UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE
CAMPUS DE NATAL
CURSO DE CIÊNCIA DA COMPUTAÇÃO

JHONATTA DANIEL SILVERIO FAUSTINO

SEGURANÇA EM RSM: UM GUIA DE PREVENÇÃO PARA USUÁRIOS BASEADO EM CENÁRIOS REAIS DE RISCOS

Natal
2014

.

JHONATTA DANIEL SILVERIO FAUSTINO

SEGURANÇA EM RSM: UM GUIA DE PREVENÇÃO PARA USUÁRIOS BASEADO EM CENÁRIOS REAIS DE RISCOS

Monografia apresentada à Universidade do Estado do Rio Grande do Norte UERN como requisito obrigatório para obtenção do título de Bacharel em Ciência da Computação.

ORIENTADOR (A): ISAAC LIMA DE OLIVEIRA FILHO

Natal
2014

JHONATTA DANIEL SILVERIO FAUSTINO

SEGURANÇA EM RSM: UM GUIA DE PREVENÇÃO PARA USUÁRIOS BASEADO EM CENÁRIOS REAIS DE RISCOS

Monografia apresentada à Universidade do Estado do Rio Grande do Norte UERN como requisito obrigatório para obtenção do título de Bacharel em Ciência da Computação.

ORIENTADOR (A): ISAAC LIMA DE OLIVEIRA FILHO

Aprovado em: ____/_____/_____

BANCA EXAMINADORA

_____

PROF. ME. ISAAC LIMA DE OLIVEIRA FILHO

Universidade do Estadual do Rio Grande do Norte – UERN

_____

PROF.ME. BARTIRA PARAGUAÇU FALCAO DANTAS ROCHA

Universidade do Estadual do Rio Grande do Norte – UERN

_____

PROF. DR. FRANCISCO DANTAS DE MEDEIROS NETO

Universidade do Estadual do Rio Grande do Norte – UERN

Natal

2014

“Não tenha medo da vida, tenha medo de não vivê-la. Não há céu sem tempestades, nem caminhos sem acidentes. Só é digno do pódio quem usa as derrotas para alcançá-lo... Lute pelo que você ama.”

Augusto cury

.

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter sempre me abençoado, com saúde, paz e felicidade e também por ter me dado força para superar todas as dificuldades que apareceram em meu caminho.

Agradeço a minha mãe (Mara Silvério Faustino), meu pai (Francimar Gomes Faustino), minhas irmãs (Anna Daniele e Anna Amélia) e ao meu filho (Pedro Alexandre Jales Faustino) que nunca deixaram de acreditar, sempre me deram força e por terem sempre acreditado na minha competência.

Agradeço ao professor Isaac de Lima Oliveira Filho por ter sempre passado conhecimentos fundamentais para minha formação.

A todos os professores do Curso de Ciência da Computação, que contribuíram imensamente para a minha formação.

Agradeço em especial a minha noiva Aniele Martins por toda contribuição e incentivo nos momentos da empolgação, incentivo e muito amor.

Agradeço aos meus amigos de longa data Thales, Waldney e Adail, que sempre me ajudaram de alguma forma.

.

RESUMO

O advento das Redes Sociais Móveis vem sendo impulsionado pela rápida evolução dos dispositivos móveis, a adoção em massa desses dispositivos por parte da população e o crescimento importante das Redes Sociais. Além disso, é inegável que, atualmente, a grande maioria da população possui e usa exaustivamente estes dispositivos. Porém, a massificação das Redes Sociais Móveis desencadeou problemas relacionados à insegurança dos dados pessoais, associados aos criminosos virtuais. Criminosos virtuais usam ferramentas, tais como técnicas psicológicas avançadas, chamadas de engenharia social, para analisar e vascular redes e perfis sociais mal protegidos, obtendo assim, informações pessoais e privadas, que serão usadas contra as contra suas vítimas. Neste cenário, surge a necessidade de orientar os usuários no que diz respeito à segurança, no ponto de vista da privacidade. Portanto, neste trabalho, propõe-se um estudo sobre as Redes Sociais Móveis e suas vulnerabilidades, através do uso de aplicações bastante difundidas entre os internautas brasileiros que utilizam dispositivos portáteis. Sabendo-se que o elo mais fraco da relação entre usuário e a rede social é o usuário, foi criado um guia de segurança que objetiva minimizar problemas relacionados a perda de privacidade, quando os mesmos estiverem fazendo uso das aplicações sociais.

Palavras-chave: Redes Sociais Móveis. Vulnerabilidade. Segurança. Engenharia Social.

.

ABSTRACT

The advent of Social Mobile Networks has been driven by the fast evolution of mobile devices, the widespread adoption of these devices by the population and the substantial growth of Social Networks. Moreover, it is undeniable that today the vast majority of the population owns and uses these devices, extensively. However, the widespread use of Social Mobile Networks triggered problems related to insecurity of personal data, which are associated with cybercriminals. Cybercriminals use tools such as advanced psychological techniques, called social engineering, to analyze poorly secured networks and social profiles, getting personal and private information that will be used against their victims. This scenario indicates the need to guide users regards safety, from the privacy perspective. Therefore, this work proposes a study on the Social Mobile Networks and vulnerabilities using applications widely spread among Brazilian internet users who use portable devices. Knowing that the weakest link of the relationship between user and social networking is the user, a safety guide that aims to minimize problems related to loss of privacy, when they are making use of social applications, was created.

Keywords: Mobile Social Networks. Vulnerability. Safety. Social Engineering.

.

LISTA DE FIGURAS

.

.

LISTA DE TABELA

.

LISTA DE GRÁFICOS

.

LISTA DE SIGLAS

MSN	Mobile Social Networks
OSN	Online Social Networking
API	Application Programming Interface
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
PIN	Personal Identification Number
URL	Uniform Resource Locator
GPRS	General Packet Radio Services
WAP	Wireless Application Protocol
SMTP	Simple Mail Transfer Protocol
MM	Mobile Malware
SSID	Service Set Identifier
MAC	Media Access Control
AP	Acess Point
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
SSL	Secure Sockets Layer
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
WEP	Wired Equivalent Privacy
MSK	Master Session Key
EAP	Extensible Authentication Protocol
IETF	Internet Engineering Task Force

.

SUMÁRIO

.

.

1 INTRODUÇÃO

As redes Sociais On-line são um fenômeno recente, mas assumiram um papel de enorme destaque nas relações sociais, na sociedade e no mundo dos negócios (ZHANG et al., 2010). A sua utilização, apesar de alguns problemas que serão relatados neste trabalho e de outros que seguramente irão surgir, é francamente positiva (FABRICIO TAROUCO, 2013). É desejável que os mecanismos de controle e de proteção de privacidade que, aos poucos, têm sido implementados possam evitar um intranquilidade na sociedade, para que as redes sociais On-line possam continuar a evoluir e a consolidar, sem sobressaltos, a sua presença nas nossas vidas (ZHANG et al., 2010).

Recentemente um estudo mostrou que o principal destino da Web em celulares inteligentes são sites de Redes Sociais On-line (RSO) (LI, CHEN, 2009). Cada vez mais, além de uma página na Internet, ou mesmo em substituição de um site próprio, grupos, empresas e pessoas individuais marcam presença nas redes sociais como o Linkedin, Facebook, Twitter, Instagram, Google+. Redes sociais On-line são definidas como aqueles sistemas que permitem: a construção de um personagem através de um perfil ou página pessoal; a interação através de comentários; e a exposição pública da rede social de cada ator (SOARES ARIEL, 2013).

Redes sociais móveis (RSM) facilitam que seus usuários compartilhem suas atualizações de status a qualquer momento e lugar (LI e CHEN, 2009). RSM fundamentadas em localização tornam possível o encontro de novos amigos com base na aproximação geográfica, sendo assim é provável que os mesmos encontrem-se pessoalmente (LI e CHEN, 2009). Isso é apenas algumas das milhares de funções que essas aplicações podem vos proporcionar, é claro que a sua utilização não se restringirá a localização de pessoas. Verifica-se, no entanto, que nas redes sociais existem outros atores para além das pessoas singulares: as empresas que estão acompanhando a evolução dessas Mídias Sociais, para se ter uma maior interação com seus clientes. Em 2012, estudos realizados pela Empresa de telefonia Sony Ericsson adiantou que o número de smartphones no mundo deverá triplicar até o ano de 2018, com isto chegará a 3,3 bilhões de aparelhos móveis em uso (PATRICK CERWALL, 2012; FABRICIO TAROUCO, 2013).

O amanhã da computação está diretamente ligado aos aparelhos móveis (JUSTIN RATTNER, 2013, Intel). De acordo com o executivo, além das diversas

.

funcionalidades que os smartphones já possuem, eles também serão mais conscientes dos costumes e da vida diária de seus usuários. As próximas gerações de dispositivos terão aparelhos que “perceberão o contexto”, onde o mais importante será eles saberem onde se está indo e antecipar suas necessidades (FABRICIO TAROUCO, 2013). Neste cenário de tanta evolução ficam em aberto as questões sobre a segurança em relação aos Cibercriminosos, pois, um celular desprotegido associado a uma rede “insegura” do ponto de vista de proteção dos dados, assim como, na autenticidade do acesso ao sistema, podem resultar numa invasão muito cara a privacidade individual, possibilitando fatos como adulteração de dados ou até mesmo um roubo via *Mobile Banking*, por exemplo. Para que uma rede tenha o mínimo de segurança possível em padrões internacionais, ela deve seguir algumas normas básicas de segurança: confidencialidade, integridade, disponibilidade e autenticidade, normas necessárias para garantir a privacidade das comunicações, possibilitando comunicações seguras através de redes inseguras (ROSIANE CONSTANTE, 2010). As normas acima apresentadas não se referem apenas a sistemas computacionais, mas sim a todo e qualquer modelo de informação, dados e comunicações.

Com embaso nesse contexto tem-se alguns exemplos dos ataques mais comuns em redes sociais. Espionagem: Se o tráfego na interface aérea não for fortemente criptografado, um invasor pode espionar ou interceptar dados importantes ou ligações telefônicas confidenciais. Analise do lixo: O lixo é uma das fontes mais ricas de informações para Engenheiros Sociais. Engenharia social: O ser humano possui várias vulnerabilidades que são exploradas pelos Engenheiros Sociais, tais como, confiança, curiosidade, medo, ingenuidade, entre outros.

Devido a estes fatos, torna-se interessante, pesquisas e trabalhos no sentido de buscar diminuir ou solucionar parcialmente alguns dos problemas relatados. Portanto este trabalho tende a contribuir para formação de conceitos, técnicas e cenários mais seguros para RSM.

1.1 Justificativa

As Redes Sociais surgiram muito antes da internet, isto é, os relacionamentos com outros indivíduos ocorriam em um campo de futebol, escola, empresa, igreja, entre outros. Já na década de 1990 houve a popularização da internet, aliada à já estabelecida utilização dos computadores pessoais, permitindo a criação de novas

.

Redes Sociais, denominadas de Redes Sociais On-line como: AOL Instant Messenger (1997), *My Space* e *LinkdIn* (2003), *Orkut e Facebook* (2004), *Twitter* (2006) e *Instagram* (2010). Nessas comunidades on-line, os indivíduos podem se comunicar utilizando-se dessas ferramentas e com isso a distância física deixou de ser uma limitação para a constituição de novas amizades e reforçar as relações com amigos de longa data.

A constante evolução tecnológica permitiu grandes transformações mercadológicas, como o surgimento dos Smartphones PCs, que possibilitaram as pessoas que já faziam uso das Redes Sociais, porem em suas residências, usá-las em qualquer ambiente como: na rua, shopping, carro e etc. No entanto, em paralelo ao crescimento do uso, veio também o crescimento com a preocupação em relação ao teor e grau das informações compartilhadas, do ponto de vista da privacidade e segurança das informações. Portanto observa-se que além dos mecanismos de segurança e privacidade oferecido pelos softwares para os mais variados sistemas operacionais dos dispositivos móveis, percebesse que o elo mais fraco é o fator humano. Diante disso o desenvolvimento desse trabalho possui como principal contribuição a criação de um material que possa ser utilizado para orientar o usuário a se proteger de riscos ao usar uma Rede Social On-line, além de oferecer meios de solucionar determinados problemas quanto ao meio que o usuário está conectado.

1.2 Objetivo

1.2.1 Objetivo Geral

Desenvolver um guia prático de segurança em RSM, baseado em cenários reais.

1.2.2 Objetivos Específicos

- Identificar a perspectiva e comportamento dos internautas quanto aos crimes virtuais;
- Propor cenários e técnicas de segurança para RSM;
- Pesquisar sobre ataques relacionados à engenharia social, especificamente focando os sites relacionados anteriormente;
- Realizar levantamento das falhas humanas através de estatística de perfis sociais;
- Definir os tipos de ataques mais utilizados pelos engenheiros sociais;

.

- Propor ações que visem facilitar e fortalecer o combate aos crimes virtuais;
- Desenvolver material para auxílio de usuários de RSM.

1.3 Trabalhos Relacionados

Nos últimos anos, têm surgido diversas soluções de segurança e privacidade para Redes Sociais Móveis. (BEACH et al., 2009) apresentam um sistema de servidor de identidade de acordo com a geolocalização do usuário. Construído com o objetivo de resolver os problemas de segurança e privacidade em redes sociais móveis. Os autores defendem no seu trabalho que para alcançar uma maior segurança e privacidade, os usuários devem esconder suas identidades durante a distribuição de certas informações pessoais obtidas a partir de redes sociais móveis existentes, isto porque as aplicações estão cada vez mais correlacionadas com as redes sociais permitindo assim uma maior facilidade para a localização de seus usuários. De acordo com (LI et al., 2011), a criação de novos protocolos de preservação à privacidade nas redes sociais móveis, faz-se necessário. (NAWAZ et al., 2012) colaborando com essa ideia, desenvolveram um protótipo de arquitetura de identificação segura, baseado na *Generic Authentication Architecture* (GAA) a qual é especificada pelo Projeto de Parceria de 3° Geração (3GPP), para a inscrição e autenticação através *User Identity Module* (USIM[1]) de usuários em um grupo de Rede Social fechado.

A segurança proposta por esse projeto é relacionado com a troca de chaves para USIM, para assim fornecer identificação segura em Redes Sociais Móveis.

(DOS SANTOS, 2011) apresenta *MySocial*, uma aplicação social móvel baseada em localização, que possui como objetivos indicar a localização dos usuários para seus contatos das redes sociais on-line e possibilitar que os usuários realizem o acompanhamento da localização dos contatos que estão próximos em tempo real. A aplicação *MySocial* pode ser usada em cenários de computação pervasiva[2].

As informações do contexto social e de localização dos usuários serão adquiridas a partir da API de Web Service da infraestrutura, porém o método de

[1] **Usim:** É uma aplicação 3G/4G utilizada por parte das operadores de redes móveis para que o processo de autenticação seja mais eficaz entre o cliente e os servidores de aplicativos, diferentemente da aplicação SIM que é utilizada pela tecnologia 2G.

[2] **Computação Pervasiva:** Este tipo de computação define uma nova maneira de relacionar usuários humanos e dispositivos computacionais, isto é, possibilita aos usuários, compartilhar interesses em comum e interajam entre si para realizar atividades de interesse comum, em qualquer lugar, a qualquer momento.
.

segurança não foi mencionado nessa aplicação, mas deveria, pois essa aplicação faz uso da localização dos usuários e com isso diversas informações confidencias podem ficar expostas.

1.4 Estrutura do Trabalho

O capítulo dois apresenta o conceito de redes sociais móveis, computação pervasiva, computação móvel, arquitetura das principais RSM utilizadas. Neste mesmo capítulo as principais vulnerabilidades para as Redes Sociais Móveis são abordadas.

O capítulo três discorre sobre as principais vulnerabilidades que as Redes Sem fio podem proporcionar aos usuários on-line, mostrando como elas está presente em nosso cotidiano. Neste capítulo será possível verificar os principais mecanismos de segurança adotados para administrar ou minimizar as vulnerabilidades existentes.

O capítulo quatro aborda estudos de caso, fazendo uma junção da Engenharia Social e o modo como as ferramentas *Sniffers* são utilizadas pelos Crackers/hackers para obter informações sigilosas, destacando-se as vulnerabilidades.

O capítulo cinco trata do estudos de caso realizados no capítulo anterior, com o intuito de levantar um guia de segurança para que os usuários de RSM se conscientizem no uso adequado dessas redes sociais e mídias sociais.

Por fim no capítulo seis, será apresentada a conclusão do trabalho desenvolvido, assim como, pontos para trabalhos futuros.

.

2 REDES SOCIAIS MÓVEIS

A transferência dos conceitos e das tendências atuais em redes sociais, bem como, o uso dos recursos dos dispositivos móveis como: notebooks, netbooks, aparelhos celulares e smartphones possibilitaram o surgimento das redes sociais móveis (RSM) (ALVES et al., 2012). Os smartphones, em especial, estão se tornando cada vez mais baratos, acessíveis e com grandes funcionalidades disponíveis, tais como, câmera digital, vídeo, GPS, conexões Wi-Fi, 3G, *Bluetooth*, dentre outros. Consequentemente, tem-se tornado cada vez mais comum as pessoas estarem sempre portando seus dispositivos móveis, passando grande parte do tempo conectadas à Internet, em qualquer lugar, a qualquer momento.

Com o avanço no paradigma de Computação Pervasiva motivou o surgimento de uma área conhecida como: Redes Sociais Móveis ou Redes Sociais Pervasivas, que estuda a relação entre este paradigma e as redes sociais da web 2.0 (BEN MOKHTAR, CAPRA, 2009, ACM; WEISER, 1991). Para que esse paradigma funcione corretamente é essencial que as aplicações recuperem as informações do ambiente no qual os usuários se encontram, com a finalidade de prover serviços e executar tarefas em favor deles (SATYANARAYANAN 2001; SAHA e MUKHERJEE 2003; LOUREIRO et al. 2007).

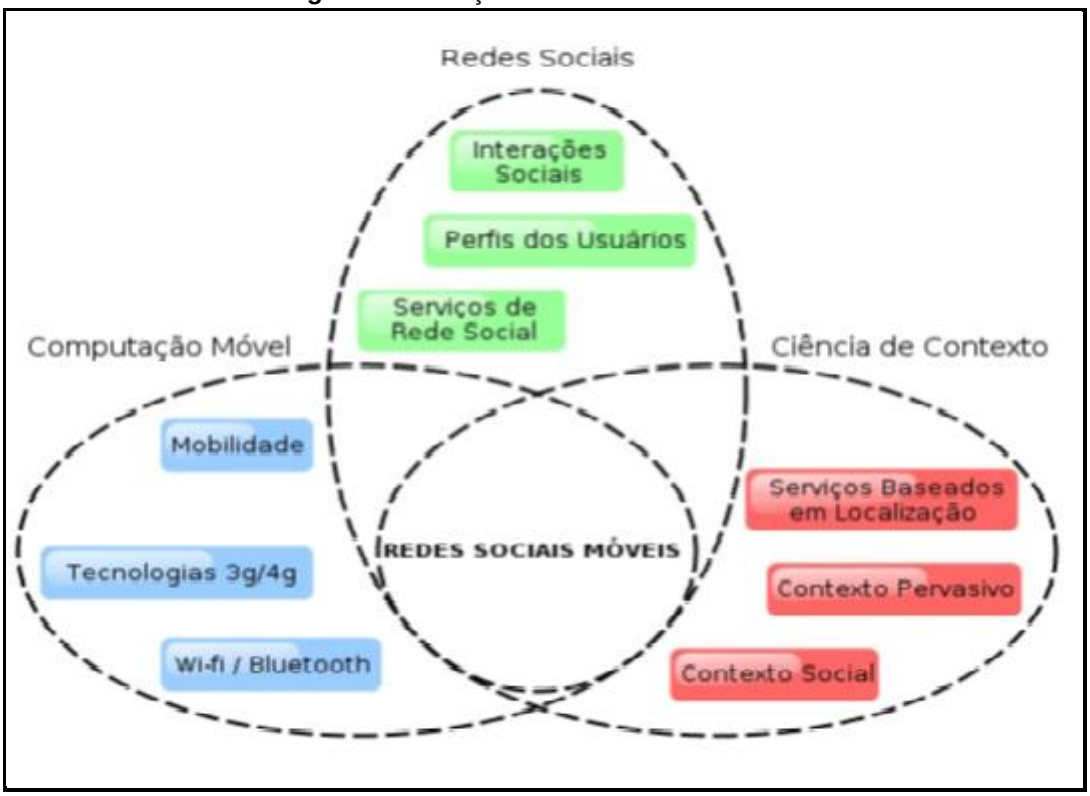
RSM podem ser vistas como uma combinação de três áreas do conhecimento: Redes Sociais, Computação Móvel e Ciência de Contexto, uma extensão do conceito formalizado em (KAYASTHA et al., 2011).

Computação Móvel, é caracterizada pela presença de dispositivos portáteis, cada vez mais comuns devido aos avanços na fabricação de componentes eletrônicos. Esses dispositivos possuem uma considerável capacidade de processamento, com recursos para comunicação sem fio e armazenamento de dados (LOUREIRO et al.,2009).

Contexto é definido como sendo qualquer informação que pode ser utilizada para caracterizar a situação de uma entidade. Entidade pode ser classificada como pessoa, lugar ou objeto que seja considerado relevante na interação do usuário com as aplicações (DEY, 2000). Sistemas sensíveis ao contexto são habilitados para adaptar suas funcionalidades e comportamentos de acordo com o contexto atual do usuário sem sua explícita intervenção. Um exemplo, cada vez mais comum, de sistemas sensíveis ao contexto são aqueles que usam dispositivos móveis acoplados a sensores GPS. Esses sensores obtêm a localização geográfica dos usuários, o que

permite ao sistema oferecer-lhes informações direcionadas ao local em que eles se encontram, como informações turísticas, mapas com melhores rotas para os destinos, entre outras. A combinação da três áreas é ilustrada na figura 1.

Figura 1: Definição de redes sociais móveis



Fonte: Figura adaptada de WEISER, 1991

No que diz respeito a utilização dos dispositivos móveis em redes sociais, destaca-se a transferência tendências da Web 2.0 para *Mobile* 2.0, ou seja, os usuários comuns também podem colaborar para a geração de conteúdos e se fazer mais presente e participativo, perdendo a característica de receptor passivo, para se tornar agente de disseminação de informações através de ferramentas como blogs, chats, sites de relacionamentos etc. Redes sociais móveis procuram aliviar alguns dos desafios de interagir com outras pessoas em público. Estes serviços usam tecnologia móvel para facilitar o intercâmbio de informações sociais ou locacional entre os usuários para incentivar a interação face-a-face.

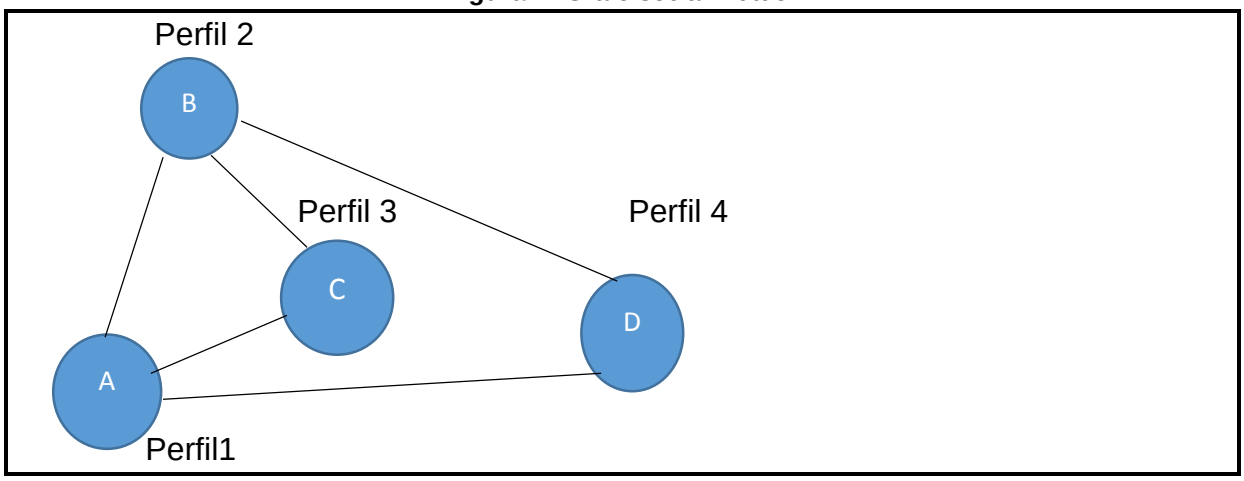
Aplicações de RSM, também chamadas apenas de aplicações sociais móveis, podem auxiliar pessoas a manterem contato entre si em qualquer lugar, a qualquer momento, e também prover recomendações em tempo real sobre pessoas, lugares e eventos ou até mesmo entregar conteúdo personalizado em função do contexto geo-social (localização, co-localização ou lugares em que os usuários se encontram,

.

exemplos: *Facebook, WhatsApp, Twitter, Instagram*). A semântica, a natureza e os tipos de relacionamentos criados com esses elos podem variar de aplicativo para aplicativo, mas, são genericamente representados por um grafo, juntamente com os perfis dos usuários, chamado de Grafo Social. No Grafo Social, os vértices expressam os perfis dos usuários e as arestas os relacionamentos entre eles (TELES et al., 2013).

Um grafo social pode ser visto quando um usuário do vértice A possui uma ligação com o usuário do vértice B, onde essa ligação é feita através de uma aresta que une os dois vértices. Os usuários conectados por uma aresta são amigos um do outro (HAN et al., 2012). Essa relação entre os usuários é mutua, assim como, ocorre na rede social *Facebook*, onde o perfil A é amigo do perfil B mutuamente, como pode ser visto na figura 2.

Figura 2: Grafo social mútuo

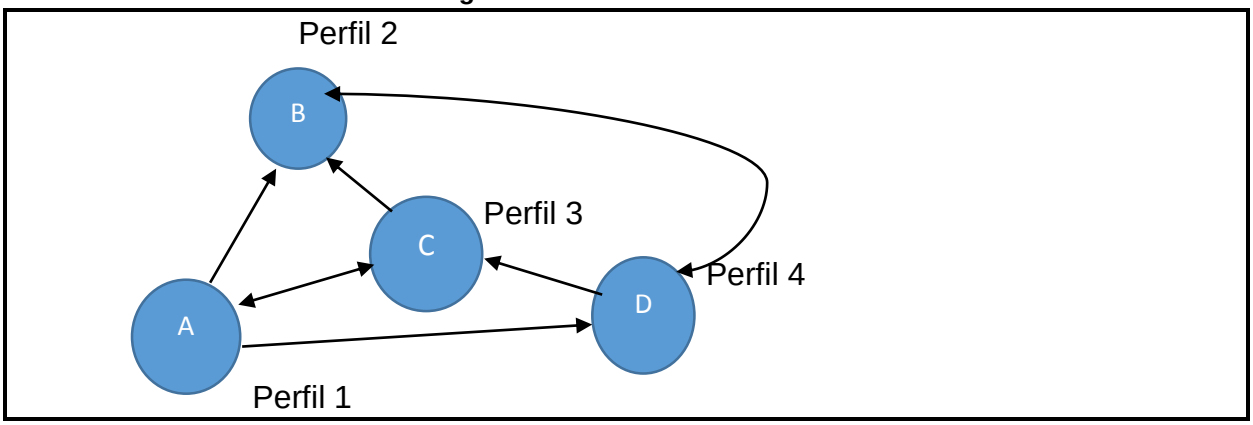


Fonte: Figura Adaptado de Teles ed al., 2013)

Entretanto, dependendo da rede social, essa aresta possui uma orientação. Este é o caso de redes sociais como, *Twitter* e *Instagram* onde os usuários tem a opção de “seguir” ou não, assim como ocorre no relacionamento entre o Perfil C e Perfil B, isto é, o Perfil C está seguindo o Perfil B, mas B não segue C (TELES et al., 2013). Como ilustrado na figura 3.

.

Figura 3: Grafo social orientado



Fonte: Adaptado de Teles ed al., 2013

2.1 ARQUITETURA RSM

A maioria dos softwares sociais móveis existentes confiam em servidores centrais e exigem uma conectividade de infraestrutura para funcionar (PIETILÄINEN, 2010). As infraestruturas para RSM serão mencionadas logo abaixo.

2.1.1 Arquitetura centralizada

RSM centralizadas ou baseadas na Web utilizam serviços de redes sociais como: *Facebook*, *Twitter* para aquisição de informações por meio de dispositivos móveis (KAYASTHA et al., 2011; JABEUR et al., 2013). Existem inúmeras aplicações para RSM baseadas na web para usuários móveis para apoiar e fornecer esses serviços.

Aplicações Web são aplicações desenvolvidas utilizando a linguagem HTML e JavaScript, estando disponíveis por um servidor web e sendo executadas, por exemplo, pelo navegador do celular (IBM WORKLIGHT, 2012; CHARLAND, LEROUX, 2011). Esta é uma estrutura de cliente-servidor, em que o utilizador móvel é o cliente e o servidor central do fornecedor de conteúdo é o servidor. O conteúdo criado pelos provedores de conteúdo é injetado para os usuários móveis através do servidor. Os usuários móveis podem também atualizar e compartilhar o conteúdo com outros usuários de RSM através do servidor centralizado (JABEUR et al., 2013).

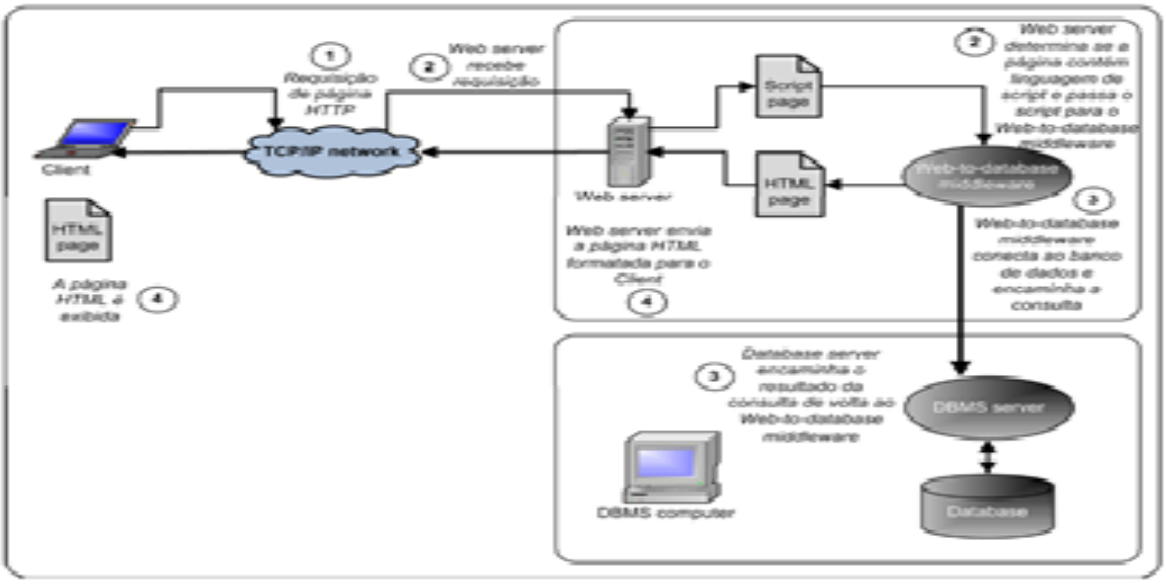
A arquitetura centralizada constitui a base de suporte na internet RSM onde os usuários móveis dependem de atualizações de provedores de conteúdo, como: *Facebook, Twitter*. A vantagem de uma arquitetura centralizada incluem a simplicidade de implementação do serviço e a elevada eficiência de controle centralizado. No entanto, essa mesma arquitetura pode ter um único ponto de falha

.

que é o congestionamento no servidor, isto é, quando um grande número de utilizadores móveis acessam os serviços ao mesmo tempo (KAYASTHA et al., 2011).

A primeira camada é representada pelo navegador e protocolo de serviço. O lado servidor apresenta componentes em diversas tecnologias tais como: PHP, Java Servlets, juntamente com os componentes que interagem com o banco de dados, constituem a camada intermediária. A terceira camada corresponde ao servidor do sistema de banco de dados, constituído pelos dados da aplicação e o sistema de gerenciamento de banco de dados. A figura da arquitetura pode ser vista na figura 4.

Figura 4: Componentes de uma Arquitetura Centralizada baseada na web



Fonte: Figura adaptada de Rob e Coronel, 2009.

Alguns exemplos de aplicações web: *IPhone Facebook App* é uma aplicação móvel que permite que os usuários possam interagir com *Facebook* (FACEBOOK, 2014). Google Earth é uma outra aplicação móvel socialmente consciente baseado na web utilizada para apresentar tráfego ao vivo, rotas de trânsito e imagens no nível de rua utilizado por diversas empresas e websites na internet (GOOGLEMAPS, 2014).

2.1.2 Arquitetura Descentralizada

RSM descentralizadas são ainda objeto de pesquisa acadêmica e de comunidades de códigos aberto, afim de implantar e implementar para que futuramente possam substituir os fornecedores centralizados (SHARMA; DATTA, 2012).

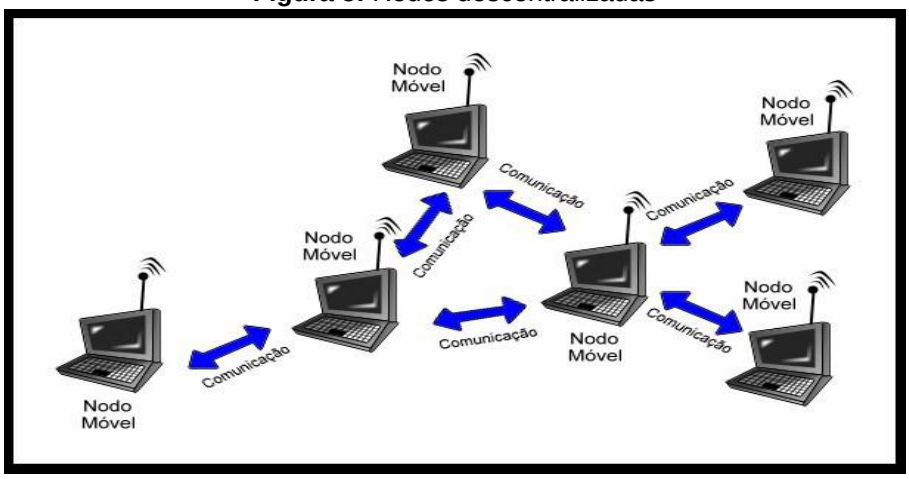
.

Os motivos para uma possível substituição da arquitetura é devido algumas fragilidades da centralizada como escalabilidade de desempenho, privacidade e a dependência de um fornecedor (DATTA et al., 2010).

RSMD (Redes Sociais Móveis Descentralizadas) são implementadas em uma plataforma de gerenciamento de informações distribuída, como uma rede de servidores de confiança ou sistemas peer-to-peer (P2P), isto é, um grupo de usuários móveis é formulado para divulgar dados entres eles sem se conectar a um servidor, ou seja, usando apenas as tecnologias de redes existentes, Wi-fi e *Bluetooth* (NAZIR et al., 2009; JABEUR et al., 2013).

Os usuários móveis interagem uns com os outros com base em seus interesses comuns e padrões de mobilidade formando assim grupos de RSM's distribuídos. O fluxo de dados nesta arquitetura distribuída pode ser através de outros usuários móveis, bem como, os pontos de acesso (KAYASTHA et al., 2011). De acordo com a figura 5.

Figura 5: Redes descentralizadas



Fonte: Figura Adaptada de Nassu e Duarte, 2005

Como a formação das RSM nessa abordagem é realizada de forma oportunista, em um esquema descentralizado, as redes criadas não armazenam no decorrer do tempo as informações sobre quais foram as comunidades formadas, nem informações sobre membros destas comunidades. Caso essas informações sejam armazenadas, esse processo ocorrerá nos dispositivos móveis dos usuários, os quais ainda apresentam restrições de processamento e armazenamento. Portando, um servidor descentralizado não é interessante (SANTOS et al., 2011).

.

2.2 VULNERABILIDADES PARA RSM

Os dispositivos móveis armazenam uma enorme quantidade de informações sensíveis dos usuários, tais como contatos, SMS recebidos e enviados, histórico de ligações, e-mails, fotos, vídeos, histórico de navegação, informações de localização, senhas de acesso a serviços on-line e informações financeiras (ZHANG et al, 2010). A segurança dos dispositivos móveis não manteve o ritmo como a segurança dos computadores tradicionais. Técnicas de segurança, tais como firewalls, antivírus e criptografia, são incomuns em celulares, sistemas operacionais de dispositivos móveis e não são atualizados com tanta frequência como em computadores (RUGGIERO; FOOTE, 2011).

Nos aplicativos e sistemas operacionais dos dispositivos, podem existir vulnerabilidades que possibilitam a execução remota de códigos ou o vazamento das informações por ele para outros dispositivos, ou até mesmo para outras entidades remotas (BRAGA, 2012).

Esses problemas com a segurança vem se agravando de diversas formas com o passar dos anos e com o aumento dos usuários das RSM. Dispositivos móveis compartilham muitas das vulnerabilidades dos computadores, isto é, os atributos que tornam os telefones móveis fáceis de transportar, usar e modificar, torna os smartphones vulneráveis a uma série de ataques. As vulnerabilidades vão desde Roubo de Sessão, Redes sem Fio, *Phishing*, Falhas de Autenticação, *Bluetooth*, SMS/MMS e de Engenheiros Sociais (COLLINS, 2008).

No entanto serão relatado as vulnerabilidades mais conhecidas, pois falar sobre cada uma demandaria muito tempo e não caberia em um só trabalho.

2.2.1 Bluetooth

Bluetooth é uma tecnologia de rádio de curto alcance, que pode transmitir dados através de obstáculos físicos, na faixa de 10m a 100m. Os dispositivos Bluetooth utilizam a faixa de frequência de 2,4 GHz (o mesmo intervalo da tecnologia Wi-Fi 802.11), porém esta frequência muda entre os países devido as regulamentações nacionais. O protocolo Bluetooth visa unificar diferentes tecnologias de transmissão de dados sem fio entre dispositivos eletrônicos móveis e estáticos, como PCs, telefones celulares, notebooks, PDAs, televisores, aparelhos de som, e até mesmo eletrodomésticos como geladeiras e máquinas de lavar (ZANERO et al.,

.

2007)**.** Portanto nessa seção verifica-se que os dispositivos Bluetooth já estão sujeitos a tipos sofisticados de ataques.

2.2.1.1 Capturar Endereços Durante a Comunicação

Ocorrem quando dispositivos Bluetooth estão visíveis para emparelhar com outros dispositivos, é no intervalo do emparelhamento que um usuário malicioso grava o endereço (PIN) e a chave de ligação. Depois de encontrar o PIN e a chave, um usuário malicioso pode decifrar todas as comunicações trocadas entre os dispositivos emparelhados ou se passar pelo dispositivo vítima (BOSE; SHIN, 2006).

2.2.1.2 Erros de Software

Erros de implementação podem fazer o software do *Bluetooth* ficar altamente vulnerável a ataques remotos. A incapacidade de verificar o nome do dispositivo remoto em uma aplicação Bluetooth pode levar o invasor a enviar qualquer cadeia de comando no lugar do PIN do dispositivo remoto para um usuário-alvo, e assim assumir o controle do dispositivo (HAGER, MIDKIFF, 2003).

2.2.2 Engenharia Social

O ataque mais conhecido é *Bluejacking*, onde o usuário malicioso elabora cuidadosamente um nome para o dispositivo, como exemplo “amigo”. Assim para concluir o processo o usuário malicioso solicita permissão para o emparelhamento. Após o usuário-alvo autorizar, mensagens de texto fraudulentas são enviadas fazendo com que os usuários-alvos utilizem seus códigos de acesso, e dessa forma o agressor passa a ter acesso a lista telefônica, calendário ou arquivos que residam no dispositivo (SU et al., 2006).

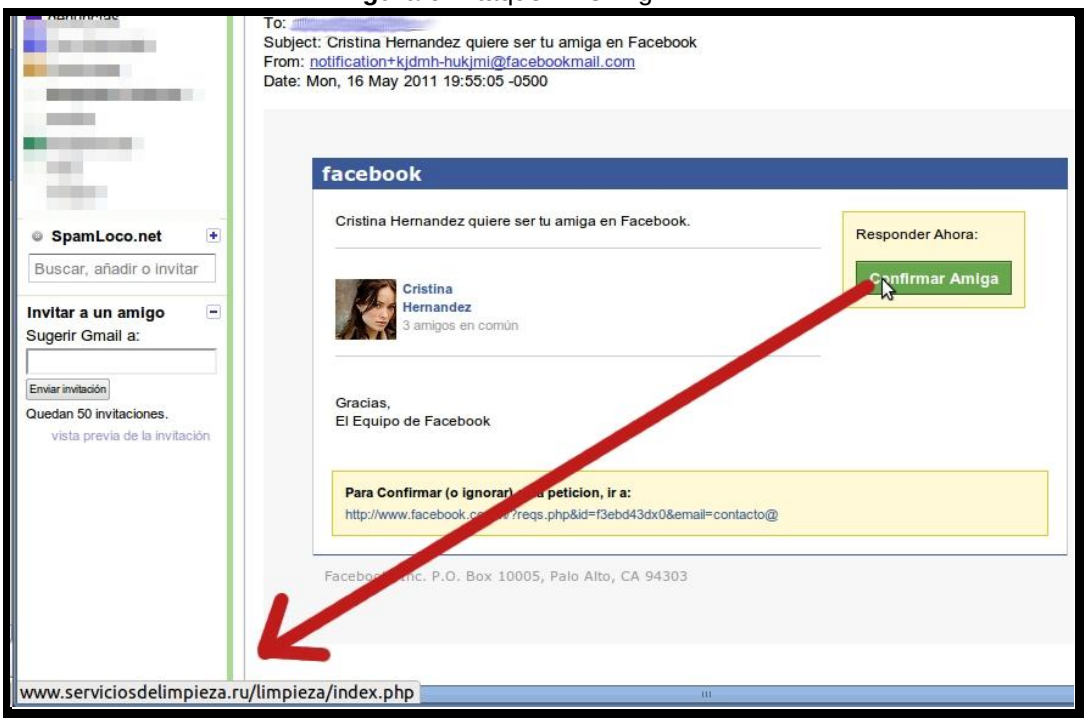
2.2.3 Phishing

Os ataques de *Phishing* utilizam comunicações eletrônicas para enganar os usuários, para assim instalar softwares maliciosos ou conseguir informações sigilosas. E-mail de *Phishing* é um ataque comum em computadores estáticos, porém com o avanço dos dispositivos móveis esses ataques tornaram-se ainda mais perigosos pois os usuários tem a liberdade de acessar seus E-mails de qualquer lugar, de acordo com ilustração da figura 6. Usuários de dispositivos móveis também são vulneráveis ao *Phishing* de chamadas de voz conhecido como *"Vishing"* e mensagens SMS / MMS conhecido como *"Smishing"* (PAUL, FOOTE, 2011).

.

Phishing traz o mesmo risco em smartphones como o faz nas plataformas desktop. Na verdade, muitos usuários confiam no seu dispositivo móvel mais que em seus computadores e, portanto, são mais vulneráveis ao *Phishing* (LEAVITT, 2011).

Figura 6: Ataque Phishing



Fonte: Adaptada de DUNHAM, 2008

2.2.3.1 Smishing

Os SMS são serviços de mensagens curtas que fornecem a capacidade de enviar e receber mensagens de texto através de uma rede móvel. O serviço é único, pois tem um comprimento máximo para escrita de 160 caracteres, requer baixa largura de banda e fornece garantia de entrega das mensagens dentro de um período especificado (IBEKWE, ALJAREH, 2012).

Entretanto o serviço de SMS não é totalmente seguro para fazer transporte de dados sensíveis, até porque os atuais meios de segurança não garantem proteção contra modificações, espionagem e etc (ANUAR et al., 2008).

Os ataques *Smishing* ocorrem quando a vítima recebe um serviço de SMS e são atraídos a clicar em uma URL para baixar o *mobile malware* ou ser redirecionado para sites fraudulentos. Outro tipo de ataque bem conhecido ocorre em aplicativos de músicas, onde ao pressionar a pasta de destino o usuário é enviado para outro Web site onde é solicitado o número do seu telefone para que ocorra a liberação do

.

download, mas o que realmente ocorre é a instalação de um cavalo de Tróia (DUNHAM, 2008).

O MMS é um aperfeiçoamento de SMS, que permite o envio de objetos multimídia, como imagens, vídeo, áudio e texto aprimorado, além de mensagens de texto simples, utilizando infraestrutura *Gprs e Wap, Smtp e Http* como protocolos de transmissão. Atualmente, com uma câmera e um microfone instalado em cada dispositivo móvel moderno, o envio de multimídia via MMS em dispositivos móveis está se tornando um fenômeno de crescimento rápido, programado para ser o acessório padrão para uma mensagem de texto (DUNHAM, 2008).

Os ataques de MMS são estruturadas de forma semelhante às mensagens de e-mail da internet, que consistem de um cabeçalho e um corpo, como pode ser visto na figura 7 (MULLINER, VIGNA, 2006).

Figura 7: Ataque Smishing

Fonte: Adaptada de DUNHAM, 2008

Todas os riscos e vulnerabilidades vistos neste capítulo trazem consequências ruins para qualquer usuário, independentemente do tipo de serviço que o mesmo esteja utilizando. As redes sociais móveis são consideradas alvos fáceis por terem diversos níveis de usuários, como também os mais variados tipos de informações disponíveis na rede. Estas redes sociais podem ter outras falhas de entrada, sem necessariamente depender de ataques ou falhas de proteção nos serviços oferecidos. Por exemplo, no próximo capítulo, serão apresentadas os tipos de redes que são utilizadas pela maioria dos usuários. Estes usuários fazem uso destas redes em diversos lugares como: Trabalho, Shopping, Casa, Faculdade, entre outros. No entanto, as Redes Sem Fio conhecidas pelo padrão 802.11, possuem diversas vulnerabilidades que serão abordadas a seguir, assim como, os mecanismos de prevenção para essas vulnerabilidades também serão abordados.

.

3 ATAQUES E MECANISMOS DE SEGURANÇA PARA REDES IEEE 802.11

As redes sem fio que atendem ao padrão 802.11 foram aprovadas pelo Instituto de Elétrica e Eletrônica (IEEE) no ano de 1999. É uma rede de transmissão de dados desenvolvida para oferecer acesso à rede independentemente da localização, através de ondas de rádio ao invés de uma infraestrutura cabeada (LANE, 2005).

A especificação 802.11 usou a frequência de 2,4 GHz e oferecia uma taxa máxima de transferência de dados de 1 a 2 Mbps. Porém com o passar dos anos a quantidade de dados para transferência aumentou e a insegurança acompanhou toda essa evolução, sendo necessárias outras versões do padrão mais robustas. As versões mais conhecidas que inclusive são utilizadas pelos dispositivos móveis são: 802.11a, 802.11b, 802.11g e 802.11n (SINGH, GURPINDER, 2013).

Com o advento do Wi-Fi, tecnologias sem fio tornaram-se baratas, fáceis de usar e disponíveis para um grande número de pessoas e empresas. A maioria dos telefones celulares vendidos para os consumidores de hoje vêm com quase todos os equipamentos necessários a tecnologia de redes sem fio. Os benefícios das redes sem fio incluem: Conveniência, Mobilidade, Produtividade e Implantação de Expansão (CHOI et al., 2008).

À medida que a tecnologia Wi-Fi avança, suspeita-se que ela seja um grande distribuidor de *Mobile Malware* (MM). Junto com Bluetooth, estes representam os canais mais rápidos até agora para um Hacker espalhar calmamente MM sem causar medo ou chamar a atenção dos usuários de dispositivos móveis (DUNHAM, 2008).

3.1 VULNERABILIDADES SEM FIO

As funcionalidades das redes Wi-Fi também apresentam um dos seus maiores problemas em termos de vulnerabilidade, a exploração dos dados transmitidos (PELECHRINIS; ILIOFOTOU, 2011). WI-FI é um meio de transmissão, onde não há maneira de controlar de onde a informação é enviada e quem tem acesso a ela. Muitos indivíduos e organizações desenvolveram ferramentas capazes de analisar o tráfego da rede, um exemplo *“sniffers”* (COOLE; WOODWARD, 2012). A ferramenta quando utilizada dentro da faixa de transmissão de uma rede Wi-Fi, pode ser usada para capturar todos os pacotes que viajam na rede Wi-Fi gratuita. Mesmo quando a criptografia é utilizada, ainda há importantes informações que estão disponíveis a qualquer pessoa dentro do alcance de uma rede Wi-Fi gratuita, isso inclui o nome da

.

rede, conhecido como o SSID, os endereços MAC de ambos AP e os clientes e uma série de outras informações (AIME; CALANDRIELLO, 2007).

As redes Wi-Fi consistem em três componentes básicos: os pontos de acesso (AP) que fornecem uma conexão com a rede organizacional; os dispositivos (laptops, smartphones, PDAs, etc.) e Usuários (CHOI et al., 2008), como ilustrado na figura 8.

Figura 8: Componentes da rede Wi-Fi

3.1.1 Denial of service (DOS)

Um (DoS) ocorre quando um Hacker bombardeia continuamente um alvo AP (ponto de acesso) ou a rede com pedidos falsos, mensagens de falhas e outros comandos. Com isso usuários legítimos não conseguem ter acesso a rede, pois a mesma fica muito lenta devido as várias requisições e pode até fazer com que a rede deixe de funcionar (TARIQ, 2011).

Porém nos ataques DoS tradicionais, os atacantes usam uma única máquina para enviar repetidamente mensagens para um alvo, utilizando-se da largura de banda e completando o ataque. No entanto, isso não é mais praticado por vários motivos. Em primeiro lugar, a maioria dos grandes servidores e qualquer alvo digno teria uma grande largura de banda suficiente para lidar com uma única máquina, a menos que fosse outro grande servidor. Isso geralmente não é o caso, por isso, na maioria dos casos, o alvo seria realmente capaz de lidar com o ataque, mesmo que o seu serviço é um pouco mais lento para a duração. Em segundo lugar, a maioria dos servidores apenas permitem um certo número de pedidos por um determinado período de tempo a partir de uma única máquina. Isto significa que o invasor logo começa a ter suas mensagens rejeitadas, eliminando o ataque. Por fim, o endereço IP atacante seria bem documentado após o ataque e fácil de rastrear (SOOD et al., 2011).

Portanto nos dias de hoje a forma mais popular de um ataque DoS é um ataque distribuído de negação de serviço (DDoS). Alguns métodos de ataque *Denial of Service* que podem ser lançados na rede através do uso abusivo de protocolos: UDP ataque de inundação, TCP ataque de inundação. (CHOI et al., 2008).

.

3.1.2 Acesso não autorizado

No acesso não autorizado, o usuário ganha acesso à rede e pode obter dados e usar a largura de banda da rede facilmente. O atacante pode violar a confidencialidade e integridade do tráfego de rede, ouvindo os pacotes, alterando os requisitos, enviando e recebendo as mensagens (WELCH; LATHROP, 2003).

3.1.3 Man in the middle (MITM)

O ataque MITM em um canal SSL (*Secure Sockets Layer*), ocorre quando um hacker redireciona o tráfego de um usuário de dispositivo móvel através de um AP (ponto de aceso), interceptando todas as solicitações de conexão SSL. O hacker então responde ao cliente com certificado digital falso e, simultaneamente estabelece uma sessão SSL com o destino da solicitação alvo. Se o cliente aceita o certificado digital falso, o atacante pode passar dados entre as sessões SSL com a capacidade de ler e modificar o tráfego (YUAN et al., 2010).

Contra esses ataques MITM, a principal esperança de uma conexão verdadeira é uma mensagem de aviso de um certificado inválido dado pelo navegador. Infelizmente, se um atacante apresentar um certificado que passa a validação PKI ou chave pública do navegador, nenhum aviso será emitido para o usuário. Normalmente, a única maneira de obter um certificado digital falso para passar a validação PKI seria encontrar um problema de implementação, como um ataque no algoritmo da página. Estes ataques de implementação são válidos apenas até que os bugs de software sejam corrigidos ou substituídos (BENTON, KIM, 2011).

3.1.4 Sequestro de sessão

Sequestro de sessão é uma ameaça comum e grave para a rede local sem fio (WLAN) de segurança. Sequestro de sessão combina negação de serviço (DoS) e de falsificação de IP. Esse tipo de ataque vem evoluindo junto com a proliferação das redes sem fio, particularmente os pontos de acesso WI-FI abertos, exemplo: shopping, aeroportos, lojas, bibliotecas e a liberdade de ferramentas de fácil manuseio como *Firesheep*, bastante popular desde o seu lançamento em dezembro de 2010 (TARIQ, 2011).

No ataque Sequestro de sessão o hacker captura o MAC da vítima com privilégios de rede, forçando o usuário de dispositivo móvel conectado a um AP terminar sua ligação através de uma mensagem com endereço MAC AP falso. Em

.

seguida, associa-se ao AP com o endereço MAC da vítima assumindo a sessão, podendo utiliza-la para qualquer fim que desejar (GILL, SMITH, CLARK, 2006).

3.1.5 Espionagem

As redes sem fio usam ondas de rádio para transferência de pacotes, por isso é fácil ouvir o tráfego de rede ou até mesmo se conectar a uma rede, tendo assim acesso aos protocolos utilizados na rede WI-FI, tamanho dos pacotes e várias outras características do pacote. No entanto, apenas ouvindo o tráfego de rede não necessariamente produzem resultados se os dados são criptografados com criptografia forte. Se a criptografia WEP é usada, é mais provável que os hackers possam, com algum esforço e auxílio de ferramentas como *Wardriving descriptografar* as informações que eles interceptaram (YUAN et al., 2010).

3.2 MECANISMOS DE SEGURANÇA

O uso das redes sem fio abriram enormes brechas na segurança de sistemas em rede. Isso acontece porque as informações são fáceis de serem capturadas, basta apenas um conhecimento simples e o auxílio de ferramentas *sniffer*.

Devido as vulnerabilidades mencionadas na seção anterior, nesta sessão serão relatados os principais algoritmos de criptografia e autenticação para segurança das redes sem fio.

3.2.1 Wi-fi protected access (WPA)

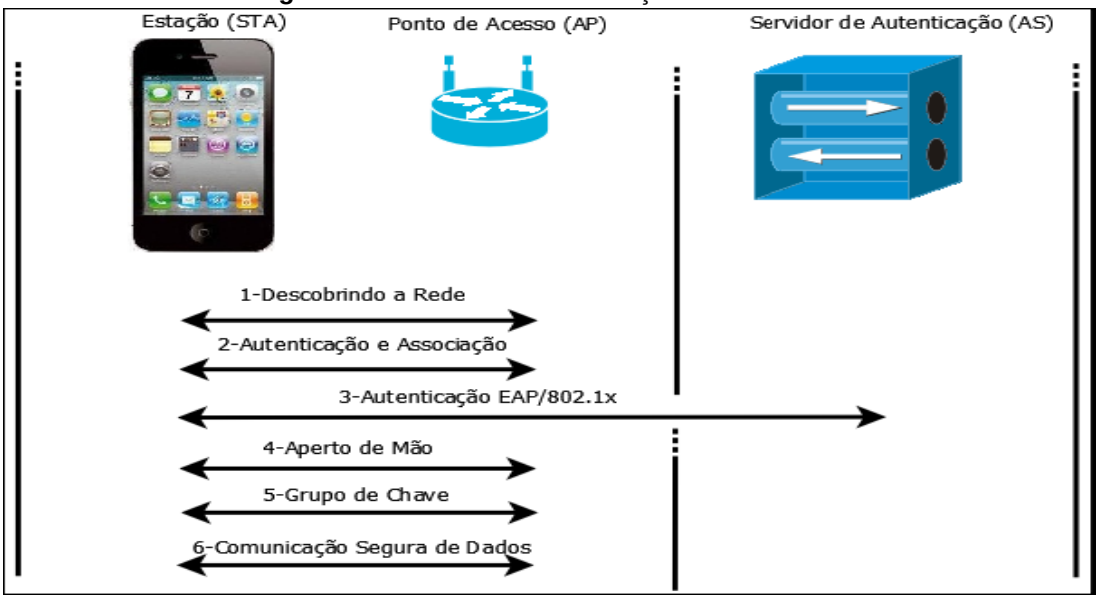
WPA introduziu uma variação que é conhecida como WPA chave pré-compartilhada ou WPA (PSK). Ela fornece criptografia forte e encapsulamento para autenticação. O processo de autenticação envolve três entidades: Estação (STA), *Access Point* (AP) e servidor de autenticação (AS). Geralmente, um processo de autenticação de sucesso significa que a estação e o ponto de acesso verificou a identidade de ambos e gerou algum segredo compartilhado para posterior comunicação de dados segura (XING et al., 2008).

A configuração de uma rede sem fio com características de segurança robusta é considerada uma tarefa complicada e demorada. Embora a emenda IEEE 802.11i tenha introduzido um grande número de melhorias de segurança, os objetivos de segurança mais comuns (incluindo a confidencialidade, integridade, disponibilidade e controle de acesso) ainda estão sob sérias ameaças (LASHKARI et al., 2009).

A emenda IEEE 802.11i introduziu o conceito de uma rede de segurança robusta (RSN). Uma RSN é definida como uma rede de segurança sem fio que só

permite a criação de robustos de segurança Associações de rede (RSNA). O processo de autenticação envolve três entidades: Estação sem fio (STA), ponto de acesso (AP) e do servidor de autenticação (AS) e seis etapas que serão detalhadas e ilustradas na figura 9 (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).

Figura 9: Processo de autenticação IEEE 802.11i



Fonte: Figura Adaptada de XING et al., 2008

- Etapa 1 (Descobrindo a rede): o ponto de acesso anuncia periodicamente sua política 802.11i de segurança em um canal especifico do quadro aviso ou responde a solicitação da estação sem fio (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).
- Etapa 2 (Autenticação e Associação): após uma estação selecionar um ponto de acesso disponível, é hora de uma autenticação e associação mútua por parte de cada dispositivo através da troca de chaves pré-compartilhadas (PSK). A troca de chave é necessária para que cada dispositivo tenha a certeza da legitimidade de ambos e possa ter uma troca de pacotes segura (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).
- Etapa 3 (Autenticação EAP/802.11x): a estação e o servidor de autenticação executam autenticação mútua e algum segredo em comum, isto é, a chave mestre da sessão (MSK). Este passo não existe se PSK já não estiver pré-instalado entre a estação e o ponto de acesso (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).

.

- Etapa 4 (Aperto de Mão): o ponto de acesso e a estação sem fio usam deste aperto de mão para confirmar a existência do PSK, e com isso as portas 802.11x são desbloqueadas para a troca de pacotes de dados (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).
- Etapa 5 (Grupo de Chaves): em caso de aplicações *multicast,* os pontos de acesso irão gerar novos grupos de chaves temporárias (GTK) e distribuirão estes GTK as estações sem fio. Estes apertos de mão pode não estar presente se o GTK foi distribuído na fase 4, os estágios podem ser repetidos várias vezes usando o mesmo PSK (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).
- Etapa 6 (Comunicação segura de Dados): usando PTK ou GTK, as estações e os pontos de acesso constroem canais de transmissão secretas e, assim, realizam robustos confidencialidades dos dados (MITCHELL; CHANGHUA, 2005, ZHENG et al., 2005, XING et al., 2008).

Logo, se as estações sem fio mudarem para um novo ponto de acesso, estas estações sem fio irão realizar outras autenticação 802.11x completas com o servidor de autenticação para obterem novos PSK. Contudo, por motivos de desempenho o PSK de uma estação sem fio pode ser armazenado em cache pelas estações e os pontos de acesso, para, caso queiram associar-se novamente depois o PSK em cache pode ser reutilizado sem outra autenticação completa (XING et al., 2008).

Esta característica do IEEE 802.11i apresenta uma vulnerabilidade potencial, como exemplo um ponto de acesso em uma LAN sem fio comprometida fingindo ser legitima e assim obtendo todos os PSKs das estações sem fio que já se conectaram ao dispositivo. Como mencionado anteriormente as estação sem fio e os pontos de acesso tem a opção de armazenar em cache os PSK, por um período de tempo. Com esta informação, o ponto de acesso pode enganar as estações sem fio e autenticar-se usando os PSK armazenados, e isso pode ser feito utilizando alguns analisadores de rede sem fio como *Wireshark.* Um ponto de acesso comprometido pode, assim, ganhar o controle sobre a estação sem fio, conectando-o a uma rede adversária. Portanto, um novo protocolo EAP, que pode fornecer autenticação para ambas as estações sem fio e pontos de acesso tanto durante a fase de conexão inicial e a situação de roaming, é necessário (ZHENG et al., 2010).

.

3.2.2 Eap-Tls

O padrão original IEEE 802.11 fornecia apenas alguns mecanismos básicos de autenticação, tais como chave de estabelecimento e senha de verificação pré-compartilhada entre o usuário e servidor, conhecida como WEP, porém WEP mostrou bastante vulnerabilidades, porque um Hacker pode obter acesso através de mensagens interceptadas (HOUSLEY; ARBAUGH, 2003). Para melhorar o padrão original, foi proposta IEEE 802.11i (WPA) e (WPA2). IEEE 802.11i introduziu protocolos para gerenciamento de chaves, criação e aperfeiçoamento como criptografia e autenticação. O IEEE 802.11i faz a sua gestão de chave de segurança por meio de algoritmos e protocolos. A presente vulnerabilidade de autenticação mencionada na seção anterior para o IEEE 802.11i, é a principal razão para atualizá-lo para o novo padrão IEEE 802.11x que utiliza um protocolo conhecido como EAP (DHANANJAY et al., 2013).

EAP é um protocolo para autenticação de acesso, utilizado no IEEE 802.11x WLANs, no entanto, ele tem sido adotado por outros padrões sem fio como IEEE 802.11i. Mecanismos de autenticação construídas em EAP são chamados métodos EAP e os requisitos para os métodos EAP em autenticação WLANs foram definidos pela organização de padrões IETF RFC 4017. A intenção do RFC 4017 é que os métodos EAPs utilizados para autenticação de LANs sem fio suportem a autenticação mútua e de derivações de chaves (FAN; LIN; HSU, 2013; HE, 2005).

Os métodos EAPs foram implementados para o uso integrado com protocolos de acesso sem fio padrões, de tal forma que as chaves geradas em uma execução EAP sejam usados para proteger contra *Crackers/Hackers* sem fio e os mais sofisticados ataques ativos de MITM. Com a crescente exigência de segurança e o aumento da complexidade nas aplicações, o alcance dos objetivos e características de segurança foram estendidos para incluir a autenticação do servidor, estabelecimento de chave, privacidade e muitos outros recursos. Para isso foram implementados os seguintes métodos EAP: EAP TLS, EAP-TTLS, EAP-PEAP e EAP FAST (CHEN; WANG, 2005).

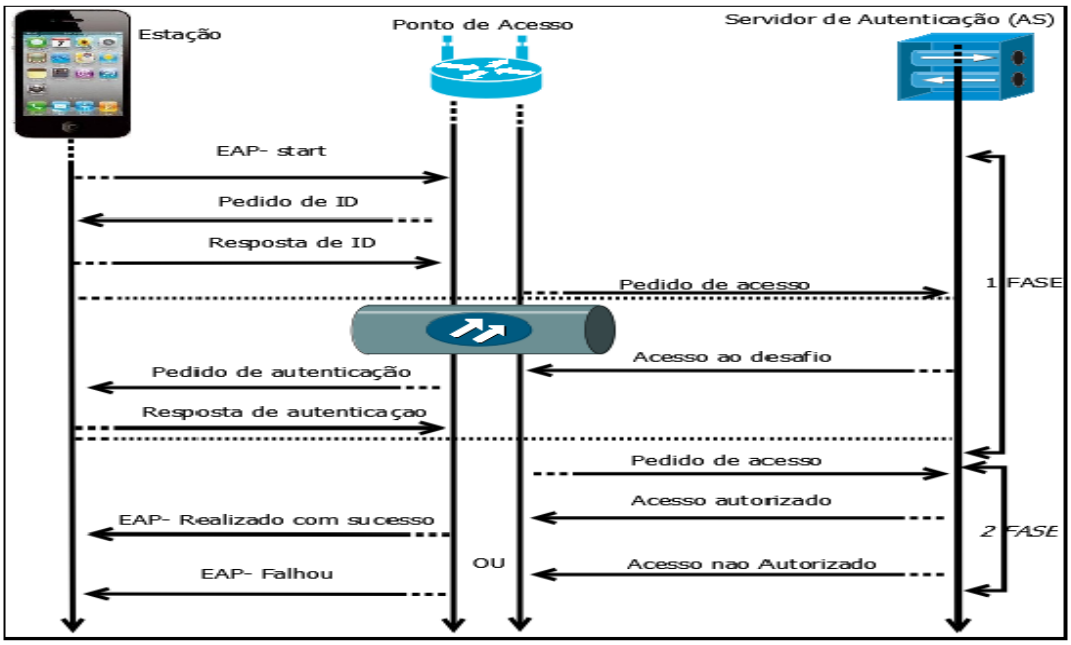
Métodos EAPs baseado em túnel como EAP-TLS determinam a forma de encapsular um protocolo de túnel em mensagens EAP e, em seguida, executam o método EAP ou outro método de autenticação dentro do túnel, que normalmente é o TLS (YANG; ZHU, 2010). Geralmente, os métodos EAPs baseados em túneis

.

especificam quais protocolos de túneis são usados, mas, não restringe os métodos de autenticação que podem ser usados no interior dos túneis. O principal motivo para EAP baseado em túnel é para ativar a proteção de privacidade, através da troca de identificadores do servidor com os clientes móveis exclusivamente pelo túnel, evitando assim a identificação de qualquer elemento por parte de um hacker (CHEN; WANG, 2005).

EAP-TTLS é um método baseado em túnel EAP que se estende EAP-TLS para troca de informações entre cliente e servidor, usando um túnel seguro estabelecido pelo método TLS, ao mesmo tempo que utiliza um método EAP ou um protocolo para autenticação tipo: PAP, CHAP, MS-CHAP. Portanto, esse processo EAP-TTLS compreende duas fases, como ilustrado na figura 10.

Figura 10: Mecanismo de conexão EAP-TLS



Fonte: Figura Adaptada de KARTALOPOULOS et al., 2011.

- Fase 1: A estação representa um nó móvel, autenticador é geralmente um ponto de acesso (AP), e o servidor de autenticação é geralmente o servidor RADIUS que é responsável pela autorização, autenticação e contabilidade (AAA). Após a estação e o ponto de acesso estabelecer uma ligação de dados através do protocolo PPP, a comunicação entre a estação e o servidor de autenticação começa. A comunicação entre a estação e o servidor, acontece dentro do túnel juntamente com outro método EAP ou protocolo de autenticação da estação (ATSUYA; AYED; TERAOKA, 2011).

.

- Fase 2: O servidor RADIUS receberá o pedido de acesso juntamente com as credencias da estação e irá verificar usando esquemas de autenticação junto ao seu banco de dados se as informações estão corretas. Caso as informações estejam a conexão será estabelecida com sucesso, caso contrário o servidor não autorizará o acesso à rede (ATSUYA; AYED; TERAOKA, 2011).

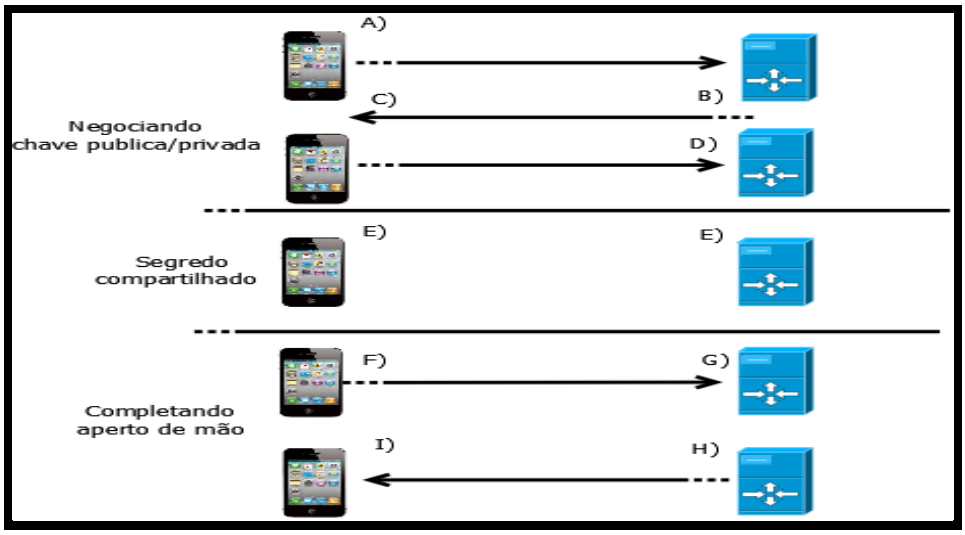
3.2.3 Ssl

Implantado em navegadores da Web, SSL tornou-se de fato o padrão para comunicações seguras de Internet. O principal objetivo do SSL é fornecer segurança do início ao fim, contra um ataque ativo MITM. Sendo assim o protocolo SSL se destina a garantir a confidencialidade, autenticidade e integridade para as comunicações entre o cliente e o servidor. SSL é usado para administrar remotamente infraestrutura virtual baseada em nuvem e no envio de dados locais para armazenamento baseado em nuvem; transmissão de dados de pagamento dos clientes de servidores de comercio eletrônico para processadores de pagamento, como o *PayPal* e Amazon; autenticação de servidores para aplicações móveis em *Android* e *iOS* (GEORGIEV et al., 2012).

O protocolo SSL é destino a proteger os usuários da internet contra ataques MITM, esse tipo de ataque quebra a validação do certificado SSL que é feita entre o cliente e o servidor. Alguns programas como (*PayPal* e Amazon) utilizam apenas bibliotecas SSL, como *OpenSSL*, *GnuTLS*, JSSE, bem como bibliotecas de transporte de dados de alto nível, tais como Apache *HttpClient* e *Urllib*, ou seja, esse descuido ocorre pois deveria ser implementado o protocolo SSL. Com isso um ataque MITM permite ao usuário mal intencionado colher inúmeros cartões de credito, nomes, endereços dos clientes de qualquer comercio que façam uso desses programas de processamento de pagamento (SUGA, 2012). O passo a passo para adquirir uma conexão segura com o protocolo SSL, é ilustrado na figura 11.

.

Figura 11: Mecanismo de conexão SSL



- Passo 1 (negociando): O primeiro passo é o reconhecimento entre o usuário e o servidor: A) Olá cliente e algoritmos suportados. B) Olá servidor, algoritmos escolhidos e envio do certificado SSL. C) verifica a chave pública do certificado SSL e criptografa a chave. D) descriptografa a chave pública utilizando a chave privada do servidor.
- Passo 2 (Segredo compartilhado): E) No segundo passo é criado um túnel para que seja calculada o valor da chave simétrica, que usuário e servidor irão utilizar.
- Passo 3 (Completando aperto de mão): Para concluir a autenticação SSL entre usuário e servidor. F) usuário: cria um algoritmo *hash* utilizando a chave simétrica. G) usuário: compara o algoritmo *hash* do cliente com a versão do servidor também criada com a chave simétrica compartilhada. H) servidor: analisa o algoritmo *hash* do cliente e envia novamente. I) servidor: agora o cliente e o servidor conhecem o algoritmo e a chave simétrica, autorizando uma seção SSL segura entre os mesmos.

Neste capítulo, buscou-se detalhar as várias vulnerabilidades que as Redes Sem fio oferecem. Discutiram-se algumas técnicas para identificação dessas vulnerabilidades, bem como mecanismos adequados para tentar resolver esses problemas. No próximo capítulo serão utilizadas as técnicas discutidas neste corrente capítulo assim como conceitos relacionados as vulnerabilidades de serviços, como também, técnicas de ataques de descoberta de informações sigilosas em RSM. Estas situações serão discutidas no estudos de caso propostos neste trabalho.

.

4 ESTUDO DE CASO

Neste capítulo, serão descritos os três estudos de caso realizados sobre segurança em RSM, bem como, a metodologia e as ferramentas necessárias para a elaboração dos testes.

4.1 METODOLOGIA DE TESTES

Nessa seção será introduzida a descrição dos estudos de caso que serão utilizados para alcançar os objetivos desse trabalho. Esses estudos de caso representam ambientes os quais usuários de RSM podem encontrar-se. Os estudos de caso 1 e 2, mostram como os *hackers* podem utilizar qualquer ferramenta de análise de rede para fazer coleta de dados de usuários em redes, à fim de capturar dados privilegiados. Nesse sentido, uma das variáveis utilizadas para o teste nesta pesquisa, foram os dados sem proteção coletados pela ferramenta *Wireshark,* após a aplicação da mesma no ambiente de rede. Os possíveis dados coletados são: senhas fracas, ausência de conhecimento em segurança em tecnologia da informação (TI), protocolos e aplicações vulneráveis que não começam com HTTPS. A seguir, será descrito a metodologia dos cenários:

O primeiro estudo de caso aborda o funcionamento da ferramenta *Wireshark,* e através dessa ferramenta será feita uma análise na rede para verificar possíveis dados sigilosos. Logo, busca-se demonstrar a eficácia da ferramenta e a ineficácia de aplicativos que usam o protocolo HTTP, para isso utilizará *Wireshark* na coleta de pacotes enquanto um usuário usa a internet. A partir do processo de coleta, será possível analisar todos os aplicativos que o usuário acessou, onde o foco será nos aplicativos que usam HTTP. Outras ferramentas auxiliaram na criação desse estudo de caso, como *Nmap* e *Languard*, na coleta de informações sobre o host e portas das máquinas que estavam na rede.

O segundo estudo de caso terá a mesma metodologia do cenário 1 já citada, entretanto o foco será nos aplicativos que usam o protocolo HTTPS. Busca-se demonstrar nesse estudo de caso que o uso de protocolos confiáveis por parte de usuários pode lhes garantir uma maior tranquilidade no acesso as suas aplicações. Assim como, para o primeiro estudo de caso, também se fizeram necessárias as ferramentas *Nmap* e *Langurad.*

A metodologia utilizada no terceiro estudo de caso fundamentasse nos ataques de Engenheiros Sociais. Para o desenvolvimento do mesmo será levado em conta

.

uma análise quanto ao nível de privacidade dos usuários na rede social facebook. A finalidade dessa análise é avaliar o quão o usuário é descuidado com as informações que ele torna pública. Deste modo, propõe-se uma classificação de usuários em RSM, quanto a nível de privacidade de suas respectivas contas existentes. Logo após essa análise e identificação de usuários, que deixam suas informações expostas, será criado três perfis de acordo com as informações capturadas desses usuários. A conclusão desse cenário termina com o envio de convites de amizade para outros usuários a partir dos perfis falsos, afim de coletar o maior número de informações que possam beneficiar o Engenheiro Social.

4.2 FERRAMENTAS UTILIZADAS

Nesse tipo de pesquisa, é necessário a utilização de ferramentas automatizadas que possam descobrir informações úteis sobre qualquer alvo. Esses programas podem realizar operações como: varreduras na rede, traçar rotas até o alvo, consultar o seu domínio e diversas outras tarefas que tenham o intuito de lhe ensinar mais sobre o seu alvo. Logo abaixo, é possível ler sobre alguns desses programas.

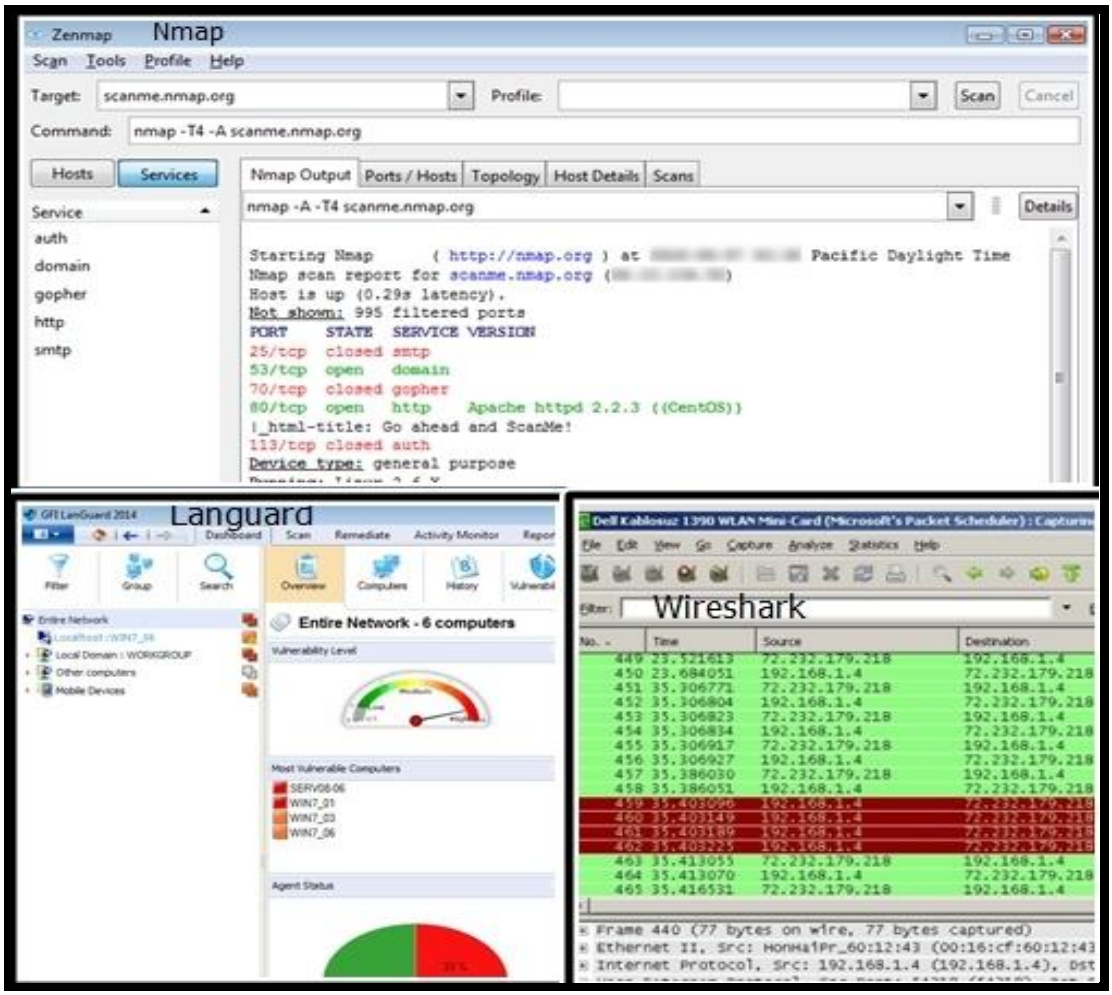
Wireshark é um programa executado em um dispositivo de rede que recebe passivamente todos os quadros da camada de enlace de dados que passam através de adaptadores de redes do dispositivo. A ferramenta captura dados que são dirigidos a outras máquinas, salvando-o para análise posterior. Pode ser usada legitimamente por um administrador de rede ou sistema para monitorar e solucionar problemas de tráfego de rede, isto é, identificar pacotes errados e usar os dados para identificar os gargalos e ajudar a manter a transmissão eficiente de dados da rede. *Wireshark* não foi desenvolvida para hacker ou roubar informações, porem tudo tem seu lado obscuro (QADEER et al., 2010).

Network Mapper (*Nmap*) é um software de código aberto para exploração de rede ou auditoria de segurança. *Nmap* localiza e identifica todas as portas TCP e UDP para determinar quais hosts estão disponíveis na rede, quais serviços (nome e versão do aplicativo) os usuários estão oferecendo, quais sistemas operacionais (e versões de SO) eles estão executando, quais tipos de pacotes filtros ou firewalls estão em uso, e dezenas de outras características (ABBOTT et al., 2006).

Languard Network Security Scanner (LNSS) é um software não gratuito capaz de identificar o nome do host, seu endereço IP, serviços que estão rodando e suas

respectivas falhas em computadores de uma rede, apresentando seu relatório em formato HTML e XML. A ferramenta *Languard* varre a rede, executa mais de 15.000 avaliações de vulnerabilidade, identifica todas as ameaças de segurança possíveis e fornece as ferramentas que o administrador precisa para corrigir muitas das vulnerabilidades (POSEY, 2011). Na figura 12 é possível visualizar a interface de cada ferramenta.

Figura 12: Interface de cada programa

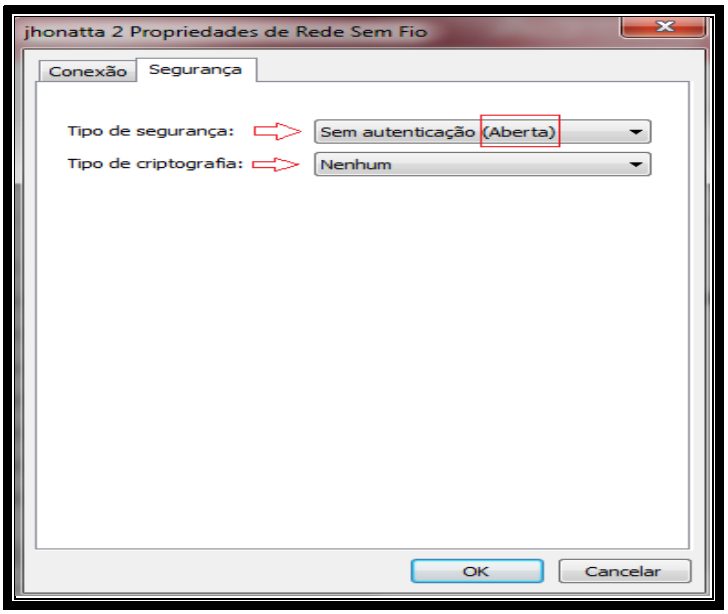


4.3 ESTUDO DE CASO 1: ACESSO EM REDES ABERTAS

Para o estudo de caso 1, a proposta baseia-se no acesso do usuário a uma aplicação através de uma rede sem fio aberta, utilizando protocolos não confiáveis, onde o usuário fornece dados pessoais: E-mail e Senha para uma aplicação Web. Na mesma máquina será utilizada a ferramenta *Wireshark* para “analisar” todo o tráfego que passa na interface de rede. Na figura 13, é possível verificar o tipo de segurança que está sendo utilizado.

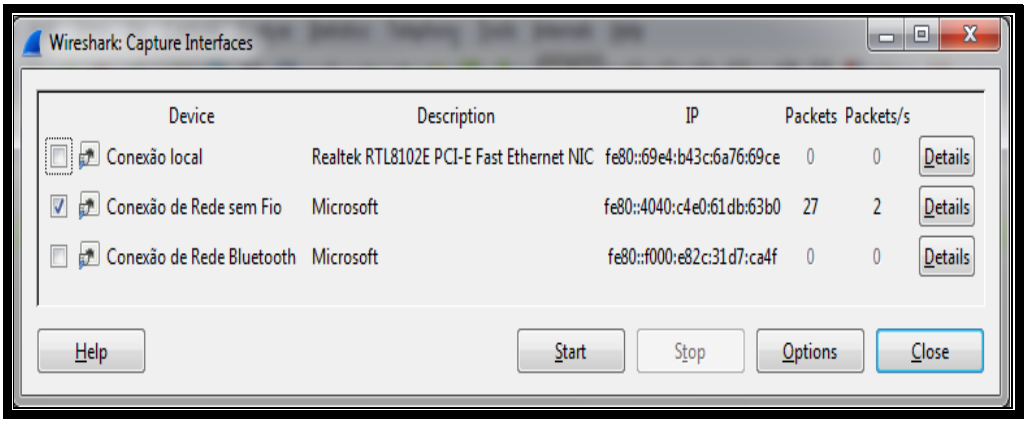
.

Figura 13: Status da Rede sem fio



Na figura 14, o atacante fará uso da ferramenta *Wireshark*, onde terá a opção de escolher qual interface será utilizada para fazer a varredura na rede. A interface utilizada para captura de pacotes é “Conexão de Rede sem fio”, nessa interface ocorre a maior captura de pacotes. Após definir a interface é só iniciar a captura apertando o botão *“Start”*.

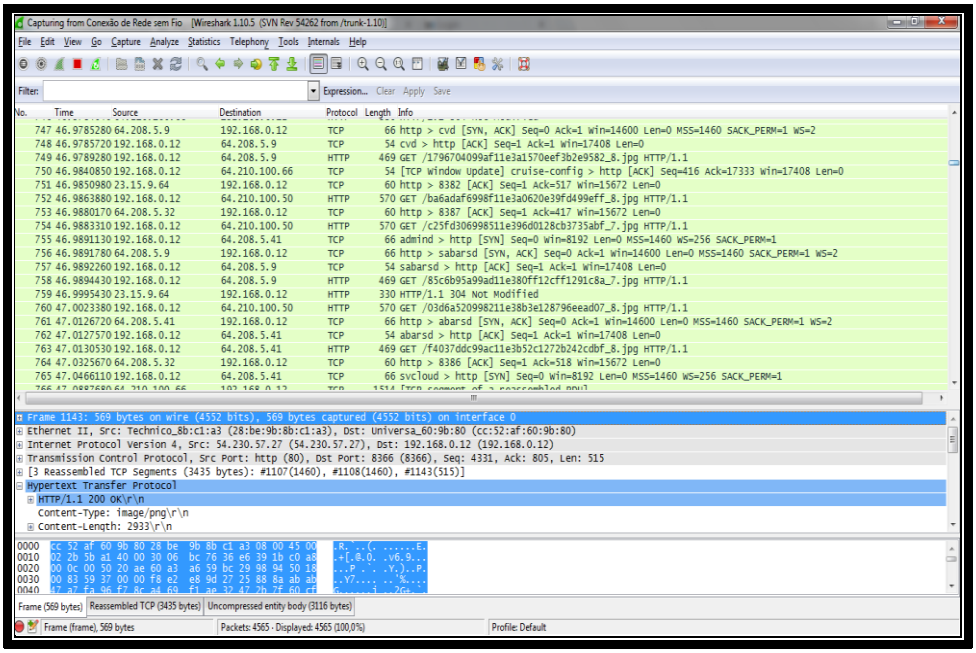
Figura 14: Tipo da Interface de captura



Dado início o processo de coleta de pacotes, o período de tempo vai depender da quantidade de pessoas que atualmente usam a rede ou alguns minutos se houver apenas a atividade de rede acontecendo. Ao iniciar, o *wireshark* deverá exibir informações de todos os usuários da rede, através de protocolos, como pode ser visto na Figura 15.

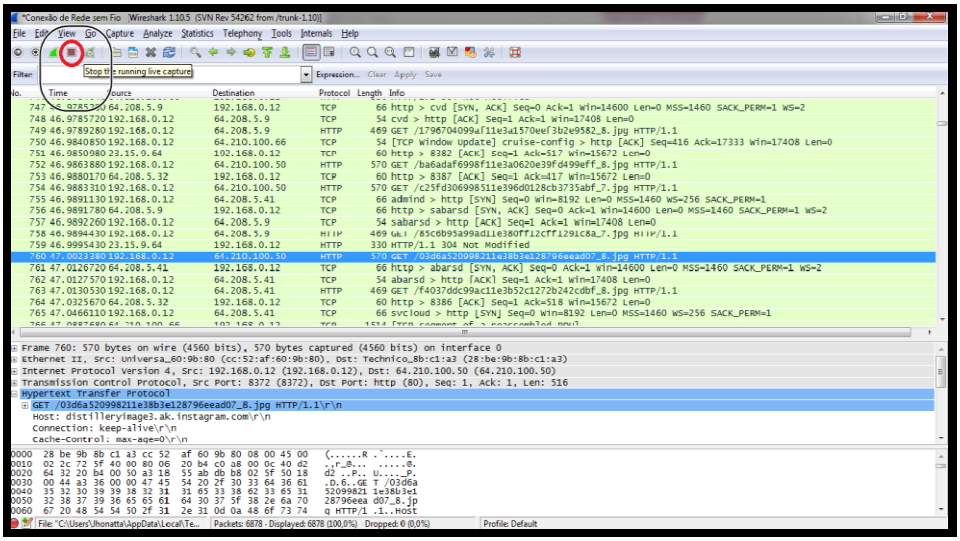
.

Figura 15: Tela de captura do *wireshark*



Logo após a captura de uma quantidade especifica de pacotes, no intervalo de 3 a 5 minutos, a captura deve ser finalizada clicando no botão “Stop”, como ilustrado na Figura 16.

Figura 16: Pacotes sniffer após termino da captura de sessão



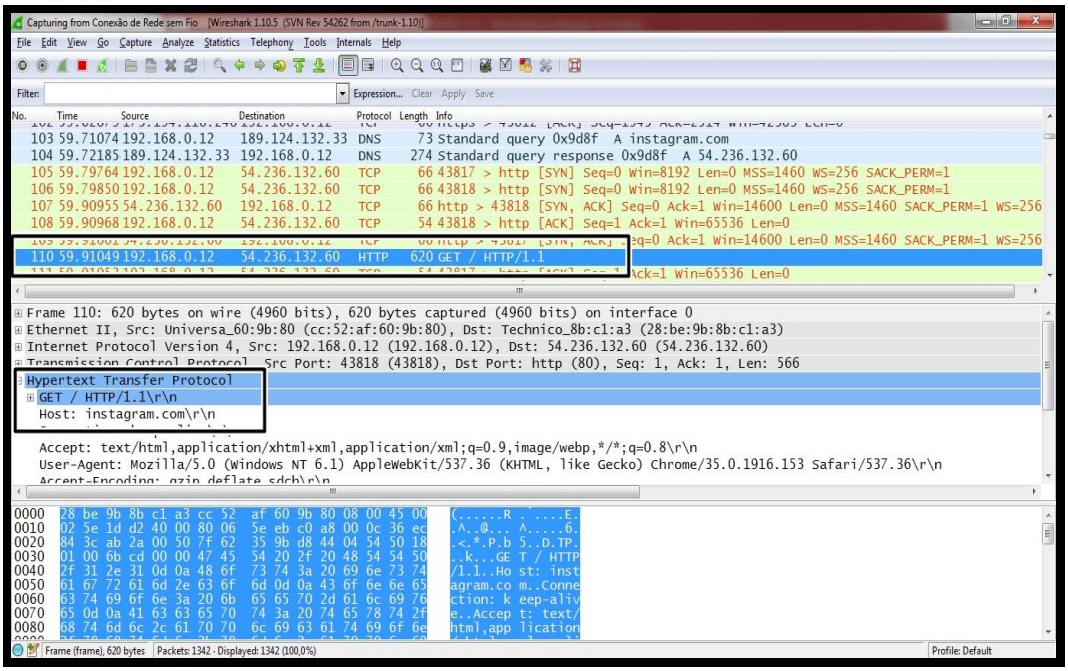
Logo após finalizar a captura, é necessário analisar cada *cookie*[3] do usuário, que foi transferido em um dos pacotes capturados através da varredura na rede, essa captura poderia ter sido feita através de outro computador. A análise será feita no método *Post* (http), onde normalmente consta informações de E-mail e Senha, isso

[3] **Cookie:** São arquivos pequenos que inclui pedidos e respostas do protocolo de transferência de hipertexto (HTTP).
.

ocorre porque o servidor não utiliza criptografia SSL/TLS para assegurar as informações.

Analisando a Figura 17 abaixo, é possível ver que o usuário solicitou ao servidor acesso a rede social *Instagram*, porém não foi possível capturar pacotes que normalmente teriam as informações de E-mail e Senha, isso ocorreu porque a solicitação foi feita para um servidor que utiliza criptografia SSL.

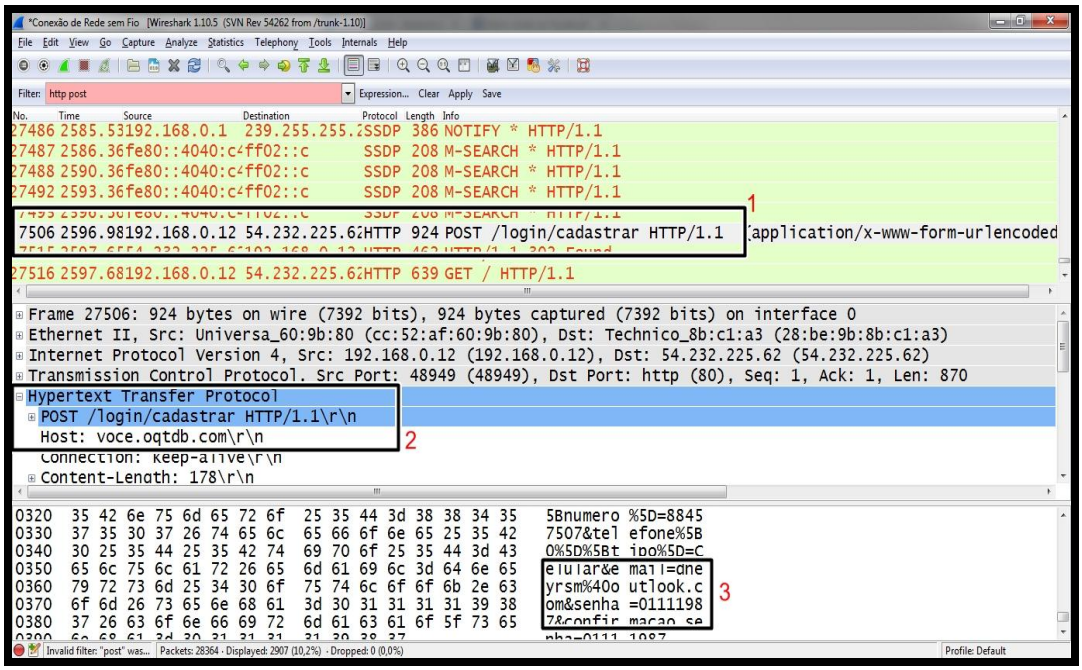
Figura 17: Mostra os detalhes do pacote selecionado



Continuando a análise, é possível visualizar um outro método *Post* com protocolo “HTTP”. Nesse pacote pode ser identificado alguns dados importantes, pois certamente o usuário solicitou acesso para um servidor que utiliza criptografia SSL/TLS. Na Figura 18, é possível ver o site o qual o usuário fez a requisição para o acesso, bem como o IP de destino e a informação mais importante que foi capturada pela ferramenta pode ser vista logo abaixo em formato “txt”, isto é, E-mail e Senha. Com essas informações qualquer usuário malicioso pode submete-las as outras aplicações, já que os usuário tendem a colocar as mesmas informações para diversas aplicações.

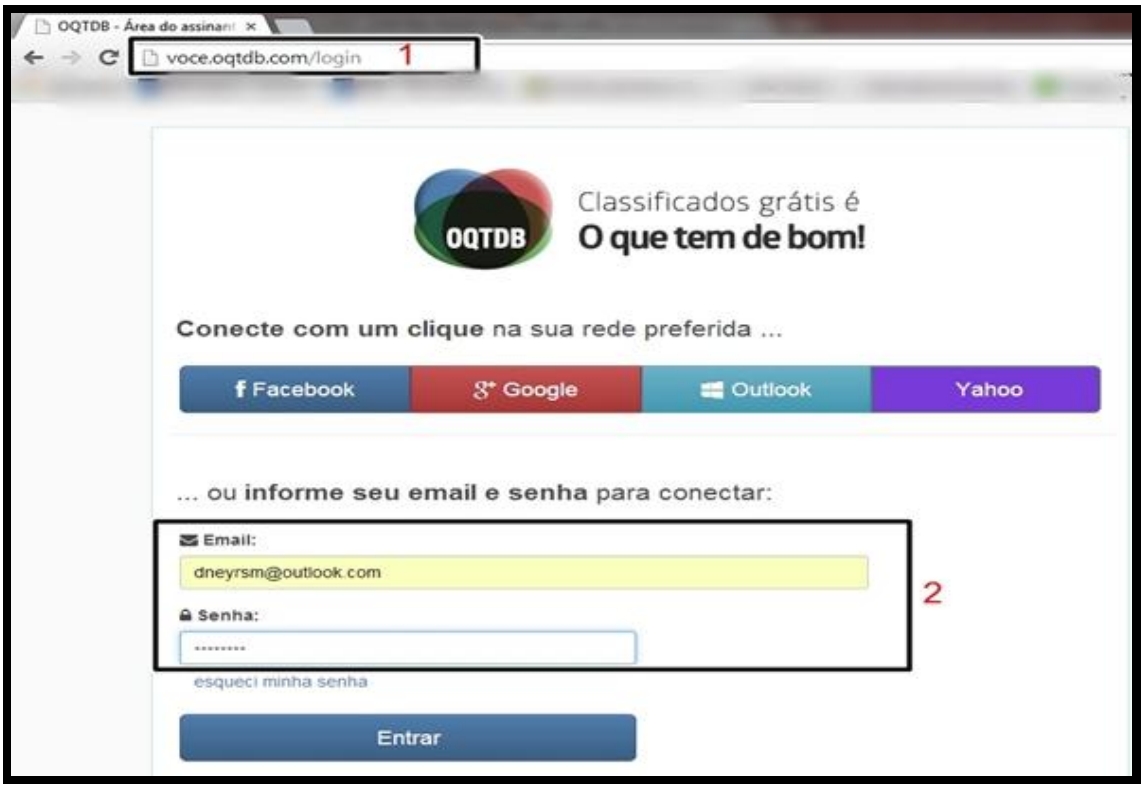
.

Figura 18: Dados do Pacote em “txt”



Após conseguir as informações, o atacante pode utilizar o endereço de *“Host”*, para inserir os dados capturados. Na figura 19, exibe-se a aplicação que o usuário fez acesso.

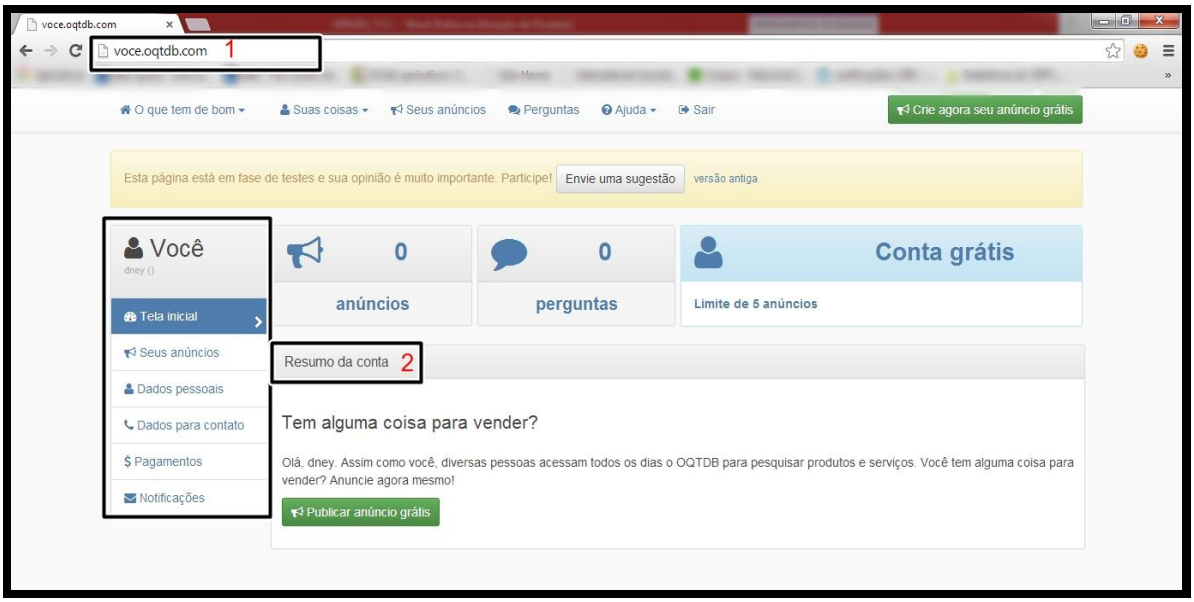
Figura 19: Site para acessar a conta



.

Na figura 20, qualquer usuário que tenha seus dados capturados por um *Cracker/Hacker*, pode ter seus dados utilizados para pratica de crimes virtuais.

Figura 20: Acesso a conta



4.3.1 Vulnerabilidade

O uso de aplicações que não possuem o certificado SSL, pode levar o usuário a diversas dores de cabeça, pois suas informações trafegam pela rede sem nenhuma criptografia. Como foi relatado no estudo de caso 1, a rede virtual é um “campo minado” para o público em geral e principalmente para aqueles que não tomam nenhum cuidado no uso delas, pois a qualquer hora uma pessoa pode ser vítima de uma fraude.

4.3.2 Solução

O SSL é um requisito obrigatório em sites que implementem funcionalidades de autenticação ou introdução de dados sensíveis. Para isso é de extrema importância que os utilizadores verifiquem se um site possui criptografia SSL (HTTPS) e se os dados certificados foram criados por uma entidade certificadora.

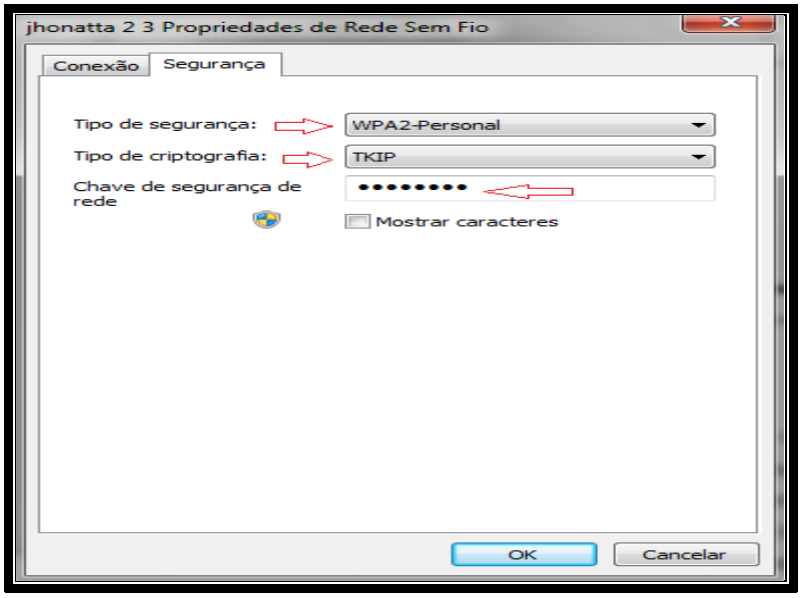
4.4 ESTUDO DE CASO 2: ACESSO EM REDE PROTEGIDA

Para o estudo de caso 1, a proposta baseia-se no acesso do usuário a uma aplicação através de uma rede sem fio aberta, utilizando protocolos não confiáveis, onde o usuário fornece dados pessoais: E-mail e Senha para uma aplicação Web. Na mesma máquina será utilizada a ferramenta *Wireshark* para “analisar” todo o tráfego

.

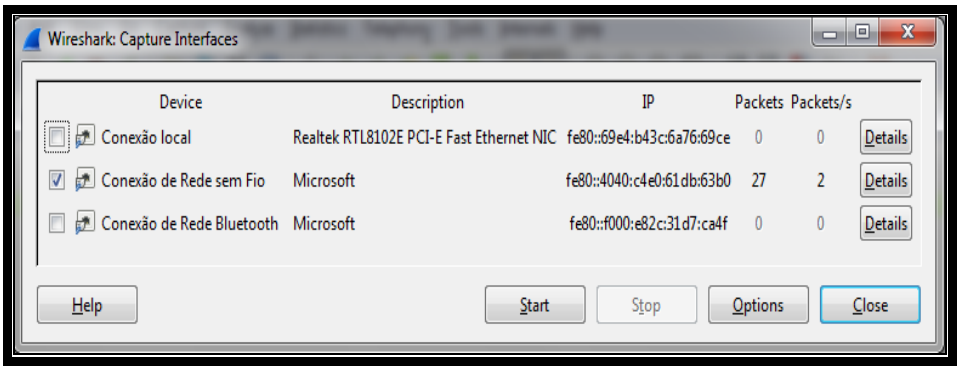
que passa na interface de rede. Na figura 21 é possível constatar o status protegido da rede.

Figura 21: Status da Rede sem fio



Na figura 22, o atacante fará uso da ferramenta *Wireshark*, onde terá a opção de escolher qual interface será utilizada para fazer a varredura na rede. A interface utilizada para captura de pacotes é “Conexão de Rede sem fio”, nessa interface ocorre a maior captura de pacotes. Após definir a interface é só iniciar a captura apertando o botão “*Start*”.

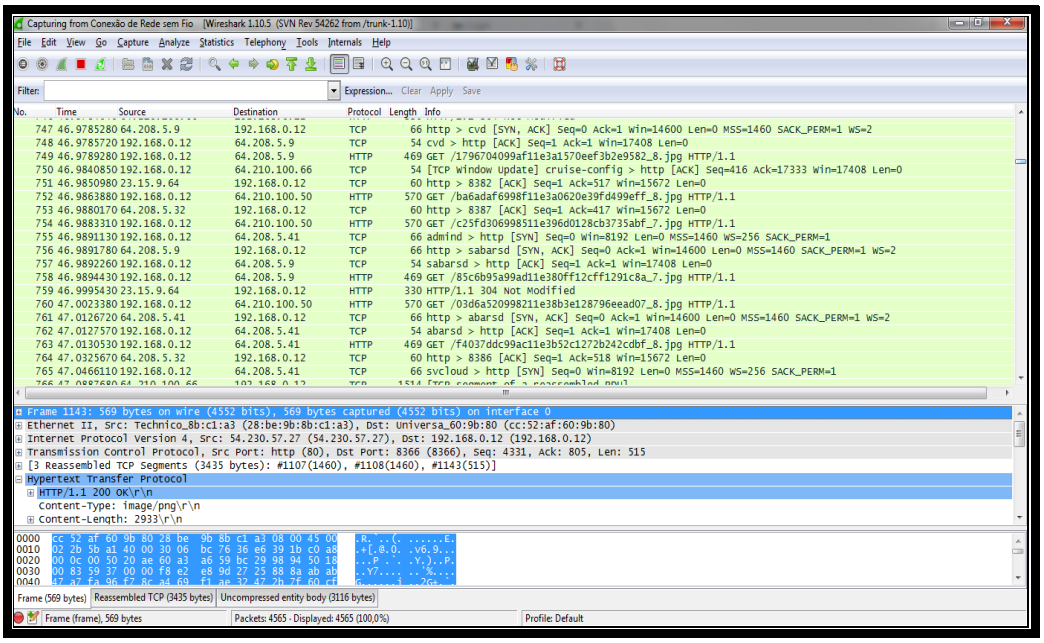
Figura 22: Tipo da interface de captura



Dado início o processo de coleta de pacotes, o período de tempo vai depender da quantidade de pessoas que atualmente usam a rede ou alguns minutos se houver apenas a atividade de rede acontecendo. Ao iniciar, *wireshark* deverá exibir informações de todos os usuários da rede, através de protocolos, como pode ser visto na Figura 23.

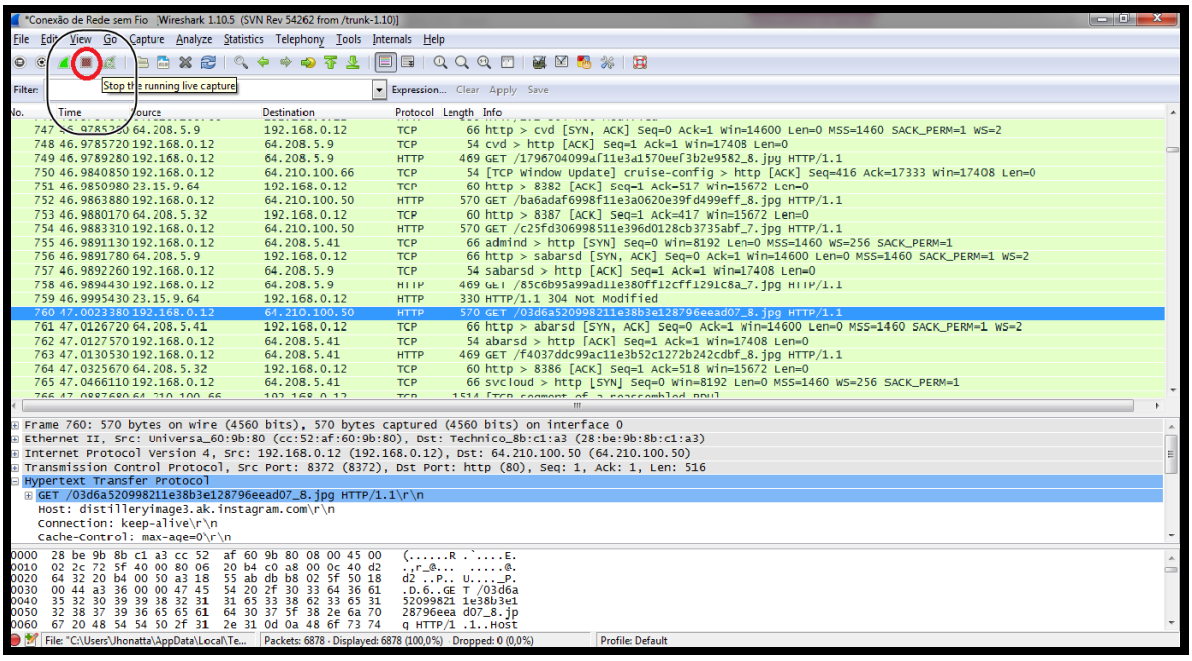
.

Figura 23: Tela de captura do *wireshark*



Logo após a captura de uma quantidade especifica de pacotes, no intervalo de 3 a 5 minutos, a captura deve ser finalizada clicando no botão *"Stop"*, como visto na Figura 24.

Figura 24: Pacotes sniffer após termino da captura de sessão



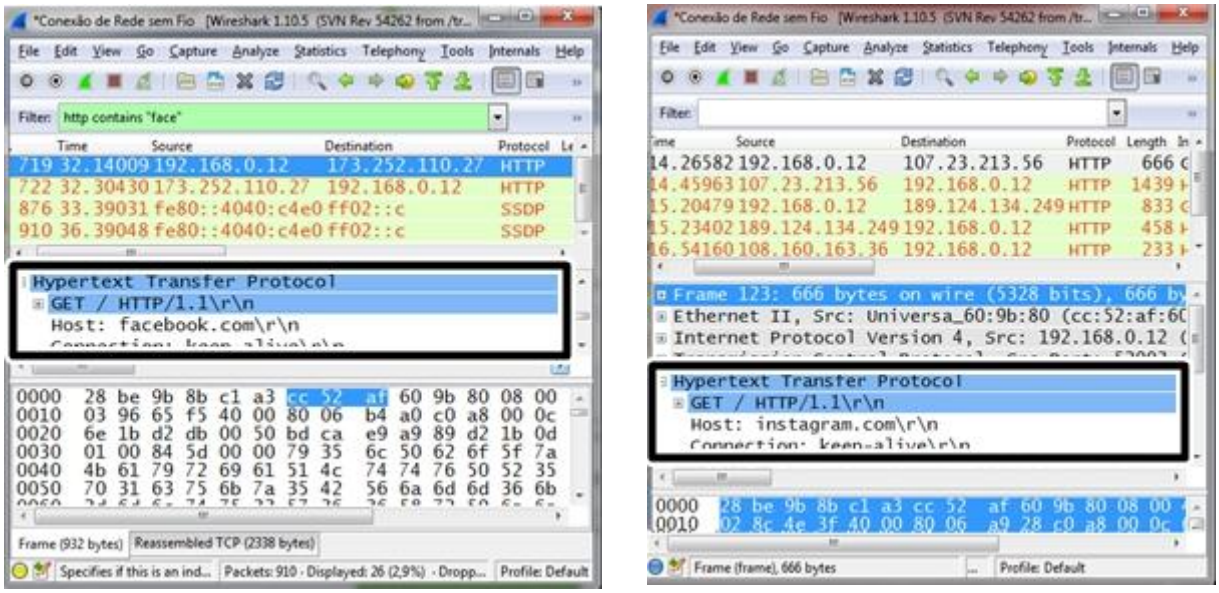
Logo após finalizar a captura, é necessário analisar cada cookie do usuário, que foi transferido em um dos pacotes capturados através da varredura na rede, essa captura poderia ter sido feita através de outro computador. A análise será feita no

.

método *Post* do protocolo “SSL”, onde normalmente consta as informações de E-mail e Senha.

Analisando a Figura 25 abaixo, é possível perceber que o usuário tentou acessar a rede social *Facebook* e *Instagram*.

Figura 25: Mostra os detalhes do pacote selecionado



A ferramenta *Wireshark* conseguiu capturar o acesso de um usuário a duas Redes Sociais, *Facebook* e *Instagram*, no entanto diferentemente do estudo primeiro estudo de caso, não é possível ver os dados de E-mail e Senha do usuário, pois, o mesmo fez uso de uma sessão HTTPS, isto é, uma sessão HTTPS faz uso de um mecanismo de proteção SSL/TLS, onde o TLS garante a integridade dos dados transmitidos entre as duas partes envolvidas (cliente e servidor) e também fornece autenticação forte para ambas as partes.

4.4.1 Vulnerabilidade

Nos últimos anos tem-se assistido a uma grande variedade de ataques ao mecanismo de SSL/TLS. Um ataque que vale ser ressaltado é renegociação SSL: a renegociação SSL, ocorre tanto por parte do cliente como pelo servidor, a qualquer momento. Para o cliente solicitar renegociação o cliente envia uma mensagem “cliente olá” no canal criptografado já estabelecido e o servidor responde com um “servidor olá” e, em seguida, a renegociação segue o processo de aperto de mão normal. O servidor pode iniciar a renegociação enviando ao cliente uma mensagem “olá *request*”. Quando o cliente recebe o pedido, o cliente envia a mensagem “cliente olá” e o processo de aperto de mão ocorre (Figura 10 e 11).

.

É nesse processo de renegociação que um atacante injeta texto simples no lugar da vítima podendo sequestrar a sessão HTTPS ou até mesmo realizar negação de serviço (Figura 10 e 11).

4.4.2 Solução

Para diminuir o risco de Roubo de Sessão e MITM alguns desenvolvedores aconselham desativar a renegociação por parte do servidor. Entretanto já existem alguns servidores que aceitam a SSL renegociação. Portanto a solução ideal seria que os servidores que aceitam a renegociação segura, indicasse-a durante a fase de negociação SSL.

4.5 ESTUDO DE CASO 3: ENGENHARIA SOCIAL

Para o terceiro estudo de caso, a metodologia de teste é Engenharia Social, uma tática muito usada pelos *Cracker/Hackers*, que consiste de meios não-técnicos para obter informações privilegiadas. As informações privilegiadas podem ser: informações sobre uma certa pessoa, endereço residencial, telefone, lugares mais frequentados, familiares, entre outras informações que podem ser de grande valia para um atacante de engenharia social. Geralmente, é um mestre em enganar e iludir as pessoas.

O objetivo desse estudo de caso é mostrar algumas técnicas da engenharia social aplicada a maior rede social da atualidade, *Facebook*. Através dessas técnicas, é possível fazer com que alguém execute alguém software malicioso, como *keyloggers* ou *trojans*, fornecendo informações privilegiadas, ou mesmo através de um fake em uma rede social conseguir dados suficientes para roubar uma identidade. Às vezes, apenas uma simples conversa é suficiente para um usuário comum fornecer as informações que o engenheiro social precisa saber. Diante destes cenários, foi necessário uma coleta de dados baseada nos perfis da rede *facebook*, verificando e armazenando quais são os usuários mais propícios a serem vítimas destes atacantes. Para isso realizou-se uma coleta aleatória de 30 usuários do *facebook*, utilizando um perfil fake. Em virtude desta análise, a tabela 1 e o gráfico 1 apresentam em quantidades de usuários, quais informações, assim como, qual a porcentagem de usuários demonstram pouco cuidado em relação aos dados pessoais publicados de modo indireto no seu respectivo perfil.

.

Tabela 1: Dados coletados (privado)

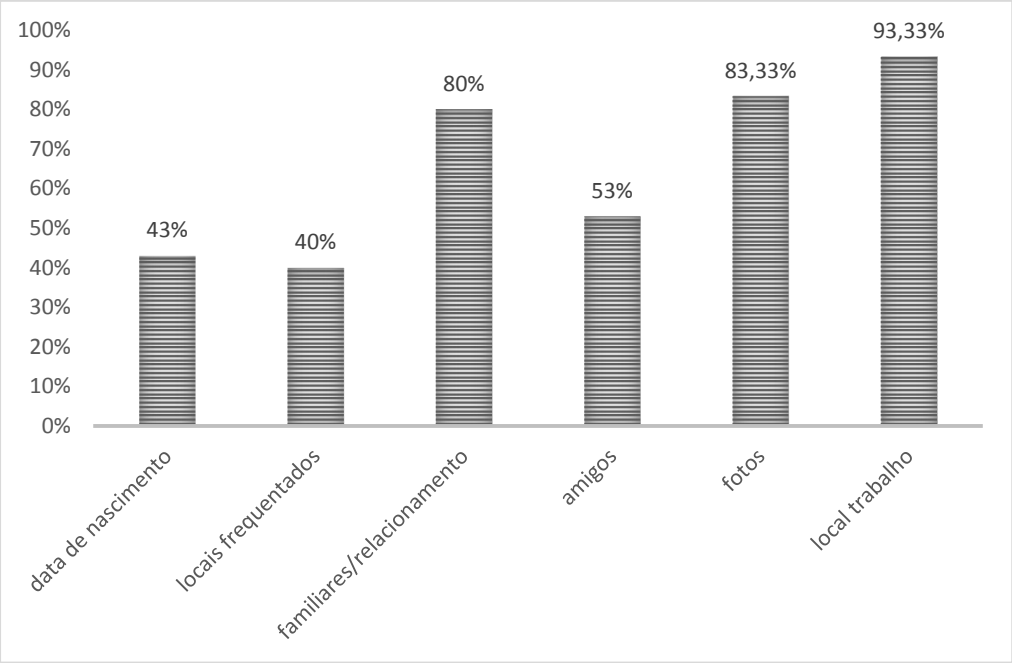
Dados coletados	N° de Usuários	Consequências
Amigos	16	Possíveis vítimas do fake, *Malware, keyloggers*.
Data nascimento	13	Senhas de e-mail e redes sociais, acesso a certidões de nascimento.
Fotos	25	Material suficiente para criar um fake, isto é, roubo de identidade, cometer crimes virtuais, difamação de caráter.
Familiares/Relacionamento	24	Dados para extorsão, chantagem.
Local de trabalho e Telefone	28	Dados utilizados em sequestro relâmpago e movimentos contra você.
Posicionamento geográfico	12	Traçar a rota da vítima, horários.

De acordo com a tabela 1 é necessário definir as principais consequências de uma privacidade comprometida. **Amigos**: Quando um usuário de uma rede social como *facebook* tem sua privacidade comprometida, seus amigos se tornam potenciais vítimas também. **Data de nascimento**: A data de aniversário completa é uma das mais valiosas peças de dados pessoas que os ladrões de identidade pode usar, isto é, parece até uma informação inofensiva, no entanto torna-se uma informação bastante útil para os engenheiros sociais, principalmente para obter outras informações privilegiadas acerca do usuário, pois, dependendo da determinação de um engenheiro ele pode com algum esforço descobrir até uma certidão de nascimento. **Fotos**: Deve ser bem resguardada, pois, o uso delas por parte de ladrões de identidade pode refletir muito mal no futuro. **Familiares/Relacionamento**: Expor seus familiares, bem como seus relacionamentos pode facilitar para que ladrões cometam fraudes, extorsão, chantagens e isso ocorre normalmente por ligações telefônicas. **Local de trabalho e Telefone**: A divulgação do seu local de trabalho e telefone pode fazer os ladrões traçarem sua rota, seu dia-a-dia, fazendo com que você

.

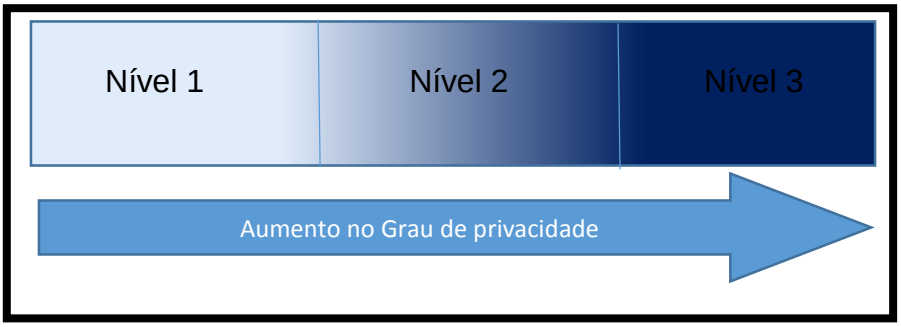
fique altamente vulnerável para situações de sequestro, roubo e etc. **Posição geográfica**: Dado pessoal bem comum dos usuários da rede social *facebook*, onde o mesmo informa na grande maioria sua atual localização, e isso expõe uma importante informação, a de que você não está em casa. Para alavancar nosso estudo o gráfico 1 demonstra em porcentagem as principais informações que os usuários de redes sociais divulgam na hora de preencher seus perfis.

Gráfico 1: Percentual do Dados Coletados



Os critérios de análise dessas informações foram definidos como: Nível 1: Iniciante, perfis sem nenhuma privacidade. Fácil de identificar data de nascimento, local de trabalho, telefone, e-mail, familiares/relacionamentos e amigos. Nível 2: Moderado, perfis com parte de suas informações pessoas públicas. Nível 3: Avançado, perfis de usuários cujo o nível de privacidade é muito alto, onde não é possível visualizar nenhum item do perfil. A figura 26 ilustra a classificação dos níveis de usuários quanto a privacidade e segurança dos mesmos.

Figura 26: Mostra os níveis de segurança dos usuários (privado)



.

Essa classificação foi utilização para escolher a composição de cada perfil *fake* utilizado neste estudo de caso. Todos os perfis criados foram marcados com a sigla RSM no final dos seus nomes como referência ao tema do trabalho.

O primeiro perfil mostrado na figura 27, do usuário “Faustino”, foi criado visualizando que o perfil do usuário real enquadrava-se no tipo de segurança nível 1, isto é, suas informações, imagens, familiares, amigos estavam públicas.

Figura 27: Perfil de “Faustino”, primeiro usuário criado para a experimentação

O segundo perfil mostrado na figura 28, do usuário “Andrade”, foi criado com base no nível 2, onde parte de suas informações e imagens estavam públicas.

.

Figura 28: Perfil de “Andrade”, segundo usuário criado para experimentação

Logo após criar os dois perfis, 12 convites de amizade foram lançados para a rede de amigos dos usuários reais. Escolhidos aleatoriamente entre os homens e mulheres. Os convites não tiverem nenhuma tentativa de manipulação, visto que, o teste tenta mostrar a ação de um verdadeiro Engenheiro Social. O gráfico 2 e 3 representam os resultados dos convites enviados.

Gráfico 2: Quantidade de convites "Perfil 1"

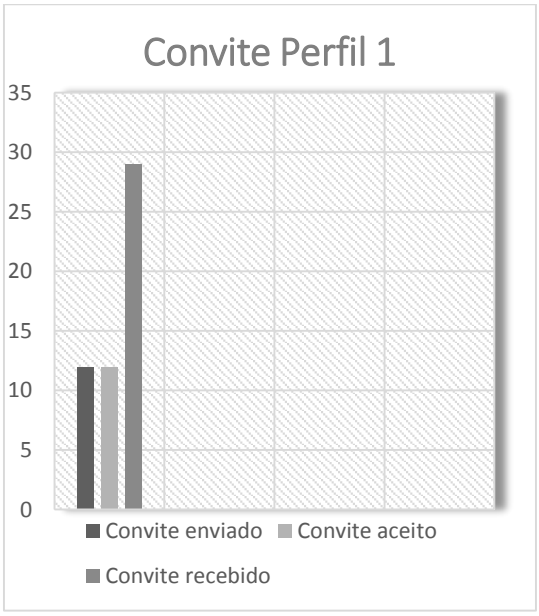
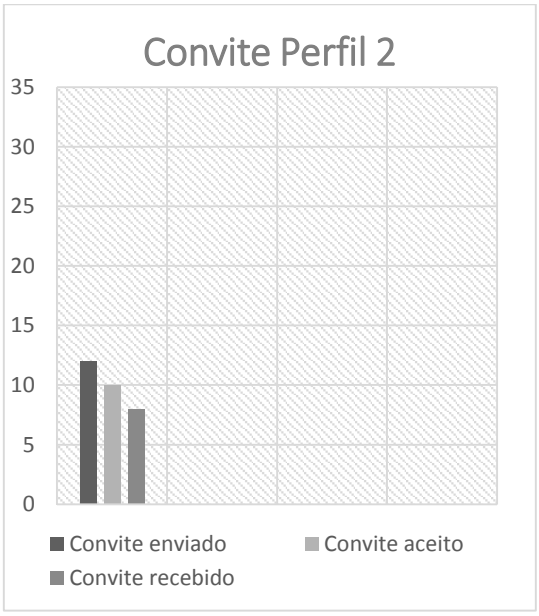


Gráfico 3: Quantidade de convites "Perfil 2”



.

Este resultado é, portanto, bastante relevante, já que mostra o nível de descuido dos usuários que receberam o convite, bem como os que enviaram. Pois em nenhum momento houve alguma tentativa de contato para saber sobre o novo fake do usuário real.

O nível 3 é onde o usuário possui uma constante preocupação com a sua privacidade, como pode ser visto na figura 29. Na figura 29 é possível observar que o usuário do perfil se encaixa perfeitamente no nível 3, isso porque o usuário não disponibiliza nenhuma informação que comprometa sua privacidade, isto é, suas informações só podem ser visualizadas por amigos.

Figura 29: Perfil de “Gomes”, terceiro usuário criado para experimentação

Diante disso fica claro que o perfil ideal do ponto de vista da privacidade para qualquer usuário de uma rede social, é sem dúvida um perfil que não disponibiliza nenhuma informação válida para ajudar um Engenheiro Social na incubação do seu crime. Portanto neste capítulo, buscou-se mostrar através de cenários reais de riscos as várias vulnerabilidades que os usuários de aplicações sócias estão expostos. O desenvolvimento desses cenários serviram como embaso para o capítulo seguinte, que será feito um guia de segurança para auxiliar os usuários de redes sociais móveis.

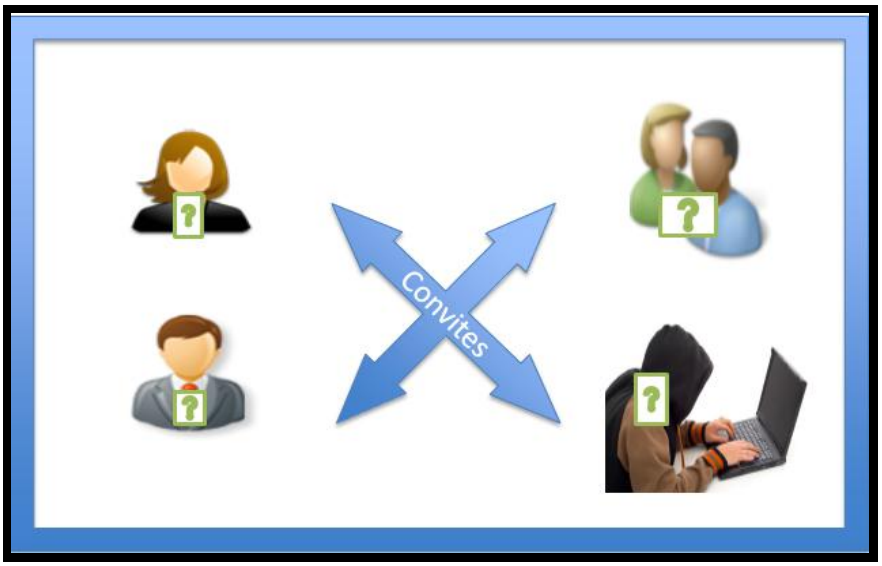
.

5 GUIA DE PREVENÇÃO PARA O USUÁRIO

Existem centenas de milhões de pessoas que utilizam as redes sociais on-line, logo existe uma boa chance de que estes usuários publiquem, compartilhem e transfiram conteúdo dos mais diversos gêneros. Estas informações compartilhadas permitem a estes usuários manterem contato sem muito esforço com qualquer outro usuário. No entanto, muitas pessoas além de seus amigos e conhecidos estão interessados nas informações que são postadas nas redes sociais, por exemplo, os ladrões de identidade, golpistas, *Crackers/Hackers*, entre outros. Portanto este guia foi embasado nos principais tipos de ataques mencionados ao longo deste trabalho. Logo, este guia servirá de auxílio para que os usuários de Redes Sociais Móveis possam reduzir os riscos de violação na privacidade.

DICA 1: O usuário deve ser cauteloso sobre quem está tentando fazer amizade com você on-line, incluindo via e-mail e sites de redes sociais.

Figura 30: Dica 1



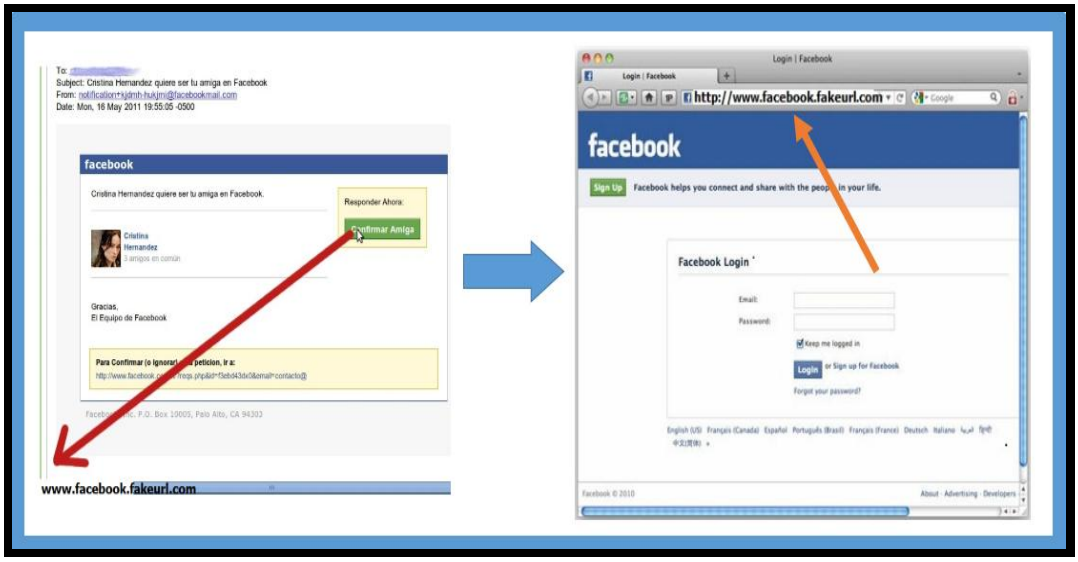
DICA 2: O usuário nunca deve divulgar informações pessoais do seu trabalho ou site pessoal.

Figura 31: Dica 2

.

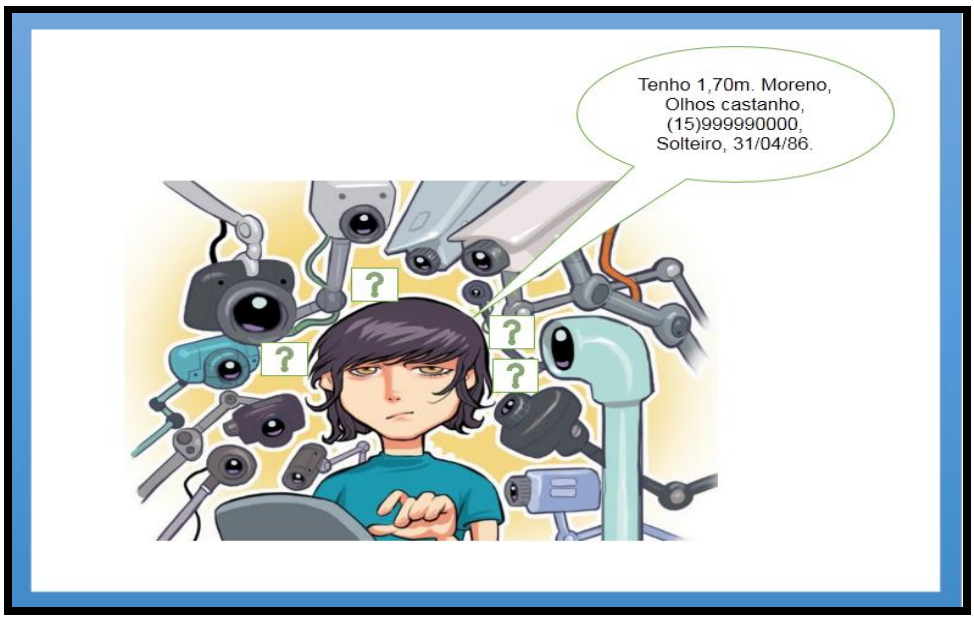
DICA 3: O usuário deve ficar sempre atento a ataques de *phishing*, isto é, não clique em links no corpo de um e-mail a menos que você tenha certeza que o remetente é legitimo ou ligue para o remetente para verificar se o mesmo é legitimo.

Figura 32: Dica 3



DICA 4: O usuário deve estar sempre atento a qualquer publicação sobre si mesmo, quer no seu perfil ou em suas mensagens - tais como números de telefone, fotos de sua casa, local de trabalho ou na escola, o seu endereço ou o aniversário.

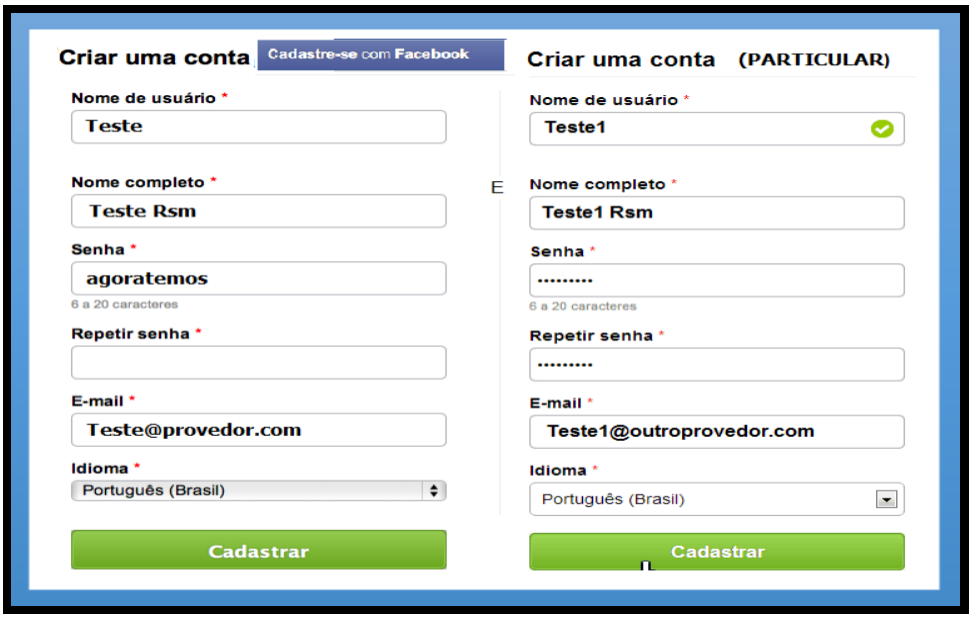
Figura 33: Dica 4



.

DICA 5: O usuário deve configurar uma conta de e-mail separado para se registrar e receber e-mails da rede social. Dessa forma, se você quiser fechar sua conta / página, você pode simplesmente parar de usar essa conta de e-mail. Criação de uma nova conta de e-mail é muito simples e rápido de fazer uso de tais provedores como Hotmail, Yahoo! Mail ou Gmail.

Figura 34: Dica 5



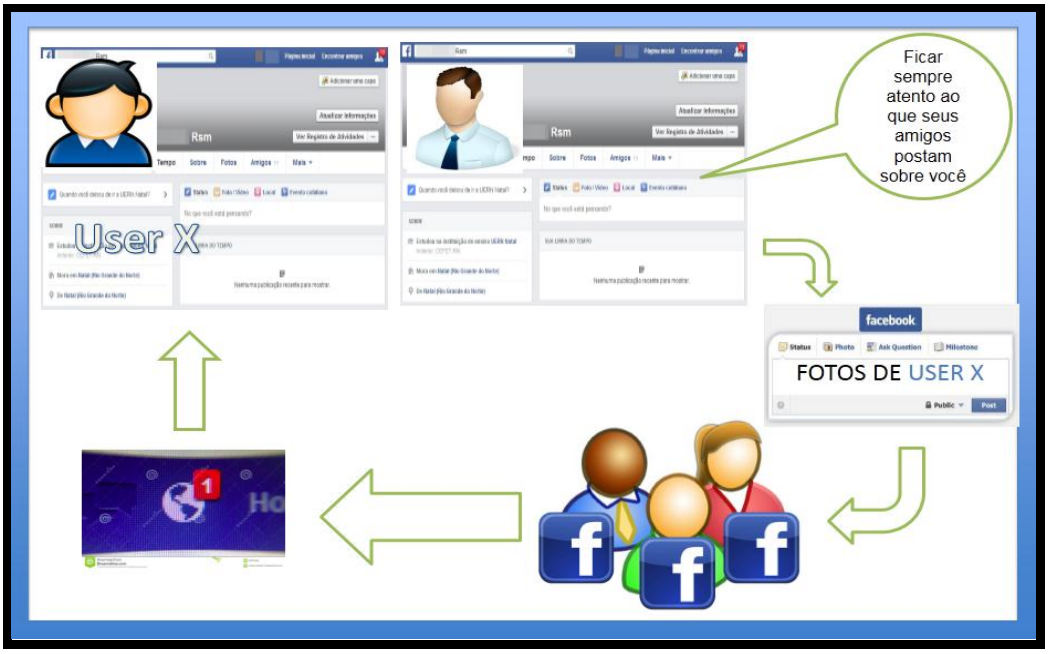
DICA 6: O usuário deve manter o seu perfil fechado e permita que somente seus amigos possam ver o seu perfil. Você também pode especificar a privacidade de uma mensagem ou publicação específica e controlar quantas informações compartilha com aplicativos (como jogos e testes).

Figura 35: Dica 6

.

DICA 7: O usuário deve estar ciente do que seus amigos postam sobre você, ou respondem as suas mensagens, especialmente sobre os seus dados pessoais e atividades.

Figura 36: Dica 7



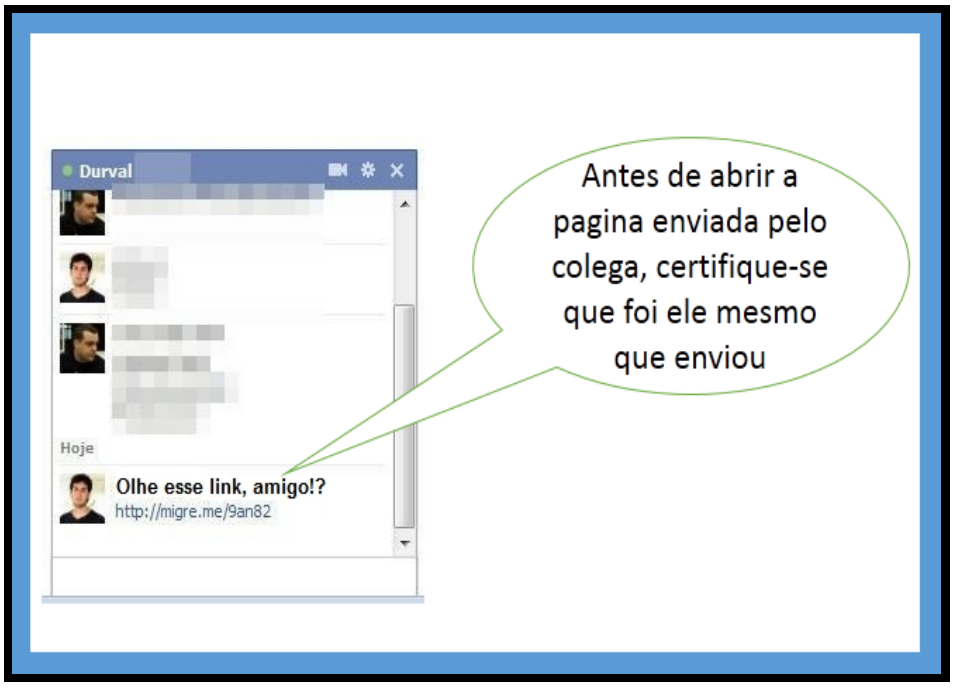
DICA 8: O usuário deve assegura-se que possui um antivírus eficaz e atualizado antes de ficar on-line, bem como atenção a solicitações de amigos falsos e mensagens de pessoas físicas ou empresas, convidando-o a visitar outras páginas ou sites.

Figura 37: Dica 8

.

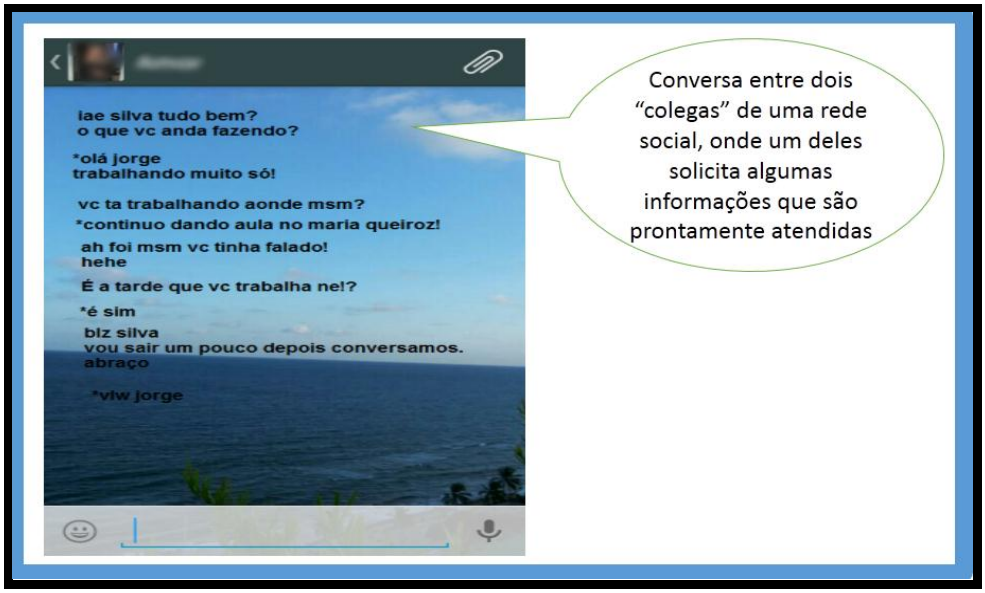
DICA 9: O usuário nunca deve clicar em *links* que recebe através de mensagens instantâneas de pessoas que você não conhece e confia, e que você nunca se encontrou na vida real.

Figura 38: Dica 9



DICA 10: O usuário deve ter muito cuidado com a divulgação de qualquer informação confidencial a um estranho que você encontra através de mensagens instantâneas. Mesmo informação aparentemente inocente, como o nome do seu empregador, pode ser usado contra você por fraudadores.

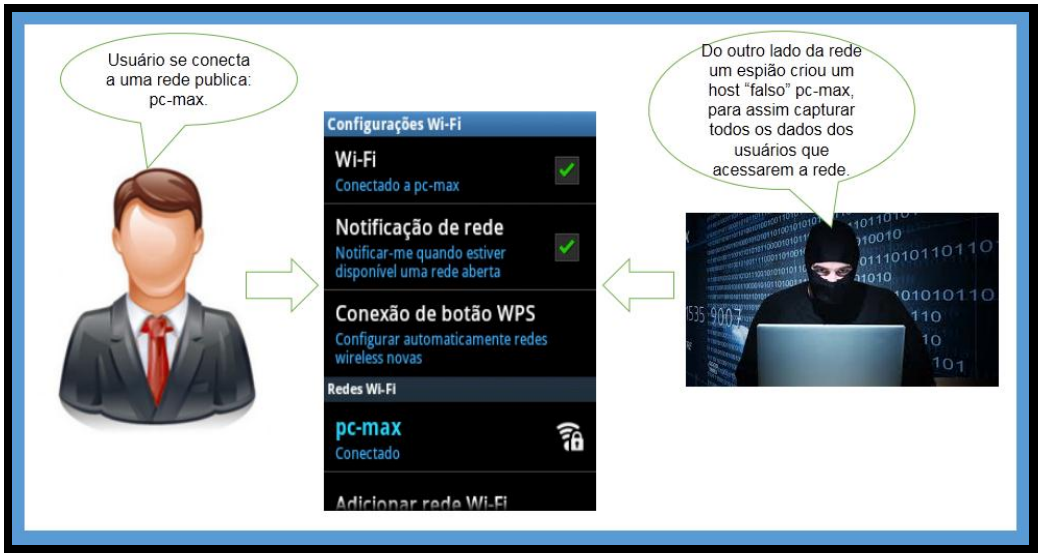
Figura 39: Dica 10



.

DICA 11: O usuário deve evitar entrar em redes Wi-Fi e *hotspots* desconhecidos em redes Wi-Fi públicas. Os atacantes podem criar falsas *hotspots* Wi-Fi projetados para atacar telefones celulares e pode monitorar as redes Wi-Fi públicas para dispositivos inseguros e assim roubar informações dos usuários.

Figura 40: Dica 11



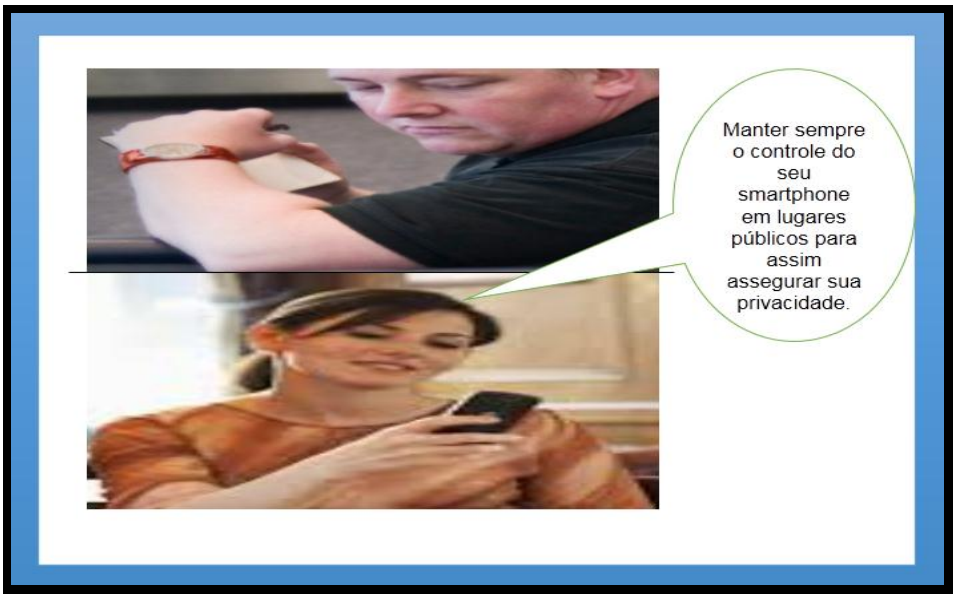
DICA 12: O usuário não deve enviar senhas ou informações de cartão de crédito. Os criminosos que utilizam a rede sem fio pode roubá-los. Se você precisar fazer transações sensíveis, use apenas sites seguros. Olhe para o endereço da Web para https:// em vez de http:// e procurar um cadeado bloqueado.

Figura 41: Dica 12

.

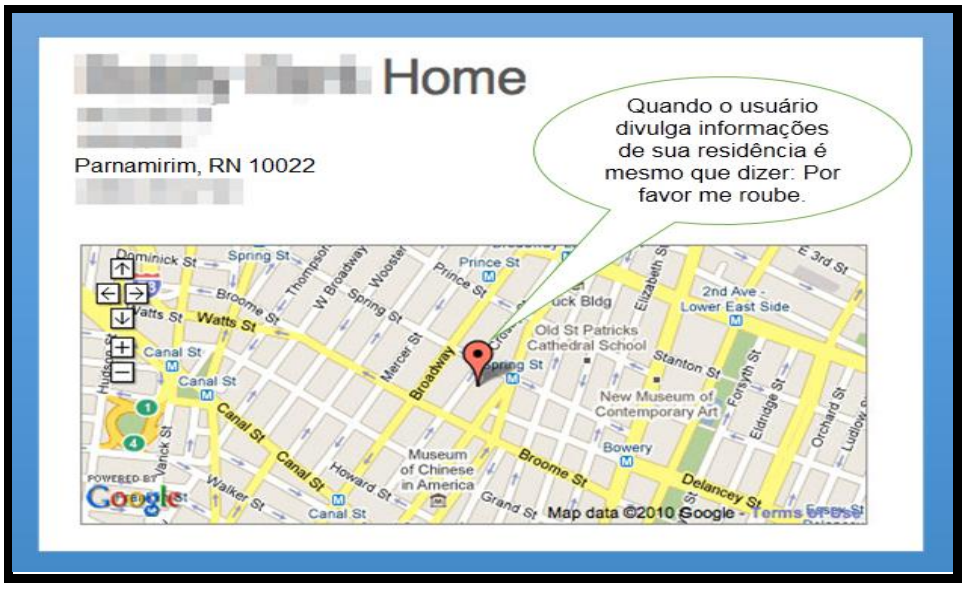
DICA 13: O usuário deve sempre manter o controle físico do dispositivo, especialmente em lugares públicos.

Figura 42: Dica 13



DICA 14: O usuário nunca deve divulgar os planos de férias, especialmente as datas em que vai realizá-la. Os assaltantes podem usar essas informações para roubar a sua casa enquanto você estiver fora da cidade.

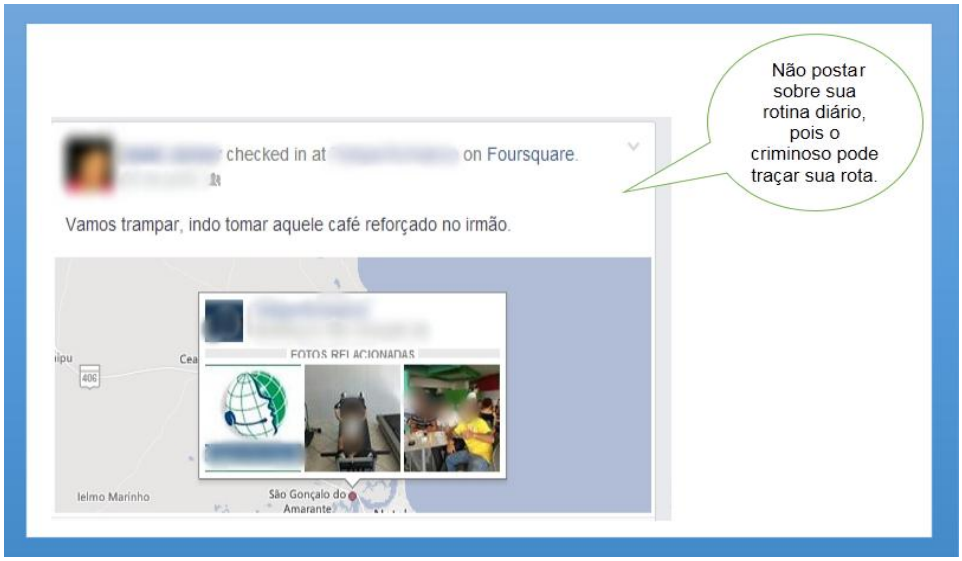
Figura 43: Dica 14



.

DICA 15: Se o usuário usa uma rede social de reconhecimento de local, não tornar público onde sua casa é porque as pessoas vão saber quando você não está lá. Na verdade, você deve ter cuidado ao postar qualquer tipo de local porque os criminosos podem usá-lo para secretamente rastrear sua localização. Pela mesma razão, ter cuidado para não compartilhar sua rotina diária. Postando o caminhando para seu trabalho, para onde você vai no seu intervalo do almoço, ou quando você vai voltar para casa é arriscado, pois pode permitir que um criminoso possa rastreá-lo.

Figura 44: Dica 15



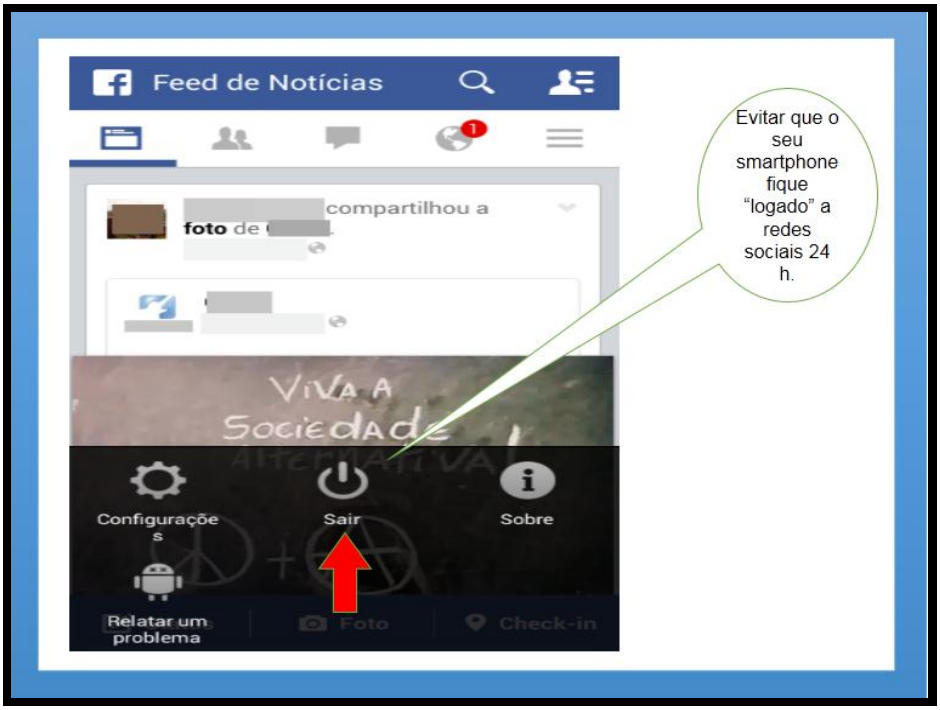
DICA 16: Se o usuário receber uma solicitação para se conectar com alguém e reconhecer o nome, verificar a identidade do titular da conta antes de aceitar o pedido. Considere chamando-o individualmente, isto é, envie um e-mail para a sua conta pessoal ou até mesmo fazer uma pergunta na qual apenas o seu contato seria capaz de responder.

Figura 45: Dica 16

.

DICA 17: O usuário sempre deve certificar-se de fazer logoff de sites de redes sociais quando já não houver necessidade de estar conectado. Isto pode reduzir a quantidade de rastreamento de sua navegação na web e ajudará a evitar a infiltração de estranhos a sua conta.

Figura 46: Dica 17



Portanto, lembre-se que nada do que você posta on-line é temporário. Qualquer coisa que você postar pode ser armazenado em cache, copiados e essa informações podem ser usadas a qualquer momento.

.

6 CONCLUSÃO

Neste trabalho, foi proposto um guia de segurança para que os usuários de Redes Sociais Móveis possam interagir nos mais diversos ambientes sociais com segurança, garantindo também maior privacidade dos seus dados compartilhados nessas Redes Sociais. Esse guia foi embasado nos principais tipos de ataques, como funcionam e como evitá-los.

Além do embasamento teórico, as técnicas utilizadas para compor o guia de segurança foram escolhidas a partir de avaliações realizadas no decorrer desta pesquisa. Objetivou-se que elas fossem as mais simples possíveis para a obtenção de um desempenho satisfatório do guia de segurança. Esse objetivo foi alcançado através da utilização da ferramenta *Wireshark* e da análise da engenharia social.

Com este trabalho, foi possível conhecer as diversas ferramentas de cunho preventivo no que tange a roubo de informações, e também constatar a lacuna existente no que concerne à pratica da engenharia social. Conclui-se então que o guia de segurança, proposto para diminuir essa lacuna, cumpre bem o seu papel e apresenta resultados satisfatórios.

Como trabalhos futuros, para aprimoramento do guia de segurança, cogita-se utilizar outras ferramentas bem como investigar o surgimento de outras redes sociais móveis.

.

REFERÊNCIAS BIBLIOGRÁFICAS

ABBOTT, Jonathon et al. Automated recognition of event scenarios for digital forensics. In: **Proceedings of the 2006 ACM symposium on Applied Computing**. ACM, 2006. p. 293-300.

AIME, Marco Domenico; CALANDRIELLO, Giorgio; LIOY, Antonio. Dependability in wireless networks: can we rely on WiFi?. **Security & Privacy, IEEE**, v. 5, n. 1, p. 23-29, 2007.

ATSUYA, Yuki; AYED, Souheil Ben; TERAOKA, Fumio. Network access authentication infrastructure using EAP-TTLS on diameter EAP application. In: **Proceedings of the 7th Asian Internet Engineering Conference**. ACM, 2011. p. 56-63.

BEACH, Aaron et al. Whozthat? evolving an ecosystem for context-aware mobile social networks. **Network, IEEE**, v. 22, n. 4, p. 50-55, 2008.

BENEVENUTO, Fabrıcio et al. Detecting spammers on twitter. In: **Collaboration, electronic messaging, anti-abuse and spam conference (CEAS)**. v. 6, 2010.

BENTON, Kevin; JO, Juyeon; KIM, Yoohwan. SignatureCheck: a protocol to detect man-in-the-middle attack in SSL. In: **Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research**. ACM, 2011. p. 60.

BEZERRA, Jéssica Mayza. Compartilhamento de informações no Facebook: o caso das citações atribuídas a Jean Wyllys. 2013.

BOSE, Abhijit; SHIN, Kang G. On mobile viruses exploiting messaging and bluetooth services. In: **Securecomm and Workshops, 2006**. IEEE, 2006. p. 1-10.

CHA, Meeyoung et al. Medindo Influência usuário no Twitter:. The Million Follower Falácia **ICWSM** , v.10, p. 10-17, 2010.

CHEN, Jyh-Cheng; WANG, Yu-Ping. Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience. **IEEE Communications Magazine**, v. 43, n. 12, p. 26-32, 2005.

CHOI, Min-kyu et al. Wireless network security: Vulnerabilities, threats and countermeasures. **International journal of Multimedia and Ubiquitous Engineering**, v. 3, n. 3, 2008.

CHOI, Min-kyu et al. Wireless network security: Vulnerabilities, threats and countermeasures. **International journal of Multimedia and Ubiquitous Engineering**, v. 3, n. 3, 2012.

COOLE, Michael; WOODWARD, Andrew; VALLI, Craig. Understanding the Vulnerabilities in Wi-Fi and the Impact on its Use in CCTV Systems. 2012.

DATTA, Anwitaman et al. Decentralized online social networks. In: **Handbook of Social Network Technologies and Applications**. Springer US, 2010. p. 349-378.

.

SOOD, Meenakshi; DAVID, L; KAJLA, Mahesh Kumar. Router based approach to mitigate DOS attacks on the wireless networks. In: **Proceedings of the 2011 International Conference on Communication, Computing & Security**. ACM, 2011. p. 569-572.

DEY, Anind K. et al. The context toolkit: Aiding the development of context-aware applications. In: **Workshop on Software Engineering for wearable and pervasive computing**. 2000. p. 431-441.

DORES, Wellington et al. Uma abordagem descentralizada para encurtamento de URLs. **Revista de Iniciação Científica**, v. 12, n. 3, 2013.

DOS SANTOS, Daniel Bruno Alves. Infraestrutura para o Desenvolvimento de Aplicações Pervasivas Cientes de Redes Sociais. Dissertação de mestrado. UFCG. Centro de Engenharia Elétrica e Informática. 2011.

DUNHAM, Ken. **Mobile malware attacks and defense**. Syngress. Local: editora, 2008. Disponível em

FAN, Chun-I.; LIN, Yi-Hui; HSU, Ruei-Hau. Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs. **Parallel and Distributed Systems, IEEE Transactions on**, v. 24, n. 4, p. 672-680, 2013.

GEORGIEV, Martin et al. The most dangerous code in the world: validating SSL certificates in non-browser software. In: **Proceedings of the 2012 ACM conference on Computer and communications security**. ACM, 2012. p. 38-49.

HAGER, Creighton T.; MIDKIFF, Scott F. An analysis of Bluetooth security vulnerabilities. In: **Wireless Communications and Networking, 2003. WCNC 2003. IEEE**. IEEE, 2003. p. 1825-1831.

HAGER, Creighton T.; MIDKIFF, Scott F. Demonstrating vulnerabilities in Bluetooth security. In: **Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE**. IEEE, 2003. p. 1420-1424.

HANNE, Michelle et al. Analysis of vulnerability to facebook users. In: **Proceedings of the 18th Brazilian symposium on Multimedia and the web**. ACM, 2012. p. 335-342.

HOUSLEY, Russ; ARBAUGH, William. Security problems in 802.11-based networks. **Communications of the ACM**, v. 46, n. 5, p. 31-34, 2003.

IBEKWE, Ikechukwu; ALJAREH, Salem. SMS Security: Highlighting Its Vulnerabilities & Techniques Towards Developing a Solution, 2012.

JABEUR, Nafaâ; ZEADALLY, Sherali; SAYED, Biju. Mobile social networking applications. **Communications of the ACM**, v. 56, n. 3, p. 71-79, 2013.

KAYASTHA, Nipendra et al. Applications, architectures, and protocol design issues for mobile social networks: A survey. **Proceedings of the IEEE**, v. 99, n. 12, p. 2130-2158, 2011.

.

KLASSEN, Myungsook. Twitter de dados de pré-processamento para detecção de spam. In: **COMPUTING FUTURO 2013, a Quinta Conferência Internacional sobre Tecnologias Futuras Computacional e Aplicações.** P. 56-61.

DHANANJAY M.Dakhane; KSHITIJ R.Mawale1; RAVINDRA L.Pardhi. Authentication Methods for Wi-Fi Networks. v.2, 2013

KWAK, Haewoon et al. What is Twitter, a social network or a news media?. In: **Proceedings of the 19th international conference on World wide web**. ACM, 2010. p. 591-600.

LASHKARI, Arash Habibi; TOWHIDI, Farnaz; HOSSEINI, Raheleh Sadat. Wired Equivalent Privacy (WEP). In: **Future Computer and Communication, 2009. ICFCC 2009. International Conference on**. IEEE, 2009. p. 492-495.

LEAVITT, Neal. Mobile security: Finally a serious problem?. **Computer**, v. 44, n. 6, p. 11-14, 2011.

LOUREIRO, Antonio Alfredo Ferreira et al. Computação Ubíqua Ciente de Contexto: Desafios e Tendências. **Anais do XXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SRBC 09)**, 2009 (91641007).

MITCHELL, John C; CHANGHUA He. Security Analysis and Improvements for IEEE 802.11 i. In: **The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University, Stanford**. 2005. p. 90-110.

MULLINER, Collin; VIGNA, Giovanni. Vulnerability analysis of mms user agents. In: **Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual**. IEEE, 2006. p. 77-88.

PELECHRINIS, Konstantinos; ILIOFOTOU, Marios; KRISHNAMURTHY, Srikanth V. Denial of service attacks in wireless networks: The case of jammers. **Communications Surveys & Tutorials, IEEE**, v. 13, n. 2, p. 245-257, 2011.

PIETILÄINEN, Anna-Kaisa et al. MobiClique: middleware for mobile social networking. In: **Proceedings of the 2nd ACM workshop on Online social networks**. ACM, 2009. p.49-54.

PIETILÄINEN, Anna-Kaisa. **Opportunistic Mobile Social Networks at Work**. 2010. Tese de Doutorado. Ph. D. Thesis, Université Pierre et Marie Curie, Paris.

POSEY, Brien. **GFI network security and PCI compliance power tools**. Elsevier, 2011.

QADEER, Mohammed Abdul et al. Network traffic analysis and intrusion detection using packet sniffer. In: **Communication Software and Networks, 2010. ICCSN'10. Second International Conference on**. IEEE, 2010. p. 313-317.

SHARMA, Rajesh; DATTA, Anwitaman. Supernova: Super-peers based architecture for decentralized online social networks. In: **Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on**. IEEE, 2012. p. 1-10.

.

SINGH, Mr Harjit; SINGH, Er Gurpinder. Wireless Networking Security (—Secured-Nim‖: Blocking Misbehaving Users In Anonymizing Networks‖). **International Journal**, v. 3, n. 5, 2013.

SUGA, Yuji. SSL/TLS Status Survey in Japan-Transitioning against the Renegotiation Vulnerability and Short RSA Key Length Problem. In: **Information Security (Asia JCIS) Seventh Asia Joint Conference on**. IEEE, 2012. p. 17-24.

TARIQ, Muhammad Imran. WIRELESS SECURITY AND THREATS. **Islamic Countries Society of Statistical Sciences**. v. 21, p. 717-729, 2011.

WELCH, Donald; LATHROP, Scott. Wireless security threat taxonomy. In: **Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society**. IEEE, 2003. p. 76-83.

XING, Xinyu et al. Security analysis and authentication improvement for IEEE 802.11i specification. In: **Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE**. IEEE, 2008. p. 1-5.

YANG, Fan; ZHU, Ping. An EAP_TTLS_SPEKEY Method for Single EAP_Based Auth Mode of IEEE 802.16 e PKMv2. In: **2010 International Conference on Computational Intelligence and Software Engineering**. 2010. p. 1-4.

YUAN, Xiaohong et al. Visualization tools for teaching computer security. **ACM Transactions on Computing Education (TOCE)**, v. 9, n. 4, p. 20, 2010.

ZANERO, Stefano; MERLONI, Claudio; CARETTONI, Luca. Studying bluetooth malware propagation: The bluebag project. **IEEE Security & Privacy**, v. 5, n. 2, p. 0017-25, 2007.

ZHENG, Xinliang et al. A dual authentication protocol for IEEE 802.11 wireless LANs. In: **Wireless Communication Systems, 2005. 2nd International Symposium on**. IEEE, 2005. p. 565-569.

.