Estudo de segurança em dispositivos móveis

Jamilson Bine[1], **Josiel Neumann Kuk**[1]

[1]Departamento de Ciência da Computação
Universidade Estadual do Centro-Oeste (UNICENTRO)
Caixa Postal 3010 – 85040-080 – Guarapuava – PR – Brasil

jamil_bn@hotmail.com, josiel@unicentro.br

Abstract. *Mobile devices are evolving rapidly and became popular. The new devices have various types of connections and an intense exchange of data. To protecting the data from mobile devices, some techniques are used. Through research, this paper will present some of these techniques, and also will address some forms used by attackers to information theft. The end will be described an analysis about the panorama of security on mobile devices.*

Resumo. *Dispositivos móveis estão evoluindo rapidamente e se tornaram populares. Os novos aparelhos possuem diversos tipos de conexões e uma troca de dados intensa. Para defender os dados dos dispositivos móveis, algumas técnicas são utilizadas. Por meio de pesquisas realizadas, este trabalho apresentará algumas dessas técnicas, e também abordará algumas formas utilizadas pelos invasores para roubo de informação. Ao final será descrita uma análise sobre o panorama da segurança em dispositivos móveis.*

1. Introdução

A segurança da informação é um tema frequente no meio da computação, sendo que a cada ano a tecnologia evolui as formas de acessar aos dados que deseja. E em contrapartida os invasores buscam formas de interceptar tais dados de diferentes maneiras. Aparelhos como *smartphones*, *tablets*, *Personal Digital Assistant* (PDA), entre outros que possuem ações similares à de computadores, se tornam alvos mais constantes de ataques. A partir do século XX aconteceu essa grande transformação, e muito se deve aos desenvolvimentos das Tecnologias da Informação e da Comunicação (TIC) e em particular da *Internet* [Tomaél e De Jesus 2010].

Esses alvos estão sendo mais visados pelo motivo de terem se tornado tão populares nos últimos anos, onde a utilização desses dispositivos cresceram consideravelmente. Pequenos aparelhos possuem inúmeras informações pessoais, as quais são muito valiosas. Atualmente temos um número elevadíssimo de atividades realizadas via dispositivos móveis, tais como: conversação, troca de mensagens, acesso a *home banking*, acesso a sistemas privativos, etc. Nesses contextos é de extrema importância manter a segurança. Desenvolvedores e fabricantes buscam sempre aumentar a segurança e confiabilidade em manter as informações de seus usuários. Existem vários meios utilizados para esses fins, sendo um dos principais a criptografia. Essa técnica funciona em uma gama de casos mais gerais [Forouzan 2013].

O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos [Soares et al. 1995]. Com esse intuito a comu-

nidade tecnológica procura sempre evoluir mais rapidamente, prevendo possíveis falhas à proteção das informações pessoais.

Diante do alto consumo desses dispositivos, as empresas de diversos ramos já fazem parte de um negócio crescente na área, que são aplicativos voltados para vendas, serviços especializados e até mesmo negócios de alta relevância [Monteverde e Campiolo 2014]. Os bancos também passaram a investir nesse ramo. Um exemplo disso são as ações bancárias, onde são possíveis de serem realizadas com poucos toques na tela de um *smartphone*. Porém essa troca de informações do usuário e banco estão sujeitas a ataques, o que ocasionaria uma falha prejudicial ao cliente. As transmissões de informações possuem sistemas de segurança em redes sem fio, porém nem sempre é possível prever que serão eficazes contra as ameaças em dispositivos móveis. Esse é um dos exemplos de vulnerabilidades contidas em um aparelho, que são na forma lógica e física.

Através da disseminação dos dispositivos móveis, surgiu o movimento *Bring Your Own Device* (BYOD), que consiste em utilizar o dispositivo pessoal no local de trabalho. Tal ação trouxe praticidade e até mesmo mais agilidade na troca de informações internamente, mas a preocupação com a segurança da informação aumentou para os profissionais da área. Dados internos de empresas podem ser transferidos rapidamente para os dispositivos, mas assim como os computadores, eles também são suscetíveis a infecções de vírus, *spywares* e roubos de informações.

O foco dessa pesquisa será apontar por alguns meios e como são possíveis os roubos das informações pessoais em dispositivos móveis. O tema segurança está em diversos debates atuais da computação, e o principal motivo disso são devido às vulnerabilidades que se encontram nas novas tecnologias. Como trabalhos e materiais correlatos a esse tema normalmente são encontrados em sites de empresas de segurança, a abordagem aqui é mais genérica em termos de sistema operacional, tentando englobar assuntos que sejam tratados pelos sistemas estudados, diferentemente de outros artigos científicos os quais em sua maioria tratam especificamente de um único sistema operacional.

O restante do artigo está organizado da seguinte maneira: a Seção 2 trata dos dispositos móveis; sistemas operacionais para dispositivos móveis são discutidos na Seção 3; na Seção 4 é descrito a segurança da informação; exemplos de ataque e defesa em dispositivos móveis são apresentados na Seção 5; resultados e discussões estão na Seção 6 e na Seção 7 são apresentadas as conclusões finais e trabalhos futuros.

2. Dispositivos Móveis

A ideia da criação de um aparelho pelo qual o usuário pudesse se comunicar através de diferentes locais teve início em 1947, mas a grande dificuldade encontrada era o limite tecnológico da época [Nicolai et al. 2012]. Por isso, a ideia apenas se tornou um conceito, não tendo continuidade nesse projeto. Em 1973 ocorreu a primeira experiência de uma ligação entre um dispositivo móvel e um telefone fixo, e para que ele acontecesse foram utilizadas as teorias já criadas em 1947 [Morimoto 2009].

A *Motorola* se tornou a fabricante mais evidente a partir disso, realizando as primeiras fabricações, e em 1983 passou a vender o primeiro modelo, chamado de *DynaTAC* 8000x, porém não obteve sucesso entre os consumidores devido ao alto valor de mercado.

Com esse invento sendo tão inovador para a época, foi possível atingir os objetivos de tornar possível a comunicação em diferentes locais, não apenas no meio doméstico ou de trabalho. Mas logo se percebeu que poderia deixar o aparelho mais agradável e muito mais versátil, e para que isso acontecesse foi necessária uma evolução do *hardware* e *software*. E assim os modelos já continham uma pequena memória interna para armazenamento de contatos, calculadoras, era possível já identificar de quem estava recebendo alguma chamada, troca de mensagens de texto, entre algumas outras funções. Alguns anos depois do acesso a *Internet*, já se tinham telas coloridas, com câmera fotográfica e com reproduções de músicas.

Os aparelhos nos quais são possíveis instalar e desinstalar aplicativos, são miniaturizados e que possuem um processamento até mesmo maior que alguns computadores, pertencem à categoria de *smartphone* [Morimoto 2009]. É possível dizer que essa nova categoria surgiu junto com os *handhelds* e *palmtops*, os quais fizeram muito sucesso nos anos 90. Alguns deles conseguiam até rodar o *Microsoft Disc Operating System* (MS-DOS) e certos modelos ofereciam a oportunidade da instalação de alguns programas de computador.

O termo mobilidade envolve os principais aparelhos em alta no mercado mundial. E esse conceito engloba aqueles sistemas que podem facilmente ser carregados fisicamente ou que possuem o poder de continuar operando enquanto se encontra em movimento. Existem características próprias para que algum aparelho possa estar classificado como móvel, entre as principais delas se encontram: o tamanho reduzido, o baixo consumo de energia, a memória e o processamento de dados, e o monitoramento do nível de energia para a prevenção da perda de dados [Morimoto 2009].

Para ser considerado um dispositivo móvel, tal aparelho tem que possuir o poder de realizar tarefas que são facilmente executadas por meio de texto, áudio, vídeo e Internet, e ter características próprias que o distingue de outros meios: ser pessoal; receber informações a todo o momento; ser levada pelo seu usuário a qualquer lugar; ter canais de pagamento já integrados; e estar presente nos momentos de impulso criativo [Fling 2009].

A transmissão em seus primeiros modelos era por meio de um sistema analógico de transferência de voz. Depois disso surgiram outros meios digitais, como *Code Division Multiple Access* (CDMA), *Global System for Mobile Communications* (GSM) na qual teve a *2nd Generation* (2G), *3rd Generation* (3G) e *4th Generation* (4G), entre todos esses modelos, o 4G é o mais utilizado para os aparelhos mais novos do mercado.

Por meio desses dispositivos busca-se proporcionar que seus usuários possuam um rápido acesso às informações desejadas diante de qualquer lugar. Assim a importância da computação móvel se tornou mais reconhecida, chegando ao patamar de ser considerada a quarta revolução na computação [Mateus e Loureiro 1998].

O desejo de estar sempre conectado ao mundo digital torna a mobilidade muito mais presente na vida pessoal, e como consequência fornece maneiras mais eficazes de se trabalhar. Em 2011 houve um crescimento de 100% no uso de *Internet* móvel e, especificamente no Brasil, em maio de 2012 já havia 14% da população com acesso à *smartphone* [Andrade et al. 2013].

Essa área atrai cada vez mais executivos devido ao seu crescimento acentuado, mostrando que há muitas chances de lucros com aplicações móveis. Uma pes-

quisa realizada pela Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, apresenta que entre os executivos entrevistados em 14 países, 77% deles consideram que a mobilidade é uma das 5 principais prioridades para o seu negócio, e com isso sobe o número daqueles que recuperam 100% do investimento realizado [Brasscom 2014]. Assim o termo "Negócios Móveis" é mais frequente em meio à tecnologia, também conhecido como *Mobile Business* (*M-Business*) [Fenn e Linden 2001].

3. Sistemas Operacionais

Conforme as tecnologias foram ganhando um maior poder computacional, diferentes formatos e se tornando mais leves, se exigiu sistemas que pudessem tirar o máximo de proveito das suas capacidades de processamento.

Um sistema operacional deve gerenciar o *hardware* e *software* do aparelho por meio de um conjunto de programas, e proporcionar uma interface com o usuário [Silberschatz et al. 2004]. Então, algumas empresas já renomadas no ramo tecnológico, passaram a desenvolver plataformas com a finalidade de atender às demandas dos dispositivos móveis. Sendo assim atualmente existem três delas que se destacam tanto no mercado brasileiro como nos demais países. Isso se comprova na Figura 1, gerada a partir de dados de maio de 2014 [De Almeida et al. 2014].

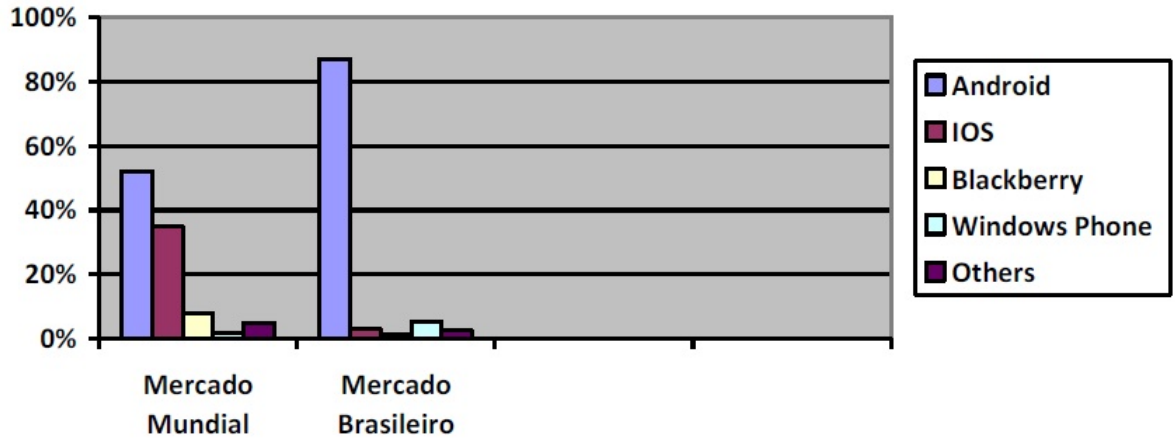

Figura 1. Principais sistemas operacionais no mercado brasileiro e mundial, em 2014 [De Almeida et al. 2014].

O sistema operacional *Android*, que é baseado em *Linux*, lidera tanto no mercado brasileiro como demais países, muito em função da sua facilidade de uso e por estar presente na maior parte dos novos aparelhos por meio de preços mais acessíveis [De Almeida et al. 2014].

Cada um dos SOs é composto de características próprias, fazendo com que a grande parte dos aplicativos devam ser projetados exclusivamente para a plataforma pretendida. A seguir os sistemas operacionais mais relevantes em ambos os mercados são abordados.

3.1. Android

Por meio de quatro sócios se deu início ao projeto de criação do sistema *Android*, pela *Android Inc*, localizada em Palo Alto, Califórnia, EUA [Nicolai et al. 2012]. E foi em 2006

que a *Google* adquiriu os direitos da empresa, e com isso passou a dar mais importância à continuidade do projeto, dando ênfase para que o mesmo se tornasse um sistema operacional *open-source* para dispositivos móveis.

Dessa forma se chegou ao sistema que hoje está em grande parte dos aparelhos do mercado mundial, como é possível se perceber na Figura 1. Após a continuação do projeto, a *Google* resolveu passar o desenvolvimento e manutenção para o grupo *Open Handset Alliance* (OHA) [Scota et al. 2010].

O grupo OHA é composto por mais de 40 empresas, de diferentes ramos tecnológicos, como semicondutores, telefonia, fabricante de celulares, entre outros ramos afins [Gonçalves 2011].

A Figura 2 representa a arquitetura do sistema disponibilizada pelos desenvolvedores [Android 2015]. Por meio dessa representação, os desenvolvedores pretendem proporcionar um maior conhecimento sobre o *Android Open Source Project* (AOSP), a aqueles que desejam contribuir com o avanço do projeto.

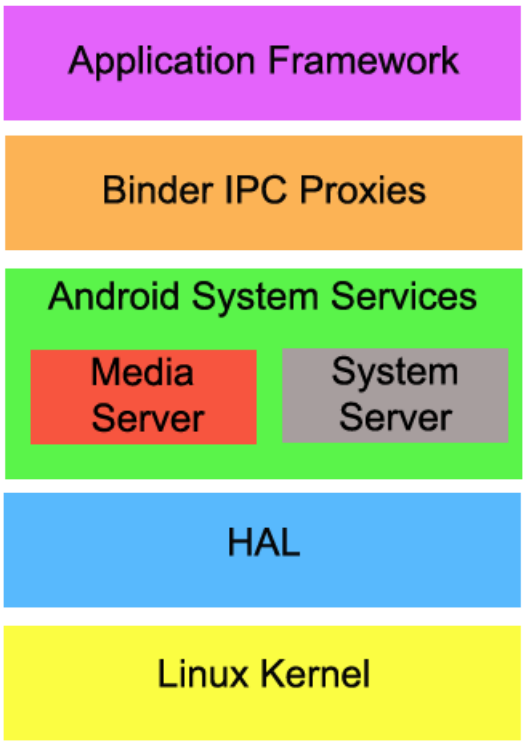

Figura 2. Arquitetura do Sistema *Android*.

- *Application Framework*: essa é a camada em que os mais interessados serão os desenvolvedores de aplicativos, principalmente quando for necessário criar *drivers* como ligação do aplicativo com o *hardware*.
- *Binder IPC Proxies*: esta camada serve basicamente para fazer chamadas aos serviços do sistema quando forem solicitados pelo aplicativo, onde o desenvolvedor tem pouco envolvimento com o processo que isso se dá.

- *Android System Services*: a *Application Programming Interface* (API) faz o acesso ao *hardware* por meio dos serviços do sistema, com a finalidade de utilizar as funções de dois grupos específicos: mídia ou sistema.
- *Hardware abstraction layer* (HAL): o sistema utiliza essa camada para que aplicações desenvolvidas em mais baixo nível possam acessar certos *drivers* do aparelho. Então dessa forma o desenvolvedor que fizer uso desses acessos, deverá projetar a aplicação especificamente para o aparelho que desejar, fazendo com que o *Android* siga as definições feitas geralmente em forma de bibliotecas.
- *Linux Kernel*: nessa camada se encontra o núcleo do *Android*, como o *kernel* e uma versão baseada do próprio sistema *Linux*, nada difere no desenvolvimento dos *drivers*. Contém alguns recursos a mais, para que o sistema seja mais eficaz quanto à versão móvel.

3.2. iOS

O seu surgimento se deu a partir da intenção que a *Apple* tinha de desenvolver um sistema operacional para uma das suas criações mais inovadoras, o *smartphone iPhone*. Ele se destacou principalmente por executar tarefas de maneira eficiente, algo que outras empresas tentaram fazer porém não conseguiram êxito [Querino Filho 2013]. Rapidamente a *Apple* percebeu que esse SO poderia ser utilizado em outras tecnologias, e assim deixou de ser uma exclusividade do *iPhone* para ser o sistema principal dos *iPods*, *iPads* e até mesmo da *Apple TV* [Milani 2012].

O *iPhone* foi lançado em 29 de junho de 2007, e Steve Jobs, até então o presidente-executivo da *Apple* [Isaacson 2011], deixou claro que o sistema operacional do dispositivo foi baseado no *Mac OS X*, e sem possuir um nome até o seu lançamento foi logo rotulado como *iPhone Operating System* (iOS) [Garcia 2013].

A arquitetura do sistema é representada pela Figura 3, a qual é apresentada pela própria *Apple* [Apple 2015]. Ela é composta por 4 camadas e são descritas da seguinte forma [Garcia 2013]:

- *Cocoa Touch*: responsável pela interação do aparelho com o usuário, sendo a camada de mais alto nível dessa arquitetura. A partir da API fornecida aos desenvolvedores são criadas as tarefas de comunicação com arquivos, multitoque e os meios de interações;
- *Media*: como seu nome já sugere, essa camada trabalha com medias em geral, como animações, vídeos e áudios, e tecnologias que são utilizadas em jogos, como *OpenGL for Embedded Systems* (*OpenGL* ES) e *Quartz*.
- *Core Services*: certos serviços do SO são gerenciados por essa camada, é onde o programador pode ter acessos aos principais serviços, um dos mais claros exemplos é a manipulação de arquivos e também ao *SQLite*.
- *Core OS*: essa camada é a de mais baixo nível entre todas e também considerada o núcleo do sistema todo, e nela que se tratam questões como segurança e como se faz a comunicação do SO. Além disso, faz o gerenciamento de fatores como *sockets*, os certificados, gerenciamento de energia e entre outros.

3.3. Windows Phone

Entre os três principais sistemas, esse foi o último a ser lançado, a *Microsoft* o anunciou oficialmente em 21 de outubro de 2010 [Nunes 2014]. A fama obtida pela *Microsoft* nos

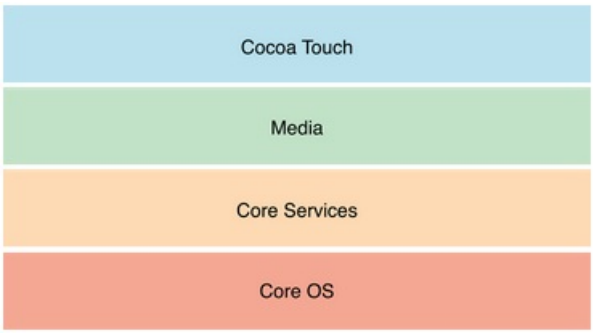

Figura 3. Arquitetura do iOS [Apple 2015].

anos 90 era graças ao sistema que tomou conta de grande parte dos computadores, assim tentaram obter o mesmo sucesso em meio aos celulares e novos dispositivos que vinham se destacando [Mônaco e Do Carmo 2012].

A primeira tentativa da empresa entrar no mercado de dispositivos móveis foram os *Pockets Personal Computers*. No início obtiveram uma grande aceitação dos usuários, mas devido à complicações do aparelho isso mudou rapidamente. O sistema pouco intuitivo e recursos do aparelho foram alguns dos fatores para esse acontecimento [Mônaco e Do Carmo 2012].

Após fracassos na área móvel, perceberam que deveriam mudar sua estratégia para conseguir competir com a *Apple* e a *Google*. Com isso surgiu o *Windows Phone*, esse sistema de nada parecia ou era uma modificação do sistema que era utilizado antes, conhecido como *Windows Mobile*. Alguns dos principais pontos do novo e mais moderno sistema operacional móvel da *Microsoft* são [Nunes 2014]:

1. Uma padronização do *hardware* com os fabricantes;
2. O desejo do usuário se tornou um dos focos do sistema;
3. Foi criada uma área específica para interação do usuário com suas experiências sociais, conhecida como *Hub*.

A Figura 4 apresenta a arquitetura da versão mais atual do sistema, *Windows Phone* 8.1, e conforme descrito em *Windows Phone architecture overview*, para o funcionamento efetivo do sistema aparece um pacote com bibliotecas e uma coleção de *drivers* chamada de *Board Support Package* (BSP) [Windows Phone 2015]. Essa BSP é construída pelo fabricante da *Central Processing Unit* (CPU), e tem a principal função de realizar a ligação entre o *hardware* e as inicializações dos *drivers* de baixo nível.

Demais *drivers* contidos na arquitetura são disponibilizados por dois grupos, um deles é o *Original Equipment Manufacturer* (OEM) que destinam seus *drivers* para suporte dos componentes do aparelho, e o outro grupo é formado por *Independent Hardware Vendor* (IHV) que produzem alguns componentes específicos para cada aparelho.

O SO e o *kernel* possuem uma personalização feita pela própria *Microsoft*. Acima do *kernel* ficam serviços com o objetivo de realizar a interação com o usuário do aparelho, contendo também as estruturas de programação dos aplicativos.

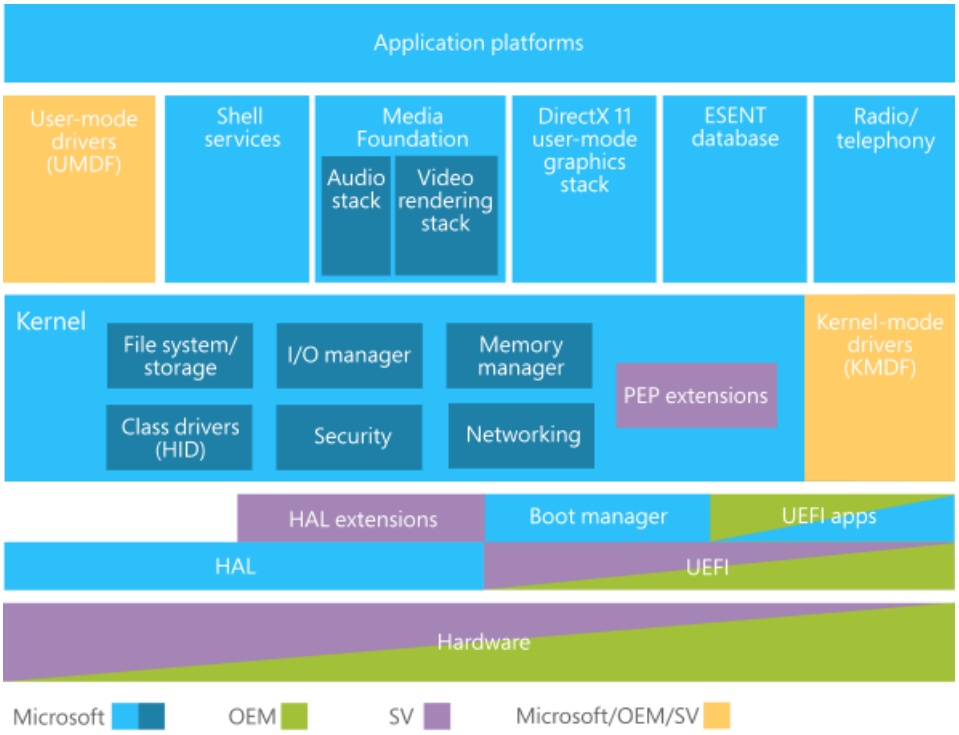

Figura 4. Arquitetura do *Windows Phone* 8.1 [Windows Phone 2015].

3.4. Outros

Além dos três principais sistemas do mercado citados anteriormente, existem outras opções de SOs. Alguns exemplos:

- *BlackBerry*: criado pela *Research in Motion*. Uma característica interessante sobre esse sistema é o serviço *Blackberry Messenger* (BBM), o qual faz a troca de mensagens em até 200 Kbps[1], por meio da tecnologia *Explicit Data Graph Execution* (EDGE) [Spadari 2015];
- *Firefox OS*: projeto realizado pela *Mozilla*. Uma das boas características é a rápida velocidade em apresentar as informações pretendidas pelo usuário. O objetivo inicial da empresa é implantar o sistema em *smartphones* de baixo custo [Mozilla 2015];
- *Silent OS*: a segurança é a principal característica, e é algo que vem atraindo mais usuários. Com diversos tipos de criptografias o sistema pretende garantir a segurança da informação [Blackphone 2015].

A próxima seção trata sobre a segurança da informação.

4. Segurança da Informação

A portabilidade obtida com diversos modelos de aparelhos móveis acarretou em uma maior satisfação ao usuário, porém consigo apareceram diversas vulnerabilidades em seus sistemas. As aplicações criadas para cada sistema cresceram muito com o avanço da área, e também se tornaram um dos principais meios de entrada para os invasores

[1]Kbps: *Kilobyte per second*, representa uma unidade de transmissão de dados.

[Batista et al. 2013]. Os problemas de segurança que se encontravam em computadores passaram a afetar também a área móvel.

Um grande fator que elevou o aumento do uso de dispositivos móveis, foi o crescimento do uso de redes sem fio (*Wireless*), pela sua fácil instalação e baixo custo de implementação [Caçador 2014]. A principal rede desse ramo é a *Wireless Fide-lity* (Wi-Fi), e ela segue as especificações do padrão *Institute of Electrical and Electronics Engineers* 802.11 (IEEE 802.11). Porém o uso delas diminuem a segurança do tráfego de informação, pois não é fisicamente possível garantir a preservação dos dados. Quando se utiliza uma *Local Area Network* (LAN) é possível restringir o acesso dos seus usuários, algo de extrema relevância no meio corporativo [Moretti e Bellezi 2014].

Com tamanha evolução que se teve na tecnologia da informação, as eficazes Centrais de Processamento de Dados (CPD) que se tinham no começo da disseminação computacional, onde todos os dados digitais de uma empresa ficavam concentrados, ficaram para trás e atualmente a questão de segurança é muito mais complexa. As informações não ficam armazenadas em apenas um local, pode se encontrar a mesma informação em diversos meios, como *pendrive*, *Compact Disc* (CD), *e-mail* e em variados dispositivos móveis [Gabbay 2006].

Alguns elementos que estão diretamente envolvidos na segurança da informação [Cerutti 2012]:

- Pessoas: as pessoas nesse esquema se tornam o pilar principal da segurança, pois elas que colocam em prática os processos contidos em uma organização. Elas devem conhecer sobre o quão importantes são para a segurança das informações da empresa e que sejam responsáveis pelos seus atos;
- Processos: os processos quando são bem produzidos, dividem a responsabilidade da segurança da informação, sendo que não ficará apenas para a equipe de segurança toda a culpa em caso de falhas. Por meio de métodos traçados, ou seja, a maneira correta de realizar certas ações, já se diminui o risco à segurança;
- Ferramentas: por último, são apresentadas as ferramentas, que nela constam os recursos físicos e lógicos relacionados à segurança, onde auxiliam os processos da empresa. Tendem a tornar mais fácil a implementação das políticas de segurança da informação. Entre elas se encontram várias funcionalidades, como criptografia, defesa contra ameaças, identificação do usuário e a gestão da segurança.

Com tantas evoluções nas tecnologias, a segurança se torna cada vez mais primordial para simples usuários, como para corporações de extrema relevância. Abaixo são apresentados cinco fatores relevantes para garantir a segurança de um sistema [Pinto e Gomes 2011] :

- Confidencialidade: esse princípio diz que certas informações não podem ser acessíveis às pessoas não autorizadas.
- Integridade: para que o sistema tenha esse princípio, ele deve garantir que não há informação com alterações intencionais ou propositalmente. A produção, o tráfego e armazenamento de informações da sociedade é enorme, tornando a integridade importante.
- Autenticidade: pessoas autorizadas são as únicas que devem ter o privilégio de criar ou enviar informações. Isso é seguido por meio de senhas para o sistema no qual se pretende utilizar.

- Disponibilidade: as informações devem estar acessíveis ao usuário sempre que ele desejar, de nada adiantaria os demais princípios serem seguidos, se o usuário não poder utilizar a informação quando lhe for útil.
- Não – repúdio ou irretratabilidade: se refere ao ato de alguém que está participando de um processo não poder negar a realização de uma comunicação ou transação efetuada pelo mesmo.

4.1. BYOD

A dependência que os dispositivos causaram em seus usuários, o fizeram indispensáveis em qualquer momento do dia. Até mesmo durante o trabalho diário, seu uso se tornou constante, desse modo surgiu a tendência conhecida como "*Bring Your Own Device*". Ela fez com que as corporações tornassem de grande valia essa dependência dos aparelhos, integrando-os com o dia a dia do trabalho, podendo fazer com que as informações necessárias de trabalho sejam mais acessíveis a qualquer momento.

Custos de *hardware* e de suporte foram reduzidos nas empresas, porém a insegurança na rede interna aumentou de forma significativa, pois basta um aparelho estar infectado por algum vírus para afetar a todos conectados na mesma rede. Além desse risco, há também a questão de se carregar dados da empresa, caso o aparelho seja roubado ou seja perdido, essas informações ficarão comprometidas [VMware 2013].

O uso de dispositivos no ambiente de trabalho proporcionou uma maior liberdade e também maior chance de inovação por parte do empregado, mas a complexidade da segurança corporativa aumentou, com novos desafios [Cisco 2012].

5. Exemplos de Ataque e Defesa em Dispositivos Móveis

Em termos de tecnologia, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil em seu glossário define ataque como sendo "qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede" [CERT.br 2015]. Isso pode ser dividido entre dois tipos, sendo passivos e ativos [Pinto e Gomes 2011]:

- Ataque passivo: esse tipo de ataque faz com que as informações sejam copiadas ou analisadas com o intuito de encontrar padrões de comunicação ou do seu conteúdo. Essa análise do tráfego se busca identificar entre quais usuários está acontecendo a comunicação, quando isso acontece, o tamanho da mensagem, a frequência da troca de mensagens. Tais dados são muito úteis para se conseguir diversos tipos de informações. Apenas constatando essa troca de informações em uma rede, já pode se revelar muito sobre os usuários.
- Ataque ativo: os ataques desse tipo são aqueles que conseguem interferir diretamente ou indiretamente no funcionamento do sistema. Ataques que utilizam táticas de engenharia social e os ataques físicos são claros exemplos.

Os atacantes são indivíduos que possuem um certo conhecimento sobre o funcionamento básico dos sistemas e tentam obter algo em relação a cada ataque. Cada invasor pode receber uma designação, segundo o seu nível de conhecimento e as intenções pretendidas em seus ataques, tais como [Dumont 2006]:

- *Hacker*: esse nome é dado àqueles que já possuem um grande conhecimento sobre tecnologias, tanto que em geral são programadores ou administradores de rede. O

objetivo dos *hackers* é encontrar defeitos para resolvê-los, não buscam prejudicar ninguém em seus ataques. As tentativas de ataques basicamente são para apontar pontos vulneráveis em questões de segurança.

- *Cracker*: tal designação é dada para os invasores que tendem a prejudicar as vítimas de seus ataques. Trabalham em prol de obter ganhos ou em apenas gerar danos financeiros.
- *Phracker*: esses indivíduos são os que trabalham especificamente com telefonia, suas ações básicas são realizar ligações sem gerar custos, instalar escutas e reprogramar centrais telefônicas.
- *Larner*: são aqueles que buscam conhecer mais sobre o universo dos *hackers*. Não possuem uma única definição quanto ao tipo de ataque que realizam, podem ser com intenções de *hacker* ou de *cracker*. Seus conhecimentos são limitados, e em muitos casos recorrem aos programas ou parte deles já desenvolvidos por outras pessoas e disponíveis na *Internet*.
- *Script Kiddie*: são considerados oportunistas, de forma que buscam uma invasão que seja fácil, pois não possuem um conhecimento tão amplo quanto às tecnologias e suas seguranças. Se utilizam de métodos prontos que encontram na *Internet*, e sem um objetivo específico, tentam colocar essas formas em prática para obter acesso à conta de usuários.

5.1. Malware

Um programa com intenções de se instalar em um computador sem que haja a permissão do seu usuário é conhecido como *Malicious Software* (*Malware*), e possui como principal objetivo causar algum tipo de dano ao equipamento. Os principais alvos desses códigos são os ganhos econômicos em prol do seu criador, tentando captar dados confidenciais, práticas de golpes e até mesmo espalhar spam [Manson 1999].

Com diversas atualizações feitas ao longo dos anos, em vários setores tecnológicos, a segurança ainda não torna todos os sistemas impenetráveis, sendo assim a principal preocupação de seus usuários. *Malwares* de maneira geral são eficientes e é uma das ameaças que mais traz perigo, pois em questão de pouco tempo pode afetar de maneira global toda a rede de computadores [Kariston e Mazzola 2002].

Esse *software* malicioso pode ser dividido em algumas categorias [Damatto e Rall 2011]:

- Vírus: consiste em um código criado com o objetivo de se disseminar, espalhando-se pelos computadores, isso se dá mediante a um programa hospedeiro. Ele afeta em âmbito de *hardware*, *software* e os dados contidos na máquina em qual ele se encontra. A cada execução do programa infectado, ele tende a tentar se instalar em demais computadores. É possível que ele tente outras ações no modelo de carga, criando *back-door* ou negando a utilização de alguns serviços.
- Vermes (*Worms*): com o auxílio da rede, esse código mal intencionado autopropagável tenta entrar em outros computadores. Isso acontece por meio do consumo de recursos da rede ou de um sistema local. Eles podem ser executados sem que haja a aceitação do usuário ou até mesmo o conhecimento prévio dele, de modo a se espalhar, e assim como o vírus, ele pode causar ações de carga também. *Worms* e vírus possuem características parecidas, mas os *worms* são basicamente um subconjunto dos vírus. Os vírus conseguem se espalhar entre os arquivos do sistema,

enquanto os *worms* consegue se propagar sem afetar outros arquivos, basta ele estar instalado para tentar afetar demais aparelhos.

- Cavalo de Tróia: tem a aparência de algo inofensivo para a segurança do equipamento, mas nele há códigos com o intuito de se explorar ou o causar danos ao sistema no qual foi executado. Um dos principais portais pelo qual eles conseguem acesso ao equipamento do usuário é o *e-mail*. As funções básicas dessa ameaça é interromper o trabalho do usuário, pode dar acesso a um *hacker* ter acesso às informações pessoais do aparelho, roubando os dados ou fazendo alterações no seu sistema.
- *Spyware*: ele possui a denominação de *spybot* ou *software* de rastreamento também. Um *spybot* busca executar algumas funções sem que haja o consentimento do usuário, colhendo informações pessoais, modificando as configurações do navegador de *Internet*, tornando o desempenho do aparelho em um nível muito inferior e invadir a privacidade do usuário.
- *Adware*: esse tipo de código malicioso tem como objetivo principal apresentar anúncios em grande quantidade, realizando essa ação sem que o usuário possa aprovar ou rejeitar. Eles afetam o desempenho do sistema e também alguns deles contém funções de rastreamento.

5.2. Trojans SMS

Essa ameaça, também conhecida como *Trojan-SMS.AndroidOS.FakeInst.ef*, consiste em um código malicioso visando atacar apenas os telefones móveis. Ao executar o arquivo em que o trojan se encontra, ele se encarrega de enviar um *Short Message Service* (SMS) para números *premium* sem que o usuário tenha consciência do que está acontecendo. Esses números servem para efetuar cobrança, inscrevendo o usuário em certos serviços [Goujon e Ramos 2013].

Para que não seja percebida a infecção do aparelho, o código esconde as mensagens oriundas do serviço contratado, deixando visível apenas as mensagens que sejam de outras pessoas ou outros serviços. Como os demais *malwares* ele tende a proporcionar ao atacante um lucro sobre essa ameaça.

Ele tem dificuldades para se instalar em qualquer região, pois em cada país há um modelo de números diferentes para atender esses serviços. Mas os seus criadores estão proliferando essa ameaça de maneira bem rápida pelos continentes, onde antes predominava entre os países europeus, hoje são encontrados em locais da Ásia, Américas, África e Oceania [Goujon e Ramos 2013]. O *Android* é o sistema que mais recebe investida desse tipo de ataque, e por isso a *Google* intensificou o seu reconhecimento aos aplicativos que se encontram no *Google Play Store*. Por conta dessas ameaças estarem armazenadas em outros locais, é algo que tende a continuar obtendo vítimas.

Ao fazer a instalação de um aplicativo, o usuário pode perceber que o mesmo pede acesso para algumas ações. Dependendo do aplicativo que se pretende instalar, é possível perceber algumas ações suspeitas em relação aos *Trojans* SMS. Caso seja um jogo, e no momento da instalação precisa dar permissão para a aplicação enviar mensagens de texto e receber mensagem de texto, há uma grande chance dela estar infectada. Em alguns deles são descritas informações acerca de *premium-rate* no momento de aceitar um acordo de licença, que se refere a esses serviços de cobrança, porém quem desenvolve esse *malware* deduz que um número mínimo de usuários estão dispostos a ler os acordos e termos.

Após a aceitação do usuário, a aplicação busca obter duas informações, a *Mobile Country Code* (MCC) e a *Mobile Network Code* (MNC), que respectivamente são equivalentes ao código do país e o código referente a qual empresa telefônica o número pertence. Por meio das informações coletadas, ele busca liga-las com os dados inseridos pelo seu criador, e encontra para quais números serão enviadas as mensagens de texto [Goujon e Ramos 2013].

5.2.1. Ransomware

Em forma de *malware* essa ameaça tem aparecido com maior frequência para usuários de diversos sistemas. Quando essa ameaça consegue controle sobre o dispositivo do usuário, ele fará a encriptação de dados pessoais com uma senha de *n* dígitos. Também é possível comprometer a utilização do sistema todo, não apenas o acesso às informações. Com isso feito, apresentará uma mensagem para o usuário, na qual indica que a chave para descriptografia será enviada mediante ao pagamento de uma certa quantia estipulada pelo atacante [F-Secure 2014]. Obviamente é impossível saber se essa chave de fato será acessível ao usuário após o pagamento, tanto que já houve relatos em que usuários pagaram e não receberam retorno algum [Donohue 2014].

A Figura 6 apresenta uma mensagem de um aparelho com sistema iOS que foi infectado pelo *ransomware*.

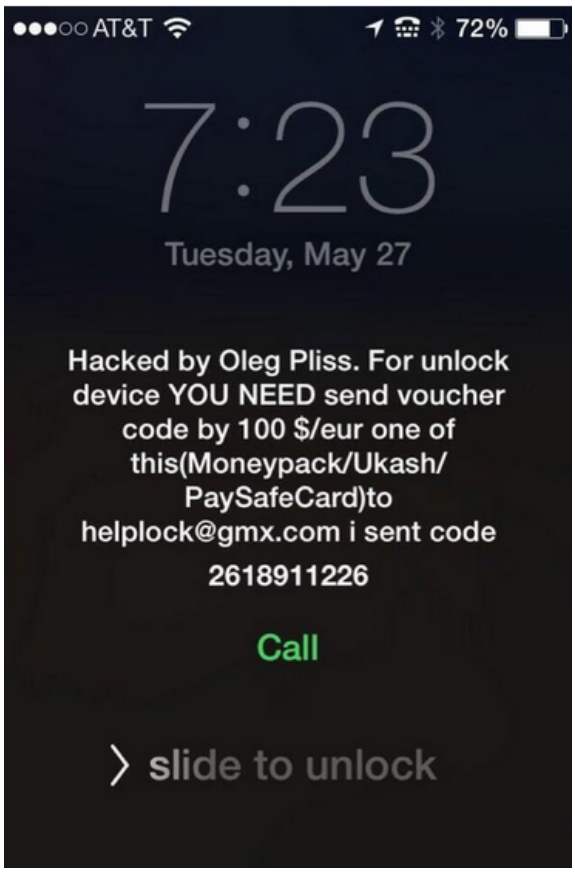

Figura 5. Exemplo de mensagem ao usuário em um sistema iOS [Donohue 2014].

Ele consegue acesso ao dispositivo por meio da técnica *phishing* que será vista na próxima seção e também pode ganhar acesso quando o usuário entra em um site que possua essa ameaça. Autoridades nacionais são utilizadas pelos atacantes para tentar enganar que o usuário infringiu alguma lei, para que o golpe seja mais realista e tenha uma chance maior de sucesso [Kaspersky 2015].

5.3. Engenharia Social

A engenharia social consiste em se utilizar de conhecimentos empíricos e científicos de uma maneira sociável para obter acesso à informações pessoais. Ou seja, um atacante por meio dessas técnicas tenta atingir alguém com o propósito de conhecer alguns dados pessoais dela, sem muito esforço, fazendo com que a vítima seja induzida a fornecer seus dados sem o devido conhecimento sobre as ações que ocorrerão a partir disso.

O ataque ocorre a partir do momento em que algum usuário adquire confiança sobre o invasor, sem saber as reais ações pretendidas por ele. As técnicas de engenharia social são utilizadas em vários ramos, não se aplicam apenas à tecnologia, podendo encontrar falhas em organizações físicas e jurídicas.

Kevin Mitnick, um dos mais famosos *hackers* americanos, na década de noventa por meio de técnicas com esse conceito efetuou diversos ataques com sucesso [Pinto e Gomes 2011]. Em seu livro, A Arte de Enganar, ele cita que a empresa pode possuir os melhores sistemas para segurança que o dinheiro possa comprar, porém o indivíduo ainda estará vulnerável [Mitnick e Simon 2003]. A segurança não está ligada apenas em seus sistemas computacionais, mas envolve muito a questão das pessoas envolvidas em todo o processo. E nem sempre elas sabem a importância que possuem para a garantia da segurança.

Em um recente caso, atacantes produziram um falso aplicativo do *Angry Birds Space*, onde usuários comuns inocentemente instalavam em seus aparelhos, sem desconfiar que se tratava de um programa com um *malware* para tentar obter o controle do aparelho [Anscombe 2012]. Alguns ataques ocorrem tentando atingir a curiosidade dos usuários, como falsos vídeos de celebridades por exemplo. Alguns ataques evidenciam claramente que pertencem a essa categoria, como:

- Wi-Fi *Evil Twin*: *hotspots* são pontos que dão acesso à rede Wi-Fi, estão cada vez mais comuns em locais públicos. E com o auxílio desses pontos, os atacantes criam um ponto de acesso com um nome comum relacionado a algum estabelecimento conhecido. Esse ponto proporcionará ao atacante uma forma de visualizar o tráfego da rede, podendo até mesmo interferir na troca de dados de algum usuário com os servidores de destino. A partir do momento que o usuário realizar o acesso a essa rede, o nome dela ficará gravada e pode ser conectada automaticamente em outro momento. Por meio de ferramentas de *hacking*, podem ser criadas telas de autenticações falsas, quando o usuário imagina inserir informações necessárias para a conexão da rede, é só o atacante obtendo algum tipo de acesso ao aparelho. E com isso o invasor pode conseguir senhas, dados de contas bancárias, logins e outros tipos de dados da vítima que sejam interessantes a ele [Martin 2015].
- *Phishing*: essa tática é utilizada há muito tempo pelos atacantes, e consiste em envio de *e-mails* falsos para as vítimas. O esperado nesse ataque é que o usuário

em uma forma de sentir necessidade acabe realizando o que se pede na mensagem. Bancos são as empresas mais utilizadas nas mensagens enviadas, buscando atingir o usuário com assuntos relacionados à conta irregular, limite de cartão ou algum novo programa de segurança bancário. A Receita Federal é outro artifício utilizado pelos atacantes, com mensagens relacionadas ao Imposto de Renda, tenta fazer o usuário acessar algum *link* que levará ao ataque [Rafael 2013]. A Rede Nacional de Ensino e Pesquisa mantém um catálogo das principais ameaças de *phishing*, com diversas formas de ameaças relatadas no território brasileiro [Centro de Atendimento a Incidentes de Segurança 2015]. Na Figura 7 um exemplo de ameaça contida no famoso mensageiro *WhatsApp*, aplicativo que funciona em qualquer SO para dispositivo móvel. Essa mensagem foi identificada contendo um *spyware* que instala uma lista de permissão para o aplicativo. No momento que o usuário aceita uma possível atualização, os recursos de espionagem são ativos. O invasor pode obter acesso em lista de contatos, mensagens de texto, registos de chamadas para arquivos multimídia, *e-mails*, histórico do navegador, informações de identificação do dispositivo como número de telefone, endereço do *Internet Protocol* (IP), código do cartão *Subscriber Identity Module* (SIM) e a localização geográfica do usuário. Arquivos vindos de outras *links* se torna possível também, ou até mesmo de algum dispositivo remoto. O invasor poderá realizar a execução de comandos em diretórios como / *system* / *bin* / *sh*, ou por meio de soquete ouvir comandos antes de retransmitir resultados de volta para o servidor [Ilascu 2014].

- *Spear Phishing*: derivando do formato *phishing* essa técnica faz ataques com o objetivo de atingir alguma pessoa ou organização. Assim o atacante busca apresentar em sua mensagem um formato que faça com que a vítima realmente acredite que pertence a alguém de sua confiança. A busca principal nesse tipo de ataque é conseguir acesso a algum sistema de informação em que a vítima é conectada. Assim o ganho econômico, segredos ou informação militar é o principal tipo de dado que o invasor tenta obter [Pais et al. 2013].
- *Footprinting*: basicamente o ataque busca agregar informações sobre o usuário, realizando uma avaliação de quando e como será o melhor momento para obter algum tipo de ganho da vítima. As formas para se conseguir essas informações são variadas, podendo ser por meio de uma ligação que simule alguma pessoa fictícia até profundas análises em data centers (centro de processamento de dados de uma empresa) ou planta de um edifício [Pais et al. 2013].
- Engenharia Social por ligações telefônicas: como visto no *footprinting* um dos meios é o invasor se passando por outra pessoa durante uma ligação. Esse tipo de ataque ainda é muito utilizado, pois o fato de se conversar com alguém, falando e ouvindo outra pessoa, mostra uma maior interação social, podendo gerar até mesmo uma confiança mais rapidamente por parte da vítima. O Serviço de Apoio ao Cliente (SAC) é utilizado por maior parte dos atacantes para se conseguir informações pessoais [Pais et al. 2013].
- *Dumpster Diving*: uma análise do lixo de uma empresa pode revelar muito sobre ela, até mesmo apresentar alguns pontos falhos em sua segurança. Alguns exemplos disso são dados de listas telefônicas, manuais, calendários com anotações, organogramas entre outros. Isso pode mostrar formas do invasor obter êxito em seu ataque [Pais et al. 2013].
- Engenharia Social Inversa: essa forma de ataque pode ser dividida em três etapas:

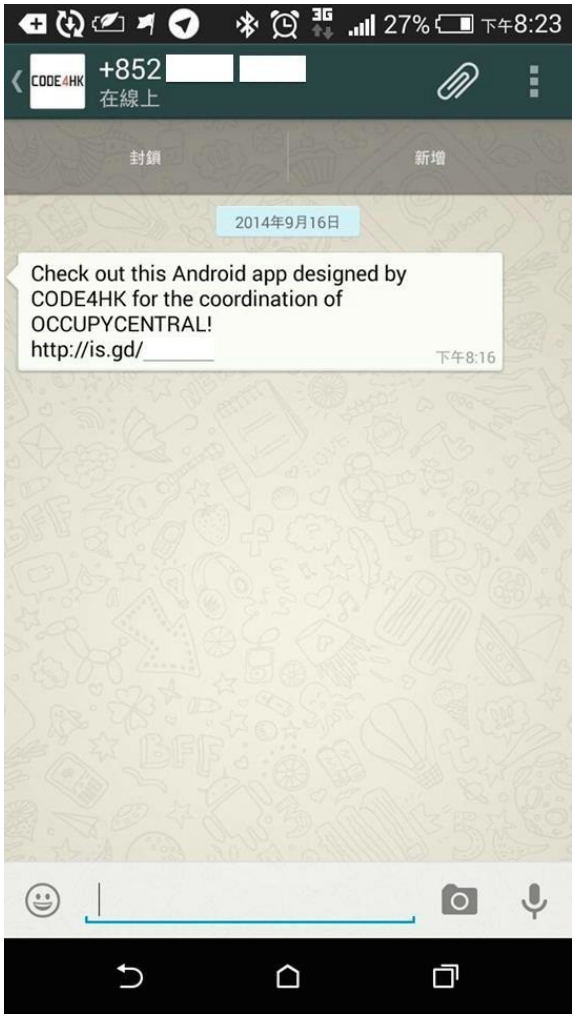

Figura 6. Exemplo de tentativa de ataque via *WhatsApp* [Ilascu 2014].

sabotagem, anúncio e assistência. A sabotagem acontece quando o atacante passa a criar problemas de acesso, depois disso ele se diz ou anuncia que ele é a pessoa certa para resolver isso, porém que necessita de certas informações para realizar tal feito. Assim a empresa não observará que se trata de um ataque, pois a falha será corrigida assim que o atacante ganhar o acesso aos dados que queria. Então, esse ataque é quando o atacante se passa por alguém de extrema importância para executar alguma tarefa. Com um bom planejamento, explorada e possui uma boa execução, o ataque tende a ter sucesso [Pais et al. 2013].

5.4. MMS

Multimedia Messaging Service (MMS) são as mensagens que enviam conteúdos multimídias via celulares ou *e-mails*. Elas se tornaram uma recente ameaça para usuários do SO *Android*. Essa brecha dada pelo sistema foi descoberta por pesquisadores da *Zimperium Mobile Security*, onde estimaram que pode afetar cerca de 950 milhões de *smartphones* [Zimperium 2015]. Essa falha foi encontrada a partir da versão 2.2 do sistema até as mais recentes.

Por meio dessas MMSs podem ser enviados códigos específicos, disfarçados como

mensagens de vídeo. Dessa maneira o atacante consegue executar os códigos remotamente, podendo obter acesso às câmeras, microfone e em algumas outras funções importantes do aparelho. Em versões mais antigas do *Android*, não era necessário nem a interação do usuário com a mensagem para que o invasor conseguisse afetar o sistema. Os códigos que o atacante insere nesse método pode instalar cavalos de tróia, quais dão ao invasor acesso em informações pessoais, como fotos, vídeos, *e-mails* e senhas.

A *Google* criou um *patch* para evitar que isso voltasse a ocorrer, e posteriormente foi repassado para os fabricantes, porém nem todas elas disponibilizaram essa atualização a todos os seus usuários. Quem utiliza versões customizadas pela fabricante pode não ter um acesso tão rápido a essa solução [SegInfo 2015].

5.5. Ataques na Camada de Aplicação

A *Open Web Application Security Project* (OWASP) mantém um projeto na *Internet* focado em segurança de aplicações *Web*. Em uma das vertentes de seu projeto, focam em segurança móvel, conhecida como OWASP *Mobile Security Project*. Com esse projeto eles buscam proporcionar um maior conhecimento sobre a criação de aplicações mais seguras [Open Web Application Security Project 2015].

Com o auxílio de empresas que realizam estatísticas de vulnerabilidades móveis, como *WhiteHat*, *Pure Hacking*, *Secure Network*, *Hewlett-Packard* (HP), entre outras, o grupo OWASP realizou um ranking dos 10 principais riscos móveis que envolvem autenticações remotas, recursos de computação em nuvem integrados à aplicações móveis [Open Web Application Security Project 2015]. A lista de 2014 incluiu os seguintes riscos:

- Controles fracos do lado servidor: as ameaças desse risco consistem em qualquer tipo que busca uma fonte de entrada não confiável por meio de um serviço API de *back-end*, serviço *Web* ou um servidor de aplicação *Web* normal. Usuários, *malwares*, aplicativos vulneráveis são exemplos de fonte de entrada para essas ameaças.
- Insegurança no armazenamento de informações: aparelhos roubados são exemplos de ameaça ao armazenamento de informações, *malwares* e aplicativos são outras formas que o invasor encontra para obter acesso aos dados. Quando o invasor consegue fisicamente o aparelho, pode obter as informações pessoais dele por meio de *softwares* de computador. Esses programas dão ao invasor acesso aos diretórios de aplicativos de terceiros que frequentemente mantém informações pessoais armazenadas.
- Proteção insuficiente na camada de transporte: os aplicativos em geral funcionam com a troca de informações na forma de cliente-servidor, ou seja, os processos do lado cliente são enviados ao servidor, e depois de processado o servidor envia uma resposta ao cliente. Essa transmissão acontece por meio de uma rede de *Internet*, passando também pela rede da operadora. Os dados podem ser interceptados durante esse tráfego, é onde o invasor tenta explorar as vulnerabilidades. Eles exploram essas vulnerabilidades ao monitorar a rede compartilhada com a vítima ou por meio de *malwares*. Em geral quando direcionam seus ataques é mais fácil obter êxito, quando devem monitorar o tráfego em uma rede de operadora o ataque se torna mais difícil de ser efetivo.

- Vazamento não intencional de dados: versões de aplicativos legítimos quando alterados, *malwares* e o acesso físico do invasor ao dispositivo podem ser as formas dessa vulnerabilidade ser explorada. Por meio de programas forenses[2] o invasor pode realizar ataques, se ele tiver o aparelho em mãos. Quando o ataque acontece por um aplicativo, ele é desenvolvido com a função da API realizar chamadas para o ataque.
- Autorização e autenticação fraca: geralmente as vulnerabilidades de autorização e autenticação são exploradas por ataques automatizados com o auxílio de ferramentas. A partir do momento que o invasor consegue identificar a vulnerabilidade na autenticação, ele realiza uma falsificação ou desvio da autenticação por meio de pedidos de serviço para o servidor *back-end* do aplicativo móvel e ignora qualquer interação direta com o aplicativo. O *malware* como em outros riscos é um dos artifícios utilizados para esse tipo de ataque. A interceptação de *botnets*, que consistem em computadores conectados à *Internet* gerenciados por um computador central, é outra forma utilizada pelos atacantes.
- Quebra de criptografia: pessoas que tem acesso físico aos dados criptografados de uma maneira inadequada, podem conseguir obter as informações que desejam. *Malwares* são outra maneira utilizada pelos invasores para obter esse acesso. Quando o invasor consegue capturar algum pacote em um tráfego de rede pode acontecer essa quebra de criptografia também.
- *Injection* do lado cliente: qualquer aplicativo móvel feito com más intenções podem ser a origem de *injections* com códigos maliciosos no dispositivo móvel do usuário. Nesses ataques o invasor utiliza textos básicos que exploram a sintaxe do interpretador da aplicação móvel. Diversas fontes de dados podem se tornar um ataque desse tipo, inclusive os próprios aplicativos.
- Decisões de segurança não confiáveis por meio de entradas: as principais ameaças desse tipo são meios que podem passar entradas não confiáveis para as chamadas de métodos. Alguns exemplos desses meios são aplicativos, *malwares* e também usuários. Invasores que possuem acesso ao aplicativo podem realizar chamadas intermediárias e alterar resultados por meio dos parâmetros.
- Manipulação imprópria de sessão: realizado por qualquer pessoa ou aplicação que tenha acesso ao tráfego de *Hypertext Transfer Protocol* (HTTP) ou dados de *cookies*. Métodos como acesso físico ao aparelho e ao tráfego da rede, ou *malwares* são utilizados pelos atacantes.
- Falta de proteção aos binários: engenharia reversa em códigos de aplicações é um meio utilizado pelos atacantes. Após fazer isso, eles modificam o código com o intuito dessa aplicação executar algumas funções sem que o usuário perceba. Ferramentas automatizadas fazem essa engenharia reversa, depois o atacante facilmente altera para um *malware*. A insegurança aos binários dentro das aplicações podem expor a aplicação e gera riscos técnicos e até de negócios caso consista em alguma propriedade corporativa. Essa falta de proteção que permite ao atacante poder realizar a engenharia reversa e posteriormente modificar a aplicação. Mesmo com proteção é possível que seja realizada a engenharia reversa, então a proteção não resulta em uma aplicação completamente segura em relação a esse ataque, é apenas uma forma de dificultar essa ação.

[2]Programas Forenses: ferramentas para realizar análise, interpretação, documentação e apresentação de dados digitais.

5.6. Ataques Físicos

Os ataques físicos são aqueles em que o invasor possui o aparelho em mãos para realizar a tentativa de roubo das informações pessoais. Em geral se utilizam ferramentas forenses para acessar aos dados.

Uma pesquisa realizada pela *Consumer Reports* Centro Nacional de Pesquisa nos Estados Unidos, apresentou que em 2014 houve 2,1 milhões de roubos à *smartphones*. Mesmo com um número tão alto, ainda assim foi inferior aos 3,1 milhões de 2013. A diminuição desse tipo de ação pode ser representado pelas táticas utilizadas pelas empresas, para proporcionar ao usuário uma forma de tornar o aparelho inoperável após o roubo ou extravio. Esses números representam os furtos e não quantos deles foram alvos de roubo de informação, mas é possível se pensar em quantas informações há em um dispositivo e se está sob o poder de terceiros é suscetível o vazamento de informações, por exemplo vazamentos de fotos íntimas [Deitrick 2015].

Na Califórnia o acesso remoto para inoperabilidade se tornou lei, onde diz que todos os novos aparelhos móveis do estado devem conter essa proteção contra roubos, ou até mesmo extravio. Foi conhecida como lei "*kill switch*", e obriga que a tecnologia possua algum modo de se bloquear o aparelho remotamente. Esse conceito já era uma tentativa de algumas empresas oferecerem uma maior segurança para seus clientes, onde se tinham alguns aplicativos capaz de realizar tal feito [Vaas 2015].

Tomar algumas precauções como uso de senhas, padrão de desbloqueio e utilizar algum recurso que seja possível o acesso remoto, podem diminuir o sucesso do invasor.

5.7. Tipos de Defesas

Esta seção tem por objetivo apresentar algumas das formas de defesas que são implementadas diretamente na comunicação de sistemas computacionais. E também alguns recursos que os usuários comuns podem utilizar para diminuir a efetividade dos ataques sofridos.

5.7.1. Criptografia

Esse conceito de defesa acontece por meio de algoritmos, onde tentam ocultar uma mensagem ao codificá-la, mas com a mesma fórmula pode se retornar para a mensagem original. É um dos principais termos vistos quando o assunto é segurança, principalmente por ter se tornado tão importante no momento de assegurar a privacidade da informação em comunicações e nas redes públicas e privadas. Quando algum invasor tenta obter acesso aos dados que trafegam na rede ou comunicação, a criptografia dos dados tornará o acesso dele à informação muito mais difícil.

A Figura 8 exemplifica como é realizado o ato de encriptar dados. Nela o primeiro elemento envia uma mensagem para um destinatário, o algoritmo de criptografia altera os dados, ou seja, altera as informações contidas. Quando o usuário final recebe a mensagem, ela passa pelo mesmo algoritmo, que realiza a decodificação dos dados, apresentando a mensagem original da comunicação.

Dois tipos de criptografia são mais utilizados, sendo a simétrica também conhecida como chave privada, e a assimétrica que também é chamada de chave pública

Figura 7. Método de criptografia de dados. Adaptado de: [Castelló e Vaz 2007].

[De Carvalho 2014]:

- Criptografia Simétrica: A criptografia simétrica começou a ser implantada nas tecnologias a partir de 1970, e foi o único meio utilizado até o surgimento da assimétrica. Com o uso de uma chave única para o emissor e para o receptor da mensagem, é o modo que o sistema desse tipo faz a criptografia dos dados. Em outros termos é possível dizer que a chave é privada entre aqueles que estão realizando a troca de dados [Konics 2014].
  A Figura 9 ilustra como funciona a codificação dos dados por meio de uma chave privada. A mensagem é criptografada com a mesma chave que o receptor recebe no final da comunicação. A chave é compartilhada entre os envolvidos na troca de dados, e é crucial que seja feito de uma forma segura, para que o atacante não tenha acesso a ela. Se o atacante conseguir o algoritmo de criptografia e a chave, ele poderá visualizar a verdadeira mensagem.

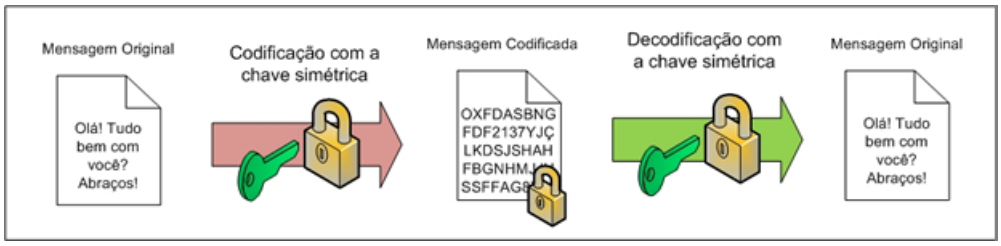

Figura 8. Criptografia Simétrica [Konics 2014].

  Sua simplicidade e rapidez a torna muito eficiente para troca massiva de mensagens e com mensagens que são longas. Um dos sistemas mais utilizados por esse tipo de criptografia, foi desenvolvido pela IBM, qual foi denominada de *Data Encryption Standard* (DES). Se tornou de tamanha importância que os Estados Unidos a adotaram como uma norma oficial do processamento de informações federais em 1977 [Simões 2013].
  A IBM a implementou com funções de consultas em tabelas, e com chaves compostas de 56 *bits*. Um fato curioso sobre esse sistema foi um desafio criado para apresentar a sua forte segurança. Existiam 72 quatrilhões de chaves possíveis, e após 18 quatrilhões de tentativas, os atacantes conseguiram obter a mensagem real por meio de tentativa e erro em 1997 [Simões 2013].
  3DES e *Advanced Encryption Standard* (AES) são outros exemplos de algoritmos utilizados, respectivamente um é formado por três chaves de 56 *bits*, e o outro pode ser implementado com chaves de 128, 192 ou até 256 *bits* [Cisco 2015].
- Criptografia Assimétrica: A criptografia assimétrica faz uso de chaves específicas para cada processo, ou seja, uma somente para criptografar e outra apenas para

descriptografar os dados. Isso diminui a chance de um possível invasor conseguir visualizar a real mensagem, tendo em vista que se conseguir uma das chaves, não dará garantias que conseguirá a segunda [Cisco 2015].
A chave pública realiza a combinação com uma chave privada, onde o emissor destina uma chave pública para o remetente da comunicação. Com essa chave, o remetente utiliza uma chave privada para criptografar a mensagem. O compartilhamento da chave pública por parte do remetente é necessária para efetivar a criptografia e descriptografia. Quando for preciso o emissor descriptografar a mensagem, fará uso da chave pública do remetente com sua própria chave privada [Cisco 2015].
A Figura 10 demonstra o funcionamento de uma criptografia assimétrica. Nela a chave amarela é utilizada para criptografar os dados, enquanto a chave verde é utilizada para a descriptografia deles.

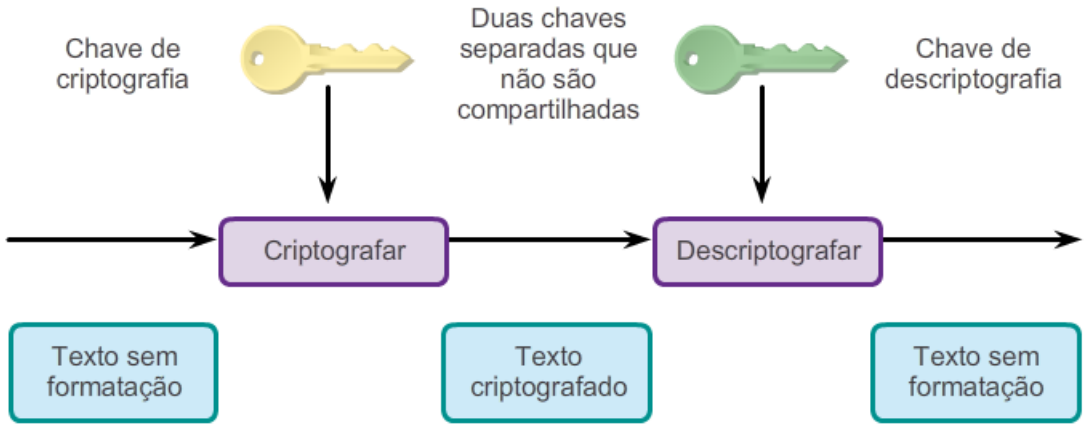

Figura 9. Criptografia Assimétrica [Cisco 2015].

O ato de encriptar dados não é útil apenas para o tráfego de informações em uma rede, é algo muito frequente em sistemas operacionais móveis. Com o tamanho e peso reduzidos dos aparelhos atuais aumentam as chances de extravio, e também são constantes alvos de roubos. Nesses casos a criptografia pode ajudar para que as informações do dispositivo não sejam expostas para terceiros. Qualquer informação considerada sigilosa pelo usuário, ou seja, informações sensíveis podem ser encriptados.

A *Apple* implementa no iOS a criptografia AES 256 em seus aparelhos, com a opção *Data Protection* fornecida para o usuário utilizar em suas entradas e saídas de informações. O *hardware* de cada aparelho possui uma chave específica, que em caso de perda ou roubo, o aparelho apagará todas as informações contidas nele caso erre 10 vezes o *Personal Identification Number* (PIN) [ESET 2014].

No sistema *Android* a criptografia é oferecida para o usuário poder utilizar tanto em seu cartão externo como na memória interna do aparelho. O método é feito ao nível do *kernel*, com a implementação *dm-crypt* de que é um subsistema do *kernel Linux*, e também da AES128 com *Cipher Block Chaining* (CBC) [Cibrão e Gonçalves 2012].

O sistema *Windows Phone* também dá suporte para criptografia de dados, porém apenas para dados armazenados na memória interna do aparelho. Por meio da tecnologia

BitLocker e do método AES 128 é feita a encriptação dos dados. A opção é dada ao usuário, e quando ativada ele automaticamente passa a encriptar todos os dados. Uma chave é gerada e protegida pela *Trusted Platform Module* (TPM) que somente a libera para componentes de inicialização confiáveis [Shpantzer 2015].

Além dos sistemas oferecerem alguns tipos de criptografia da informação, existem aplicativos disponíveis nos repositórios da *Apple Store*, *Play Store* que se refere aos dispositivos *Android* e na *Marketplace* para aparelhos com sistema *Windows Phone*.

5.7.2. Antivírus

Depois da tamanha expansão de ataques em dispositivos, a segurança ganhou um foco ainda maior. Isso fez com que o antivírus, indispensável em computadores, passar a ser uma das formas de garantir a segurança de seus dados. Esse tipo de programa tenta se manter ao máximo atualizado quanto às principais ameaças, e foca em tentar detectá-las quando for exigido [Freire 2002].

Grandes empresas desse ramo, como *Eset*, *Kaspersky*, *Avast*, entre outras, possuem versões para a maior parte das plataformas móveis. Versões gratuitas são limitadas quanto a alguns aspectos, mas possuem uma eficiência muito boa. As versões pagas são disponíveis também, e indicadas principalmente para empresas e corporações, levando em consideração que a segurança não depende de apenas uma pessoa, e sim de um grupo [Av-Comparatives 2013].

Quando aparelhos mais antigos eram roubados, o ladrão apenas trocava o chip e poderia utilizá-lo normalmente. Com o auxílio dos antivírus isso pode ser evitado, alguns deles dão a opção *Theft Protection*, ela torna possível o acesso remoto ao aparelho e dá a opção de apagar todas as informações contidas nele [Av-Comparatives 2013].

Alguns usuários tendem a não utilizar esses programas devido ao consumo de bateria e à perda de desempenho que eles pensam causar ao aparelho. A *AV-Comparatives* realizou um teste com antivírus em 2013 no sistema *Android*, e os testes apontaram que a bateria não é tão afetada como se pensa. A partir de tarefas cotidianas de um usuário comum como visualização de vídeos, acesso a sites, realização de ligações, entre outras, se constatou que entre os 16 principais *softwares* testados, apenas dois consumiram mais que 3% da bateria [Av-Comparatives 2013]. No mesmo teste foi realizado um comparativo entre identificação de *malwares*, onde todos possuíram uma taxa de acerto superior a 90%. Isso representa que a segurança fornecida pelos programas possuem extrema eficiência sem comprometer o desempenho do dispositivo.

5.7.3. Firewall

Essa técnica é utilizada para defesa no tráfego de rede, e pode ser implementada em *hardware* e *software*. Ela determina que operação de envio ou recepção de informação pode ser executada. O seu funcionamento tem uma definição simples, que é liberar acessos permitidos e bloquear os indesejados [Alecrim 2013].

A Figura 11 representa com um muro o bloqueio feito pelo *firewall*, onde ele

pode controlar o acesso feito por qualquer tipo de rede, como no exemplo há a rede 3G, *Explicit Data Graph Execution* (EDGE), *General Packet Radio Service* (GPRS), Wi-Fi e *Bluetooth*.

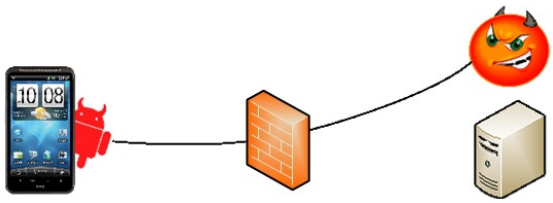

Figura 10. Barreira criada pelo *firewall* [University of Michigan 2012].

O acesso se dá por meio de uma configuração que pode ser feita pelo usuário. Ele pode definir que não nenhum tráfego seja realizado, como também pode fazer que com que o tráfego seja liberado a partir de uma permissão dada pelo administrador da rede. Outras definições permitem que alguns tráfegos sejam permitidos automaticamente. Os modelos mais avançados podem definir alguns acessos mais direcionados para um sistema de segurança, ou até garantir uma maior segurança em autenticações de usuários [Alecrim 2013].

5.7.4. Conscientização

Como já pôde ser visto na Seção 3, as pessoas são um dos principais pilares para assegurar a segurança da informação. O próprio Mitnick considera que a quebra do "*firewall* humano" é mais fácil do que se dedicar em outras técnicas para ataque [Mitnick e Simon 2003].

Por motivos como confiança demais nas aplicações ou até mesmo ingenuidade por parte dos usuários, a questão segurança não é tratada como se devia. Isso acarreta em algumas decisões equivocadas, e quando se trata da tendência BYOD nas empresas, isso ganha um tamanho mais significativo. Com o crescimento das redes sociais, os usuários passaram a expor mais suas informações. Grande parte dos usuários frequentes de redes sociais revelam informações pessoais para outras pessoas, após adquirir uma certa confiança nelas [Rosa et al. 2012]. A interação entre desconhecidos é uma tendência ainda maior via redes sociais, e os engenheiros sociais são astutos ao explorar esses meios para atingir suas vítimas.

O uso de tecnologias mais avançadas é importante para diminuir as chances de ataque. Algumas delas fornecem a visualização dos acessos pessoais, o que traz uma maior comodidade para chefes de empresas por exemplo [Kaspersky 2006].

Se as pessoas perceberem o tamanho da importância que possuem em assegurar que seus dados não serão invadidos, passarão a ter uma forma diferente de agir referente às tecnologias.

6. Resultados e Discussão

O presente trabalho aborda algumas formas utilizadas pelos invasores para roubo de informações ou controle de aparelhos móveis, e alguns métodos de defesas implantadas. Durante as pesquisas realizadas foi possível perceber que o sistema *Android* é o mais perseguido pelas táticas de ataques, mas não é possível comprovar se isso ocorre dado o número elevado de usuários ou por ser um sistema de código aberto, onde é possível tentar encontrar algumas vulnerabilidades (ou por alguma outra característica). O sistema iOS e *Windows Phone* possuem a seus códigos fechados, que de certa forma dificulta a ação de ataques ao sistema. Vale ressaltar que, mesmo o Android ser baseado em *Linux* e ter seu código aberto, não necessariamente isso motiva a ser um sistema vulnerável.

Uma grande parte dos ataques são por meio de táticas de Engenharia Social, e ela é uma das formas mais antigas de ataque, e eficaz. A curiosidade das pessoas é explorada de diversas formas, tanto com mensagens sobre escândalos de famosos, prêmios (atacando a cobiça..) até intimações judiciais (dentre muitas outras). Os usuários de todos os sistemas são alvos desses ataques e podem ser afetados por *malwares* com objetivos de controle das ações do aparelho ou acesso às informações pessoais.

Foi possível perceber que o fator humano é o mais suscetível aos ataques, independente das tecnologias de defesas implantadas em sistemas ou empresas. As pessoas podem derrubar barreiras que impedem o acesso dos atacantes em informações ou tarefas dos sistemas.

As defesas descritas na Subseção 5.7.1 são maneiras de se proteger de ataques, porém não garantem que as informações nunca sejam acessadas por pessoas sem as devidas autorizações. O principal motivo é a constante evolução dos ataques, que talvez não inovam a técnica, mas sim em como interagir com a vítima. Para isso há dicas que se podem seguir para evitar perda de dados, como uso de antivírus, realizar aquisições de aplicativos diretamente do repositório da empresa do sistema operacional, evitar acessos à *links* de *e-mails* suspeitos, entre outras.

O BYOD é uma realidade vivida em um número maior de empresas a cada ano, onde a responsabilidade com a segurança dos dados é mais preciosa. As vantagens nessa tendência faz com que as empresas passem a aderir ao uso dos aparelhos de seus funcionários com assuntos de trabalho. Porém qualquer perda de dados pode resultar em um prejuízo para a empresa, por isso é levado em conta tal risco quando a empresa pretende passar a utilizar esse meio de trabalho.

Com as intensas ações dos invasores sobre os dispositivos, empresas tentam encontrar formas de garantir uma maior segurança sobre os dados de usuários e corporações. Uma tecnologia que está ganhando espaço no mercado de *smartphones* é o *BlackPhone*, que se trata de um celular com características de um aparelho móvel normal, mas seu sistema é todo voltado para a segurança. Ele se baseia no *Android* puro, e com as devidas modificações constatadas como necessárias pela empresa *Silent Circle*, surgiu o *Silent OS*. O sistema dele apresenta diversas criptografias em ligações, troca de e-mails, troca de mensagens, e outros tráfegos de dados. Devido ao número de criptografias realizadas pelo aparelho seu desempenho poderia ser comprometido, mas seu projeto foi tão bem construído que os usuários não demonstram sentir uma lentidão em seu uso. Com essas criptografias a chance de alguma mensagem do usuário ser lida por um atacante é muito

menor. Outro conceito utilizado nele foi o *Spaces*, que cria "espaços" representando outros dispositivos em um aparelho só, com isso é possível ter a divisão de dados da empresa com os pessoais, já que não há o compartilhamento de um espaço com o outro.

É possível apontar que os sistemas com código fechado possuem uma propensão menor a receber investidas de ataques e que sejam mais vulneráveis aos ataques. Contudo não é possível afirmar que não haja roubo de dados desses sistemas, pois em grande parte dos ataques eles são genéricos. Outra constatação é o uso da criptografia como principal forma de defesa no tráfego de dados em redes. Essa técnica possui uma eficácia alta contra a perda de dados. E por fim o usuário é considerado como o principal motivo do sucesso por parte do atacante. Por meio da persuasão o usuário é ludibriado, e para isso mensagens de diversas conotações são utilizadas para que haja uma interação com a vítima.

Os *malwares* atualmente estão surgindo com a principal função de afetar usuários dos sistemas móveis, e para muitos deles é necessária o acesso do usuário a algum *link* ou aceitação de algum recebimento de dado. Para que isso se torne menos recorrente, o usuário precisa passar a reconhecer os verdadeiros riscos que há em se utilizar os dispositivos, principalmente com o uso deles em redes abertas. Vírus e ataques diversos não é há muito tempo uma exclusividade dos computadores, o perigo com as informações contidas nos aparelhos já é uma realidade com a qual deve-se passar a se preocupar. Empresas da área de tecnologia passam a tomar como prioridade encontrar soluções e orientar seus funcionários quanto a segurança durante o uso desses dispositivos.

7. Conclusões e Trabalhos Futuros

Este trabalho abordou um estudo e análise de segurança em dispositivos móveis, com foco em *Android*, iOS e *Windows Phone*, que são alguns dos principais sistemas operacionais utilizados atualmente. Foram relatados alguns aspectos de ataque e defesa, desde responsabilidade das tecnologias quanto dos usuários.

Demonstrou-se alguns problemas e soluções possíveis para que as informações sejam asseguradas e de confiança. Normalmente cada sistema opera sobre técnicas e mecanismos diferentes de defesa. Sendo assim, aqui nesse trabalho foi feito um levantamento genérico de atividades de ataque e defesas, sendo que existem ataques e vulnerabilidades específicas para cada sistema (que não foi o objetivo desse estudo).

Apesar da abordagem ser genérica, com uma pesquisa rápida é possível descobrir que o sistema operacional *Android* possui uma gama mais ampla de atividades de ataques. Esse assunto pode se tornar complexo, pois não é possível provar que ele possui maior quantidade de ataques e vírus por ter um maior número de usuários ou se seu sistema realmente é mais vulnerável que os demais analisados.

Como trabalhos futuros são indicados o uso de testes de penetrações para tornar prático os conceitos estudados. Novamente, o *Android* possui ferramentas mais acessíveis em relação aos demais sistemas. Exemplos são o sistema *BackTrack Linux* e o *BlackPhone*.

Um outro estudo futuro pode abordar as técnicas e tecnologias de rastreamento com recursos (principalmente) de dispositivos móveis, tais como apresentadas nos filmes *Fast and Furious* 7 (com o "Olho de Deus") e *Batman Dark Knight*.

Referências

Alecrim E. (2013). O que é firewall? - conceito, tipos e arquiteturas. Disponível em: <http://www.infowester.com/firewall.php>. Acessado em: 5 ago. 2015.

Andrade A. W., Agra R., e Malheiros V. (2013). Estudos de caso de aplicativos móveis no governo brasileiro. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2013/0070.pdf>. Acessado em: 7 abr. 2015.

Android (2015). Android interfaces. Disponível em: <https://source.android.com/devices/>. Acessado em: 4 mai. 2015.

Anscombe T. (2012). A engenharia social ainda é a maior ameaça contra os consumidores. Disponível em: <http://blog.winco.com.br/avg/a-engenharia-social-ainda-e-a-maior-ameaca-contra-os-consumidores/>. Acessado em: 17 mai. 2015.

Apple (2015). About the ios technologies. Disponível em: <https://developer.apple.com/library/prerelease/ios/navigation/>. Acessado em: 2 jul. 2015.

Av-Comparatives (2013). Mobile security review. Disponível em: <http://www.av-comparatives.org/wp-content/uploads/2013/08/avc_mob_201308_en.pdf>. Acessado em: 04 jun. 2015.

Batista A. L. P., Dellaquila B. L., e Balthazar G. d. R. (2013). Análise da segurança de aplicativos na plataforma android através da adoção de patterns. Disponível em: <http://cbsoft2013.unb.br/miniplop/miniplop-artigos >. Acessado em: 18 mai. 2015.

Blackphone (2015). Privatos. Disponível em: <https://blackphone.ch/privat-os/>. Acessado em: 25 mar. 2015.

Brasscom (2014). Mobilidade. Disponível em: <http://www.brasilitplus.com/brasilit/upload/download/1416333251mobilidade.pdf>. Acessado em: 7 abr. 2015.

Caçador D. M. (2014). Segurança e mobilidade em redes ieee 802.11. Disponível em: <http://repositorio.ucp.pt/bitstream/10400.14/17480/1/Dissertação Mestrado SSI Daniel Cacador Final - Revista.pdf>. Acessado em: 25 abr. 2015.

Castelló T. e Vaz V. (2007). Tipos de criptografia. Disponível em: <http://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html>. Acessado em: 10 mai. 2015.

Centro de Atendimento a Incidentes de Segurança C. d. A. a. I. d. S. (2015). Catálogo de fraudes. Disponível em: <http://www.rnp.br/servicos/seguranca/catalogo-fraudes >. Acessado em: 20 ago. 2015.

CERT.br Centro de Estudos R. e. T. d. I. d. S. n. B. (2015). Glossário. Disponível em: <http://cartilha.cert.br/glossario >. Acessado em: 15 jul. 2015.

Cerutti F. (2012). Necessidade e componentes gerais da segurança da informação. Disponível em: <http://www.diegomacedo.com.br/necessidade-e-componentesgerais-da-seguranca-da-informacao/>. Acessado em: 15 jul. 2015.

Cibrão D. e Gonçalves R. (2012). Disponível em: <http://web.fe.up.pt/ jmcruz/ssi/ssi.1112/trabs-als/final/G4T10-android-final.pdf>. Acessado em: 23 abr. 2015.

Cisco (2012). Byod: Uma perspectiva global. Disponível em: <http://www.cisco.com/web/about/ac79/index.html>. Acessado em: 10 jun. 2015.

Cisco (2015). Capítulo 7: Protegendo a conectividade de site para site. Disponível em: <http://www.ct.utfpr.edu.br/deptos/cisco/material/CCNA5.0/4 - Conexão de Rede/course/module7>. Acessado em: 3 jul. 2015.

Damatto F. C. e Rall R. (2011). Disponível em: <http://www.fatecbt.edu.br/seer/index.php/tl/article/view/107>. Acessado em 19 jun. 2015.

De Almeida I. P., Assunção L. R., Simões T. L., e Lima J. F. (2014). Visão sobre dispositivos e sistemas operacionais móveis. Disponível em: <http://200.131.5.234/ojs/index.php/anaisviiisimposio/article/view/45/32>. Acessado em: 1 abr. 2015.

De Carvalho S. L. (2014). Autoridades certificadoras e segurança na assinatura digital. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/3870>. Acessado em: 15 mai. 2015.

Deitrick C. (2015). Smartphone thefts drop as kill switch usage grows. Disponível em: <http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm>. Acessado em: 26 jun. 2015.

Donohue B. (2014). Ransomware malware targets apple users. Disponível em: <https://blog.kaspersky.com/ransomware_targets_ios_osx/4903>. Acessado em: 15 jun. 2015.

Dumont C. E. S. (2006). Segurança computacional: Segurança em servidores linux em camadas. Disponível em: <http://www.ginux.ufla.br/node/137>. Acessado em: 7 mai. 2015.

ESET (2014). Guia de criptografia. Disponível em: <http://www.eset.com.br>. Acessado em: 22 jul. 2015.

F-Secure (2014). Threat report h2. Disponível em: <https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014>. Acessado em: 10 jun. 2015.

Fenn J. e Linden A. (2001). Trends for 2002 to 2007: up the slope of enlightenment. gartner group article top view. Disponível em: <https://www.gartner.com/doc/351126>. Acessado em: 23 mar. 2015.

Fling B. (2009). *Mobile design and development: practical techniques of creating mobile sites and web apps*. p. 37-39.

Forouzan B. A. (2013). *Redes de Computadores: uma abordagem top-down*. Porto Alegre: AMGH, p. 726-730.

Freire B. B. d. L. (2002). Sistema antivírus baseado em agentes móveis - sistema sabam. Disponível em:

<https://repositorio.ufsc.br/bitstream/handle/123456789/84181/196059.pdf>. Acessado em: 23 mai. 2015.

Gabbay M. S. (2006). Fatores influenciadores da implementação de ações de gestão de segurança da informação :um estudo com executivos e gerentes de tecnologia da informação das empresas do rio grande do norte. Disponível em: <http://repositorio.ufrn.br:8080/jspui/handle/123456789/14985>. Acessado em: 17 abr. 2015.

Garcia M. A. P. (2013). Filtros de imagens para ios. Disponível em: <http://www.tcc-computacao.tiagodemelo.info/monografias/2013/tcc-mario-angel.pdf>. Acessado em: 22 abr. 2015.

Gonçalves J. C. (2011). Uso da plataforma android em um protótipo de aplicativo coletor de consumo de gás natural. Disponível em: <http://www2.dainf.ct.utfpr.edu.br/esp/monografias-de-especializacao-da-turma-vi-2010-2011>. Acessado em: 20 mai. 2015.

Goujon A. e Ramos P. (2013). Boxer sms trojan. Disponível em: <http://www.welivesecurity.com/>. Acessado em: 13 jul. 2015.

Ilascu I. (2014). Advanced android remote access trojan aimed at hong kong protesters. Disponível em: <http://news.softpedia.com/news/Advanced-Android-Remote-Access-Trojan-Aimed-at-Hong-Kong-Protesters-460684.shtml>. Acessado em: 3 jun. 2015.

Isaacson W. (2011). *Steve Jobs A Biografia*. 1.ed. São Paulo: Companhia das Letras, p. 657-670.

Kariston P. e Mazzola V. B. (2002). *Modelo das Tríades Conjugadas.* Anais do IV Simpósio Segurança em Informática SSI'2002.. São Paulo: CTA/ITA, p. 45-54.

Kaspersky (2006). O elo mais fraco. Disponível em: <http://www.kaspersky.com.pt/artigos/BIT_SegurancaNaEmpresa_Dez2006.pdf>. Acessado em: 13 mai. 2015.

Kaspersky (2015). Centro de segurança na internet. Disponível em: <http://www.kaspersky.com/pt/internet-security-center/threats/ransomeware>. Acessado em: 10 jun. 2015.

Konics (2014). O que é criptografia? Disponível em: <http://www.konics.com.br/blog/?p=1742>. Acessado em: 23 jun. 2015.

Manson M. (1999). Estudio sobre vírus informáticos. Disponível em: <http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml?monosearch>. Acessado em: 13 jul. 2015.

Martin R. (2015). Avoiding social engineering attacks through security education training and awareness. Disponível em: <http://www.infosecwriters.com/Papers/RCrockett_Social_Engineering_Education.pdf>. Acessado em: 10 ago. 2015.

Mateus G. R. e Loureiro A. A. F. (1998). *Introdução a Computação Móvel*. Belo Horizonte: UFMG, p. 1-55.

Milani A. (2012). *Programando para iPhone e iPad - Aprenda a construir aplicativos para o iOS*. São Paulo: Novatec Editora, p. 14-19.

Mitnick K. e Simon W. (2003). *A Arte de Enganar*. 1.ed. São Paulo: Makron Books, p. 21.

Mônaco T. e Do Carmo R. M. (2012). *Desenvolvendo Aplicações para Windows Phone*. Rio de Janeiro: Brasport, p. 1-14.

Monteverde W. A. e Campiolo R. (2014). Estudo e análise de vulnerabilidades web. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0065.pdf>. Acessado em: 27 mar. 2015.

Moretti C. e Bellezi M. A. (2014). Segurança em redes sem fio 802.11. Disponível em: <http://revistatis.dc.ufscar.br/index.php/revista/article/view/73>.

Morimoto C. E. (2009). *Smartphones: Guia Pratico*. Porto Alegre: GDH Press e Sul Editores, p. 432.

Mozilla (2015). Firefox os. Disponível em: <https://www.mozilla.org/pt-BR/firefox/os/1.1/>. Acessado em: 17 set. 2015.

Nicolai B. B., De Oliveira D. M., Moraes N., e Da Silva W. L. (2012). Google android - a plataforma, seus componentes e suas versões. Disponiível em: <http://www.williamluis.com.br/wp-content/uploads/2013/10/TCC-Google-Android-Final.pdf>. Acessado em: 8 mai. 2015.

Nunes F. (2014). Avaliação de técnicas e mecanismos para entrada e saída de informações em dispositivos móveis. Disponível em: <http://aberto.univem.edu.br/bitstream/handle/11077/998/Fernando Nunes.pdf>. Acessado em: 13 mai. 2015.

Open Web Application Security Project O. W. A. S. P. (2015). Owasp mobile security project. Disponível em: <https://www.owasp.org/index.php/Mobile>. Acessado em 14 ago. 2015.

Pais R., Moreira F., e Varajão J. (2013). Engenharia social (ou o carneiro que afinal era um lobo). Disponível em: <http://hdl.handle.net/1822/26251>. Acessado em: 12 mai 2015.

Pinto P. M. T. N. e Gomes A. R. L. (2011). Segurança na conectividade wifi em dispositivos móveis: Estudo de caso do iphone. Disponível em: <http://revistas.unibh.br/index.php/dcet/article/viewFile/331/406>. Acessado em: 11 mai. 2015.

Querino Filho L. C. (2013). *Criando aplicativos para iPhone e iPad : uma abordagem prática do nível básico ao avançado*. São Paulo: Novatec Editora, p. 22.

Rafael G. d. C. (2013). Ataques de engenharia social. Disponível em: <http://www.tiespecialistas.com.br/2013/10/ataques-engenharia-social/>. Acessado em: 20 mai. 2015.

Rosa A. C., Da Silva B. D., e Da Silva P. L. (2012). Análise de redes sociais aplicada à engenharia social. Disponível em: <https://repositorio.uninove.br/xmlui/bitstream/handle/123456789/163/128-360-1-DR analise de redes sociais.pdf>. Acessado em: 18 mai. 2015.

Scota D. F., De Andrade G. E., e Xavier R. d. C. (2010). Configuração de rede sem fio e segurança no sistema operacional android. Disponível em:

<http://www.ppgia.pucpr.br/ jamhour/RSS/TCCRSS08B/Daniel Fernando Scota - Artigo.pdf>. Acessado em: 25 abr. 2015.

SegInfo (2015). Descoberta vulnerabilidade que permite atacar smartphones android através de mms. Disponível em: <http://www.seginfo.com.br/>. Acessado em: 5 ago. 2015.

Shpantzer G. (2015). Implementing hardware roots of trust: The trusted platform module comes of age. Disponível em: <http://www.sans.org/reading-room/whitepapers/analyst/implementing-hardware-roots-trust-trusted-platform-module-age-35070>. Acessado em: 12 ago. 2015.

Silberschatz A., Galvin P. B., e Gagne G. (2004). *Sistemas Operacionais com Java*. 6.ed. Rio de Janeiro: Elsevier, p. 3-18.

Simões D. A. (2013). Implementando segurança nas redes de comunicação através de vpn na internet: Um estudo de viabilidade. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/3238>. Acessado em: 23 jun. 2015.

Soares L. F. G., Lemos G., e Colcher S. (1995). *Redes de computadores: das LANs, MANs e WANs às redes ATM*. Rio de Janeiro: Campus, p. 448.

Spadari A. (2015). Sistemas operacionais para celulares e dispositivos móveis. Disponível em: <http://br.ccm.net/faq/11106-sistemas-operacionais-para-celulares-e-dispositivos-moveis>. Acessado em: 17 set. 2015.

Tomaél M. I. e De Jesus J. A. G. (2010). *Informação em múltiplas abordagens : acesso, compartilhamento e gestão*. Londrina: UEL, p. 18-24.

University of Michigan U. o. M. (2012). Cell network security holes revealed, with an app to test your carrier. Disponível em: <http://www.eecs.umich.edu/eecs/about/articles/2012/firewall_hack.html>. Acessado em: 11 mai. 2015.

Vaas L. (2015). Smartphone anti-roubo "kill switch"lei entra em vigor na califórnia. Disponível em: <https://nakedsecurity.sophos.com/pt/2015/07/02/smartphone-anti-theft-kill-switch-law-goes-into-effect-in-california/>. Acessado em: 25 jul. 2015.

VMware (2013). The byod opportunity. Disponível em: <http://www.vmware.com/files/pdf/view/VMware-BYOD-Opportunity-Whitepaper.pdf>. Acessado em: 12 jun. 2015.

Windows Phone W. P. (2015). Windows phone architecture overview. Disponível em: <https://sysdev.microsoft.com/en-us/Hardware/oem/>. Acessado em: 16 mai. 2015.

Zimperium (2015). Experts found a unicorn in the heart of android. Disponível em: <http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/>. Acessado em: 31 jul. 2015.