RISCOS DE SEGURANÇA NA COMPUTAÇÃO MÓVEL

Thaís Antunes Bione[1], Fernando Antonio Aires Lins[2], Dayanne Cristina de Araujo Barbosa[3]

Introdução

Com a evolução e facilidade de acesso a tecnologia, o consumo de aparelhos eletrônicos tem aumentado em grande escala. Pesquisas relevam que o Brasil é o quarto país do mundo em *smartphones*, afirmação que permite que se tenha noção da proporção na qual se chegou a marcante presença de tais dispositivos móveis no dia a dia atual do nosso país e do mundo.

Ao se analisar o lado socioeconômico, pode-se perceber que este avanço é um significativo ponto positivo, pois o mesmo está diretamente ligado a uma possível melhoria nas condições de poder aquisitivo da população, uma vez que o custo para adquirir um *smartphone* é maior em comparação ao custo necessário para se adquirir um eletrodoméstico mais simples. Contudo, esse avanço pode representar um grande risco de segurança, pois dados confidenciais podem estar trafegando em redes inseguras e serem acessados por pessoas não autorizadas.

Como não bastasse o uso dos serviços desses dispositivos para uso pessoal (devido à praticidade e comodidade), muitas empresas têm oferecido a seus funcionários a oportunidade de acesso e manipulação de dados internos através de *smartphones*. Essa condição fornecida pelas empresas trata-se de uma iniciativa interessante, pois proporciona ao funcionário uma maior liberdade, além de também o privilegiar com flexibilidade no acesso.

Porém, na realidade toda essa facilidade vem seguida de um grande problema: os riscos que a utilização de modo imprópria ou até mesmo maliciosa pode trazer ao usuário final, independente de ser uma pessoa física ou uma empresa. Portanto, o objetivo principal deste artigo é o levantamento de riscos e soluções atuais na área de segurança para dispositivos móveis (mais especificamente, celulares *smartpthones*), com a finalidade de se expor os riscos existem e o que pode ser feito para mitigar os mesmos.

Material e métodos

Foram realizadas pesquisas através da leitura de artigos já publicados (nacionais e internacionais), como também, busca em sites e blogs mais acessados por usuários finais na tentativa de reduzir a incidência dos ataques que vêm sendo executados com maior frequência.

Para que os frutos das pesquisas acima citadas pudessem ser mais detalhadamente analisados, optou-se por direcionar o campo de pesquisa para o sistema operacional Android, pelo fato de ser o mais utilizado atualmente pela sociedade. Há uma estimativa de que a cada dia aproximadamente um milhão e meio de aparelhos começam a utilizar esse sistema operacional no mundo.

Antes de ir ao encontro das soluções, é importante identificar os principais problemas encontrados e que podem comprometer o princípio da segurança da informação. Estes problemas estão descritos na próxima seção e darão subsídios para a compreensão de que soluções podem ser adotadas.

Resultados e Discussão

Apesar de uma grande parte dos usuários de dispositivos móveis terem noção de que não se trata de um serviço totalmente seguro, pode-se afirmar que uma parcela expressiva dos mesmos não tem o cuidado necessário na hora de decidir quais aplicativos instalar no seu *smartphone* Android (por exemplo). Poucas são as fontes que alertam o consumidor de riscos corridos por uso inadequado.

Atualmente, pode-se afirmar que uma das principais ameaças de segurança envolvendo dispositivos móveis **reside no próprio usuário** que, inadvertidamente, acaba por clicar em links maliciosos e consequentemente instalando *malwares* (*softwares* que põem em risco a segurança do dispositivo) em seu aparelho. No sistema operacional Android, a instalação desses *malwares* (vírus) é bastante frequente através dos aplicativos disponíveis na própria loja da marca, a Google Play.

Adicionalmente, as ameaças não se resumem apenas a este tipo, pois existe uma grande vulnerabilidade através do próprio **canal de comunicação** (rede sem fio), seja por meio da utilização do Bluetooth ou da rede Wireless. É possível que pessoas não autorizadas tenham acesso a dados presentes em um dispositivo mesmo sem autorização do proprietário (através de interceptação de dados ou até mesmo fazendo invocações remotas através da rede). Para isso, basta apenas que esses serviços acima citados tenham sido configurados de tal sorte que permitam o aparecimento de brechas de segurança.

[1] Primeira Autora é Aluna do Departamento de Estatística e Informática, Universidade Federal Rural de Pernambuco. Rua Dom Manoel de Medeiros, s/n, Dois Irmãos, Recife, PE, CEP 52171-900. E-mail: thaisbione@gmail.om

[2] Segundo Autor é Professor do Departamento de Estatística e Informática, Universidade Federal Rural de Pernambuco. Rua Dom Manoel de Medeiros, s/n, Dois Irmãos, Recife, PE, CEP52171-900. E-mail: faires@gmail.com

[3] Terceira Autora é Aluna do Departamento de Estatística e Informática, Universidade Federal Rural de Pernambuco. Rua Dom Manoel de Medeiros, s/n, Dois Irmãos, Recife, PE, CEP 52171-900. E-mail: dayanne.araujo8@gmail.com

É necessário destacar que as ameaças referenciadas ocorrem em conjunto com o fato de que nem todos os dispositivos móveis utilizam criptografia em todos os aplicativos. A criptografia procura permitir que apenas o real destinatário tenha acesso à informação. Com a falta dessa prática, os dados da mensagem podem ser acessíveis a qualquer pessoa que os buscam (estarão navegando em "texto livre", facilitando a leitura após uma possível interceptação de terceiros).

É evidente que as grandes empresas de sistemas operacionais para dispositivos móveis vêm lutando para acabar com as vulnerabilidades e por isso possuem equipes destinadas a encontrar e corrigi-las. Além disso, como pode-se ver na Tabela 1, já são aplicadas algumas práticas para combater as ameaças conhecidas (ex.: autenticação). O problema é que, à medida que as empresas inovam em soluções, os *crackers* (pessoas que criam os softwares maliciosos) também se atualizam e surgem com novas formas de ataque.

Para mitigar os riscos de segurança anteriormente apresentados, é salutar a adoção de uma política (ou pelo menos práticas) de segurança relacionada ao dispositivo móvel. A responsabilidade de um uso relativamente seguro não é apenas das empresas dos sistemas as quais pertencem os dispositivos, mas cabe também ao usuário final uma maior preocupação em relação ao que se está fazendo. Por exemplo:

i) Ao instalar um aplicativo, o usuário deve ler os comentários de outros que já usaram o mesmo, verificando, por exemplo, se há classificação positiva, se é um vírus, etc;
ii) Não clicar em links sem que se conheça o remetente (e evitar até mesmo links enviados por pessoas conhecidas, mas que não tem uma razão aparente de existir, ex: sorteios);
iii) Desativar Bluetooth enquanto não o utilizar e permitir disponibilidade apenas para dispositivos pareados (dispositivos que têm permissão de acesso).

Existem diversas outras técnicas que podem ser empregadas para mitigar os riscos. Algumas delas podem ser encontradas na Tabela 2, que se encontra no final deste resumo.

Conforme anteriormente citado, as empresas apresentam práticas com o objetivo de proporcionar um uso mais seguro (Tabela 1). Porém, com o passar do tempo, tais ações vêm se tornando obsoleto, com isso, surgiu a ideia de uma segurança mais reforçada, representada na Tabela 2. Por exemplo, para ataques como a criptoanálise (tentar descobrir um texto já criptografado), foi incluída a imagem digital, que é usada como um segundo nível de autenticação. Uma prática bastante aplicada é a *shared secret*, representado por um dado conhecido apenas pelos envolvidos e interessados em um dado a ser trocado, em busca de uma autenticação mais segura.

Um fato que para muitos não alerta risco, é a perda ou roubo do aparelho. É bastante preocupante saber que além de dos registros da agenda telefônica, os dados de multimídia (como fotos, vídeos) poderão estar sendo visualizados e, inclusive compartilhados. Na Tabela 2 foi dada uma solução para tal agravante: o *poisonpill*, que consiste em uma mensagem enviada para o dispositivo, capaz de apagar todos os seus dados. O envio desta mensagem fica restrito ao proprietário.

Como conclusão final, pode-se afirmar que o aumento do número de ativações de dispositivos móveis (especialmente *smarphones*) é visível e que esse fato é preocupante ao se pensar na segurança do serviço. Conclui-se também que não há ainda soluções concretas para resolver tal incidência uma vez que os resultados são frutos da interação homem/dispositivo, e isso reduz as possibilidades de segurança do próprio sistema operacional. Desta forma, para se reduzir tais riscos, é sugerido que os usuários tenham um maior cuidado e adotam uma política de segurança para o uso de dispositivos móveis, onde a mesma pode, por exemplo, restringir a utilização de produtos desconhecidos não verificados (em ambientes como o Google Play) e sugerir configurações para o aparelho a fim de sanar possíveis furos de segurança.

Agradecimentos

A minha mãe e amigos, e ao orientador e professor, Fernando Antonio Aires Lins.

Referências

Sathyan, J; Sadasivan, M., Multi-Layered Collaborative Approach to Address Enterprise Mobile Security Challenges, IEEE, 2010.

Pinto, P.M.T.L.N.; Gomes, A.R.L. Segurança na conectividade wifi em dispositivos móveis: estudo de caso do iPhone. Revista e-xacta, v.4, n.3 (2011). <http://revistas.unibh.br/index.php/dcet/article/view/331/406>

CERT.br, Fascívulo segurança em dispositivos móveis, 2013. <http://cartilha.cert.br/fasciculos/dispositivos-moveis/fasciculo-dispositivos-moveis-slides.pdf>

Kai Qian, C.D.L.; Minzhe Guo, P.B.; Mobile Security Labware with Smart Devices for Cybersecurity Education in Integrated STEM Education Conference, 2012

Assis, L.; Brasil é o quarto país do mundo com maior nímero de smartphones. <http://www.ebc.com.br/tecnologia/galeria/audios/2013/08/brasil-e-o-quarto-pais-do-mundo-com-maior-numero-de-smartphones.>

Schmidt, E.; Google tem 1,5 milhões de Androids ativados por dia http://itweb.com.br/107044/google-tem-15-milhao-de-androids-ativados-por-dia.

Tabela 1 - Soluções para vulnerabilidades em dispositivos móveis

	Soluções					
Riscos Vulnerabilidades	Autenticação	Dados Encriptografados	Autenticação Multifator	One-Time Password	Autenticação fora da banda	Autenticaçãoe autorização de Bluetooth
Criptoanálise		x		x		
Clonagem de Dispositivos		x				
Escutas	x	x		x		
Falsificação de Conteúdo	x	x		x		
Autenticação Inadequada	x		x	x	x	
Dispositivos Perdidos		x				
Ataque ao Bluetooth		x				x

Tabela 2 – Soluções avançadas para vulnerabilidades em dispositivos móveis

	Soluções						
Risco e Vulnerabilidade	Elementos Seguros	Imagem Digital	Compartilhamento Secreto	*Poisonpill*	Rastreamento do Dispositivo	Memória Encriptografada	Validar Provedor de Serviço
Criptoanálise	x	x	x			x	
Clonagem de Dispositivos	x						x
Escutas	x	x	x				
Falsificação de Conteúdo	x	x	x				
Autenticação Inadequada	x		x				
Dispositivos Perdidos	x			x	x	x	x
Ataque ao Bluetooth		x	x		x		