senha foi realizada com sucesso nos seguintes métodos de autenticação: WEP, WPA e WPA2.

4 Discussão

Durante a análise, percebeu-se que o fator mais importante para que a quebra de senha seja concluída com sucesso, é o arquivo que o *AirCrack* utiliza como dicionário. Neste caso, se a senha para autenticação estiver dentro arquivo, o *software* irá apresentar a mesma. Caso a senha autenticadora não esteja gravada no arquivo, o *software* não conseguirá descobrir a senha. Este método não oferece garantia total de que o *hacker* descubra a senha. Mas, é uma boa ferramenta para quem está iniciando na área de segurança da informação.

5 Conclusão

Com este estudo breve de redes sem fio, foi possível conhecer melhor o processo de autenticação de algumas criptografias e a segurança que as mesmas proporcionam. Na realização dos testes nas criptografias WEP, WPA e WPA2, percebeu-se que os usuários estão totalmente vulneráveis para que *hackers*

obtenham dados facilmente. Sendo assim, o método de autenticação menos vulnerável é o RADIUS, que deve ser utilizado por empresas, pois para que dispositivos se conectem em sua rede, é estritamente necessário que o equipamento esteja no domínio da empresa, em que este método valida com o servidor de *Active Directory* da empresa, criando mais uma barreira para que *hackers* não acessem dados da rede configurada.

Referências

BACKTRACK-LINUX. **BackTrack** Linux. Disponível em: <http://www.backtrack-linux.org/>. Acesso em: 22 set. 2015.

BATTISTI, Júlio. **Redes Wireless** – Parte XXI. 2015. Disponível em: <http://juliobattisti.com.br/tutoriais/paulocfarias/redeswireless021.asp>. Acesso em: 19 set. 2015.

INTEL CORPORATION. **Rede sem fio**. 2006. Disponível em: <http://www.intel.com/support/pt/wireless/wlan/sb/cs-025307.htm>. Acesso em: 22 set. 2015.

LIFESTYLES. **A história da rede sem fio**. 2013. Disponível em: <http://www.lifestyles.com.br/index.htm/2013/02/a-historia-da-rede-sem-fio/>. Acesso em: 19 set. 2015.