DOI: 10.5748/9788599693124-13CONTECSI/PS-3788

ROGUE ACCESS POINT: INSECURITY IN ACCESSING OPEN WIRELESS NETWORKS

Jean Eurípedes Do Carmo Vieira (Faculdade Pitágoras de Uberlândia, Minas Gerais, Brasil) - jvieira.udi@gmail.com
Rogerio de Freitas Ribeiro (Faculdade Pitágoras de Uberlândia, Minas Gerais, Brasil) – rogeriofr@gmail.com

This study describes the risks when connecting to a open Wireless network. For this, the article is based on a scenario tested in a controlled environment in order to describe the risks and discuss the concerns that users of this type of network must be take into consideration. Will be presented some results of network traffic captures, that the user can have their information captured when it connects to an open Wireless network. The aim of this study is to make a contribution to the awareness of readers, which should take some precautions before connecting to an Internet network through a wireless network without security.

Keywords: Rogue AP, Wireless, Encryption, Security, Interception.

ROGUE ACCESS POINT: INSECURITY IN ACCESSING OPEN WIRELESS NETWORKS

Este estudo descreve os riscos que se corre ao se conectar a uma rede Wireless aberta. Para isto, o artigo se baseia em um cenário testado em ambiente controlado com o objetivo de descrever os riscos e discorrer sobre as preocupações que os usuários deste tipo de rede devem levar em consideração. Serão apresentados alguns resultados de capturas de trafego de rede, onde o usuário pode ter suas informações capturadas quando o mesmo se conecta a uma rede aberta. O principal objetivo deste estudo é deixar como contribuição a conscientização do leitor, que deve tomar certos cuidados antes de se conectar a uma rede Internet através de uma redes em fio não confiável.

Palavras-chave: Rogue AP, Wireless, Criptografia, Segurança, Interceptação.

1. Introdução

A Internet tornou-se essencial para várias instituições, sejam grandes ou pequenas empresas, universidades, instituições financeiras, empresas privadas ou órgãos do governo. Seja qual for o segmento de uma empresa, provavelmente esta deva ter algum tipo de serviço que é oferecido através de recursos computacionais. Estes serviços quando públicos, normalmente são acessíveis pelos usuários ou consumidores através da grande rede de computadores chamada de Internet.

Segundo (EMPRESA AGIL, 2014) "Estar bem posicionado na Internet, também é fundamental para o sucesso de um negócio. A Internet é o meio de comunicação mais eficaz e estratégico para se aproximar dos clientes e consumidores ... uma marca ou empresa que não apresenta um bom relacionamento digital com seus consumidores e clientes perdem preciosos pontos para os concorrentes. Lembre-se, muitas vezes o concorrente esta à distância e a um clique".

Vários são os motivos pelos quais estas empresas são levadas a oferecer os seus serviços através da rede mundial de computadores. Como exemplo de alguns destes motivos, não se limitando a estes, podemos citar: a redução dos custos com atendimento presencial, a não limitação do horário de funcionamento e a comodidade no uso ou consumo do serviço por parte do usuário final.

Analisando os motivos citados acima, para um caso de uma instituição bancária que ofereça o serviço de *Internet Banking*, esta se beneficiaria com o oferecimento deste serviço em todos os motivos citados.

Baseando-se apenas no primeiro motivo, que trata-se da redução de custos com o atendimento, temos o seguinte cenário. Imagine um serviço de *Internet Banking* oferecido através de uma página *Web* que suporte facilmente 200 usuários concorrentes acessando o seu saldo e realizando transferências bancárias. Para que esta empresa possa manter disponível este serviço, ela precisaria de uma infraestrutura computacional, incluindo computadores de médio porte "servidores", *links* de Internet e equipe especializada para manutenção. Em contrapartida, imagine os custos envolvidos se estes mesmos duzentos usuários decidissem ir a uma agência bancária para utilizar os mesmos serviços e ao mesmo tempo. Seriam 200 atendentes com seus encargos trabalhistas, 200 micro computadores com acesso ao sistema interno, espaço físico para acomodar os clientes e atendentes e vários outros recursos.

Mesmo sem apresentar uma planilha de custos formal entre os dois modelos de prestação de serviço (presencial e *Internet Banking*), é razoável e plausível aceitar que o modelo de serviço na Internet possui um custo relativamente menor.

Obviamente as empresas só oferecem os seus serviços e produtos na Internet, pois existem clientes e consumidores interessados e dispostos a realizar este consumo no formato digital.

Segundo (VAZ, 2007) "não saber usar a Internet em um futuro próximo será como não saber abrir um livro ou acender um fogão ...".

Segundo pesquisa realizada pela empresa Pew Research em 2014, o Brasil é o sétimo colocado entre os países que possuem adultos que acessam a Internet todos os dias. Conforme a figura 1, o Brasil possui a proporção de 75% dos adultos que acessam a Internet todos os dias.

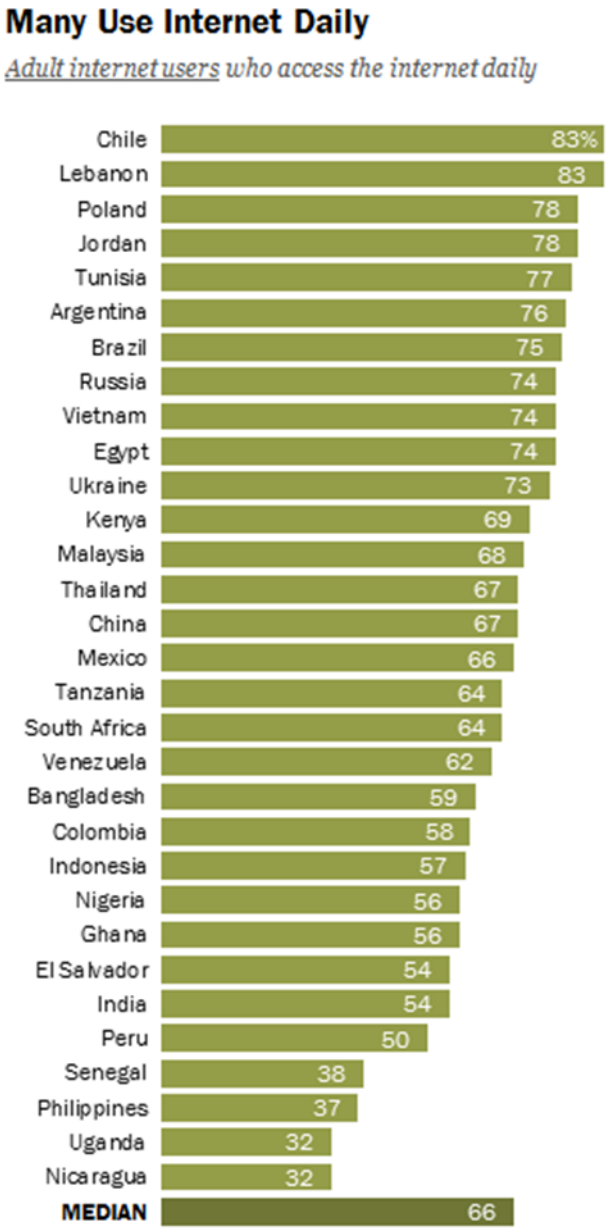

Figura 1: Adultos que utilizam a Internet diariamente.
Fonte: (PEW RESEARCH, 2014)

Um ponto importante que ainda deve ser destacado, é que as redes Wireless (Redes sem Fio), estão sendo cada vez mais, o meio físico preferido para se ter acesso à rede Internet. Isto se dá em sua maior parte pelo uso de dispositivos móveis para o acesso à Internet, como: celulares, *notebooks* e *tablets*.

De acordo com o relatório de Tecnologias da Informação e Comunicação em Domicílios realizado pelo Comitê Gestor da Internet no Brasil (CGI.br) e comentado pelo site Valor Econômico, o acesso à Internet no Brasil através do celular, triplicou nos últimos 3 anos. (VALOR ECONOMICO, 2015)

É sabido que a Internet está entre nós e o seu uso é cada dia maior, seja em nossas atividades profissionais, sociais e pessoais. Mas atrás de toda essa praticidade existe o lado

negativo deste contexto, no qual *crackers*[1] tentam causar problemas, acessando indevidamente computadores e sistemas conectados às redes de computadores, violando a privacidade, a confidencialidade, a integridade das informações e até mesmo tornando inoperantes os serviços de uma determinada empresa através de ataques conhecidos como, *DOS - Deny Of Service*[2] ou em português, negação de serviço.

Logo, o trabalho tem como tema a insegurança ao utilizar redes sem fio não confiáveis. Este trabalho partiu da seguinte problemática: quais os riscos que se corre ao se conectar a rede Internet através de uma rede sem fio aberta? Entende-se neste contexto como rede aberta, qualquer tipo de rede sem fio, onde não seja necessário o cadastro ou autenticação de acesso à esta rede com algum tipo de senha.

Esta mesma preocupação, já foi comentada em artigo sobre segurança com título "Dono de rede sem fio com senha, pode interceptar dados?" escrito por Altires Rohr. O autor relata em sua coluna sobre segurança no site da Globo.com que "... o "dono" da rede sempre tem essa capacidade. Inclusive seu próprio provedor de Internet tem acesso aos dados trafegados." (ROHR)

Assim o artigo se justifica, pois a dependência é cada vez maior dos usuários de se manterem conectados à Internet e consumirem serviços oferecidos nesta rede. Esta dependência se torna tão grande, que o desejo dos usuários em se manterem conectados se torna cada vez mais comum. Isto pode ser percebido através de uma reportagem exibida em 28 de Outubro de 2015 pela rede Globo de televisão intitulada, "Barracas da praia oferecem rede sem fio", o que reforça a existência deste comportamento por parte da população, que até mesmo em momento de lazer e descanso, em uma praia, é comum o desejo e necessidade de se manter conectado. (GLOBO.COM)

2. Metodologia

Estre trabalho busca levar ao conhecimento dos leitores quais os riscos associados ao utilizar uma rede sem fio aberta. Para atingir este objetivo será realizada uma fundamentação teórica sobre os conceitos básicos para entendimento dos riscos comentados.

Serão apresentados ainda, os resultados obtidos durante a realização de um laboratório proposto, com o objetivo de detalhar de forma prática, qual seria o nível de dificuldade que um *cracker* encontraria para realizar um ataque, para a captura de dados dos usuários que se conectarem a uma rede sem fio aberta. Neste laboratório, serão apresentadas as técnicas e ferramentas que poderiam ser utilizadas para a interceptação de informações confidenciais, como senhas de banco, usuário e senha de acessos a e-mails e redes sociais, além de outras informações sensíveis.

É importante reforçar que o objetivo final do trabalho é alertar os usuários de tais riscos e deixar como contribuição, informações de prevenção, evitando assim vários transtornos sofridos por vítimas dos ataques apresentados, além de enfatizar a importância da segurança da informação. De forma alguma, o laboratório proposto tem como objetivo incentivar ou realizar apologia a práticas criminosas. Deve ser lembrado que interceptação de dados sem autorização é passível de punição baseado na legislação Brasileira.

Além do objetivo principal, o trabalho ainda se divide em três objetivos específicos, são eles: explicar o conceito de rede *wireless* aberta; mostrar a diferença entre uma rede *wireless* aberta e uma rede controlada (criptografada); e apontar os riscos ao utilizar uma

[1] Crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos.
[2] Informações adicionais sobre o ataque de negação de serviço podem ser consultados em (LAUFER et al).

rede aberta.

No intuito de alcançar estes objetivos são apresentados os resultados obtidos após simulação em um ambiente controlado. Estes resultados demonstram parte do que um *cracker* pode conseguir realizar com um ataque conhecido como homem do meio "*Man-In-The-Middle*". Este ataque é caracterizado neste artigo pela utilização de um sistema conhecido como *Rogue Access Point* (*Rogue* AP), em português "Ponto de Acesso Fraudulento".

Assim, o artigo está estruturado da seguinte forma:

- Introdução;
- Conceituação Teórica;
- Resultados obtidos na simulação;
- Considerações finais;
- Referências.

2. Referencial Teórico

Este capítulo descreve os conceitos teóricos básicos que são necessários para que o leitor tenha um melhor entendimento sobre o assunto abordado.

2.1. Pilares da Segurança da Informação

Dentro da segurança da informação existem três aspectos chaves conhecidos como a tríade CID (Confidencialidade, Integridade e Disponibilidade). Estes três itens são considerados como os pilares básicos da segurança da informação. Desta forma, qualquer processamento, armazenamento e transmissão de dados devem atender os requisitos de segurança definidos por estes três pilares.

A confidencialidade é um aspecto que garante que as informações só devem ser acessíveis à indivíduos ou sistemas autorizados, isto é, apenas os envolvidos com autorização direta, devem possuir privilégios que permitam o acesso às informações nos contextos de armazenamento, processamento ou transmissão. Atualmente o mecanismo mais comum e considerado mais seguro para permitir o atingimento deste requisito é através do uso de algoritmos de criptografia.

A integridade é o aspecto que se preocupa em dar confiança para que seja possível atestar que uma informação não sofreu alterações de forma intencional ou não intencional. Para que este pilar seja mais bem entendido, imaginemos uma informação que está sendo transmitida entre dois equipamentos. Quando temos a condição de ter certeza que a informação que saiu do equipamento A é a mesma informação que chegou ao equipamento B, dizemos que existe o pilar da integridade, pois os dados não foram alterados durante a transmissão. Atualmente, o mecanismo mais comum e considerado seguro para atender os requisitos de integridade é uso de algoritmos de resumo ou *Hash* em conjunto com os mecanismos de criptografia.

A diferença básica entre a confidencialidade e a integridade, é que o primeiro pilar se preocupa em garantir que a informação seja de conhecimento somente das pessoas autorizadas. Já o segundo pilar, a integridade, se preocupa em apenas garantir que uma informação não foi alterada entre dois momentos específicos, independente de quem está acessando a informação.

O último pilar da tríade CID, trata do conceito relativo à disponibilidade. O pilar da disponibilidade só é atendido, quando uma informação ou ambiente computacional sempre

esteja disponível quando o usuário tiver a necessidade de acesso (informação) ou uso (ambiente computacional). Atualmente o atingimento da disponibilidade está muito relacionado à construção de sistemas computacionais redundantes, de tal forma que se um dos componentes vitais para o seu funcionamento falhe, o sistema ainda continue em funcionamento graças aos componentes secundários (redundantes).

2.2. Criptografia

Para o atingimento da maioria dos requisitos de segurança nos dias de atuais, é inevitável o uso dos conceitos de criptografia. No entanto o assunto criptografia é extenso e complexo, desta forma são abordados neste artigo apenas os conceitos básicos da criptografia simétrica. Informações sobre os processos de criptografia simétrica e assimétrica podem ser consultados em (BURNETT, 2002).

Criptografar uma informação, trata-se basicamente de um conjunto de passos que um indivíduo ou sistema realiza com o objetivo de tornar esta mesma informação, em uma informação ininteligível (não entendível) à outros envolvidos não autorizados. Isto significa que um indivíduo, mesmo que tenha acesso físico a esta informação, não terá condições de entender o real significado desta informação. Quando esta situação ocorre dizemos então que o pilar da confidencialidade foi atingido.

Imagine que José deseja armazenar um arquivo em um computador que é utilizado também por outros usuários. José deseja guardar este arquivo no computador de forma que somente ele, tenha condições de realmente conhecer o conteúdo do arquivo. Como o computador é compartilhado por outros usuários, o simples fato de armazenar (1) este arquivo localmente neste computador, criará uma situação em que os outros usuários possam ter acesso ao arquivo e conhecer o seu real conteúdo (2). A figura 2 apresenta este cenário.

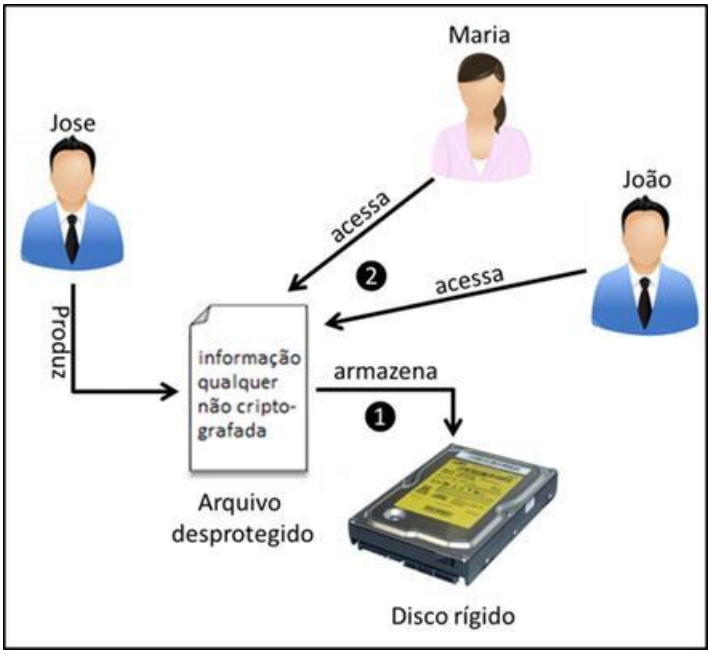

Figura 2: Cenário de arquivo desprotegido armazenado em local compartilhado.
Fonte: Criado pelos próprios autores.

Para que José consiga obter as características da confidencialidade, ele precisa armazenar este arquivo protegido (criptografado) no disco para impedir que os demais

usuários tenham condições de conhecer o real conteúdo.

A figura 3 apresenta como seria este processo. José produz um documento qualquer que necessita ser protegido (1) e utiliza um sistema de criptografia (2) para "transformar" a informação inteligível em uma informação ininteligível (4), com apoio de uma frase secreta[3] (3). O arquivo ininteligível é então armazenado em um meio qualquer de armazenamento (5). Mesmo que outros usuários não autorizados tentem acessar a informação armazenada (6), estes não terão condições de entender o conteúdo do arquivo. Para que estes possam reverter o processo de criptografia "transformação", eles precisariam conhecer a frase secreta utilizada por Jose.

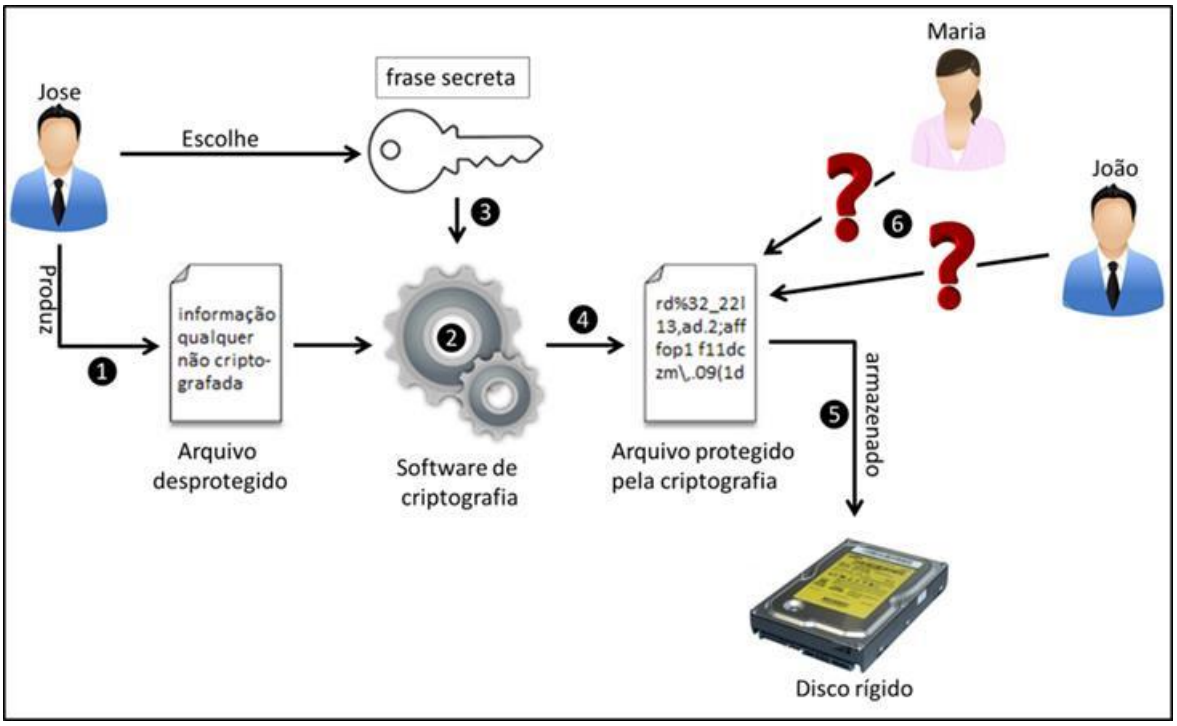

Figura 3: Cenário de arquivo protegido (criptografado) armazenado em local compartilhado.
Fonte: Criado pelos próprios autores.

Para que José possa ler o conteúdo do arquivo, ele precisará utilizar um sistema que irá realizar o processo inverso para transformar o arquivo ininteligível para o arquivo que possa ser entendido por ele. No entanto, José precisará se lembrar da mesma frase secreta utilizada no processo de criptografia do arquivo. Caso José utilize uma frase secreta incorreta, o processo de descriptografia não conseguira reverter o arquivo corretamente para a informação original. As figuras 4 e 5 descrevem o funcionamento do processo de descriptografia com a chave correta e com a chave incorreta respectivamente.

[3] Frase Secreta: Também conhecida como chave secreta na criptografia simétrica, trata-se de uma informação, conjunto de caracteres, que é utilizada pelo processo de criptografia para transformar o arquivo original em um arquivo criptografado. Quando um arquivo é criptografado várias vezes com chaves de criptografia diferentes, é gerado diferentes arquivos criptografados. Desta forma, a chave de criptografia torna-se um dos itens mais importantes em um processo de criptografia. A chave de criptografia deve ser conhecida apenas pelos usuários autorizados a conhecer o real conteúdo do arquivo. Usuários que não possuam ou não conheçam a frase secreta, não conseguirão entender o conteúdo do arquivo criptografado. Na criptografia simétrica a chave secreta que criptografa um arquivo deve ser a mesma chave para realizar o processo inverso.

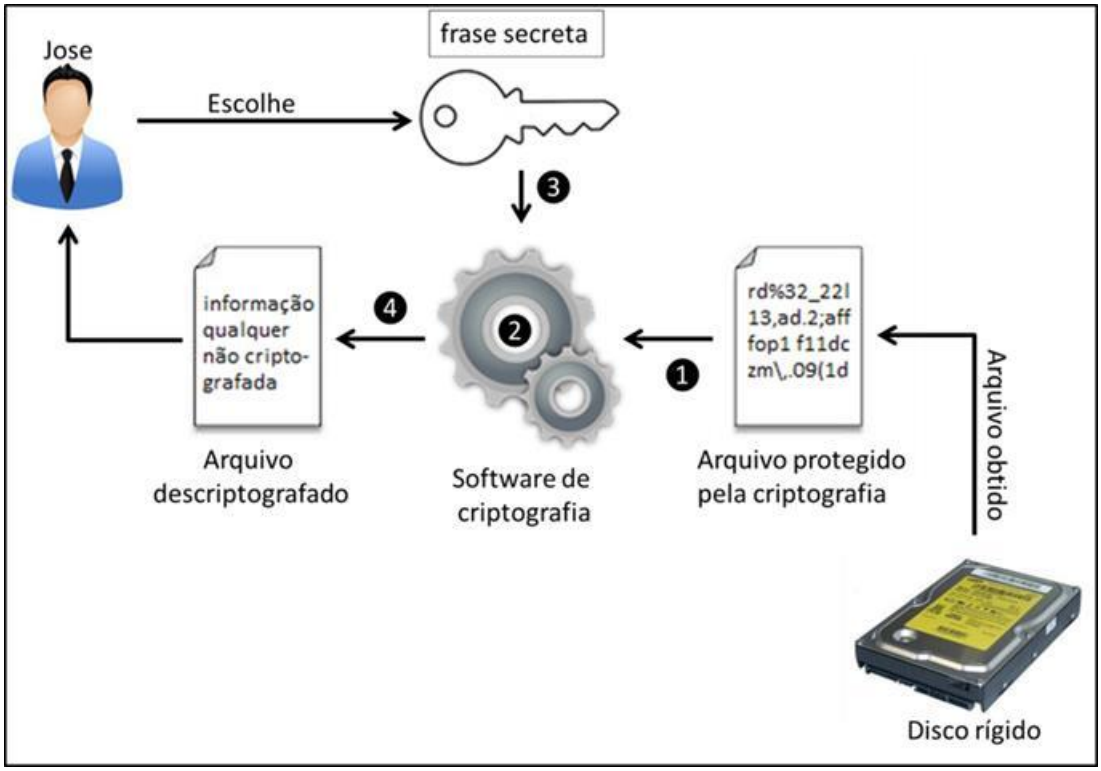

Figura 4: Processo de descriptografia utilizando a frase secreta correta. Note que o arquivo descriptografado pode ser entendido corretamente.
Fonte: Criado pelos próprios autores.

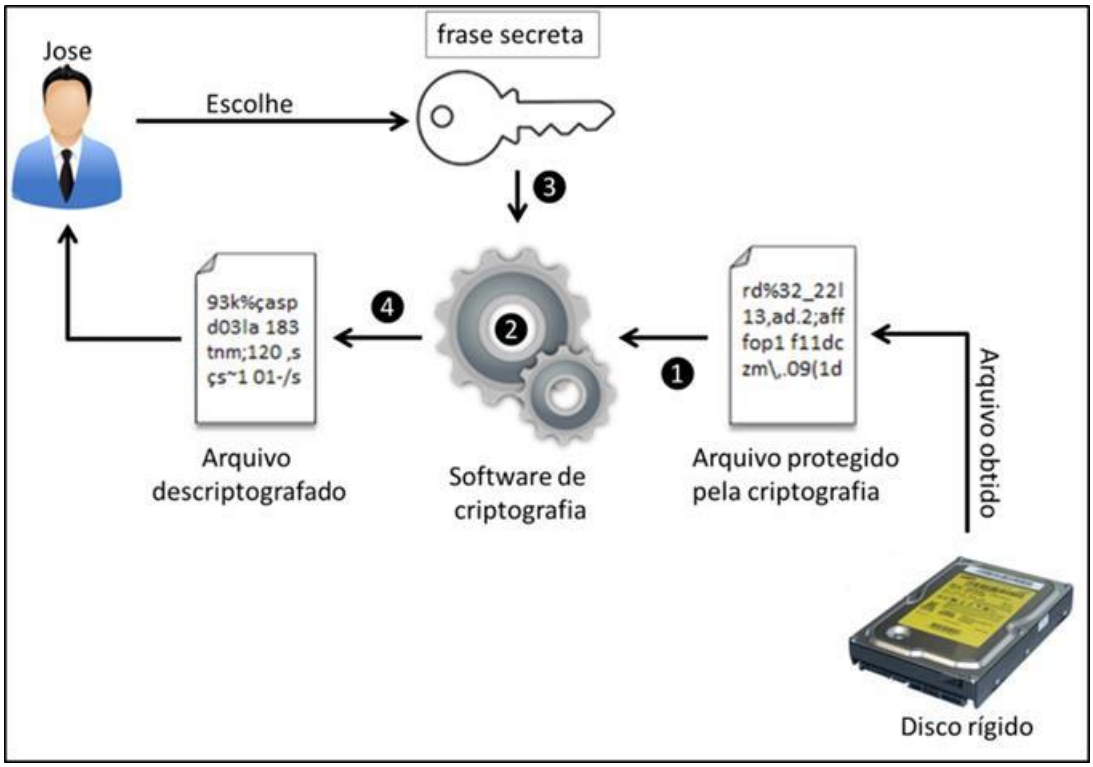

Figura 5: Processo de descriptografia utilizando a frase secreta incorreta. Note que o arquivo descriptografado não reflete a informação original.
Fonte: Criado pelos próprios autores.

Caso José também desejasse que outro usuário também pudesse ler o conteúdo do arquivo, por exemplo, Maria, ele precisará apenas compartilhar de maneira segura, a frase secreta com ela. Uma vez que Maria tenha a frase secreta, ela pode utilizar um sistema que irá realizar o processo inverso para transformar o arquivo ininteligível para o arquivo que possa ser entendido por ela. Basta que seja utilizado a frase secreta informada por José para descriptografar o arquivo. Note que agora ambos, José e Maria possuem condições de ler o conteúdo do arquivo através do processo de descriptografia.

Em uma rede sem fio, a criptografia tem como objetivo proteger a confidencialidade dos dados transmitidos entre o cliente da rede sem fio e o ponto de acesso que provê o sinal. Através deste mecanismo é possível garantir a confidencialidade dos dados trafegados na rede impedindo que indivíduos que não façam parte desta rede, não consigam ter acesso ao conteúdo.

2.3. Integridade

Conforme apresentado anteriormente, a integridade é o aspecto que se preocupa em dar confiança para que seja possível atestar que uma informação não sofreu alterações de forma intencional ou não intencional.

Nos dias atuais, o mecanismo mais comum para implementação do pilar da integridade é a utilização de algoritmos de resumo. O termo algoritmo de resumo também pode ser encontrado na literatura pela definição de *checksum* criptográfico ou função *hash*.

De maneira simplista, um *checksum* trata-se de uma informação adicionada à informação original, de tal forma, que após alguns cálculos matemáticos com a informação original, possa se dizer se a informação avaliada está correta sobre o aspecto da integridade com base no *hash*. Este processo é muito utilizado em números que possuem um dígito verificador. Como exemplo deste processo, podemos citar códigos de pagamento em sistemas bancários bem como os números de CPF. A figura 6 apresenta um cartão de CPF contendo o código de verificação destacado.

Figura 6: Digito verificador de um CPF.
Fonte: (MEIER)

Para um entendimento mais detalhado de como funciona o processo de geração de um *checksum* do CPF, pode-se utilizar como referencia o autor (MEIER). Apesar do dígito verificador de um CPF ser um processo muito mais simples do que um *checksum* criptográfico, o mesmo é útil para o entendimento geral do processo.

Em uma comunicação o mecanismo de integridade funcionaria da seguinte forma. A origem antes de enviar uma determinada informação, gera o *checksum* criptográfico e adiciona este resultado na informação original. Após esta etapa a informação mais o *hash* são transmitidos para o seu destino. Durante a receptação da informação, é necessário verificar se os dados recebidos estão íntegros, ou seja, se a informação não foi adulterada.

Para isto, no destino é executado novamente o cálculo do *checksum* e verificado se os dois resumos, o gerado na origem e o gerado no destino, são os mesmos. Se ambos os resumos forem iguais, significa que a informação não sofreu alterações entre a origem e o destino. Se os resumos forem diferentes, a informação não é integra e deve ser descartada. A figura 7 descreve o funcionamento da verificação de integridade em um mecanismo de comunicação qualquer.

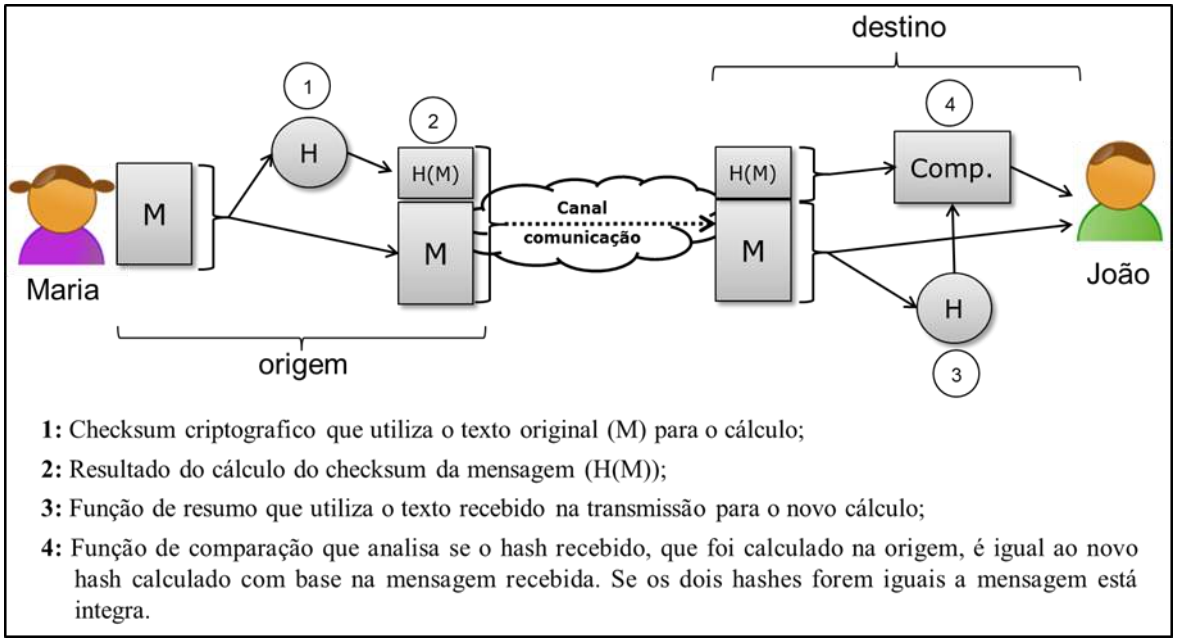

Figura 7: Verificação da integridade em uma comunicação qualquer com base no uso de algoritmos de *hash*.
Fonte: Criada pelos próprios autores.

Para impedir que o processo de integridade possa ser burlado em um ataque, é importante que o *hash* seja criptografado antes da transmissão para impedir a sua manipulação.

O mecanismo de integridade dentro de uma rede sem fio tem como objetivo identificar se os pacotes não foram adulterados entre a transmissão e recepção dos dados.

2.4. Autenticação

Na segurança da informação, a autenticação é um processo que tem com objetivo buscar a verificação da identidade real do usuário em um sistema. Este processo existe para que os usuários tenham os seus acessos controlados, garantindo que somente as pessoas autorizadas pelas credenciais de autenticação possam ter acesso ao sistema.

Apesar de existir vários mecanismos de autenticação, o mecanismo mais comum e simples de ser implementado é através da dupla usuário e senha. Neste tipo de autenticação, o usuário real possui um par de informação que o identifica, neste aso, o seu nome de usuário digital e a senha escolhida. Para que o usuário tenha acesso a um sistema que utilize este mecanismo de autenticação, é necessário no momento do acesso, que ele forneça as informações de usuário e senha conforme foram cadastradas no sistema.

A figura 8 apresenta um processo de autenticação de um usuário no sistema. A figura 9 apresenta um diagrama de sequencia com os passos mais detalhados do que ocorre neste processo.

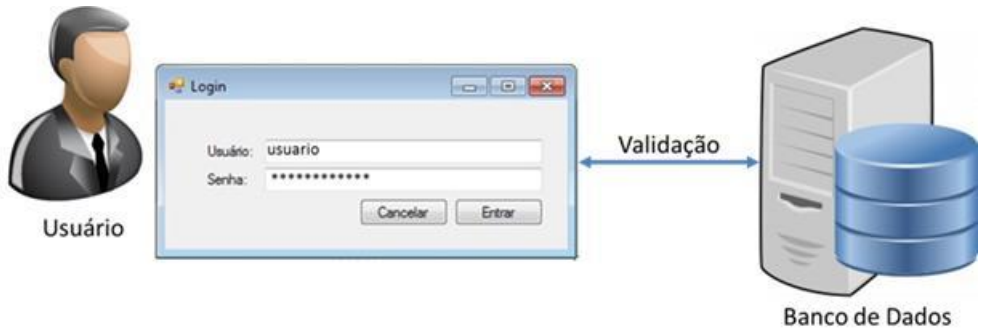

Figura 8: Exemplo de autenticação de um sistema em banco de dados.
Fonte: Fonte: Criada pelos próprios autores.

Figura 9: Diagrama de sequencia do processo de autenticação.
Fonte: Fonte: Criada pelos próprios autores.

Em uma rede sem fio, o mecanismo de autenticação quando habilitado, tem como objetivo restringir quem serão os usuários que podem fazer parte desta rede.

2.4 Conceito de Rede *Wireless* Aberta

Uma rede *Wireless* é uma infraestrutura de comunicação sem fio que permite a transmissão de dados e informações sem a necessidade do uso de cabos metálicos ou óticos. Isso é possível graças ao uso, por exemplo, de equipamentos de radiofrequência que realizam as comunicações através de ondas de rádio, ou de comunicações através de infravermelho como em dispositivos compatíveis com o *Infrared Data Association* (IrDA). Este tipo de rede também é conhecido pelo anglicismo *Wireless Network* (Rede Sem Fio).

Seu uso mais comum é em redes de computadores, servindo como meio de acesso à redes privadas ou até mesmo a uma rede pública como a Internet. Este acesso pode ser realizado a partir de locais remotos como um escritório, bares, aeroportos, parques, residências, academias ou qualquer outro estabelecimento que tenha o interesse de oferecer ao seus respectivos usuários e/ou clientes, a comodidade de uso da rede Internet durante a sua permanência nas dependências físicas do estabelecimento.

No quesito segurança, pode-se dizer que nenhuma rede ou sistema é completamente

seguro. Entretanto, para as redes sem fio se faz necessário acrescentar um fator extra na questão de segurança quando comparada à rede cabeada. A interceptação de dados em uma rede cabeada cria uma dificuldade adicional para o atacante, que deve ter acesso físico ao cabeamento ou a um dispositivo de rede como um switch ou roteador, para que seja possível a captura dos dados. Já no caso de redes sem fio, esta necessidade de ter acesso físico ao cabeamento não existe, pois as redes *Wireless* utilizam ondas eletromagnéticas como meio de acesso, tornando muito mais difícil controlar a sua abrangência. É comum que o espectro eletromagnético de um ponto de acesso à rede sem fio, possa facilmente ultrapassar os limites físicos do local que se deseja oferecer o serviço de acesso. Quando isto ocorre, é possível a detecção destes sinais, a captura e utilização das informações trafegadas nesta rede por pessoas não autorizadas que estejam ao alcance deste espectro.

A figura 10 representa esta situação exposta. Imagine um apartamento em um condomínio onde o morador realizou a instalação de um ponto de rede sem fio, para permitir que os dispositivos móveis da residência possam se conectar a rede interna e ter acesso à Internet, através de qualquer tipo de conexão como modens ou roteadores. Neste cenário o sinal deste ponto de acesso seria facilmente capturado pelos apartamentos vizinhos ou pelas áreas externas do condômino, pois o espectro eletromagnético "escaparia" para outras áreas além da área privada do apartamento.

Figura 10: Representação do espectro eletromagnético.
Fonte: Imagem adaptada pelos autores.

Devido ao baixo custo e facilidade de instalação, mesmo um leigo conseguiria instalar rapidamente uma ponto de acesso *Wireless*, com o uso de equipamentos adquiridos a um baixo custo, usando a sua configuração padrão. Essa prática leva à implementação de uma rede funcional, no entanto considerada aberta, pois esta, não utiliza recursos para proteger (criptografia) os dados sob o aspecto da confidencialidade, pois normalmente a configuração padrão dos equipamentos não traz os parâmetros de criptografia habilitados.

Uma rede para que se tenha uma configuração com os padrões aceitáveis de segurança, necessita de conhecidos adequados para a sua configuração ou até mesmo um custo maior para a aquisição de equipamentos que ofereçam uma maior quantidade de recursos de segurança e confiabilidade.

Na maioria das vezes, como estes locais não possuem uma política de controle de acesso, qualquer um pode acessar a rede, bastando estar dentro do alcance do espectro eletromagnético do ponto de acesso, ou seja, permite acesso não autorizado e não

identificado à rede, também por não utilizar comunicação criptografada, qualquer um pode capturar o tráfego e ter acesso a tudo que trafega nesta rede, como e-mails, dados confidenciais e outras informações sensíveis. Em empresas menores, muitas vezes estas redes *Wireless* abertas são instaladas em setores administrativos, o que torna ainda mais grave o problema de interceptação de dados sensíveis.

Outro problema existente com as redes Wireless aberta, é que não existe nenhum mecanismo de autenticação. Desta forma, qualquer usuário que esteja ao alcance dos sinais eletromagnéticos terão condições de acessarem esta rede e os recursos compartilhados pela mesma.

Como pode ser visto, uma rede sem fio aberta é muito vulnerável a uma série de ataques. Isto ocorre pela ausência dos mecanismos de segurança que na maior parte das vezes existem mas não são configurados e habilitados.

2.5 Diferenças entre rede aberta e rede criptografada

Uma rede aberta não possui nenhum tipo de controle de acesso e nem garantia de confidencialidade e integridade das informações trafegadas nessa rede. Já uma rede criptografada necessita de autenticação de acesso e as informações são criptografadas para que se possa ter um índice razoável de segurança.

Na figura 11, podemos visualizar um exemplo de uma rede aberta e uma rede protegida, quando um usuário realiza a escolha da rede para se conectar em um *Smart Phone* por exemplo.

Figura 11: Exemplo de uma rede aberta (WiFi Gratis) e de uma rede protegida (Netvirtua_401C1 "ícone do cadeado") sendo visualizada em um *SmartPhone.*
Fonte: Criada pelos próprios autores.

Para tornar esse tipo de comunicação viável, não só para empresas que decidem conectar seus usuários por meio de redes sem fio, mas, também, para que os usuários domésticos possam realizar suas transações financeiras com mais segurança e privacidade, deve ser utilizado uma rede sem fio protegida por criptografia. Os tipos de criptografia

disponíveis para o uso nas redes *Wireless* são o WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*) e WPA2 (*Wi-Fi Protected Access* 2).

O WEP[4] trata-se de um protocolo que foi lançado como um padrão de segurança em 1997 e tornou-se o pioneiro no assunto de proteção de redes sem fio. Ele utiliza o algoritmo RC4 para criptografar os pacotes que são trocados em uma rede sem fios e usa também uma função para detecção de erros que verifica se a mensagem recebida foi corrompida ou alterada durante a sua transmissão.

O RC4 usa uma chave secreta compartilhada que deve estar configurada no roteador *wireless* ou ponto de acesso, bem como em todas as estações que se conectam a ele (notebooks, *tablets*, celulares e outros dispositivos portáveis). A figura 12 apresenta a interface de configuração de um ponto de acesso sem fio com os algoritmos de criptografia suportados, conforme pode ser visto no campo "*Security Mode*".

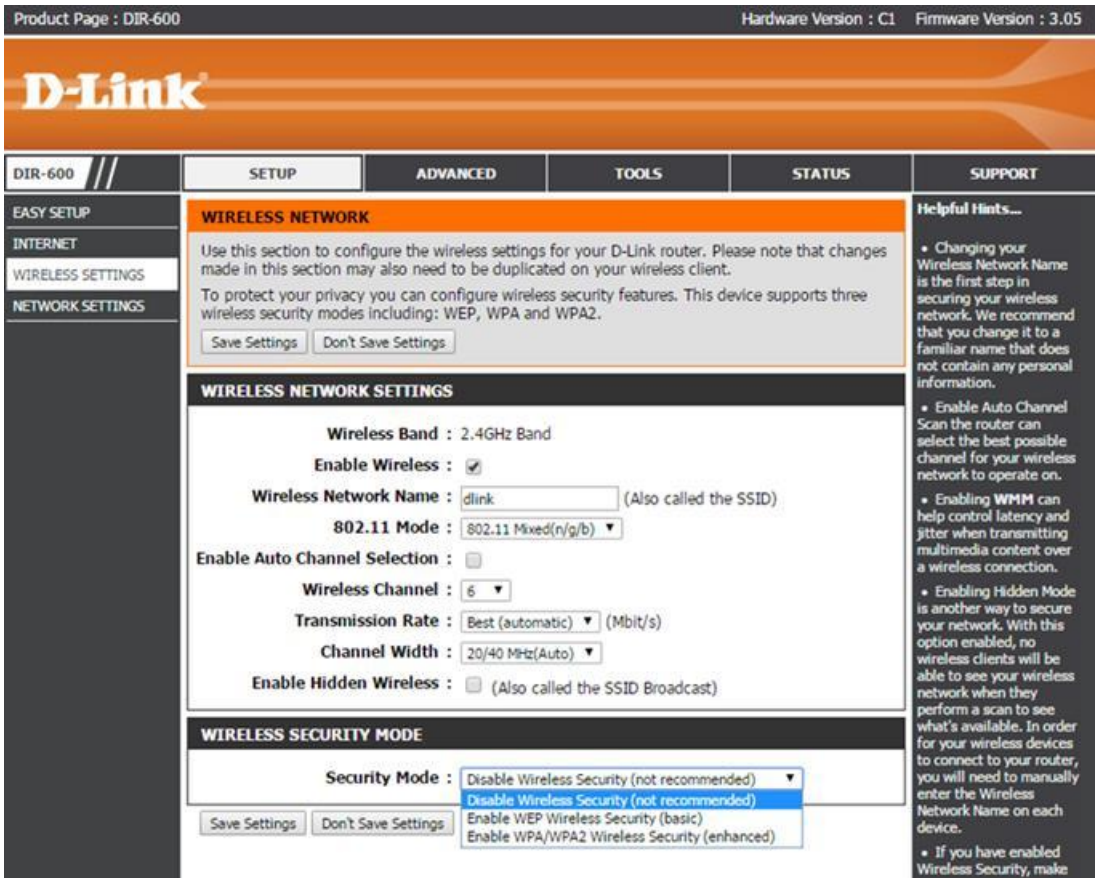

Figura 12: Página de configuração do modo de segurança do roteador D-Link DIR-600.
Fonte: Criada pelos próprios autores.

Como ocorre com o WEP, o WPA também fornece autenticação e criptografia para redes sem fio. O WPA pode oferecer uma criptografia significativamente mais segura do que o WEP, dependendo de como é configurado. No entanto, o WPA não é tão universalmente suportado como o WEP, quando falamos em pontos de acessos mais antigos.

O WPA possui dois modos, o WPA-PSK (PSK: *Pre Shared Key*), que significa chave pré-compartilhada, e o WPA-EAP (EAP: *Extensible Authentication Protocol*) que

[4] WEP: Atualmente o WEP é considerado um algoritmo de criptografia fraco uma vez que existem falhas no seu funcionamento o que permite um *cracker* descobrir as chaves pré-compartilhas através de um software específico. Como referencia sugerimos [100 Secutiry].

significa protocolo de autenticação extensível.

O WPA2 é uma versão atualizada do WPA, oferecendo segurança aprimorada e melhor proteção contra ataques. Também possui métodos de autenticação como o WPA que são o WPA2-PSK e WPA2-EAP. A figura 13 apresenta as opções de configuração, no campo *Chiper Type*, quando o método de criptografia escolhido for o WPA.

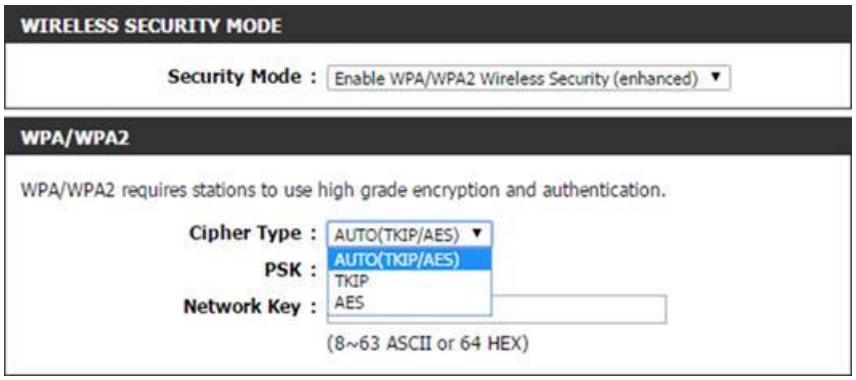

Figura 13: Página de configuração do modo de segurança WAP / WAP2.
Fonte: Criada pelos próprios autores.

Em resumo, quando o ponto de acesso está configurado para utilizar um dos mecanismos de criptografia e autenticação, os usuários só conseguirão acessar a rede sem fio, caso os mesmos possuam a chave pré-compartilhada fornecida pelo administrador ou responsável pela rede sem fio. Apesar de não existir cem por cento de segurança, dado as técnicas de quebra da rede sem fio por força bruta ou engenharia social, a utilização de redes sem fio configuradas para utilizarem mecanismos de criptografia, sempre deve ser preferido em relação ao uso de redes sem fio sem proteção. A figura 14 apresenta de forma didática uma rede com dispositivos configurados corretamente e um dispositivo não configurado.

Figura 14: Rede sem fio com autenticação de chave pré-compartilhada.
Fonte: Criada pelos próprios autores.

2.6 Riscos na utilização de uma rede aberta

Como já discutido, uma rede *Wireless* aberta, trata-se de uma rede sem fio sem proteção quanto aos aspectos de autenticação e confidencialidade (criptografia). Este tipo de rede pode ser usado como base para ataques, podendo ter como alvo tanto a rede interna quanto à rede Internet. O usuário ao se conectar nesse tipo de rede pode sofrer ataques de captura de tráfego onde seus dados podem ser interceptados, ou até mesmo sofrer outros ataques que permitam a invasão[5] do dispositivo conectado à rede. Vamos analisar este cenário. Imagine um simples restaurante ou café conforme o apresentado na figura 15.

Figura 15: Estabelecimento comercial qualquer.
Fonte: Google Images

Neste estabelecimento temos quatro usuários utilizando notebooks. Provavelmente estes usuários possuem o desejo de acessar a Internet enquanto estão sentados tomando o seu café ou aguardando o preparo de seu pedido. Considere a possibilidade de que neste mesmo estabelecimento exista um c*racker* que crie uma rede sem fio temporária, através de um software específico em seu notebook, e através desta rede sem fio ele compartilhe o acesso a Internet de um *modem* 3G, com o objetivo dos usuários se conectarem a esta rede e navegarem na Internet, conforme a figura 16.

[5] São ataque bem sucedidos a redes, sistemas ou ferramentas, visando conseguir acesso a dados/informações, onde é feita análise de vulnerabilidades, fraquezas e deficiências técnicas da infraestrutura física e lógica que hospeda o "alvo" em questão.

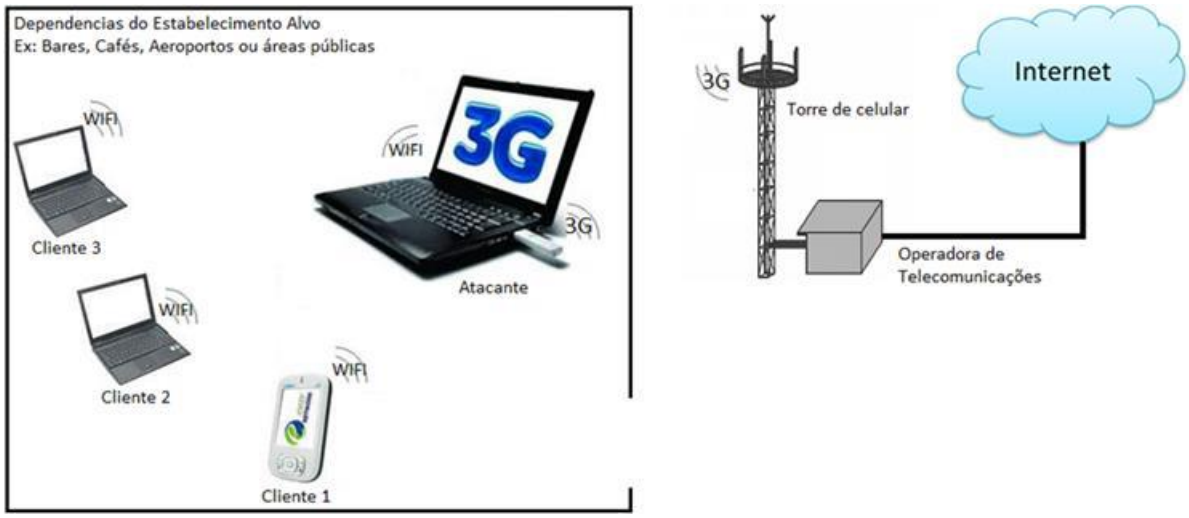

Figura 16: Um atacante com um notebook com acesso 3G à Internet compartilhando este acesso através de uma rede *WIFI* criada pelo próprio atacante.
Fonte: Criada pelos próprios autores.

Neste cenário o *cracker* poderia realizar a captura de todos os dados trafegados por estes usuários, caso eles se conectem nesta rede *WIFI* fraudulenta criada pelo próprio atacante. A figura 17 apresenta como seria visto a rede *WIFI* fraudulenta pelos clientes.

Figura 17: Rede WIFI (WiFi Gratis) detectada pelo cliente.
Fonte: Criada pelos próprios autores.

Este ataque pode ser facilmente aplicado nesse tipo de ambiente, pois as técnicas necessárias para a criação de uma rede sem fio são relativamente simples. Isto aliado ao desejo dos usuários de se manterem conectados à Internet criaria o cenário perfeito para o roubo de informações como as mencionadas anteriormente.

3. Análise em Laboratório

3.1 Anatomia do ataque de captura do tráfego

Um cracker precisaria apenas de um notebook com uma placa de rede sem fio, um *modem* 3G e algumas configurações de software para construir um ambiente propício para a captura dos dados.

Para que o ataque tenha sucesso, o *cracker* precisará realmente oferecer o acesso a Internet para que os usuários possam se conectar e navegarem. Para isto ele pode utilizar um *modem* 3G portátil para captar o sinal de Internet e posteriormente compartilhar este acesso através de uma rede sem fio utilizando a própria placa de rede sem fio do *notebook*.

A figura 18 ilustra este exemplo de um *notebook* com um *modem* 3G para captação do sinal de Internet.

Figura 18: Um *notebook* com um modem 3G conectado a porta USB a esquerda da imagem, com o objetivo de captar o sinal da Internet.
Fonte: Criada pelos próprios autores.

A figura 19 apresenta o cenário final do processo de compartilhamento do acesso Internet pelo atacante. Para isto, o atacante precisara de um modem 3G para obter o sinal de Internet. Para permitir que os clientes se conectem ao *notebook* para acessarem a rede Internet, o atacante precisara de uma placa de rede sem fio, um software para emular a rede *WIFI*, um sistema de DHCP (*Dynamic Host Configuration Protocol*) para distribuir IPs automaticamente para os clientes e habilitar o roteamento no sistema operacional. O roteamento no sistema operacional será necessário, para que os pacotes transmitidos pelos clientes através da rede *WIFI* sejam “roteados” pelo *notebook* para a conexão criada pelo *modem* 3G.

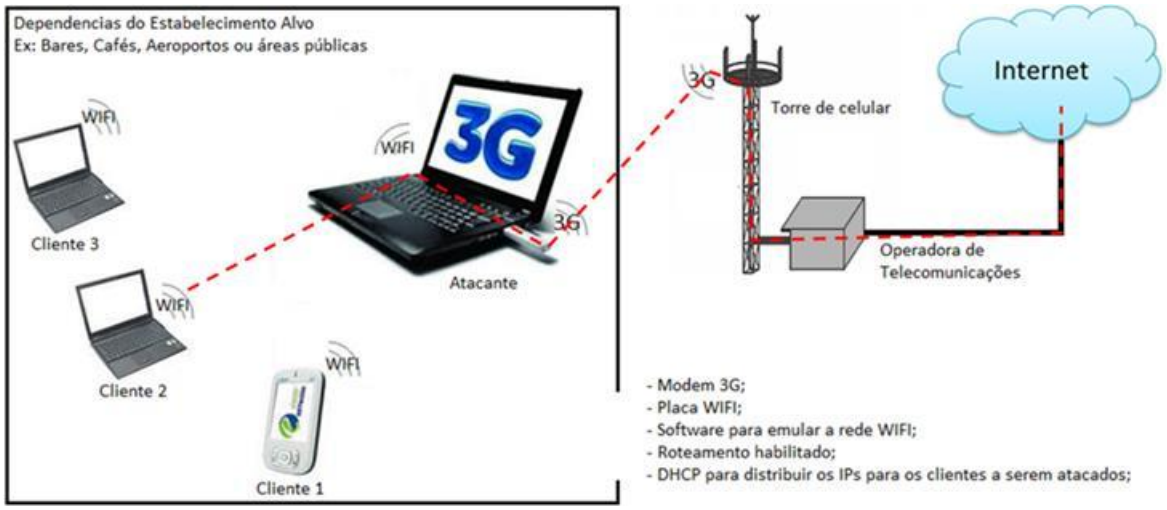

Figura 19: Atacante obtendo o sinal de Internet através de *3G* e compartilhando através de rede *WIFI*.
Fonte: Criada pelos próprios autores.

Uma vez entendido como seria o processo de funcionamento do compartilhamento do acesso à Internet, resta entender como o atacante criaria um ponto de acesso *WIFI* que se pareça verdadeiro.

3.2 Criação de uma rede WIFI fraudulenta

Para criar o ponto de acesso *WIFI* o atacante pode utilizar um software que permite a emulação de um ponto de acesso *WIFI* chamado Gerix. O Gerix trata-se de um *script* desenvolvido em Python e pode ser executado em qualquer sistema operacional Linux que tenha o interpretador Python instalado.

Nos testes de laboratório realizados, foi utilizando um computador com o Kali Linux como sistema operacional.

Para a instalação do Gerix foi realizado o *download* do *script* a partir do site Bitbucket conforme a figura 20.

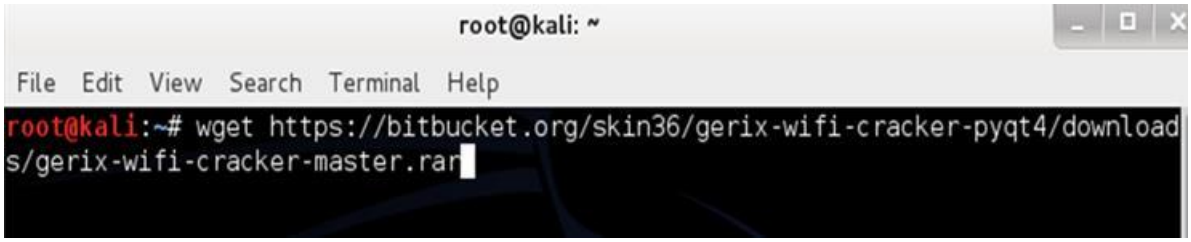

Figura 20: Download do script Gerix.
Fonte: Criada pelos próprios autores.

Após o *download*, o *software* foi descompactado e executado conforme as figuras 21 e 22.

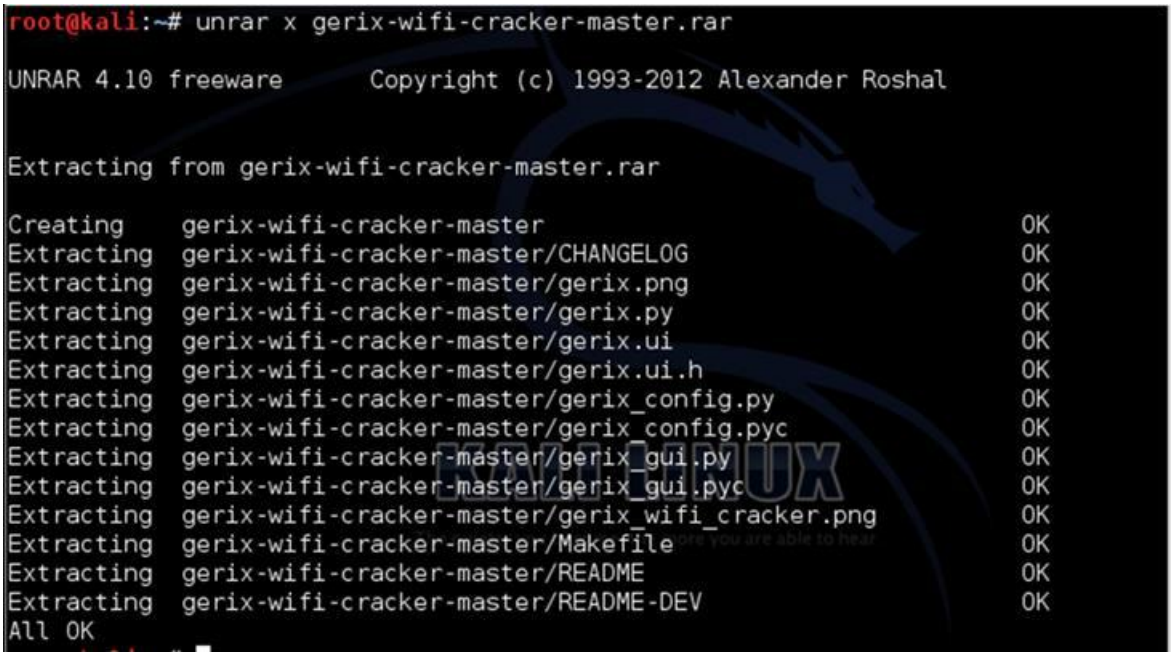

Figura 21: Descompactação dos arquivos do Gerix.
Fonte: Criada pelos próprios autores.

Figura 22: Execução do script Gerix.
Fonte: Criada pelos próprios autores.

Com o Gerix inicializado, foi executado os passos abaixo para a configuração do ponto de acesso que será utilizado pelos clientes.

No primeiro passo na aba "*Configuration",* foi selecionada a interface de rede Wireless disponível e habilitado o modo monitor[6] da placa de rede, clicando no botão "*Enable/disable monitor mode*", conforme figura 23.

[6] Modo monitor: O modo monitor trata-se de uma funcionalidade especifica disponível em algumas placas de rede sem fio que suportam o RFMON (Radio Frequency Monitor). Esta funcionalidade permite que seja possível capturar todo o trafego de uma rede sem fio em especifico, sem a necessidade de se conectar previamente nesta rede. No caso de uma rede sem fio criptografada é necessário um ataque posterior para a quebra da criptografia para que seja possível o acesso ao conteúdo real.

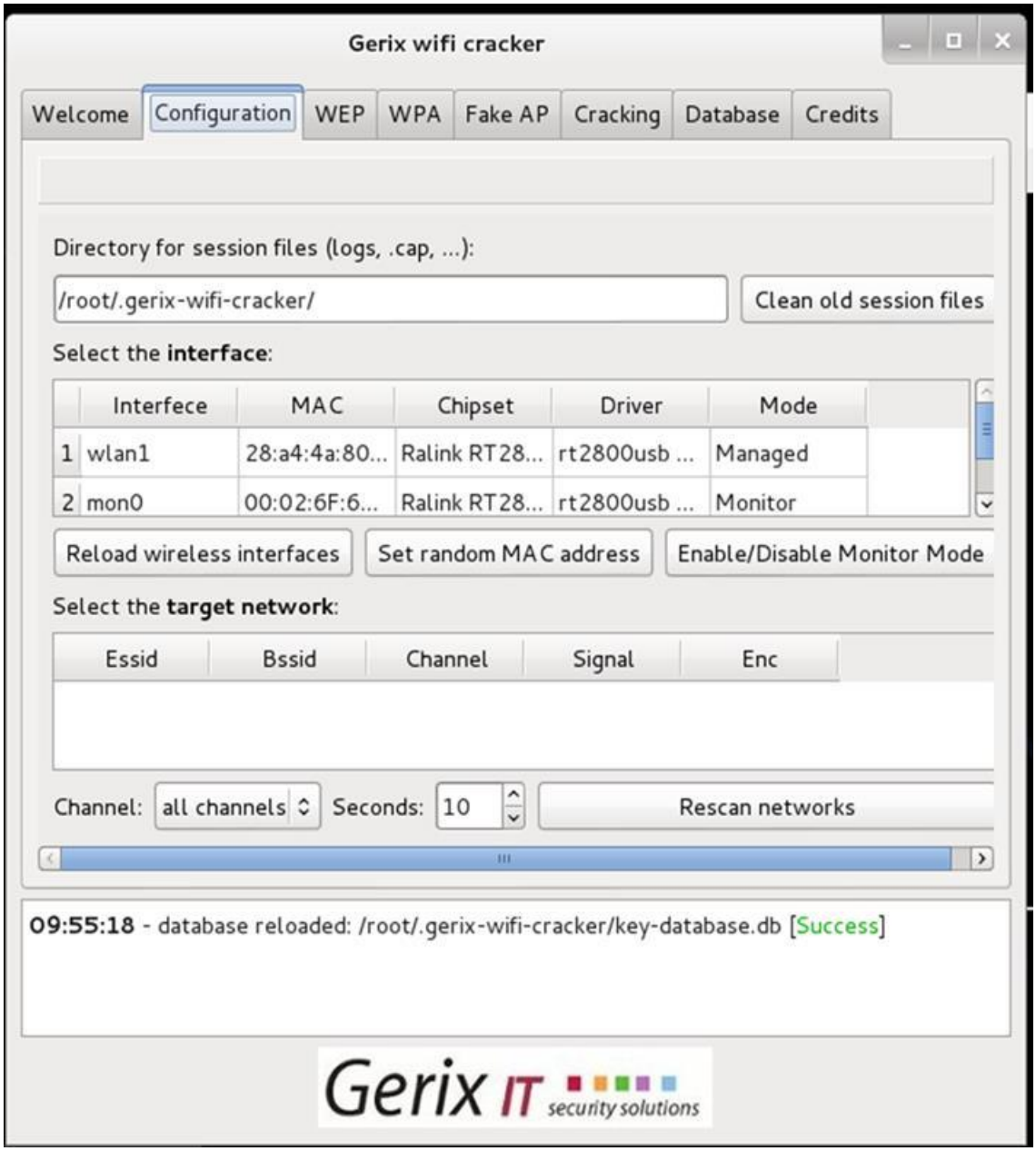

Figura 23: Tela de configuração da interface de rede em modo monitor.
Fonte: Criada pelos próprios autores.

No segundo passo, na aba "*Fake Ap"* foi digitado o nome da rede sem fio que será vista pelos usuários no campo "*Acces Point* ESSID". No campo "*Cryptography tag"*, foi selecionado a opção "none", para que a rede sem fio não requisite nenhuma senha de autenticação por parte dos usuários. A figura 24 apresenta a interface de configuração da rede sem fio fraudulenta no Gerix.

Figura 24: Tela para criação do emulador de rede.
Fonte: Criada pelos próprios autores.

No terceiro, foi iniciado a rede sem fio fraudulenta através do botão "*Start Fake Acess Point*", para que a rede sem fio seja visualizada pelos clientes ao alcance do espectro eletromagnético.

Quando os clientes conectarem nesta rede sem fio, será necessário que estes possuam um endereço IP configurado corretamente para que possa ser possível a comunicação com o *notebook* do *cracker.*

Para isto, o *cracker* pode utilizar um servidor de DHCP para distribuir automaticamente os endereços IPs corretos sem a necessidade do usuário final realizar nenhuma configuração adicional em seu dispositivo de acesso.

No quarto passo, foi configurado o arquivo dhcpd.conf localizado no diretório /etc/dhcp/ do sistema operacional conforme a figura 25.

Figura 25: Arquivo de configuração do serviço DHCP com os parâmetros ajustados.
Fonte: Criada pelos próprios autores.

Quando os usuários se conectarem à rede *Wireless* fraudulenta, estes terão um endereço IP privado que foi distribuído pelo serviço de DHCP. Somente com este endereço privado, estes usuários não conseguirão navegar na Internet. Desta forma, será necessário realizar a troca do endereço IP privado pelo endereço IP público do *modem 3G* através de uma técnica conhecida como NAT (*Network Address Translation*).

No quinto passo, foi executado alguns comandos no sistema operacional para habilitar o roteamento de pacotes e utilizado alguns comandos do *firewall* Iptables para realizar o NAT. A figura 26, descreve a sequencia dos comandos utilizados para permitir o compartilhamento da Internet do *modem 3G* com os usuários conectados à rede *Wireless* fraudulenta.

Figura 26: Comandos necessários para habilitar o serviço de roteamento do Kali Linux.
Fonte: Criada pelos próprios autores.

3.3 Captura de trafego em laboratório

Para exemplificação do processo de captura de dados sensíveis, foi simulado em laboratório, os seguintes acessos, a partir de uma máquina conectada à rede fraudulenta:

- Acesso ao site da uma empresa X;
- Acesso ao sistema de FTP de uma empresa Y;

Nestes dois cenários, foi considerando que o usuário João, um usuário fictício, estava conectado a rede fraudulenta do atacante. Durante a conexão na rede do atacante, o usuário João decidiu realizar um acesso aos sites mencionados onde o mesmo possuía um cadastro.

Como os dados do usuário estão "passando" pela máquina do atacante, através da rede Wireless fraudulenta antes de irem para a Internet, os mesmos poderão ser capturados facilmente pelo atacante, pois se tratam de protocolos sem criptografia (FTP e HTTP).

Os dados de usuário e senha capturados a seguir, são meramente fictícios, pois na realidade não possuímos acessos em nenhuma das duas empresas. Estes sites foram escolhidos aleatoriamente na Internet sem nenhum tipo de direcionamento político ou comercial.

3.3.1 Captura do trafego de autenticação do protocolo HTTP

Para a coleta das informações de acesso ao site através do protocolo HTTP, foi inicializado a captura de tráfego no Wireshark antes de realizar o acesso ao site, conforme a figura 27.

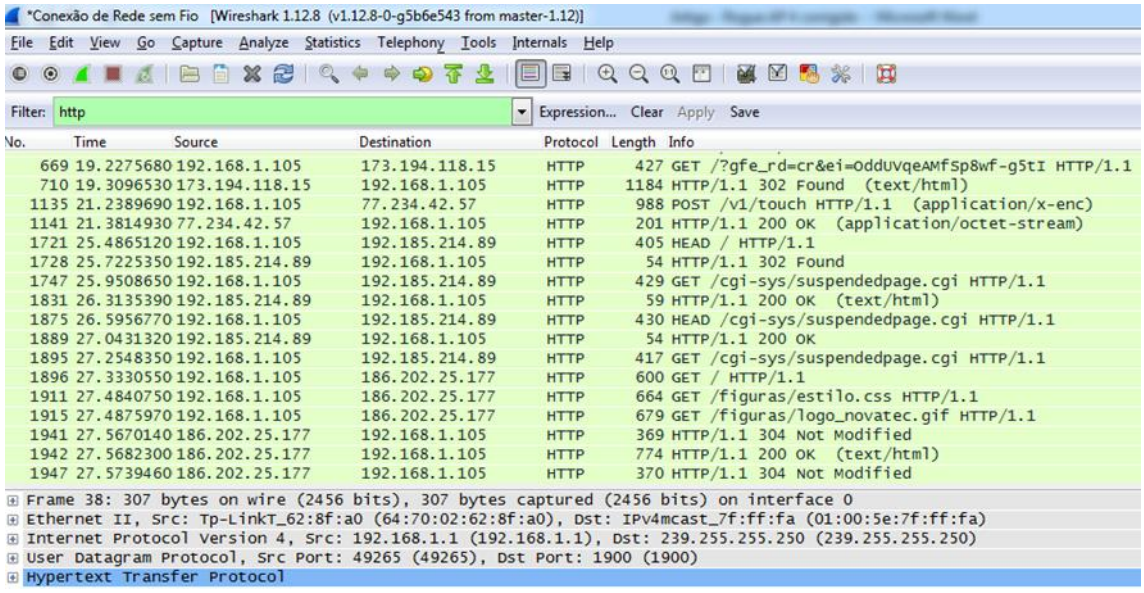

Figura 27: Captura de trafego de rede iniciada
Fonte: Criada pelos próprios autores.

Após o início da captura do trafego, foi realizado a entrada dos dados de usuário e senha no site da empresa Y, conforme a figura 28.

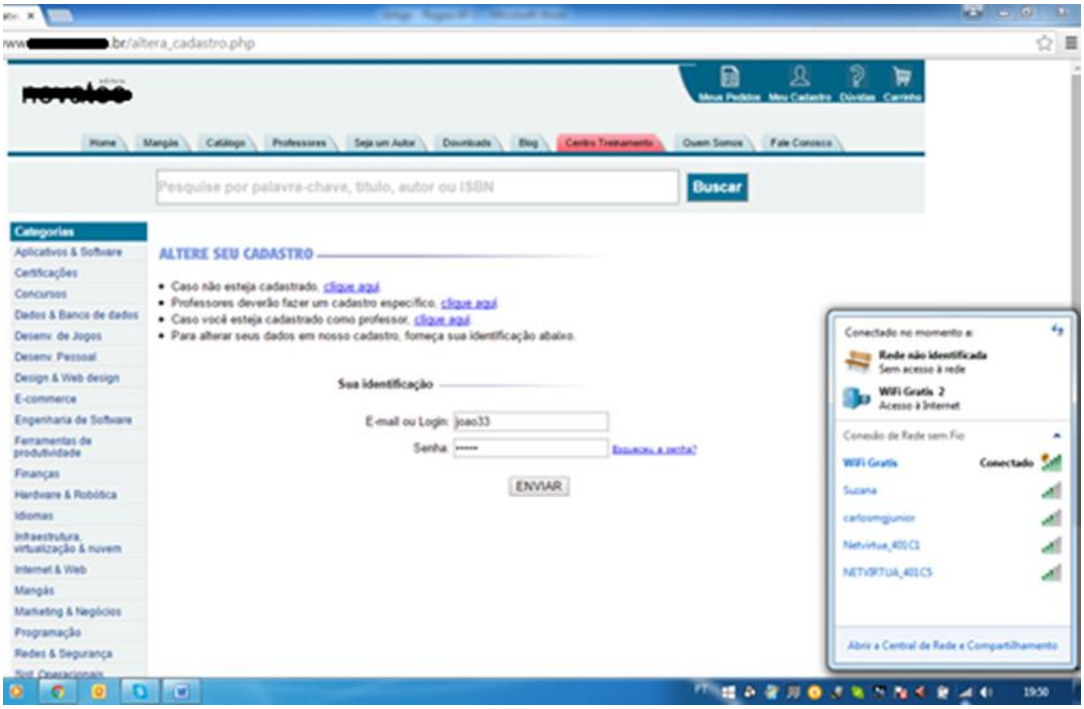

Figura 28: Página da empresa X, responsável pela atualização cadastral do usuário.
Fonte: Criada pelos próprios autores.

A figura 29 ilustra de forma didática por onde os pacotes de autenticação entre o cliente e o servidor passaram. Neste teste, o trafego foi coletado através do software Wireshark instalado na máquina do atacante.

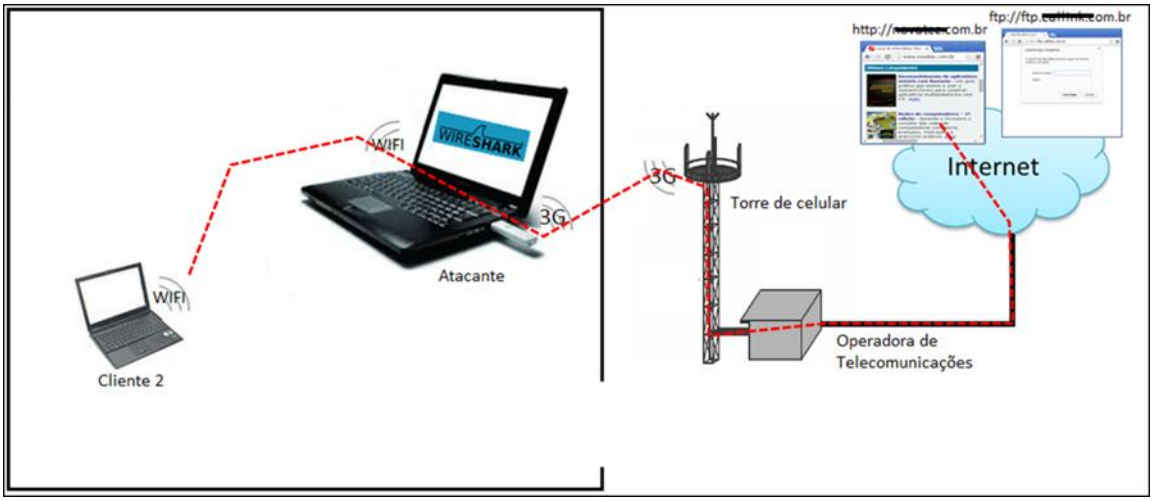

Figura 29: Caminho por onde os pacotes de autenticação ao site da empresa X trafegaram entre o cliente e o servidor da empresa.
Fonte: Criada pelos próprios autores.

Na figura 30, destacamos o pacote que continha os dados de autenticação, e com um clique do botão direito do mouse sobre a linha que representa este pacote, foi selecionado a opção "*Follow* TCP *Stream*". Esta opção do Wireshark busca todos os pacotes que fizeram parte da comunicação referente ao envio dos dados de usuário e senha, e a partir disto, exibe os dados da camada de aplicação do modelo TCP/IP que foram enviados.

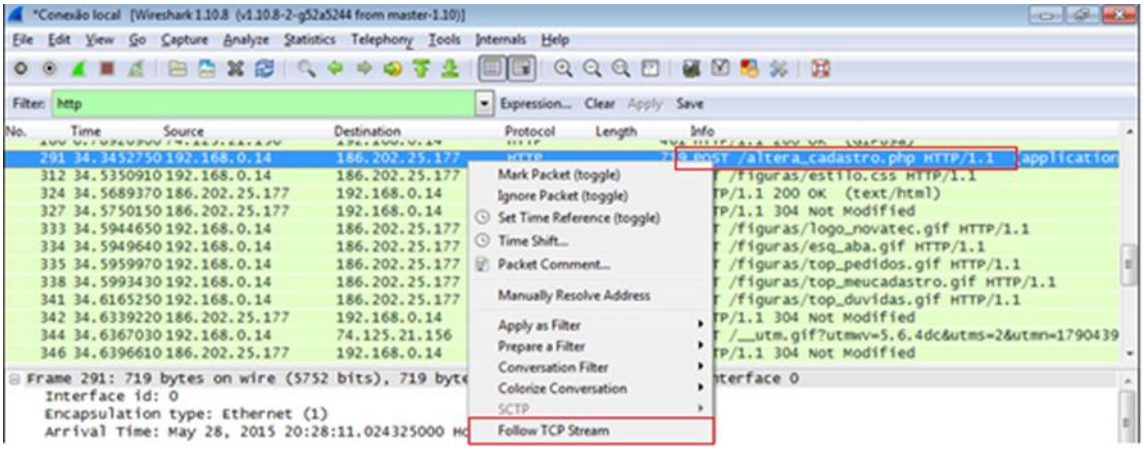

Figura 30: Identificação do pacote e captura de informações de autenticação.
Fonte: Criada pelos próprios autores.

Na janela "*Follow* TCP *Stream*" conforme a figura 31 é exibido os dados de usuário e senha. Com esta informação obtida, podemos relembrar que neste caso o atacante teria os dados de acesso do usuário João.

Figura 31: Dados de usuário (joao33) e senha (meupassword) coletados.
Fonte: Criada pelos próprios autores.

3.3.2 Captura do trafego de autenticação do protocolo FTP

Para a coleta das informações do acesso ao sistema de FTP, foi inicializada a captura de tráfego no Wireshark antes de realizar o acesso ao sistema da mesma forma que realizado no primeiro teste.

Após o início da captura do trafego, foi realizada a entrada dos dados de usuário e senha no site da empresa Y, conforme a figura 32.

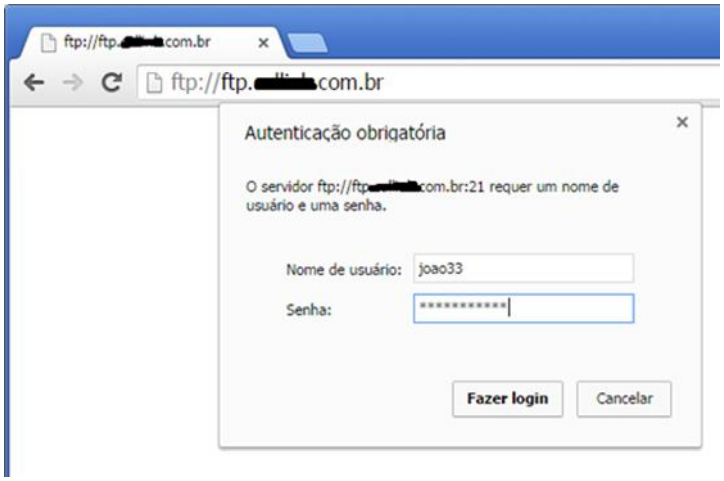

Figura 32: Página da empresa Y, responsável pela autenticação do serviço de FTP.
Fonte: Criada pelos próprios autores.

A figura 33 ilustra de forma didática por onde os pacotes de autenticação entre o cliente e o servidor passaram.

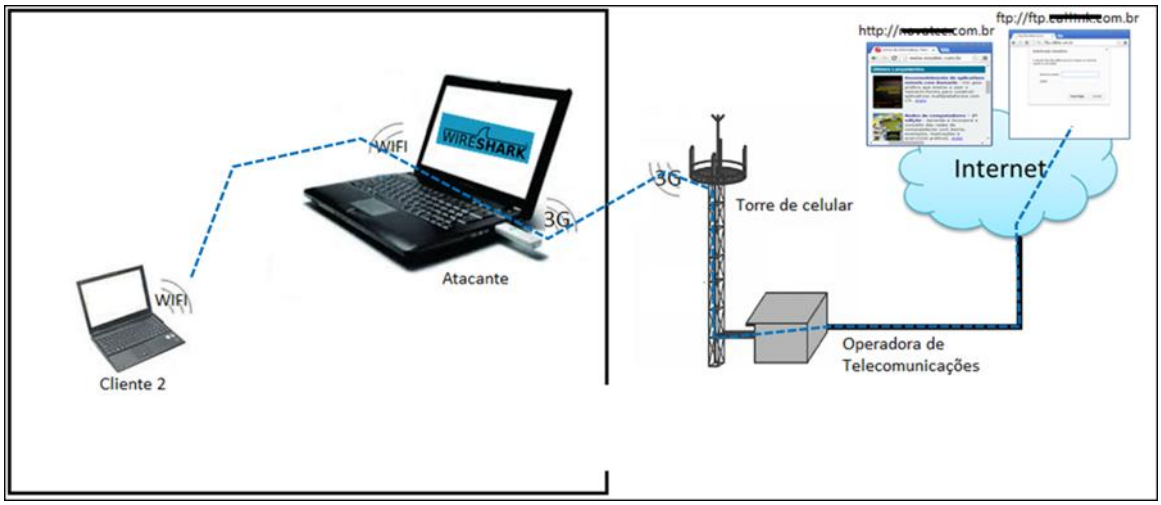

Figura 33: Trajeto do pacote de autenticação entre o cliente e o servidor da empresa Y.
Fonte: Criada pelos próprios autores.

A figura 34 apresenta os dados de autenticação usuário (joao33) e senha (senhaftp123) capturados no processo de autenticação.

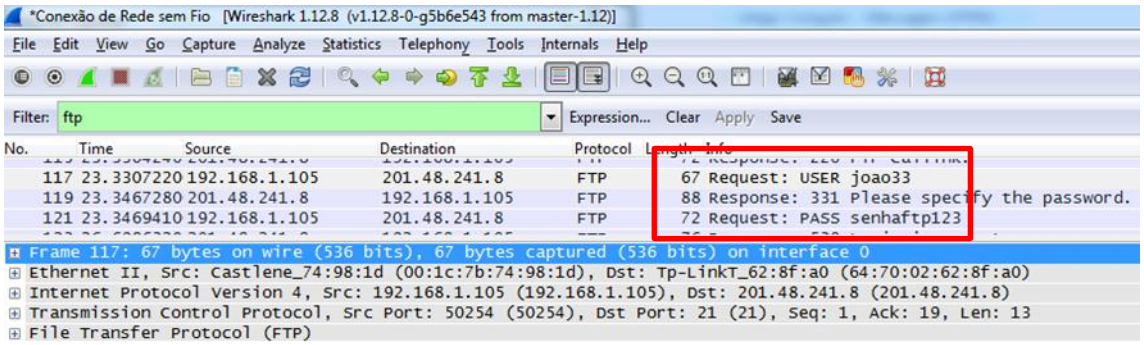

Figura 34: Captura de informações de acesso ao FTP.
Fonte: Criada pelos próprios autores.

4. Recomendações

Como recomendações para os usuários que utilizam redes *Wireless* abertas sejam providas por estabelecimentos confiáveis ou não, é importante ter a consciência de que todos os dados trafegados entre o dispositivo de acesso e a Internet podem ser capturados. Desta forma, é recomendado que este tipo de infraestrutura de acesso a Internet deve ser utilizada apenas para o uso de Internet que não contenha informações consideradas pelo usuário confidenciais.

Para reduzir os riscos de interceptação de informações sensíveis em redes *Wireless*, deve ser considerado somente o uso de redes que possuem criptografia e além disto, o uso de protocolos considerados seguros, como o caso do HTTPS. Outra recomendação que os usuários devem considerar é a sua capacitação básica para conhecer os aspectos básicos da segurança da informação, pois cabe ao usuário final avaliar os riscos que o mesmo está sujeito bem como as práticas para se defender.

5. Conclusão

É inevitável e indiscutível que as redes sem fio fazem parte do nosso cotidiano e que seu uso tenderá a aumentar nos próximos anos.

Baseado nos testes realizados em laboratório, podemos concluir que o ataque a este tipo de rede pode ser facilmente realizado, trazendo impactos significativos para os usuários deste tipo de rede, caso estes sejam alvos deste ataque. No laboratório realizado, capturamos o trafego de protocolos sabidamente inseguros, no entanto, outros tipos de protocolos e dados sensíveis, como dados de cartão de crédito poderiam ser alvos deste tipo de ataque.

No uso de redes sem fio abertas, cabe exclusivamente à responsabilidade dos usuários saberem se estão conectados a uma rede segura ou não. Caso os usuários não consigam atestar a segurança da rede que estão acessando, devem então, utilizar protocolos seguros com o objetivo de reduzir os riscos de captura dos dados. Outra opção que os usuários podem utilizar é evitar o acesso de serviços críticos quando estiverem em redes sem fio abertas. Exemplos de serviços críticos seriam realizar compras On-line (risco de acesso indevido aos dados de cartão de crédito), ou o acesso a serviços que podem gerar prejuízos financeiros, como sistemas que armazenam algum tipo de crédito como o Mercado Livre, programas de milhagens, sistemas de telefonia VOIP. Estes sistemas podem ser utilizados de maneira indevida pelo atacante, utilizando os créditos armazenados nestes sistemas, trazendo uma perda financeira para o real usuário.

Como trabalhos futuros, temos espaço para a pesquisa sobre o quanto o protocolo SSL seria uma camada de segurança útil, para a segurança em ambientes de rede sem fio abertas, uma vez que existem ataques e ferramentas disponíveis para a interceptação de uma conexão SSL.

5. Referências

100 Security. Revelando a chave WEP. Disponível em <http://www.100security.com.br/revelando-a-chave-wep/>. Acessado em 10 de Abril de 2015.

CONVERGENCIA DIGITAL. Brasil é o sétimo país no ranking global de uso da Internet. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=39200&sid=4#.VRAQ2fnF98F. Acessado em 21 de Dezembro de 2015

BURNETT, Steven; PAINE; Stephen. Criptografia e Segurança: O Guia Oficial do RSA. 2002. p. 11-113.

BRAUMANN, R., CAVIN, S., SCHMID, S. Voice Over IP – Security and SPIT. Disponível em: http://scholar.googleusercontent.com/scholar?q=cache:uYD9e_DMEZsJ:scholar.google.com/+VoIP+Security+Threats&hl=pt-BR&as_sdt=0

EMPRESA AGIL. Comunicação Empresarial: Conceito, aplicação e importância. Disponível em: <http://www.empresaagil.com.br/ebook-serie-comunicacao-empresarial-na-pratica/>. Acessado em 29 de Outubro de 2015.

GLOBO.COM. Barracas de praia oferecem Wi-Fi para clientes no Rio de Janeiro <http://g1.globo.com/jornal-nacional/noticia/2015/09/barracas-de-praia-oferecem-wi-fi-para-clientes-no-rio-de-janeiro.html>. Acesso em: 4 de Novembro de 2015.

INFOWESTER. Criptografia padrão RSFN. Disponível em: <http://www.infowester.com/criptografia.php>. Acesso em: 18 de Fevereiro de 2015.

KUROSE, James F.; ROSS, Keith W., *Redes de computadores e a Internet:* uma abordagem top-down. 5 ed. Pearson Education, 2011. p. 492-501.

LAUFER et al. Negação de Serviço: Ataques e Contramedidas. Disponível em <http://www.gta.ufrj.br/ftp/gta/TechReports/LMVB05a.pdf>. Acessado em 10 de Julho de 2015.

MEIER, Cardy. O dígito do CPF. Disponível em <http://www.profcardy.com/cardicas/cpf.php>. Acessado em 12 de Dezembro de 2015.

MORIMOTO, Carlos E., *Redes, Guia Prático:* Ampliada e Atualizada. 2 ed. Sul Editores, 2011. p. 243-257.

OLHAR DIGITAL. Qual a diferença entre hacker e cracker? <http://olhardigital.uol.com.br/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024>. Acesso em: 19 de Novembro de 2015.

PEW RESERACH. Many Use Internet Daily. Disponível em: http://www.pewresearch.org/fact-tank/2015/03/15/Spring-2014-Global-Attiudes-Survey/. Acessado em 15 de Maio de 2015.

PLANETUNIX**.** Configurando Um Servidor DHCP No Linux em: <http://www.planetaunix.com.br/2015/04/configurando-um-servidor-dhcp-no-linux.html>. Acessado em 29 de Outubro de 2015.

ROHR, Altires. Pacotão: dono de rede sem fio com senha pode interceptar dados?. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/pacotao-dono-de-rede-sem-fio-com-senha-pode-interceptar-dados.html. Acessado em 15 de Novembro de 2015.

UFRGS. Redes sem Fio - Aspectos de Segurança. Disponível em: <http://www.ufrgs.br/tri/Documentos/redes-sem-fio-aspectos-de-seguranca>. Acesso em: 19 de Fevereiro de 2015.

VALOR ECONOMICO. Acesso à internet via celular triplicou no Brasil nos últimos 3 anos. Disponível em: http://www.valor.com.br/empresas/4225532/acesso-internet-celular-triplicou-no-brasil-nos-ultimos-3-anos. Acessado em 25 de Outubro de 2015.

VAZ, Conrado Adolpho. Google Marketing: o guia definitivo do marketing digital. São Paulo: Novatec Editora, 2007.

WIRESHARK. Página oficial. Disponível em: <https://www.wireshark.org/>. Acesso em: 20 de Janeiro de 2015.