SEGURANÇA DE REDES SEM FIO 802.11: ANÁLISE DAS VULNERABILIDADES SOBRE A ÓPTICA DA SEGURANÇA DA INFORMAÇÃO

Rogério Augusto Pokojski de Souza [1], ***Claudineia Helena Recco***[1], **Marcelo Eloy Fernandes**[1]

[1]Departamento de Pós-Graduação– *Universidade Nove de Julho, UNINOVE 01156-050, São Paulo - SP* – Brazil

{*rogerkazaa*, chrecco, marceloeloyfernandes}@gmail.com

Abstract. *The security of wireless networks, specifically in the context of the analysis of the vulnerabilities found with the use of this technology, governed on the basis of the basic principles of information security and directing the established norm of the standard IEEE 802.11. Presents the general aspects of wireless networking technology, showing its main characteristics and patterns developed by entities specified, the factors of vulnerabilities of specified protocols in wireless networks, the possible loopholes and glitches that will facilitate the intrusion of various types of attacks. the methods of attacks that can compromise and weaken the security environment of a particular wireless network, the mechanisms of protection and defense employed to prevent or mitigate the risks, in the emergence of an attack or an existing fault.*

Resumo. *A segurança de redes sem fio, no âmbito da análise das vulnerabilidades encontradas com o uso desta tecnologia, regido com base nos princípios básicos da segurança da informação e direcionando à norma estabelecida do padrão da IEEE 802.11. Apresenta-se os conceitos gerais da tecnologia de redes sem fio, mostrando suas características principais e padrões elaborados por entidades especificadoras, os fatores de vulnerabilidades, seja em dispositivos de configuração de padrão de fábrica ou nos protocolos especificados em redes sem fio, as possíveis brechas e falhas que facilitará a intrusão de diversos tipos de ataques, os métodos de ataques que podem comprometer e fragilizar o ambiente de segurança de uma determinada rede sem fio, mecanismos de proteção e defesa empregados para impedir ou mitigar os riscos, no surgimento de um ataque ou uma falha existente.*

1. Introdução

As redes de computadores surgiram para um objetivo essencial: o compartilhamento dos dados entre computadores, distantes um dos outros através de uma rede cabeada. Assim, qualquer tipo de informação teria o acesso imediato.

Com a evolução dos dispositivos móveis, houve a necessidade de interconectá-los com a internet, de forma que sua mobilidade permanecesse. Foi então que se iniciou o desenvolvimento de um conceito de rede empregando radiofrequência, capaz de transmitir informações e possibilitando a conexão com a internet, onde quer que esteja, a partir de um ponto de acesso à rede sem fio.

Naturalmente, na mesma forma das redes cabeadas, no início dessa tecnologia não se tinha nenhum tipo de proteção, além disso, as redes sem fio eram totalmente abertas, sem nenhuma restrição. Segundo ASSUNÇÃO (2013, p.15) "Hoje possuímos novas medidas de segurança e controle como o WPA2, servidores de autenticação RADIUS, sistemas de prevenção a intrusos Wireless (WIPS) e outras parafernálias".

Mesmo com medidas de segurança e controle referidas no parágrafo acima, a rede sem fio não é 100% segura. Diversas vulnerabilidades podem ser exploradas através de má configuração dos dispositivos de rede sem fio, como o Access Point, brechas e falhas de criptografia como, por exemplo, dispositivos legados que utilizam a criptografia WPA (Wi-Fi Protected Access), entre outros.

De acordo com CAMPOS (2006, p.16) "Uma vez que a informação representa valor e, consequentemente, contribui diretamente para a geração de lucro, é possível afirmar, então, que a informação é um bem, um ativo da organização e, como tal, dever ser preservado e protegido." Partindo deste pressuposto, almejamos com esta pesquisa evidenciar as vulnerabilidades presentes na tecnologia de redes sem fio e compreendendo os resultados obtidos desse levantamento, no sentido de identificar técnicas e boas práticas para a proteção das informações.

Será realizada a análise das vulnerabilidades que são encontradas nas redes sem fio focando os princípios fundamentais da segurança da informação (confidencialidade, integridade e disponibilidade).

Analisar as vulnerabilidades e descrever maneiras possíveis de proteção nas redes sem fio 802.11, conforme os princípios da segurança da informação.

Entender os princípios fundamentais e conceituais de uma rede sem fio, através de informações sobre a norma aplicada e as técnicas do seu funcionamento.

Relatar as vulnerabilidades presentes que estão nessa tecnologia de rede sem fio, seja em equipamentos de configuração padrão de fábrica ou brechas em protocolos de criptografia.

Discorrer sobre os principais ataques que podem acontecer neste ambiente tecnológico.

Demostrar os principais meios de proteção, monitoramento e formas de defesas para possíveis ataques.

Nos últimos anos, a tecnologia de redes sem fio tem sido bastante difundida e explorada, com isso, trouxe consigo preocupações e problemas com inúmeros ataques ocorridos, visando a fragilizar e afetar a segurança das informações transportadas neste ambiente sem fio.

Nesse sentido, a presente pesquisa tem o propósito de detalhar especificamente a rede sem fio 802.11, que é a norma definida amplamente utilizada em redes domésticas e corporativas, propondo a expor as vulnerabilidades mais comuns encontradas em redes deste tipo e demostrando formas, bem como métodos para proteção, monitoramento e defesa, garantindo que as informações trafegadas nelas sejam seguras, respeitando os princípios da segurança da informação.

No processo de elaboração deste trabalho, partimos de hipóteses que se remetem a questões como:

a) Com a evolução tecnológica surgiram padrões que auxiliaram a rede sem fio a ter uma alta performance e gerenciamento de transmissão dos dados.

b) As técnicas de ataques contribuem para o desenvolvimento de uma base de conhecimento, afim de elaborar métodos de defesa e segurança em redes sem fio.

c) Procedimentos básicos, como evitar a utilização de senhas padrões e fáceis de serem quebradas, são formas de proteções cruciais ao uso desse ambiente de rede sem fio.

d) A rede sem fio bem configurada e devidamente protegida pode ser utilizada sem riscos iminentes de perdas de informações.

Para o desenvolvimento desse artigo foi escolhida a pesquisa qualitativa e bibliográfica, pois para discorrer o trabalho será necessário um levantamento bibliográfico e, especificamente, em segurança de redes sem fio, com fontes devidamente confiáveis, constituídas na base de livros, dissertações, monografias e sites relacionados à área de segurança da informação.

A pesquisa abrangerá os conceitos sobre a rede sem fio e como proceder sobre falhas incididas, e de que forma será necessário à implementação dos mecanismos de proteção e defesa sobre a perspectiva da Segurança da Informação. Para isso, espera-se obter o máximo de informações e dados possíveis, de forma adequada, para determinarmos quais os pontos chaves deverão ser demostrados, na perspectiva de um entendimento holístico desse assunto.

2. CONCEITOS GERAIS DE REDES SEM FIO

Para um bom entendimento do assunto sobre redes sem fio, vamos brevemente discorrer alguns conceitos gerais sobre as redes de computadores. Para ALECRIM (2013, s/p), as redes de computadores foram criadas com intuito de compartilhar informações entre computadores distantes um dos outros. As informações eram transmitidas por uma interface de rede (placa de rede) através de cabos (coaxiais ou de par trançados) dentro de uma infraestrutura planejada (eletrodutos, calhas, entre outros). Entretanto, foi notado alguns obstáculos para o uso dessa rede cabeada:

- ✓ Algumas impossibilidades de alterações do ambiente físico para a passagem de cabos;
- ✓ Limitações da transmissão do sinal em uma determinada distância, por exemplo, cabo de rede UTP só aceita transmissões dos sinais até 100 metros.

Visto os obstáculos encontrados na rede cabeada, houve a necessidade de empregar o conceito de rede que utiliza sinais de frequência, possibilitando a transmissão de informações em lugares onde não se permitia essa interconexão, estamos nos referindo às redes sem fio (wireless).

A ideia inicial das redes sem fio, segundo RUFINO (2007, p.13) partiu do conceito de complemento das redes cabeadas, correspondendo à necessidade de facilitar a expansão das redes locais de um determinado ambiente físico, sendo doméstico ou corporativo. Outras questões que levaram a iniciação dessa tecnologia foi praticidade física ao ser instalada, pois, não necessita de uma infraestrutura de cabeamento. Também temos outros fatores que influenciaram o surgimento das redes sem fio, segundo ASSUNÇÃO (2013, p.17): a mobilidade (utilizar aparelhos móveis em qualquer lugar sem perder a conexão), redução de custo (como citado anteriormente, sem que houvesse a preocupação em cabear toda a estrutura do ambiente) e aplicação de alguns conceitos da rede cabeada.

Atualmente, segundo ASSUNÇÃO (2013, p.17) existe uma extensa quantidade de dispositivos que usam redes sem fio em qualquer tipo de ambiente (doméstico ou corporativo). Entre os principais podemos citar: tablets, smarthphones, notebooks, Tvs e videogames.

Para que existisse essa infinidade de produtos e fabricantes de tal tecnologia, foi preciso o desenvolvimento de padrões específicos que tornaram os equipamentos compatíveis entre si. Conforme ASSUNÇÃO (2013, p.18) existem duas entidades que determinam padrões relativos às redes sem fio:

- ✓ IEEE – Instituto de Engenheiros Elétricos e Eletrônicos: Responsável pelas padronizações tecnológicas e protocolos referentes às telecomunicações, entre os quais, administra o Projeto 802, padrão desenvolvido que define as arquiteturas de redes de computadores, pela qual o padrão 802.11 corresponde à WLAN (redes locais sem fio);
- ✓ Wi-Fi Alliance: Antes chamado de WECA, esse consórcio é responsável por testar e certificar produtos, para que os mesmos apresentem padrões de qualidade.

2.1. FREQUÊNCIAS

Para RUFINO (2007, p.17) uma definição básica do termo frequência pode ser dita como a representação do número de ondas completas que incidem em um ponto fixo,

incorporado a um período de tempo, ou seja, o comprimento da onda. Esse processo é medido em ciclos por segundo, representada pela unidade de medida Hertz (Hz).

Conforme RUFINO (2007, p.18), a frequência do sinal está ligada, de maneira direta, com o tamanho da distância percorrida do sinal, propagado pelo ar. Isto é, quanto menor for a distância que o sinal percorre, maior será a frequência.

Os sinais de frequência utilizados em dispositivos de redes Wi-Fi, em determinadas situações, podem ser submetidos a diversas interferências. Uma delas, segundo ASSUNÇÃO (2013, p.26) é quando a banda usada que é de 2.4 GHz, pois há outros equipamentos que podem sobrepor no mesmo canal dos dispositivos wireless. O mais adequado de se evitar essas interferências é uso de dispositivos wireless que usam o canal de frequência de 5 GHz.

Os sinais de frequência não são usados exclusivamente para transmissão de dados em rede sem fio. Existem outros tipos de serviços, tais como: transmissões de estações de rádio e televisão, operadoras de telefonia móvel e de uso militar.

2.2. CANAIS

Segundo RUFINO (2007, p.18) um espectro de frequência pode ser dividido em intervalos (faixas) que são reservados para determinados serviços, regulamentados através dos órgãos internacionais e agências de regulamentação, no Brasil esse órgão é a ANATEL. Subdividindo uma faixa em várias frequências menores, é permitido que a mesma possa ser transmitida paralelamente com sinais diferentes para cada faixa. Essa subdivisão de faixas para frequências menores é chamada de canais.

Em suma, canais são espaços que auxiliam o transporte do sinal gerado por um transmissor, para qual, a informação contida nesse sinal seja entregue ao um receptor.

2.3. PADRÕES IEEE 802.11

De acordo com RUFINO (2007, p.25) “O Institute of Electrical and Electronics Engineers (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio”.

O grupo de trabalho em questão foi denominado 802.11. Segundo RUFINO (2007, p.25), esse grupo reúne várias especificações que definem basicamente como a comunicação entre dispositivos clientes e Access Points deverão operar.

Com o passar do tempo foram criadas várias características técnicas e operacionais sobre os padrões. Os padrões mais comuns que definem a norma 802.11 serão descritas na ordem que foram especificadas, conforme o quadro 1:

Quadro 1: Padrões de 802.11 de Redes Sem Fio.

Padrões 802.11	Taxa máxima de transmissão	Frequência	Compatibilidade com outros padrões
802.11	1 e 2 Mbps	2.4 Ghz	Não
802.11a	54 Mbps	5 Ghz	Não
802.11b	11 Mbps	2.4 Ghz	Não
802.11g	54 Mbps	2.4 Ghz	802.11b
802.11n	600 Mbps	2.4 Ghz/5 Ghz	802.11a/b/g
802.11ac	1.3 Gbps	5 Ghz	802.11a/n
802.11ad	7 Gbps	60 Ghz	Não definido

Fonte: Elaborada pelo autor.

3. VULNERABILIDADES EM REDES SEM FIO

Cada vez mais as redes sem fio vêm se tornando indispensáveis para o nosso cotidiano. Para RUFINO (2007, p.13) a conveniência dessa tecnologia é inegável, visto que em vários lugares como aeroportos, praças de alimentação e hotéis proporcionam conexões para o acesso à internet via redes sem fio, para qualquer um que possua um dispositivo móvel. Esses locais públicos que disponibilizam acesso às redes sem fio são conhecidos como hotspot.

As novidades tecnológicas que surgem com o foco de facilitar a comodidade dos seus usuários poderão trazer consigo preocupações, no que se refere à segurança da informação no decorrer do seu uso. Isso não é diferente com as redes sem fio.

Segundo RUFINO (2007, p.13) com a facilidade na montagem dessas redes e muitas das vezes sem precisão nos termos técnicos para realizar tal tarefa (diferentemente das redes cabeadas), muitos dos usuários (inclusive empresas e

comércios, em geral) preferem realizar a instalação dos equipamentos com a permanência da configuração padrão de fábrica, acreditando que o ato de retirar o access point ou roteador wireless da caixa e ligá-lo, já seja o suficiente para o pleno funcionamento. Devido a isso, às redes sem fio instaladas poderão ser extremamente vulneráveis, apresentando riscos e ameaças as informações trafegadas nelas.

Uma outra forma de vulnerabilidade que podemos discorrer, são as falhas e brechas encontradas nos protocolos WEP, WPA e WPA2. Essas vulnerabilidades possibilitam a promoção de diversos tipos de ataques hackers em dispositivos equipados com tais criptografias. O quadro 2 a seguir, demonstra os protocolos de criptografia existentes, apresentando o ano que foram implementados, os objetivos e suas vulnerabilidades reveladas.

Quadro 2: Vulnerabilidades dos Protocolos de Criptografia.

Protocolos	Ano	Objetivo	Vulnerabilidade
WEP	1997	- Fornecer segurança no mesmo nível que as redes cabeadas; - Aplicar dois tipos de modos de autenticação: OSA e SKA.	- Tamanho menor da chave; - Reutilização da chave estática; - Não utiliza autenticação mútua; - Sem autenticação em nível de usuário.
WPA	2003	- Providenciar dois tipos de processos distintos de autenticação: Modo Personal e Modo Enterprise; - Identificar problemas nos dados através do CRC.	- Fragilidade no algoritmo de combinação de chave; - Chave Pré-Compartilhada susceptível aos ataques de dicionário; - Riscos sobre ataques de Negação de Serviço.
WPA 2	2004	- Melhorar o método de criptografia.	- Ataques de Negação de Serviço; - Passphrase da chave PSK pequena.

Fonte: Elaborada pelo autor.

Segundo ASSUNÇÃO (2013, p.16) as vulnerabilidades poderão estar presentes em uma configuração aberta, sem nenhum tipo de mecanismo de segurança (padrão de fábrica) ou em uma configuração técnica definida, porém, fragilizada e não protegida com o devido cuidado.

Para que as vulnerabilidades apresentadas aqui sejam evitadas ou mitigadas deverão estar na óptica dos princípios básicos da segurança da informação. Esses princípios básicos segundo CAMPOS (2007, p.30) são:

- ✓ Confidencialidade: garante que as informações confidenciais fiquem acessíveis apenas para usuários autorizados ao seu acesso;
- ✓ Integridade: garante que a informação seja integra e protegida de modificações ou destruições por usuários não autorizados;
- ✓ Disponibilidade: assegurar o acesso e o uso das informações dos usuários autorizados, sempre que for necessário e sem interrupções.

4. TÉCNICAS E MÉTODOS DE ATAQUE

Vejamos a seguir, técnicas e métodos de ataque mais relevantes que permitem estudar e investigar diversas formas de vulnerabilidades já citadas nesse trabalho, além disso, ajudará a nos compreender quais são as maneiras possíveis de ocorrer o comprometimento em um ambiente de rede wireless.

4.1. ATAQUES DE QUEBRA DE CHAVES

O conceito desses ataques é primordial para o procedimento inicial de intrusão em uma rede wireless, sobretudo na quebra das chaves WEP e WPA/WPA2.

Segundo LACERDA (2006, p.5), no WEP as chaves são estáticas, tanto no processo de autenticação quanto na criptografia, e como vimos nas Vulnerabilidades WEP no tópico 2, proporcionam ataques de força bruta. Já no WPA/WPA2 ataques de dicionário sobre a chave pré-compartilhada (PSK), poderão quebrar a chave quando forem relacionadas com um arquivo de wordlist.

A seguir veremos conceitualmente esses dois tipos de ataques:

- Ataques de Força Bruta: Técnica de ataque, apesar de ser bem antiga, ainda é possível o atacante ter êxito com a mesma. Conforme LACERDA (2006, p.4), o ataque de força bruta consiste em quebrar um esquema de criptografia utilizando tentativa e erro de caractere por caractere exaustivamente, com objetivo de decifrar a senha da rede sem fio. Embora o emprego desse ataque traga

resultados, principalmente em redes que não tem uma segurança adequada, é muitas vezes, pouco essencial, pois segundo LACERDA (2006, p.4), “o número esperado de tentativas para decifrar com sucesso a chave é geralmente metade das possíveis combinações”.

- Ataques de Dicionário: Conforme ASSUNÇÃO (2013, p.113) necessitam do uso de uma wordlist (lista de palavras), que basicamente consiste em um arquivo contendo milhares de palavras ou senhas padronizadas. Fundamentalmente, esse tipo de ataque, segundo ASSUNÇÃO (2013, p.48) possibilita, pelo intermédio do ataque de AP Spoofing, decifrar a chave de rede através da captura de uma parte do handshake do WPA/WPA2. Com o handshake interceptado, aplicaremos o ataque de dicionário através da wordlist, comparando uma a uma, as palavras contidas desse arquivo, para ver se existe alguma correspondência entre as mesmas.

4.2. NEGAÇÃO DE SERVIÇO (DoS)

Como o próprio nome diz, ataque de Negação de Serviço (Denial of Service – DoS) de acordo com LACERDA (2006, p.5) consiste em torna algum serviço ou recurso inacessível. Em redes sem fio, os ataques de negação de serviço são riscos bastante preocupantes, principalmente no que se diz respeito a um dos princípios básicos da segurança da informação: disponibilidade.

Esse tipo de ataque poderá ser executado por atacantes que estejam em qualquer parte da área de abrangência da rede sem fio e podem ser distintos em duas formas (ataques da camada física e ataques de desassociação/desautenticação):

- Ataques da Camada Física: Ataques que visam afetar a camada física do modelo OSI, geralmente são realizados no intuito de sobrecarregar o espectro wireless em um ambiente específico. Este tipo de ataque tem como o objetivo de capturar o tráfego dessa rede e/ou a recusa do serviço disponibilizado à comunicação da mesma;
- Ataques de Desassociação/Desautenticação: Consiste no atacante injetar pacotes de pedido de desassociação à estação cliente Wi-Fi (vítima). Esses pacotes farão o término da associação existente entre a estação cliente Wi-Fi (vítima) e o

Access Point (AP), pois a desassociação é uma notificação e não poderá ser recusada.

4.3. ATAQUES ESPECÍFICOS

Discutiremos neste momento, ataques com o foco mais específico, podendo ser ataques mais embasados em brechas, como é o caso do ataque ao WPS ou ataques que interveem entre os lados da conexão como o Man-in-the-Middle:

- Ataque ao WPS: O atacante se utiliza de uma brecha (revelada em dezembro de 2011), onde o mesmo, consegue recuperar o código PIN, em pouquíssimas horas, por meio de ataque de força bruta. Provavelmente essa vulnerabilidade acontece, segundo ASSUNÇÃO (2013, p.144), porque todos os "pins" são numéricos e o ataque de força bruta fará combinações possíveis para encontrar o número de 8 dígitos. Além disso, o último dígito do PIN é o valor de checksum, que calcula os 7 dígitos iniciais, e assim reduz a quantidade de combinações verificadas de 10^8 para 10^7, simplificando muito o processo de quebra da chave por ataque de força bruta. Em poucas palavras, o mais recomendado para equipamentos que possui o WPS, é deixá-lo desabilitado, pois segundo MORAIS (2013, p.9) "um esquema de segurança que era razoavelmente seguro se tornou inseguro pelo seu uso";
- Ataques Man-in-the-Middle (MITM): Esses ataques poderão ocorrer de duas formas: AP Spoofing (segundo ASSUNÇÃO (2013, p.51), consiste em criar um AP falso (com a mesma SSID e BSSID do verdadeiro), que poderá desautenticar a estação cliente com o AP legítimo) e o Multipot (abreviação de Múltiplos Honeypots, consiste na criação de vários AP Spoofings através de ferramentas de softAPs, permitindo que o dispositivo cliente wireless caia em alguma AP falso).

5. MÉTODOS DE PROTEÇÃO E DEFESA

As vulnerabilidades que analisamos demonstram como a fragilidade das redes sem fio podem liberar brechas, que possibilitam a ocorrência de diversos tipos de ataques, atingindo os princípios fundamentais da segurança da informação.

Para contornar esse tipo de situação, precisamos implementar métodos e soluções de segurança capazes de impedir acessos indevidos, mitigar riscos e eliminar a falsa sensação de segurança, pois ASSUNÇÃO (2013, p.170) revela que “o pensamento que temos de ter é: a nossa rede nunca vai ficar 100% segura”.

5.1. FORMAS SEGURAS DE ACESSO ÀS REDES SEM FIO

Antes de mais nada, devemos nos assegurar que os mecanismos de proteção e defesa, de uma rede sem fio, estejam estabelecidos e funcionando de forma plena entre os dispositivos de acesso (APs e estações clientes). Alguns itens devem ser lembrados, no aspecto de garantir o acesso seguro à rede wireless, conforme a seguir:

- Alterar o SSID: Geralmente os APs vem com a configuração do SSID padrão de fábrica, sendo assim, RUFINO (2007, p.114) aconselha que seja especificado um novo SSID que não expõe a identificação do nome da empresa, inserindo um nome genérico que somente os administradores de segurança desta rede possam reconhecê-la e saber em qual local interno o equipamento esteja, (andar e setor), e mais, poderá dificultar a vida do atacante externo em identificar em qual empresa pertence o AP com o SSID de nome genérico;
- Modificar o canal padrão: Realizando esse procedimento, minimiza as interferências de sinais de rádio fazendo que diminua as chances de sucesso de um possível ataque à camada física;
- Mudar a senha padrão de administrador do AP: Desaconselha-se uso de senhas padronizadas de fábrica, tipo “admin” ou em branco, pois facilita que o atacante possa acessar o equipamento e utilizá-lo para realizar atividades maliciosas;
- Restringir o acesso do AP via HTTP ou TELNET: Conforme RUFINO (2007, p.174) “em nenhuma das duas possibilidades há criptografia envolvida, fazendo que as informações trafegadas (incluindo usuário/senha) possam ser capturadas”. Em caso da necessidade de efetuar alguma alteração das configurações do dispositivo ou atualizações de seu firmware, apenas será disponibilizado o acesso via rede cabeada;

5.2. SOLUÇÃO DE AUTENTICAÇÃO BASEADOS EM CERTIFICADOS DIGITAIS

Um dos meios de proteção de segurança das informações dos usuários é a autenticação. Conforme NAKAMURA e GEUS (2007 p.363), trata-se de um mecanismo, baseados em usuário e senha, serve como meio de verificar a veracidade da identidade do usuário. Em redes sem fio, para a necessidade de aplicação desses métodos de autenticação é aconselhável o uso dos protocolos WPA/WPA2, que são bem mais focados nesse tipo de processo, pois os mesmos disponibilizam dois tipos de modos de operação: Modo Personal e Modo Enterprise.

A figura 1 demostra os três componentes principais desse padrão de autenticação e conforme ASSUNÇÃO (2013, p.40) explica que o Suplicante é uma estação cliente wireless, que deseja se conectar a uma infraestrutura enviando um pedido de acesso ao Autenticador (geralmente é o AP), este recebe o pedido e repassa para o Servidor de Autenticação (um servidor RADIUS) que realizará a função de autenticação, checando as credenciais (identidade) do Suplicante, sendo reencaminhado ao Autenticador e respondendo se o acesso será permitido ou negado:

Figura 1: Componentes principais de autenticação.
Fonte: ASSUNÇÃO, 2013, p.39.

Esse processo detalhado logo acima utiliza o método de autenticação EAP conhecido como EAP-TLS. Segundo MORENO (2016, p.252) "é considerado o mais robusto e seguro quando se trata de sistemas de criptografia: somente as máquinas com o certificado instalado acessam a rede". Avaliado como um protocolo de segurança em nível de transporte, o EAP-TLS garante características peculiares como "criptografia de chaves públicas, autenticação mutual, negociação segura de cifras e capacidade de gerenciamento de chaves" (ASSUNÇÃO 2013, p.43).

Apesar desse mecanismo de autenticação apresentar uma alta segurança em seu emprego, existe ainda o risco, que é o próprio usuário, pois o dispositivo que o mesmo utiliza pode ser comprometido por diversas formas e técnicas hacking, assim segundo MORENO (2016, p.252) o atacante poderá se apossar do certificado do cliente ou até mesmo realizar um redirecionamento com a VPN para o acesso à rede. Portanto, deverá existir cuidados ainda maiores em dispositivos que contém esses certificados digitais ou em circunstâncias mais recomendadas, a utilização de tokens e cartões inteligentes (smartcards) com a implementação de autenticação via PIN, para que sejam armazenados os certificados de forma bem mais segura.

5.3. DETECÇÃO DE ATAQUES COM UM WIDS/WIPS

É essencial o uso de mecanismos de defesa que possam detectar ou prevenir intrusões em redes sem fio corporativas (sejam empresas médias ou de grande porte). Para isso, temos dispositivos wireless com sistemas para essas finalidades (WIDS/WIPS).

O que difere entre os sistemas, segundo MORENO (2016, p.214) é que o WIDS tem a finalidade de monitorar o tráfego e revelar as tentativas de ataque, ou seja, apenas detecta atividades maliciosas que estão ocorrendo ou que já ocorreram em algum momento, em contrapartida, o WIPS consegue atuar de forma proativa, prevenindo possíveis ataques antes deles acontecerem. Em suma, os dispositivos com esses sistemas agem detectando e evitando a maioria dos ataques que poderiam prejudicar consideravelmente a rede sem fio corporativa.

Os sistemas WIDS/WIPS trabalham com três metodologias distintas, segundo ASSUNÇÃO (2013, p.173): baseados em assinatura de pacotes (a assinatura do pacote é confrontada junto com as informações de pacotes maliciosos, contidos na base de dados), baseados em anomalias (monitora alterações repentinas do tráfego da rede com base na utilização de baselines (linha de base)) e híbrido (age tanto para alertar um possível ataque através da comparação dos pacotes, quanto para o monitoramento do tráfego por alterações em suas baselines).

Sobre a detecção de ataques, os sistemas WIDS/WIPS devem ser capazes de suportá-los e se os mesmos forem desconhecidos, deverão ser mitigados para algum nível de prevenção de intrusão. Podemos citar alguns tipos de ataques, formas de

detecção e prevenção que os sistemas WIDS/WIPS conseguem agir, de acordo com ASSUNÇÃO (2013, p.176):

- ✓ Detectar tentativas de quebra da criptografia, pelos ataques de criptoanálise WEP, força bruta e dicionário: Detecta o uso de ferramentas e técnicas direcionadas aos ataques supracitados, advertindo para possíveis roubos de dados;
- ✓ Detectar ataques de negação de serviço: Detecta e identifica sobrecarregamentos do espectro wireless (ataques à camada física) e ataques de desassociação/desautenticação através da análise do tráfego;
- ✓ Impedir ataques de AP Spoofing e Multipot: O sistema analisa o espectro wireless por completo e se houver algum dispositivo com as características de um AP Spoofing, imediatamente, o mesmo desassocia os clientes wireless legítimos e bloqueia o dispositivo malicioso.

Conforme o que foi dito até o momento, um sistema de detecção de intrusos sem fio é primordial para a segurança de uma rede corporativa. Sendo assim, podemos aplicar soluções WIDS/WIPS como Open WIPS-NG, wIDS, CISCO WIPS, entre outras, que certamente trarão resultados de eficiência nos mecanismos de defesa e proteção.

De acordo que vimos sobre a detecção de ataques, os WIDS/WIPS são capazes de detectar a presença de Access Points falsos (APs Spoofing) e assim, bloqueá-los impedindo que o atacante tenha êxito com sua técnica de intrusão. Todavia, simplesmente detectar e bloquear o dispositivo AP spoofing, não é um processo totalmente suficiente para que o método de proteção e defesa seja satisfatório. É necessário que saibamos a localização física desse dispositivo, para que possamos também saber quem é/são o(s) responsável(is) por praticar esses tipos de ataques.

Para ASSUNÇÃO (2013, p.171), existem métodos e ferramentas que conseguem determinar a localização de um dispositivo AP Spoofing. Em destaque, podemos citar a técnica de trilateração, que se baseia no emprego de pontos fixos de referência para se adquirir a localização de uma estação sem fio Wi-Fi, dessa forma, permitindo localizar a posição física do dispositivo.

5.4. POLÍTICA DE USO DA REDE SEM FIO

Segundo CHESWICK, BELLOVIN e RUBIN (2005, p.35) a política de uso de uma rede cabeada (equivale também às redes sem fio) tem como objetivo estabelecer regras e normas de utilização e ao mesmo tempo desenvolver comportamento ético e profissional aos usuários da rede. Sobre esses aspectos, é necessário que se estabeleça uma política de uso da rede sem fio respeitando os princípios éticos e culturais previstos na corporação, dando-se início após a conclusão da implantação de sua infraestrutura.

É primordial que seja discutido e dialogado com todos os stakeholders da corporação sobre a importância da implementação dessa política de segurança da informação, pois segundo ROGATTI (2009, p.52) "sem esse instrumento a instalação e o uso indevido dos pontos de acesso representarão um grande e inadmissível risco".

Para um melhor esclarecimento do assunto proposto, podemos destacar alguns tópicos essenciais, que auxiliam na criação da política de uso da rede sem fio, conforme NAKAMURA e GEUS (2007, p.196):

- ✓ Determinar quais são os usuários que serão autorizados ao uso da rede sem fio;
- ✓ Atentar-se que a segurança das informações da organização sempre será um processo contínuo;
- ✓ Compreender sobre os riscos intrínsecos sobre o uso da rede sem fio antes mesmo de sua operação;
- ✓ Compreender os métodos e as ferramentas de proteção e defesa;
- ✓ Limitar o acesso do local onde está(ão) o(s) dispositivo(s) AP(s) através da utilização de controles físicos;
- ✓ Habilitar e testar as funções de segurança pré-estabelecidas, como por exemplo: teste de intrusão na própria rede, verificando possíveis falhas ou brechas que poderão ser encontradas;
- ✓ Delinear responsáveis que farão as instalações dos APs ou de outros dispositivos sem fio;
- ✓ Definir quais tipos de arquivos poderão ser trafegados por esse meio;

- ✓ Discriminar configurações básicas para o uso da rede sem fio em dispositivos móveis, tanto em hardware (interface de rede sem fio) quanto em software (sistema operacional e antivírus atualizados), citando alguns desses exemplos;
- ✓ Descrever como lidar com incidentes de segurança ou perdas de dispositivos sem fio, mitigando possíveis riscos decorrentes a estes fatores;
- ✓ Prover treinamentos e programas de conscientização, como forma de enfatizar ainda mais a importância da segurança por esse meio;
- ✓ Definir escopo de avaliações de segurança e com que frequência as mesmas deverão ser utilizadas.

Em suma, definir uma política de uso da rede sem fio é tão imprescindível quanto dispor de métodos de detecção e monitoramento ou até mesmo o emprego de padrões atuais com métodos criptográficos mais forte, pois a mesma estabelecerá regras e normas, que atenderão os princípios básicos da segurança da informação e facilitará o entendimento e a ciência do uso dessa tecnologia com o seu usuário, prevenindo que não ocorram falhas primárias ou até mesmo técnicas de persuasão, como a engenharia social.

CONSIDERAÇÕES FINAIS

A utilização das redes sem fio representa um grau elevado de importância para sociedade como o todo, nos dias atuais, seja em sua praticidade como em sua mobilidade. Neste trabalho foi visto que a tecnologia de redes sem fio surgiu como complemento para redes cabeadas, que se limitam por ter alguns obstáculos como o impedimento de alterações do ambiente físico. Sendo assim, locais onde não se permitem uma infraestrutura por cabos, com a rede sem fio, é possível à transmissão de informações através de sinais de frequência divididos em faixas, que por sua vez, subdividido em frequências menores chamados canais.

Outro fator mencionado no trabalho tratou sobre a criação de padrões específicos em equipamentos para o incentivo do uso da tecnologia sem fio, entidades como IEEE (cuida do projeto 802, responsável pelos padrões 802.11) e Wi-Fi Alliance (testa e

certifica produtos, garantindo a qualidade dos mesmos) são essenciais para a imersão de dispositivos compatíveis entre si.

Todavia, com o advento dessa evolução tecnológica, também trouxe consigo algumas preocupações com relação à segurança da informação, decorrente da sua utilização. A partir desse momento, o artigo analisa as vulnerabilidades existentes nas redes sem fio desde a permanência da configuração padrão dos equipamentos, até o emprego das criptografias nos protocolos WEP, WPA e WPA2, apresentando suas vulnerabilidades que permitem proporcionar brechas e falhas para possíveis ataques por pessoas maliciosas.

Seguindo no ponto de vista da análise supramencionada, também foi avaliado neste trabalho, as técnicas e os métodos de ataque que exploram as deficiências que um ambiente físico não tão bem protegido oferece para um atacante, a possibilidade de obter dados sigilosos e confidenciais dos usuários que utilizam esse meio de comunicação. Métodos e ataques como quebra de chaves, negação de serviço (DoS), Homem no Meio (MITM), entre outros, demostram o quanto é necessário impedir que vulnerabilidades de segurança possam acontecer. Visto isso, foram discorridos métodos de proteção e defesa que devem ser implementados, com o objetivo de bloquear acessos indevidos (uso de solução de autenticação baseados em certificados digitais) e mitigar riscos ocorridos (como a detecção e monitoramento de ataques com o WIDS/WIPS), além da adoção de uma política especifica de segurança da informação para o uso de redes sem fio.

Assim, finalizamos o trabalho concluindo que, antes de usufruirmos da comodidade e praticidade que a rede sem fio tenha a nos oferecer, seja em uma rede doméstica ou em uma rede corporativa de média/grande porte, através de qualquer equipamento wireless (Access Point e estação cliente) é preciso garantir formas seguras do seu acesso, que assegurem melhor proteção sobre as principais ameaças e vulnerabilidades, tudo isso, dentro da óptica dos princípios básicos que regem a segurança da informação (confidencialidade, integridade e disponibilidade).

REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. “O que é Wi-Fi (IEEE 802.11)?”. 2013. Disponível em: <http://www.infowester.com/wifi.php>. Acesso em: 04 mai. 2016.

ASSUNÇÃO, Marcos Flávio Araújo. “Wireless Hacking Ataques e Segurança de Redes Sem Fio Wi-Fi.” 1. ed. Florianópolis: Visual Books, 2013.

CAMPOS, André. L. N. “Sistema de Segurança da Informação: Controlando os Riscos.” 2. ed. Florianopolis: Visual Books, 2007.

CHESWICK, Willian R.; BELLOVIN, Steven M.; RUBIN, Aviel D. “Firewalls e Segurança na Internet – Repelindo o Hacker Ardiloso.” 2. ed. Porto Alegre: Bookman, 2005.

LACERDA, Thiago de Barros. “Segurança de Redes – Montando uma LAN Segura.” 2006. Recife, PE. UFPE – CIn – Centro de Informática, 9p. Artigo produzido para o curso de Ciência da Computação. Disponível em: <http://www.cin.ufpe.br/~fab/cursos/metodologia-graduacao/2006-2/monografias/thiago-barros.doc>. Acesso em: 14 jun. 2016.

MORAIS, Eduardo Menezes de. “Segurança e Ataques em Redes WiFi”. 2013. São Paulo, SP. USP – Instituto de Matemática e Estatística. 12p. Monografia produzida para o curso de Computação Móvel. Disponível em: <http://grenoble.ime.usp.br/~gold/cursos/2013/movel/mono1st/2506-Eduardo.pdf>. Acesso em: 14 jun. 2016.

MORENO, Daniel. Pentest em Redes Sem Fio. 1. ed. São Paulo: Novatec, 2016.

NAKAMURA, Emilio T.; GEUS, Paulo L. “Segurança de Redes em Ambientes Cooperativos.” 1. ed. São Paulo: Novatec, 2007.

ROGATTI, Alex Christy. “A Segurança da Informação em Redes Wi-Fi.” 2009. Mauá, SP. Faculdade de Tecnologia de Mauá. 80p. Monografia apresentada para obtenção do título de Tecnólogo em Informática com ênfase em Gestão de Negócios.

RUFINO, Nelson Murilo de Oliveira. “Segurança em Redes sem Fio: Aprenda a Proteger suas Informações em Ambientes Wi-Fi e Bluetooth”. 2.ed. São Paulo: Novatec, 2007.