SEGURANÇA EM REDES SEM FIO: o aumento da segurança com o novo protocolo WPA3 a partir de 2019

WIRELESS NETWORK SECURITY: increased security with the new WPA3 protocol as from 2019

Hugo Santucci Rettondin – E-mail: hugo.santucci@hotmail.com

João de Lucca Filho – E-mail: joaodelucca@terra.com.br

Faculdade de Tecnologia de Taquaritinga (FATEC) – São Paulo – Brasil

RESUMO

O presente artigo objetiva apresentar os principais padrões de redes wireless e seus respectivos protocolos de criptografia que podem ser habilitados de acordo com o modelo e conhecimento do usuário, tendo foco nos padrões mais usados hoje em dia no Brasil, expondo possíveis vulnerabilidades de cada um e, apresentando a análise de um estudo de caso na qual alerta sobre uma vulnerabilidade descoberta recentemente no padrão WPA2, que foi considerado o protocolo mais seguro até poucos meses atrás. Aditivamente, alertar e mostrar de forma ilustrativa um ataque à função WPS, que muitas vezes já vem habilitada de fábrica nos roteadores, com a finalidade de proporcionar maior rapidez e facilidade ao usuário na hora de configurar sua rede wireless. Concluindo a abordagem é apresentado o protocolo WPA3 e suas novas tecnologias, buscando o aumento na segurança das redes sem fio atuais visando a proteção dos dados tanto na constituição de rede pessoal quanto na rede corporativa.

Palavras-chave: Vulnerabilidade em redes wireless. Protocolo WPA3. Ataque em redes wireless. Segurança da informação. Novo protocolo de segurança.

ABSTRACT

This article presents the main patterns of wireless networks and their encryption protocols that can be enabled according to the model and user's knowledge, and focus on standards commonly used today in Brazil, exposing potential vulnerabilities of each and presents the analysis of a case study that warns of a vulnerability newly discovered in the WPA2 standard, which was considered the safest protocol until a few months ago. The article also warns and illustratively shows an attack on the WPS function, which is often factory-enabled on the routers, in order to provide users with a faster and easier way to configure their wireless network. Following the proposal of the article is also presented the protocol WPA3 and its new technologies, seeking the increase in the security of the wireless networks aiming at the protection of the data in the implementation of personal network as in the corporate network.

Keywords: Vulnerability in wireless networks. WPA3 Protocol. Attacks on wireless networks. Information security. New security protocol.

1. INTRODUÇÃO

Pode-se dizer que a tecnologia avança de maneira exponencial, porém, o mesmo não acontece com a segurança. Muitas vezes a segurança das aplicações é negligenciada, pois o mercado mantém seu foco voltado para o desenvolvimento de novas tecnologias ao invés de desenvolver aprimoramentos de segurança para as mesmas.

Atualmente, assim como no futuro, a tendência é a de conviver rodeados pela tecnologia vinte e quatro horas por dia, em qualquer lugar e nas mais diversas atividades humanas, muitas vezes oferecendo facilidade e comodidade de uso. Sendo assim, requer o estado de segurança ao fazer uso de tais tecnologias.

O compartilhamento globalizado das informações se deve ao grande avanço das redes de telecomunicações. Por exemplo, as redes de computadores, sendo o maior canal de distribuição de informações existente nos dias atuais, sendo este canal, primordial, para o desenvolvimento de empresas. Por conta do grande volume de tráfego de dados na rede, podemos estar vulneráveis a ataques, colocando em risco informações que talvez sejam de extrema importância pessoal ou empresarial.

> A evolução das redes de computadores fez com que aumentasse a necessidade de comunicação entre os mais distintos dispositivos, não somente entre os dispositivos fixos, mas também entre os dispositivos móveis (OLIVEIRA, 2015, p. 12).

Na construção de uma rede local, a escolha por uma rede sem fio demonstra superior vantagem se comparada a uma rede cabeada. Isto pode ser explicado pelos seus custos, facilidade de instalação, mobilidade dos equipamentos, facilidade de expansão, dentre outros. Porém, tal facilidade traz consigo fatores críticos de segurança em relação à vulnerabilidade destas redes. Para que as informações trafegadas numa rede estejam seguras, devem ser respeitados cinco requisitos básicos: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-repúdio.

Por este motivo, o presente artigo tem como objetivo contribuir para o aprendizado e, consequentemente, a aplicação de tais métodos, visando o aumento na segurança das redes wireless.

2. O PROTOCOLO DE TRANSMISSÃO IEEE 802.11

Entende-se por um conjunto de especificações para redes locais sem fio (WLAN - Wireless Local Area Network), tendo como base o padrão IEEE 802.11. O nome “Wi-Fi” vem da abreviatura do termo inglês “Wireless Fidelity”.

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. Com esta tecnologia, é possível implementar redes que conectam computadores e outros dispositivos compatíveis, tais como smartphones, tablets, consoles de videogame, impressoras, entre outros, desde que estejam geograficamente próximos. Estudos apontam que sua área de cobertura pode alcançar pouco mais de 400 metros, mas para isso, irá depender de diversos outros fatores, como por exemplo, o padrão IEEE 802.11 suportado pelo roteador, assim como a potência da antena do aparelho e também barreiras físicas entre o emissor e receptor dos dados. Porém na prática, as redes sem fio domésticas costumam alcançar entre 25 e 50 metros, devido às barreiras físicas e modelos de roteadores de baixo custo.

O padrão IEEE 802.11 não exige o uso de cabos, já que efetua a transmissão de dados por meio de radiofrequência, oferecendo diversas vantagens, entre elas, permissão para que o usuário possa utilizar a rede em qualquer ponto dentro dos limites de alcance da transmissão, possibilita a inserção rápida de outros computadores e dispositivos na rede, evita que paredes ou estruturas prediais sejam furadas ou adaptadas para a passagem de fios e redução dos custos de instalação em comparação a rede cabeada.

A flexibilidade das redes sem fio é tão grande que se tornou viável a implementação de redes que fazem uso desta tecnologia nos mais variados lugares, principalmente pelo fato de as vantagens citadas no parágrafo anterior. Assim sendo, é comum encontrar redes Wi-Fi disponíveis em hotéis, aeroportos, rodoviárias, bares, restaurantes, shoppings, universidades, e outros lugares.

Para utilizar tais redes, basta ao usuário possuir um aparelho compatível com a tecnologia IEEE 802.11.

Os principais padrões IEEE 802.11 utilizados atualmente no Brasil são; 802.11a, 802.11b, 802.11g e 802.11n e 802.11ac. Sendo cada um deles, respectivamente, uma evolução do padrão anterior, visando suporte a uma maior taxa de transmissão de dados por segundo, maior área de abrangência do sinal, incremento de tecnologias buscando minimizar possíveis interferências no sinal, e nos protocolos de criptografia para transmissão segura dos dados.

3. PROTOCOLOS DE SEGURANÇA NAS REDES SEM FIO PADRÃO 802.11

Os algoritmos de segurança de redes sem fio já passaram por muitas mudanças e melhorias desde a década da primeira implementação no ano de 1990, se tornando mais

seguros e eficazes. Os protocolos de segurança sem fio são WEP, WPA e WPA2, e todos têm a mesma finalidade, porém, diferentes entre si.

Tais protocolos evitam que terceiros se conectem a rede e realizam a criptografia dos dados transmitidos através do sinal de rede sem fio.

No cenário atual, a tecnologia de rede sem fio, mesmo estando protegida e criptografada, não alcança alto nível de segurança quando comparadas as redes cabeadas. Pois as redes cabeadas, transmitem dados ponto a ponto, como do ponto A ao B. Logo as redes sem fio, para enviarem os dados do ponto A até o ponto B, transmitem os dados para todos os dispositivos que estão ao alcance da rede, portanto, qualquer um desses dispositivos conectados irá recebe-los.

A seguir são apresentados mais detalhes sobre os protocolos de segurança implementados pelo padrão IEEE 802.11.

3.1 O protocolo WEP

Wired Equivalent Privacy (Privacidade equivalente aos fios) foi o primeiro protocolo de criptografia lançado para redes sem fio. O WEP é um sistema de criptografia adotado pelo padrão IEEE 802.11.

As chaves de acesso utilizam 64 ou 128 bits e o algoritmo RC4 para criptografar os pacotes, que são transmitidos pelas ondas de rádio. Além disso, faz uso de uma função para detectar erros e verificar a autenticidade dos dados.

Poucos anos após ter sido lançado, várias vulnerabilidades foram encontradas no uso do protocolo. A principal vulnerabilidade está no fato do fornecimento de uma chave estática que é compartilhada entre todos os dispositivos conectados na rede, permitindo ataques ao protocolo.

3.2 O protocolo WPA

Wi-fi Protected Access (Wi-Fi de acesso protegido) é uma versão melhorada do WEP. Também é conhecido como TKIP (Temporal Key Integrity Protocol). O recurso surgiu em 2003 para aumentar a segurança do protocolo WEP. As principais mudanças foram no algoritmo de criptografia.

3.3 O protocolo WPA2

É considerada a versão final o WPA. A principal diferença entre o WPA e o WPA2 é a forma com a qual ele criptografa os dados. Enquanto o WPA utiliza o TKIP como algoritmo

de criptografia, o WPA2 utiliza o algoritmo AES (Advanced Encryption Standard). O algoritmo AES é o padrão de criptografia utilizado pelo Governo Norte-americano, o qual é consideravelmente mais sofisticado em comparação ao TKIP. Por conta disso, aparelhos mais antigos não suportam o WPA2, nem com um firmware atualizado.

O WPA2 é o algoritmo de criptografia padrão dos roteadores atuais, sendo considerado o melhor algoritmo em uso nos dias de hoje.

4. VULNERABILIDADES DOS PROTOCOLOS WPA E WPA2

Os protocolos WPA e WPA2 possuem características de segurança superiores às usadas pelo protocolo WEP, mas ainda assim são suscetíveis a vulnerabilidades.

Pesquisadores encontraram uma maneira de contornar a segurança oferecida pelo protocolo de rede. Sempre que alguém se conecta em uma rede Wi-Fi, um handshake é executado para criar uma nova chave de criptografia para todo o tráfego que vai existir a partir daquela conexão.

O handshake (aperto de mão, em português) é o nome do processo pelo qual duas máquinas firmam um acordo, em que uma reconhece a outra e instituem que estão prontas para iniciar a comunicação sem interferências. Para garantir a segurança dessa conversa, uma chave deve ser instalada e usada apenas uma vez.

O que a dupla fez foi um ataque (krack) que consiste na reinstalação de uma chave de acesso através da exploração do handshake (processo usado para estabelecer a chave para criptografia do tráfego de dados) do protocolo WPA2, induzindo a vítima a reinstalar determinada chave já em uso e, deste modo, os parâmetros associados ao protocolo, garantem o controle da comunicação. Tais falhas não permitem ao atacante recuperar a senha da conexão, mas sim descriptografar os dados trafegados pela rede.

Tal vulnerabilidade descoberta no protocolo WPA2 foi considerada grave, sendo que o protocolo até então, assegurava a alta proteção na transmissão dos dados nas redes sem fio modernas que estivessem fazendo uso de deste protocolo.

Os ataques funcionaram contra redes wireless pessoais e corporativas, tanto no protocolo mais antigo (WPA) quanto no mais recente (WPA2), sendo destrutivo até mesmo contra redes que usavam o protocolo criptográfico AES. A vulnerabilidade descoberta é crítica e abalou a reputação do protocolo de segurança, a reação de forte preocupação do setor empresarial e especialistas em segurança foi imediata.

5. VULNERABILIDADE DA FUNÇÃO WPS

A função WPS permite que dispositivos acessem a rede wi-fi sem a necessidade de digitar a senha da rede, quando surgir a necessidade de conectar um novo aparelho à rede Wi-Fi, basta que o botão “WPS” do roteador seja pressionado, para que então o aparelho se conecte automaticamente, sem a necessidade de utilização de senhas.

É justamente com essa função habilitada que surgem as brechas de segurança utilizadas em ataques. Isso porque a função WPS (Wi-Fi Protected Setup) é suscetível a um ataque de força bruta (ataque criptoanalítico que consiste na verificação de todas as possíveis chaves ou senhas até que a correta seja encontrada), já que a função grava em seu roteador um código (PIN) de oito dígitos.

“A vulnerabilidade deve-se a uma falha que permite determinar quando os oito dígitos estão corretos.” (DINIZ; LIJÓ; SOUSA, 2013).

E apesar da invasão de uma rede segura WPA/WPA2 através desta falha demorar por volta de 2 a 14 horas, ainda sim é um problema de segurança real, portanto, o WPS deve ser desativado ou melhor, o firmware do roteador ou ponto de acesso deve ser redefinido para versão que não possua suporte a função WPS, excluindo assim esta vulnerabilidade.

5.1. Demonstração do ataque na função wps habilitada nos roteadores

Para fins demonstrativos, foi usada a distribuição Linux com base no sistema operacional Debian, analisando a vulnerabilidade da rede através de ferramentas open-source. A ferramenta apresentada será a Aircrack-ng, usada em auditoria para análise de redes locais sem fios com protocolo 802.11.

Para fazer uso desta ferramenta, seu driver de placa de rede deve suportar o modo monitoramento bruto, podendo assim capturar e analisar o tráfego nas redes 802.11a, 802.11b e 802.11g. A ferramenta oferece suporte aos sistemas operacionais Linux, Windows e Android.

Para os comandos seguintes, teremos que ter instalado em nosso dispositivo o pacote Aircrack-ng, para isso, basta acessarmos o terminal como super usuário (root), em seguida digitarmos o comando apt-get install aircrack-ng.

Tendo o pacote instalado, o primeiro passo é verificar as placas de rede existentes em seu dispositivo com o comando iwconfig. Vale ressaltar que, para realizar o teste via wireless, não poderemos estar conectados à rede alguma.

O segundo passo é colocar a placa de rede wireless em modo monitor com o comando airmon-ng start wlan0, onde wlan0 é o nome da placa de rede do dispositivo.

"Airmon-NG é um script que pode ser usado para ativar ou desativar o modo de monitor em interfaces sem fio (LÜDTKE, 2015, p. 26)".

A ferramenta Airmon-NG faz parte do pacote Aircrack-NG citado anteriormente.

Tal comando coloca a placa de rede wireless em modo promíscuo, esta é uma configuração de recepção na qual todos os pacotes que trafegam pelo segmento de rede em que o receptor está conectado serão recebidos pelo mesmo. Após o comando, a placa wireless foi renomeada para mon0.

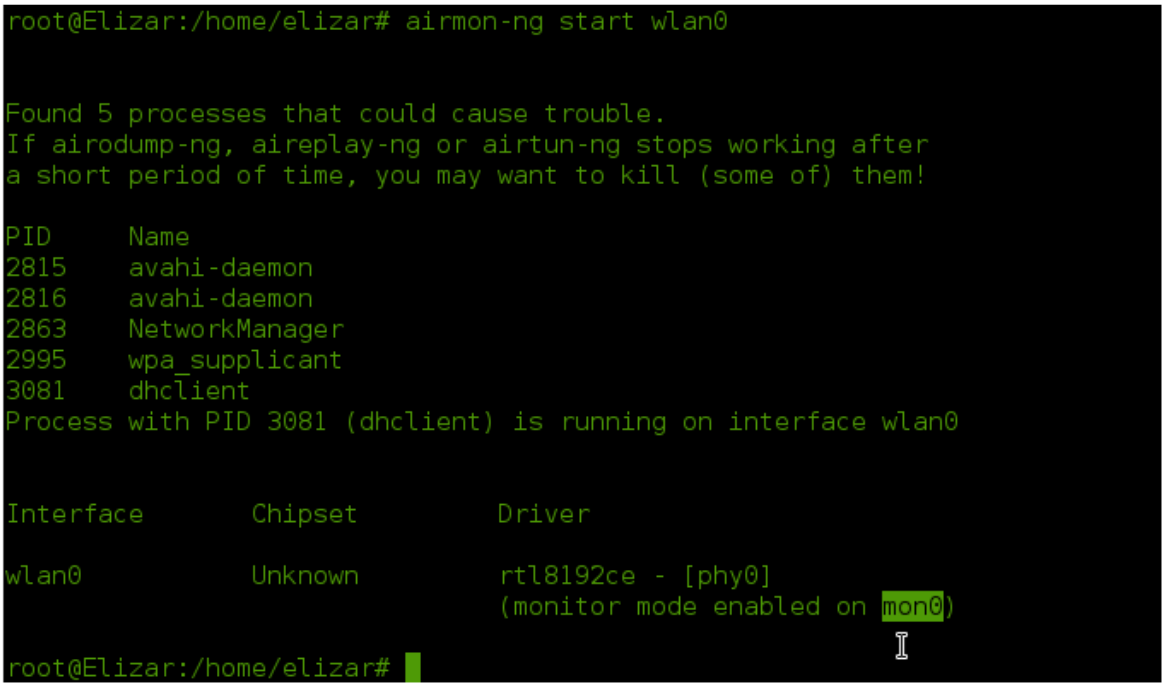

Figura 1: Botelho, E. Severino. Análise de vulnerabilidades em redes wlan doméstica com softwares livres, 9 p.

O passo seguinte é listar e identificar todos os pontos de acesso com potência de sinal dentro do alcance da interface wireless em modo monitor com o comando airodump-ng mon0.

Após o comando airodump-ng mon0, o próximo passo é copiar o endereço MAC do roteador da rede alvo e salvá-lo em algum lugar seguro, lembrando que para identificar a rede alvo, basta se atentar ao campo SSID onde será exibido o nome das redes encontradas.

Realizado os passos anteriormente descritos, vamos então dar início ao ataque usando a ferramenta Reaver.

"Reaver é uma ferramenta que pode ser utilizada para explorar uma vulnerabilidade do protocolo WPS, utilizado pelas chaves do tipo WPA e WPA2, a fim de resgatar a senha configurada no aparelho roteador (VISOTTO, 2014)".

Com o comando reaver –i mon0 –b 78:54:2E:F9:4F:C6 -vv, iniciamos o ataque. A figura abaixo mostra o processo final do ataque, sendo finalizado com duração total de 04 horas e 02 minutos.

Nesta fase serão buscados os resultados através do MAC, do PIN (e consequentemente a senha) e do SSID do roteador.

Ao final será exibido o número do PIN, o SSID e a senha da rede. É interessante notar que, independente da complexidade da senha registrada no roteador, esta será descoberta da mesma forma, uma vez que o ataque se destina a descobrir o número do PIN do roteador.

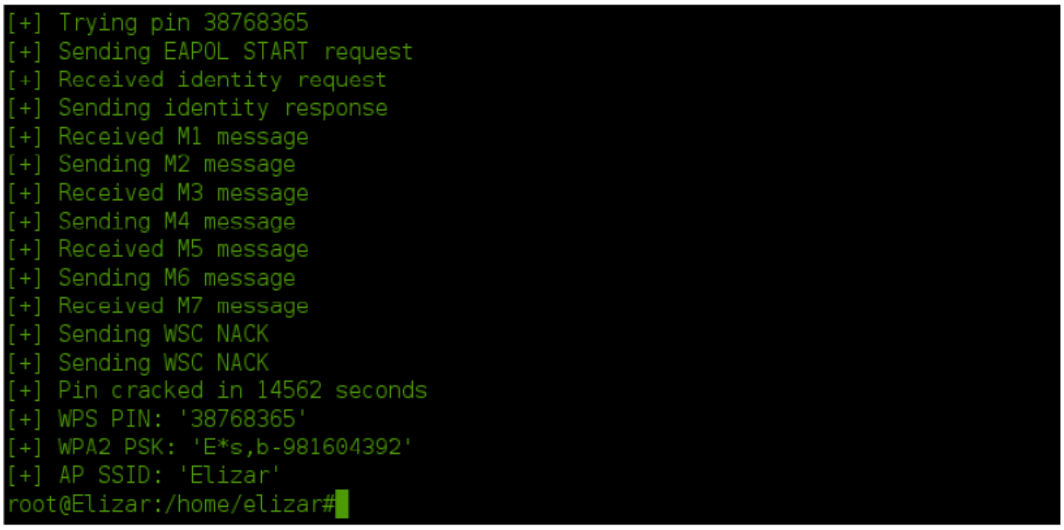

Figura 2: Botelho, E. Severino. Análise de vulnerabilidades em redes wlan doméstica com softwares livres, 12 p.

6. O PROTOCOLO WPA 3 – A POSSÍVEL SOLUÇÃO

O WPA3 é a próxima geração de segurança de redes sem fio padrão IEEE 802.11, fornecendo segurança de ponta para o mercado. Adicionando novos recursos para incrementar a segurança em redes sem fio permitindo autenticação mais robusta, maior força criptográfica para mercados de dados altamente confidenciais, mantendo a invulnerabilidade de redes de missão crítica que operem com o protocolo WPA3. Dentre as diversas melhorias, o protocolo inclui:

- Uso dos protocolos de segurança mais recentes do mercado.
- Desativação de protocolos desatualizados herdados de seu antecessor WPA2.
- Exige o uso do gerenciamento protegido (PMF) evitando que os dados possam ser interceptados durante a transmissão.

Como as redes sem fio divergem na finalidade de uso, o WPA3 inclui recursos adicionais especificamente para redes pessoais e corporativas, sendo estes:

WPA3-Personal, os usuários do recebem mais proteção contra tentativas de adivinhação de senhas, enquanto os usuários do WPA3-Enterprise podem agora aproveitar os protocolos de segurança de alto nível para redes de dados sensíveis.

O WPA3 manterá a interoperabilidade com dispositivos WPA2 durante o passar dos anos de acordo com o crescimento do mercado e posterior exigência do padrão WPA3 nos futuros modelos de roteadores.

Por enquanto, esse novo padrão não é obrigatório. A Wi-Fi Alliance estipula que sua adoção comece de fato em meados do ano de 2019, junto à próxima geração do serviço de comunicação wireless, chamado 802.11ax, que substituirá o atual 802.11ac, trazendo maior capacidade de transmissão de dados, podendo chegar a reais 10Gb/s, assim como maior área de alcance, além da melhor performance ao manter até 256 dispositivos conectados simultaneamente, o que deverá reforçar a adoção do novo protocolo de segurança.

6.1 A segurança do wpa3 para uso pessoal

O WPA3-Personal traz melhoria na proteção para usuários, fornecendo autenticação baseada em senha mais robusta, mesmo quando os usuários escolhem senhas que não possuem recomendações típicas de complexidade. Esse recurso é ativado por meio da SAE (Autenticação simultânea de iguais), que substitui a chave pré-compartilhada (PSK) no WPA2-Personal.

Os pontos principais que merecem destaque são:

- A tecnologia é resistente a ataques de força bruta off-line (algoritmo usado para descobrir a senha do SSID (Service Set Identifier) de uma rede sem fio, através da tentativa de várias senhas consecutivas, a fim de estabelecer conexão com a rede).
- Seleção de senha natural: permite os usuários escolherem senhas mais fáceis de lembrar, devido ao algoritmo de criptografia deste protocolo ser mais sofisticado.
- Facilidade de uso: Oferece proteções aprimoradas sem alterar a maneira como os usuários se conectam a rede.
- Encaminhamento: protege o tráfego de dados, mesmo que uma senha seja comprometida após a transmissão dos dados.

6.2 A segurança do wpa3 para uso empresarial

Empresas, governos e instituições financeiras têm maior segurança com o WPA3-Enterprise. O WPA3-Enterprise baseia-se no WPA2 e garante a aplicação consistente de protocolos de segurança em toda a rede.

O WPA3-Enterprise também oferece um modo opcional usando protocolos de segurança de força mínima de 192 bits e ferramentas criptográficas para proteger melhor os dados confidenciais, tais como:

- Criptografia autenticada: Proporcionando confidencialidade, integridade e garantia de autenticidade dos dados criptografados. Usando o protocolo Galois de 256 bits (GCMP-256).
- Derivação e confirmação de chave: Usado para calcular o código de autenticação de mensagem (MAC), verificando assim a integridade e a autenticidade da mensagem, cuja força de criptografia gerada pelo HMAC depende da força da criptográfica de sua função hash subjacente (no caso temos o hash SHA384), ou seja, de sua saída em bits, do tamanho e da qualidade da chave criptográfica. Usando o HMAC (Hashed Message Authentication Mode) de 384 bits com algoritmo de hash seguro (HMAC-SHA384).
- Estabelecimento e autenticação de chaves: Este protocolo permite que duas partes estabeleçam conexão criptografada mesmo em um canal inseguro. Fazendo uso do protocolo Elliptic Curve Diffie-Hellman (ECDH) e do algoritmo de assinatura digital de curva elíptica (ECDSA) de 384 bits.
- Proteção de quadro de gerenciamento robusta: Modo de operação para cifras de bloco criptográfico com tamanho máximo de 128 bits por bloco. Usando o algoritmo Galois Message Authentication Code (BIP-GMAC-256).

O modo de segurança mínima de 192 bits oferecido pelo WPA3-Enterprise garante que a combinação certa de ferramentas criptográficas seja usada e define uma linha de base consistente de segurança dentro de uma rede WPA3.

7 CONSIDERAÇÕES FINAIS

Seguindo os resultados obtidos no teste, chegou-se a confirmação da teoria citada anteriormente, mencionando o avanço tecnológico de maneira exponencial, porém, deixando de ser acompanhado pela segurança. Deste modo, apesar de todas as funções e ferramentas de segurança implementadas no protocolo WPA2 até os dias atuais, estas, não foram o suficiente, fazendo com que o protocolo se apresentasse obsoleto e pouco resiliente em relação aos métodos de ataque desenvolvidos buscando a quebra do sigilo dos roteadores e consequentemente as redes sem fio.

Vale ressaltar que, apesar de existir vulnerabilidades nos protocolos atuais, a fragilidade das redes wireless, aumenta ainda mais se os dispositivos forem mal configurados por seus utilizadores, visto que, para garantir a segurança tanto pessoal quanto empresarial, é preciso atualizar constantemente as defesas a fim de reduzir vulnerabilidades na rede.

"Nenhuma rede é 100% segura e nenhuma ferramenta ou tecnologia utilizada isoladamente garante a proteção completa contra ataques e invasões (COZER, 2006, p. 17)".

Mas, tomando algumas medidas primordiais de segurança como ocultar o nome da rede (SSID), alterar o nome de usuário e senha padrão de fábrica dos roteadores, ativar o firewall do roteador (caso possua), desativar a função WPS, manter sempre a versão mais recente do firmware do roteador e a desativação do acesso remoto, permite dificultar o ataque em tais meios de comunicação, eliminando assim brechas previsíveis, visto que se utilizados em conjunto promovem maior proteção, tendo em "mente" que uma medida de segurança pode suprir as fragilidades de outra.

Por fim, é oportuno sugerir como proposta de trabalho futuro a realização de pesquisas em relação à padronização e melhorias que serão alcançadas na prática a partir da implantação do protocolo de criptografia WPA3 por volta do segundo trimestre do ano de 2019.

8 REFERÊNCIAS

BOTELHO, E. Severino. Análise de vulnerabilidades em redes wlan doméstica com softwares livres. Instituto Federal de Educação Ciência e Tecnologia do Triângulo Mineiro – Campus Paracatu, 2016. Disponível em: <http://roitier.pro.br/wp-content/uploads/2016/11/Elizar-Severino-Botelho_3594_assignsubmission_file_ARTIGO-SEGURAN%C3%87A_DE_REDES.pdf>. Acesso em: 4 de Setembro de 2018.

Criptografia autenticada - Disponível em: <https://docs.aws.amazon.com/pt_br/kms/latest/developerguide/crypto_authen.html>. Acesso em: 5 de Out de 2018.

DINIZ, Vanderson ; LIJÓ, Maria Camila; SOUSA, Marcelo Portela. Reaver - Testes de segurança em redes sem fio. 2013. Artigo - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba 'IFPB', Campina Grande, 2013.

GRACIEINY A. BARBOSA; HELDER A. MEDEIROS. Estudo de caso: Vulnerabilidades em rede wireless. Revista Gestão em Foco - Edição nº 9 – Ano: 2017. Disponível em: <http://unifia.edu.br/revista_eletronica/revistas/gestao_foco/artigos/ano2017/057_estudo10.pdf>. Acesso em: 4 de Setembro de 2018.

Hmac User Authentication. Disponível em: <http://wiki.c2.com/?HmacUserAuthentication>. Acesso em: 5 de Out de 2018.

Krack – Key Reinstallation Attacks: falha no protocolo WPA. Disponível em: <http://tiinside.com.br/tiinside/seguranca/artigos-seguranca/17/10/2017/krack-key-reinstallation-attacks-falha-no-protocolo-wpa/>. Acesso em: 5 de Out de 2018.

LUDTKE, Rudolfo Kunde. Teste de Invasão em Redes Sem Fio 802.11. 2015. Monografia (Tecnólogo em Redes de Computadores) - Curso de Graduação em Tecnologia em Redes de Computadores, Universidade Federal de Santa Maria 'UFSM', Santa Maria, 2015. 54 p.

LÜDTKE, Rudolfo Kunde. Teste de Invasão em Redes Sem Fio 802.11. 2015. Monografia (Tecnólogo em Redes de Computadores) - Curso de Graduação em Tecnologia em Redes de Computadores, Universidade Federal de Santa Maria 'UFSM', Santa Maria, 2015. 54 p.

O que muda do Wi-Fi 802.11ac para 802.11ax: Entenda o novo padrão de Internet. Disponível em: <https://www.techtudo.com.br/noticias/2018/03/o-que-muda-do-wi-fi-80211ac-para-80211ax-entenda-padrao-de-internet.ghtml>. Acesso em: 8 Set. 2018.

OLIVEIRA, Alan Teixeira de. Análise das Vulnerabilidades das Redes Sem Fio na Cidade de Vitória da Conquista - BA. 2010. Monografia (Bacharel em Ciência da Computação) - Curso de Ciência da Computação, Universidade Estadual do Sudoeste da Bahia 'UESB', Vitória da Conquista, 2010. 72 p.

Protocolos de Segurança de Rede Sem Fio: WEP, WPA e WPA2. Disponível em: <https://www.netspotapp.com/pt/wifi-encryption-and-security.html>. Acesso em: 1 Set. 2018.

VISOTTO, Clayton. Reaver – Descobrindo senhas Wi-Fi. 2014. Tutorial. Disponível em: <https://www.vivaolinux.com.br/artigo/Reaver-Descobrindo-senhas-Wi-Fi > acessado em 16/09/2016

Vulnerabilidades WPA e WPA2 Acesso Wi-Fi. Disponível em: <http://www.infomad.com.br/blog/vulnerabilidades-wpa-e-wpa2-acesso-wi-fi>. Acesso em: 1 Set. 2018.

WPA3 – O sucessor do WPA2. Disponível em: <http://www.ten.com.br/wpa3-o-sucessor-do-wpa2/> Acesso em: 1 Set. 2018.