RISCOS NA SEGURANÇA EM REDES SEM FIO PÚBLICAS

Fernando Alves de Carvalho Filho

RESUMO

Na última década, a utilização da Internet para acesso a serviços de caráter pessoal aumentou consideravelmente, isto se deve a maior praticidade possibilitada por este veículo. Concomitantemente ao uso em locais públicos, vem a tona um perigo relacionado a segurança da exposição de dados pessoais de forma online. Este artigo tem por objetivo promover uma abordagem do uso de redes sem fio em locais públicos como restaurantes, bares, cafés e outras localidades de acesso livre a população. Muitos ataques são realizados discretamente e quase que imperceptíveis a olhos destreinados. Com os equipamentos e ferramentas corretas, é possível mitigar estes ataques.

Palavras-chave: Segurança; Tecnologia; Redes sem fio.

1 OBJETIVOS

1.1 OBJETIVOS GERAIS

Compreender o uso e perfil das atuais redes sem fio utilizadas em locais pública, aperfeiçoando a segurança das informações transmitidas e garantindo confiabilidade e autenticidade.

1.2 OBJETIVOS ESPECÍFICOS

Identificar os atuais problemas e preocupações que envolvem o uso de redes sem fio em locais públicos, analisando as vulnerabilidades e tornando o ambiente mais seguro possível para utilização.

2 JUSTIFICATIVA

Os ambientes públicos são locais frequentados por todos os tipos de pessoas, sejam elas detentoras de melhor conhecimento relacionado à tecnologia ou não, em determinado momento, essas pessoas utilizam-se de uma rede disponível para executarem serviços de caráter pessoal. Diferentemente de ambientes corporativos, não é uma pratica comum os locais públicos possuírem políticas relacionadas à segurança da informação. Diante disso, há uma grande preocupação em tornar essas redes mais seguras contra ataques de criminosos que se utilizam dessas redes para agir de má fé obtendo dados de forma ilícita e assim, prejudicar as vítimas.

3 HIPÓTESES

Frequentes ataques a redes sociais e comunicadores instantâneos com objetivo de furto de informações pessoais e sigilosas para o uso ilícito de variados tipos, tais como, extorsão, estelionato e crimes contra a honra.

4 METODOLOGIA

Pesquisas qualitativas exploratórias baseadas em levantamentos bibliográficos.

5 RELEVÂNCIA

É comum demonstrações de vários tipos de ataques comprometendo informações pessoais e secretas dos usuários. Este artigo tem como intuito explicar

e demonstrar como alguns ataques funcionam e como evitá-los, alertando dessa forma os usuários desse sistema online.

6 CONTRIBUIÇÕES

Esse trabalho visa contribuir para a pesquisa, demonstração de métodos e mecanismos de ataque direcionados a redes sem fio, bem como serviços de rede que são essenciais para utilização da rede mundial de computadores.

7 REFERENCIAL TEÓRICO

7.1 INTRODUÇÃO

Com a crescente popularidade da Internet e seus serviços, o acesso tornou-se cada vez mais necessário e constante. Pessoas de todos os tipos acessam os mais variados serviços online, entre eles podem-se destacar as redes sociais, portais de notícias e os serviços financeiros (LEMOS et al., 2012). A utilização destes através de redes públicas é uma realidade crescente, principalmente devido à baixa qualidade e custo de acesso através das redes de telecomunicação providas pelas operadoras de telefonia. Ao optar por utilizar uma rede sem fio em local público, o usuário pode estar submetendo-se a alguns riscos e ataques tais como acesso a páginas falsas, desvio de informações e captura de sinais de rádio (BRANCO, 2000). Redes sem fio utilizam sinais de rádio ou comprimento de onda óticos para transmitir e receber informações, um computador com o devido dispositivo pode escutar esses comprimentos de onda. Sendo assim, um *cracker* pode fabricar novos sinais sem fio e persuadir estações usuárias que é autentico.

Utilizaremos o termo *cracker*, conforme descrito pelo Wikipedia:

> *“Cracker [cráquer] é o termo usado para designar o indivíduo que pratica a quebra (ou cracking) de um sistema de segurança de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa contra o uso jornalístico pejorativo do termo "hacker". A criação do termo pelos hackers reflete a forte revolta destes contra o roubo e o vandalismo praticados pelos crackers.”*

Nesse contexto, este artigo descreve técnicas de invasão baseadas em redes sem fio IEEE-802.11, popularmente conhecidas como redes *Wi-Fi* ou *Wireless*, e sugere várias técnicas defensivas. Entretanto, não há intenção de denegrir a imagem e nem expor nenhum comportamento mal intencionado dos criadores desse protocolo de comunicação. Sendo assim, há neste trabalho um enfoque em descrever técnicas e métodos preventivos contra ataques de usuários mal intencionados as redes sem fio IEEE-802.11.

7.2 VISÃO GERAL

Neste tópico, teremos uma breve visão geral sobre as redes sem fio IEEE-802.11. Há consideração que o leitor possui conhecimento básico no modelo OSI e TCP/IP.

O IEEE-802.11 se refere a uma família de especificações (www.ieee802.org/11), desenvolvidas pelo IEEE para comunicação sem fio entre estações e pontos de acesso ou entre dois clientes.

7.2.1 ESTAÇÕES E PONTOS DE ACESSO

Estação é o dispositivo de rede sem fio que pode prover uma camada física utilizando uma conexão de rádio com outra estação, enquanto ponto de acesso é uma estação que possui capacidade de distribuição de serviço para outras estações associadas. O ponto de acesso normalmente é conectado a uma rede LAN utilizando conexão com fio.

A estação e o ponto de acesso possuem uma interface de rede sem fio que dispõe de um endereço *MAC (Media Access Control)*, exatamente como redes com fio. Este endereço é único, composto de um número de 48 bits, associado a sua fabricante e ao seu horário de fabricação. Este endereço de 48 bits é representado por seis octetos separados por dois pontos (AA:BB:CC:DD:EE:FF) ou por hifens (AA-BB-CC-DD-EE-FF).

O ponto de acesso possui um identificador *SSID (Service Set Identifier)* que também é conhecido como nome da rede sem fio. O *SSID* é utilizado para segmentar as ondas transmitidas. Se dois pontos de acesso diferentes estiveram próximos, o *SSID* marca cada rede sem fio, e isto permite a estação utilizadora aceitar transmissões de respectivo ponto de acesso e ignorar de outros.

7.2.2 CANAIS

As estações se comunicam utilizando frequências de rádio entre 2.4 GHz e 2.5 GHz.

7.2.3 MODOS DE INFRAESTRUTURA E *AD-HOC*

Redes sem fio IEEE-802.11 podem operar de dois modos. No modo *ad-hoc*, cada estação é um ponto para as outras estações e se comunicam diretamente, de forma que nenhum ponto de acesso é envolvido. Enquanto que, uma estação em modo de infraestrutura comunica-se apenas com o ponto de acesso. O *BSS (Basic Service Set)* é um conjunto de estações logicamente associadas umas as outras e controladas por um ou mais pontos de acessos. Juntas, operam como uma rede sem fio totalmente conectada. O *BSSID* é um número de 48 bits no mesmo formato de um endereço *MAC*. Esta informação define exclusivamente cada *BSS*. A informação deste campo é o endereço *MAC* do ponto de acesso.

7.2.4 *WEP/WPA*

WEP (Wired Equivalent Privacy) é uma senha pré-compartilhada de criptografia utilizada para codificar os pacotes transmitidos entre a estação e o ponto de acesso. O algoritmo do *WEP* utiliza chaves de criptografia de 40 bits ou 104 bits e tem como finalidade proteger redes sem fio contra espionagem. Uma função secundária do WEP é prevenir o acesso não autorizado a redes sem fio. O *WEP* criptografa os dados inseridos nos *frames* transmitidos. *Frames* de controle e gerência são sempre transmitidos sem criptografia, permitindo mecanismos de quebra de criptografia.

WPA (Wi-Fi Protect Acess) é um *WEP* melhorado. Passa a utilizar um novo algoritmo de criptografia, *TKIP (Temporal Key Integrity Protocol)*, que emprega a utilização de uma chave por pacote, dinamicamente gerando uma nova chave de 128 bits para cada pacote transmitido, prevenindo ataques que comprometeram a segurança *WEP*. Essa comunicação possui novos mecanismos de autenticidade e confiabilidade.

7.2.5 *FRAMES*

Estações e pontos de acessos irradiam e capturam frames IEEE-802.11 conforme necessário. A tipificação do formato destes *frames,* contendo informações é demonstrada na figura a seguir (Figura 01).

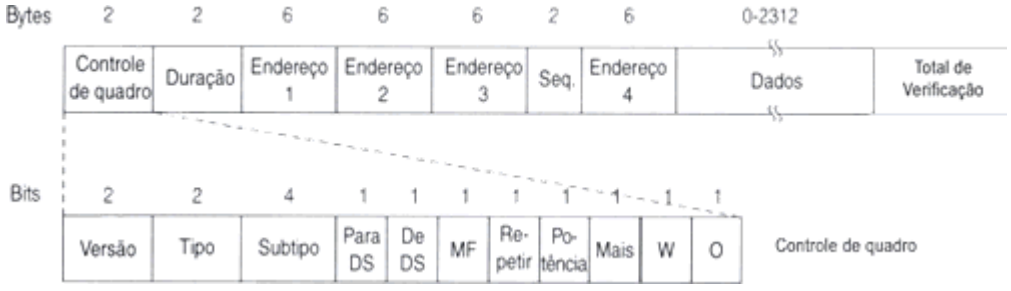

Figura 01: *Frames*

Existem três classes de *frames*: Os de gerenciamento, que estabelecem e mantém comunicações. O *SSID* é parte de uma série de *frames* de gerenciamento. Mesmo quando utilizando criptografia *WEP* ou *WPA*, mensagens de gerenciamento são sempre entregues em puro texto, visível para qualquer estação, que pode interceptar este *frame*. O *frame* de controle ajuda os dados a serem entregues, precisam ser recebidos por todas as estações e contém apenas informações de

cabeçalho, enquanto os *frames* de dados encapsulam os pacotes da camada de rede e carregam informações, tais como endereço *MAC* de origem e destino, *BSSID*¸ e datagramas do tipo*TCP/IP*.

7.2.6 *CAPTIVE PORTAL*

Na necessidade de autenticar e autorizar os usuários conectados a pontos de acesso sem criptografia na transmissão de sinais Wi-Fi, um método bastante utilizado para autenticação de clientes são os *Captive Portals,* que são responsáveis por controlar e gerenciar o acesso às redes (Figura 02).

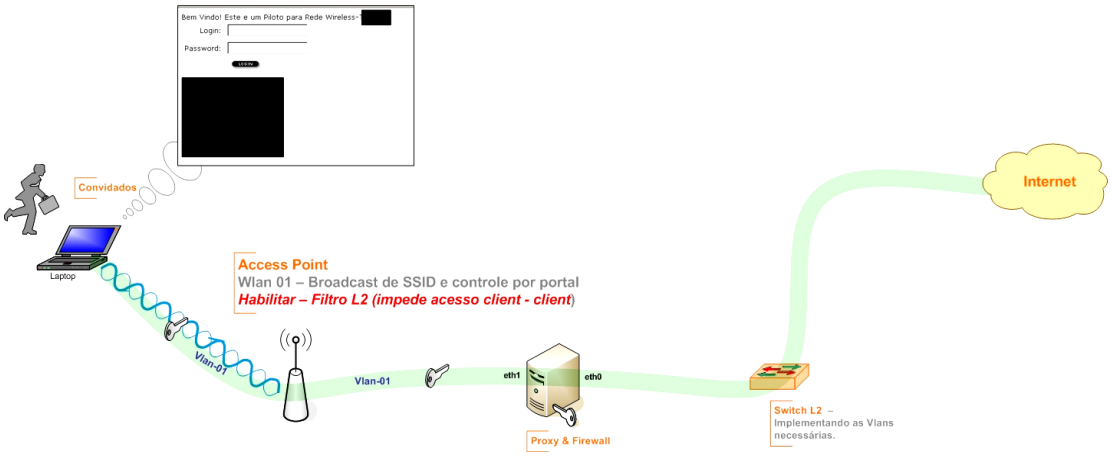

Figura 02: Autenticação realizada pelo *Captive Portal*

O convidado conecta-se a rede sem fio e ao tentar acessar algum endereço *WEB* é redirecionado para um portal de autenticação onde deve inserir usuário e senha previamente definidos para liberação de acesso. A segurança desta rede é baseada em camadas superiores do modelo *OSI*. As informações são transmitidas sem criptografia, sendo extremamente necessária a utilização de criptografia nos protocolos transmitidos neste meio. O ponto de acesso pode fornecer informações e configuração automática de servidor *proxy* seguro, permitindo navegação e acesso *WEB* protegendo os dados transmitidos.

8 ATAQUES

Existem uma variedade de ataques possíveis para redes sem fio, neste artigo iremos detalhar ataques conhecidos como *sniffing, rogue AP* e ataques de camada de enlace*.*

8.1 SNIFFING

Sniffing, é uma técnica de espionagem dos dados transmitidos, também conhecida como *Eavesdropping.* Segundo o Wikipedia, "*Eavesdropping* é uma técnica de *hacking* que se baseia na violação da confidencialidade." Essa técnica, não é uma falha do *TCP/IP*, mas sim uma opção ativa do *Ethernet* e *IEEE-802.11*.

Sniffing é uma técnica já utilizada ao longo do termo em redes com fio. Desde que, os protocolos de comunicação utilizados nas camadas superiores sejam os mesmos, essa mesma técnica é aplicada nas redes sem fio. O intuito do *Sniffing* é capturar os pacotes de camadas superiores, de protocolos utilizados para comunicações em aplicações. Uma rede sem fio aberta sem uso de criptografia, pode ser atacada por um usuário mal intencionado com a técnica de *Sniffing* e capturar dados de conexões *telnet, http, ftp* entre outros protocolos que não utilizam criptografia nas informações transmitidas. Um exemplo prático de *Sniffing* é o ato de uma determinada estação X, capturar um pacote enviado da estação A com destino estação B. O atacante pode ter acesso a informações confidenciais que não deveria. Um usuário por ora determinado apenas Bob, deseja acessar o seu banco, um atacante escutando o meio de transmissão, tem a capacidade de fazer o usuário acreditar que seu acesso ao banco deve passar por um destino, onde as informações são capturas e armazenadas para futuro uso do atacante. Dessa forma, o ataque é imperceptível para o usuário Bob.

8.2 SPOOFING

Spoofing é a técnica de mascarar, modificar um *frame* com o intuito de fazê-lo passar por um frame legitimo. É uma técnica utilizada tanto em redes com fio como em redes sem fio. O atacante constrói novos *frames* inserindo informações em

campos que contém endereços ou identificadores pertencentes a usuários legítimos, de maneira que seu equipamento não seja identificado.

8.2.1 SPOOFING DE ENDEREÇO MAC

Em uma tentativa de invasão, um atacante não deseja ser descoberto. Em todas as descobertas enviadas para redes sem fio, o atacante preenche os campos identificadores com endereços que não possam ser associados ao seu equipamento.

O controle nos pontos de acesso podem evitar estações não conhecidas de se conectar a rede. O atacante pode comprometer uma estação ou pode realizar um ataque *spoofing* modificando o campo de endereço *MAC* por um *MAC* legitimo autenticado e autorizado na rede. Endereços *MAC* são assignados no momento de fabricação de cada dispositivo de rede, contudo, existem softwares que possuem a capacidade de alterar esse endereço. Logo, o endereço *MAC* enviado em cada *frame* pode ser manipulado.

Quando um ponto de acesso não utiliza controle de acesso de endereços *MAC*, não existe necessidade do atacante utilizar um endereço *MAC* legitimo. Qualquer endereço *MAC* pode ser utilizado apenas com intuito de mascarar o endereço real do atacante.

8.2.2 SPOOFING DE ENDEREÇO IP

Substituindo o endereço IP do remetente, e em raros casos do destinatário, é uma operação comum em muitos ataques.

A camada IP dos sistemas operacionais, ao receber um pacote, confia no endereço recebido e o assume como válido. Sendo assim, esta camada adiciona este endereço validado e o atacante deve se utilizar de ferramentas que conversam diretamente com o dispositivo e que possuam ainda, a capacidade de enviar pacotes de maneira "crua", ou seja, pacotes fabricados fora das camadas do sistema operacional.

Spoofing de endereços IP é uma parte integral de vários ataques, por exemplo, um atacante pode silenciar uma estação “A” enviando pacotes para estação “B” com endereço de origem como estação A, que realizará processamento de todos os pacotes de respostas que a estação B originará.

8.3 PHISING

O termo "pishing", derivado da língua inglesa, faz uma analogia a "fishing", que significa pesca, pois é uma forma de fraude eletrônica caracterizada por tentativas de adquirir, de forma ilegal, dados pessoais, tais como senhas e números de cartão de crédito das possíveis vítimas (OLIVOA et al., 2013). Trata-se ainda, de qualquer tentativa de obter dados confidenciais através de meios eletrônicos. O mais comum é através de alterações de entradas DNS (Domain Name System), serviço responsáveis por transformar um nome, por ora determinado *www.site.com.br*, em um endereço que seja reconhecível pelos sistemas de informação. Um determinado atacante, utilizando de uma vulnerabilidade no *DNS*, altera a informação de *www.site.com.br* para um endereço em que o atacante possua controle, a partir desse momento o usuário ao acessar *www.site.com.br* acredita está acessando o *site* autêntico, quando na verdade está acessando um site clonado pelo atacante devido as alterações realizadas no *DNS*, onde as informações inseridas nesse *site* serão enviadas para o atacante. Um *cavalo de Troia* é um *malware* (programa malicioso) que age tal como na história do Cavalo de Troia, entrando no computador e criando uma porta para uma possível invasão. Utilizando de vulnerabilidades em aplicativos já instalados em computadores, o atacante utiliza um *cavalo de troia* para instalar aplicativos mal intencionados no computador vulnerável e posteriormente furtar informações dos mais diversos tipos do usuário vulnerável através da Internet.

Os grandes riscos de redes públicas são a facilidade de acesso e disponibilidade para todos os usuários. Os ataques descritos são comuns em redes públicas não protegidas e não preparadas para utilização. Se faz necessário a devida configuração e manutenção dos ativos de rede envolvidos no meio de transmissão para os usuários. Serviços como *DNS* devem ser monitorados constantemente para evitar ataques de alteração de entradas, bem como os

usuários devem ser isolados nas redes sem fio para evitar que suas informações sejam transmitidas para um falso destino.

9 SONDAGEM DE REDES SEM FIO

Um atacante pode obter bastante informações através de técnicas de *sniffing*, sem revelar a sua presença e ainda existem outras possibilidades a serem exploradas a partir da técnica de sondagem. O atacante pode enviar pacotes fabricados que podem retornar respostas validas para efetivação dos ataques. Essa técnica também é conhecida como *probing* ou busca ativa, pois, o ponto de acesso pode detectar se está sendo sondado.

9.1 DETECÇÃO DE SSID

A detecção de SSID é possível através da técnica de *sniffing*, escutando os *frames* enviados pelo ponto de acesso. Se o envio de *frames* SSID estiverem desabilitados no ponto de acesso, é possível escutar o meio para detectar solicitações de associação voluntárias de estações conhecidas ao ponto de acesso. As respostas enviadas pelo ponto de acesso a estações associadas podem ser escutadas e contém informações idênticas as enviadas por pontos de acesso que possuem *frames* SSID habilitado.

Alguns pontos de acesso possuem opção que desabilitam respostas de *frames* que não possuem o correto *SSID*. Neste caso, o atacante identifica uma estação associada e envia um *frame* de desautenticação contendo como origem o endereço *MAC* do ponto de acesso. Isso forçará a estação a se reautenticar, informando no *frame* enviado o SSID do ponto de acesso.

10 FALHAS DE CONFIGURÇÃO NO PONTO DE ACESSO

Pontos de acesso podem possui falhas de configuração, sejam estas no design do ponto de acesso ou por interfaces de usuário que proporcionam erros. Muitos pontos de acesso são configurados de maneira incorreta, com criptografia fraca ou até mesmo sem criptografia, deixando o usuário e estações mais vulneráveis a ataques.

10.1 ROGUE AP

Rogue AP são pontos de acesso não autorizados. Se um usuário não intencionado conecta um ponto de acesso não autorizado a uma determinada LAN, o mesmo pode ser utilizado para ataques em camadas superiores.

10.2 TROJAN AP

Um ponto de acesso também pode ser considerado *trojan AP* quando possui o mesmo nome de um ponto de acesso autêntico, quando transmitido com um sinal mais forte, consegue propagar o sinal de maneira que consegue associar estações que procuram o ponto de acesso autêntico, conectando-se a um ponto de acesso falso. A partir desse momento o atacante pode fornecer várias informações falsas e promover vários ataques de camadas superiores, comprometendo informações sigilosas. Para que esse acesso possa ser efetivo, é necessário que o atacante possua informações básicas sobre o ponto de acesso alvo.

11 FALHAS EM DISPOSITIVOS PONTOS DE ACESSO

É possível encontrar na Internet *sites* específicos que reúnem falhas e até mesmo códigos disponíveis com intuito de explorar determinadas falhas. Como exemplo, um determinado ponto de acesso pode travar com o envio de um *frame* fabricado com endereço *MAC* de origem idêntico ao do ponto de acesso. Outros pontos de acesso possuem serviço de *TFTP* embutidos, em que solicitam um arquivo de configuração padrão para determinado endereço IP. O atacante pode

simular ser um servidor *TFTP* e fornecer uma configuração maliciosa para o ponto de acesso.

12 NEGAÇÃO DE SERVIÇO

Determinado pela sigla *DOS (Denial of Service)* ou negação de serviço, é um ataque que tem como objetivo indisponibilizar serviços em geral, tal como autenticadores, páginas *web* e serviços de transferências de arquivos. Quando um serviço passa a receber mais requisições do que o normal, uma capacidade maior de rede e processamento é demandada para atender essas novas requisições. Entretanto, se o número de requisições continue a crescer, a capacidade de rede ou de processamento pode se esgotar, causando indisponibilidade no equipamento e consequentemente no serviço oferecido por este.

Os métodos de ataques podem ser através de falhas no software ou dispositivo provedor do serviço, bem como através de *spoofing* de endereços IP. Determinado endereço “A” provedor de serviço recebe um pacote fabricado baseado em determinada falha, ao processar o pacote recebido, o dispositivo pode romper alguma exceção ou método não detalhado através de software para tratamento do mesmo. Neste momento, o serviço pode tornar-se indisponível. Outro método utilizado é através de *spoofing*, onde vários pacotes são enviados com origens falsificadas para o destino atacado. Na tentativa de processar e responder todos os pacotes recebidos, o dispositivo pode tornar-se indisponível, utilizando toda sua capacidade de processamento.

Há uma variante do *DOS,* que é o *DDOS (Distributed Denial of Service)*, onde a negação de serviço ocorre de maneira distribuída, de forma que, várias estações enviam pacotes com endereços de origem falsificados para a uma única estação, multiplicando assim o poder do atacante.

12 ATAQUES MITM

Os ataques *MITM (Man in the midle)*, são ataques onde um endereço “X” insere informação X na comunicação entre os endereços A e B. Nem o endereço A

ou B estão cientes da presença desse endereço invasor. O atacante X captura os dados e encaminha para o endereço destino autêntico, podendo apenas observar ou manipular as informações.

12.1 MITM EM REDES SEM FIO

Uma determinada estação “A” está associada ao ponto de acesso “C”. O atacante com endereço “X” possui uma estação com dois dispositivos de rede. Em um dispositivo, o atacante permanece associado ao ponto de acesso “C”, em outro dispositivo o atacante passar a enviar *frames* para a estação “A”, fazendo acreditar que é o ponto de acesso “C”, dessa maneira a estação “A” se associa a estação “X”, onde o atacante pode visualizar e alterar informações antes de encaminhar para o ponto de acesso “C”.

12.2 ENVENENAMENTO ARP

ARP (Address Resolution Protocol) é um protocolo utilizado para resolução de endereços IP para endereços da camada de enlace ou endereços *MAC,* no caso das comunicações baseadas em Ethernet.

A camada de enlace precisa conhecer o endereço em que irá comunicar-se, pois determinada estação ao receber um pacote para ser transmitido, difunde uma mensagem na rede solicitando o endereço *MAC* de determinado endereço IP. A estação detentora do endereço IP em questão, responde a mensagem para a estação transmissora. Dessa maneira, a estação transmissora associa o endereço IP ao endereço *MAC* recebido, completando as informações necessárias para transmitir o *frame*.

Um atacante, ao escutar o meio de transmissão, pode responder solicitações *ARP* de maneira com que a estação transmissora, associe determinado endereço IP ao endereço *MAC* do atacante no lugar da estação verídica. Deste modo,

determinada estação “A”, ao enviar um pacote para estação “B”, na verdade estará enviando o pacote para a estação X, acreditando tratar-se da estação B. Fica a critério do atacante analisar as informações recebidas e repassá-las a estação verdadeira ou interceptar as informações e não encaminhá-las a estação verdadeira.

13 CONSIDERAÇÕES FINAIS

Ao optar por fornecer uma rede de acesso pública para usuários, o provedor do serviço deve estar ciente dos riscos envolvidos ao fornecer esse tipo de acesso. Os ativos de rede envolvidos devem estar em constante monitoramento para evitar que ataques ocorram no meio de acesso e prejudiquem um ou mais usuários. O usuário por sua vez também deve manter-se em alertar para os riscos existentes ao acessar as redes públicas. Manter o computador atualizado e utilizar softwares que protegem de ameaças, tais como firewalls e antivírus, ajudam o usuário a não tornar-se vítima dos possíveis ataques descritos dessas redes disponíveis nos ambientes públicos. Levando em consideração que a maioria dos ataques são imperceptíveis para os usuários, mecanismos de acesso seguro devem ser utilizados como medida preventiva. Um bom exemplo é a utilização de serviços com camadas de criptografia, como é o caso do *HTTPS* para acessos a páginas WEB e *SSH* para acesso a servidores remotos, substituindo o *telnet*.

14 REFERÊNCIAS

LEMOS, A.; PASTOR, L. ; OLIVEIRA, N. Wi-Fi Salvador: mapeamento colaborativo e redes sem fio no Brasil. *Intercom, Rev. Bras. Ciênc. Comun.*[online]. 2012, v. 35, n.1, p.183-204

NAKAMURA, E. T.; GEUS, P. L. Novatec, : . *Segurança em redes cooperativos*. 2007, 1ª Ed. (São Paulo [s.n.])

OLIVOA, C. K.; SANTINA, A. O.; OLIVEIRA, L. S. Obtaining the threat model for e-mail phishing. *Rev. Applied Soft Computing*, v. 13, 2013, p. 4841–4848

https://pt.wikipedia.org/wiki/Eavesdropping - Acessado em 26/02/2016

https://pt.wikipedia.org/wiki/Sniffing - Acessado em 26/02/2016

https://pt.wikipedia.org/wiki/Phishing - Acessado em 26/02/2016

https://pt.wikipedia.org/wiki/Address_Resolution_Protocol - Acessado em 26/02/2016

http://www.webartigos.com/artigos/seguranca-em-redes-wireless-802-11x/53409/ - Acessado em 26/02/2016

https://www.vivaolinux.com.br/artigo/Portal-de-autenticacao-wireless-(HotSpot) - Acessado em 26/02/2016