Análise das Vulnerabilidades de Segurança em Aplicativos Android

André C. A. Cavalcante[1], **Levino M. Porto**[1]

[1]Faculdade do Gama – Universidade de Brasília (UNB)
Caixa Postal 72.444-210 – Gama – DF – Brasil

{andrelink14,levinomoises}@gmail.com

Abstract. *This article describes the main security techniques that can be applied on the development of new functionalities that can ensure the security of the data persisted in mobile devices that utilize the operational system Android. These techniques may be related to the system itself, as well as mobile applications*

Resumo. *Este artigo descreve as principais técnicas de segurança que podem ser aplicadas para o desenvolvimento de funcionalidades que protejam as informações presentes em dispositivos móveis com o sistema operacional Android. Essas técnicas podem estar relacionadas ao próprio sistema, como também a aplicações móveis.*

1. Introdução

Nos últimos anos, a sociedade tem presenciado o rápido aumento na utilização de *smartphones* em seu cotidiano. A evolução dos *smartphones* é constante, sempre oferecendo melhorias no desempenho, redes de acesso e integração com os usuário por meio de sensores [Suarez-Tangil et al. 2014]. Atualmente existem diversas opções de sistemas operacionais para *smartphones*, entre os principais destacam-se o Android OS[1] e o IOS[2]. No terceiro quadrimestre de 2013 o IDC[3] mostrou que dispositivos com Android OS representam aproximadamente 80% das vendas globais de *smartphones*, enquanto que os com IOS representam aproximadamente 13%.

Os *smartphones* proporcionam recursos ao usuário que superam uma simples ligação ou o envio de mensagens. Atividades frequentes como acesso a internet, comunicação com redes sociais e interação com conteúdos multimídia são oferecidas de forma intuitiva e prática pelos *smartphones*. Com a popularidade dos *smartphones* em ascensão, ataques maliciosos visando obter informações pertinentes ao usuário ou depreciar o dispositivo ocorrem com frequência [Banuri et al. 2012]. O Android OS é mais sensível a este tipo de ataque devido a fatores como domínio do mercado e distribuição de aplicativos através de repositórios não oficiais.

Neste contexto, o objetivo deste trabalho é identificar as vulnerabilidades presentes em aplicações Android que possam afetar a segurança das informações do usuário. As perguntas formuladas são: Quais são as principais vulnerabilidades presentes em

[1]Site oficial do Android OS: $http://www.android.com/$
[2]Site Oficial do IOS: $https://www.apple.com/br/ios/$
[3]Corporação de Dados Internacional $http://www.idc.com/$

aplicações Android? Quais as técnicas de seguranças utilizadas para mitigar as vulnerabilidades encontradas? O problema considerado é: como o tema é novo, diversas vulnerabilidades estão sendo exploradas, técnicas para evitá-las não acompanham essa curva de crescimento. Para alcançar estes objetivos será utilizada a técnica de revisão sistemática. O processo da revisão consiste das seguintes fases: planejamento da revisão (desenvolvimento do protocolo de revisão e sua validação), execução da revisão (identificação de estudos relevantes, seleção de estudos, avaliação da qualidade, extração e sintetização de informações) e avaliação dos resultados obtidos.

A aplicação da revisão sistemática servirá como insumo para a criação de um catálogo contendo as principais vulnerabilidades de segurança nas aplicações Android bem como possíveis formas de mitigá-las. Este catálogo servirá de apoio para o desenvolvimento de aplicações baseadas na plataforma Android.

Este trabalho está dividido em seções. Apresenta-se na Seção 2 uma contextualização sobre segurança na plataforma Android. Já na Seção 3, o processo de revisão sistemática utilizado é descrito. A Seção 4 consiste em apresentar aspectos relacionados ao planejamento realizado para a revisão sistemática. Logo a seguir, a Seção 5 apresenta aspectos relacionados com a condução da revisão sistemática. Na Seção 6, os resultados obtidos com a revisão são analisados. Para finalizar, na Seção 7 são apresentados as considerações finais e trabalhos futuros.

2. First Page

The first page must display the paper title, the name and address of the authors, the abstract in English and "resumo" in Portuguese ("resumos" are required only for papers written in Portuguese). The title must be centered over the whole page, in 16 point boldface font and with 12 points of space before itself. Author names must be centered in 12 point font, bold, all of them disposed in the same line, separated by commas and with 12 points of space after the title. Addresses must be centered in 12 point font, also with 12 points of space after the authors' names. E-mail addresses should be written using font Courier New, 10 point nominal size, with 6 points of space before and 6 points of space after.

The abstract and "resumo" (if is the case) must be in 12 point Times font, indented 0.8cm on both sides. The word **Abstract** and **Resumo**, should be written in boldface and must precede the text.

3. CD-ROMs and Printed Proceedings

In some conferences, the papers are published on CD-ROM while only the abstract is published in the printed Proceedings. In this case, authors are invited to prepare two final versions of the paper. One, complete, to be published on the CD and the other, containing only the first page, with abstract and "resumo" (for papers in Portuguese).

4. Sections and Paragraphs

Section titles must be in boldface, 13pt, flush left. There should be an extra 12 pt of space before each title. Section numbering is optional. The first paragraph of each section should not be indented, while the first lines of subsequent paragraphs should be indented by 1.27 cm.

4.1. Subsections

The subsection titles must be in boldface, 12pt, flush left.

5. Figures and Captions

Figure and table captions should be centered if less than one line (Figure 1), otherwise justified and indented by 0.8cm on both margins, as shown in Figure 2. The caption font must be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

Figure 1. A typical figure

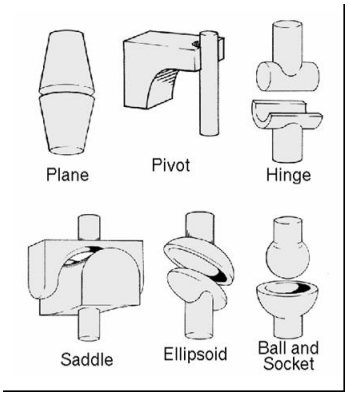

Figure 2. This figure is an example of a figure caption taking more than one line and justified considering margins mentioned in Section 5.

In tables, try to avoid the use of colored or shaded backgrounds, and avoid thick, doubled, or unnecessary framing lines. When reporting empirical data, do not use more decimal digits than warranted by their precision and reproducibility. Table caption must be placed before the table (see Table 1) and the font used must also be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

Table 1. Variables to be considered on the evaluation of interaction techniques

	Chessboard top view	Chessboard perspective view
Selection with side movements	6.02 ± 5.22	7.01±6.84
Selection with in-depth movements	6.29±4.99	12.22±11.33
Manipulation with side movements	4.66± 4.94	3.47±2.20
Manipulation with in-depth movements	5.71 ±4.55	5.37 ±3.28

6. Images

All images and illustrations should be in black-and-white, or gray tones, excepting for the papers that will be electronically available (on CD-ROMs, internet, etc.). The image resolution on paper should be about 600 dpi for black-and-white images, and 150-300 dpi for grayscale images. Do not include images with excessive resolution, as they may take hours to print, without any visible difference in the result.

7. References

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [Knuth 1984], [Boulic and Renault 1991], and [Smith and Jones 1999].

The references must be listed using 12 point font size, with 6 points of space before each reference. The first line of each reference should not be indented, while the subsequent should be indented by 0.5 cm.

References

Banuri, H., Alam, M., Khan, S., Manzoor, J., Ali, B., Khan, Y., Yaseen, M., Tahir, M. N., Ali, T., Alam, Q., and Zhang, X. (2012). An android runtime security policy enforcement framework. *Personal Ubiquitous Comput.*, 16(6):631–641.

Boulic, R. and Renault, O. (1991). 3d hierarchies for animation. In Magnenat-Thalmann, N. and Thalmann, D., editors, *New Trends in Animation and Visualization*. John Wiley & Sons ltd.

Knuth, D. E. (1984). *The TEX Book*. Addison-Wesley, 15th edition.

Smith, A. and Jones, B. (1999). On the complexity of computing. In Smith-Jones, A. B., editor, *Advances in Computer Science*, pages 555–566. Publishing Press.

Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., and Blasco, J. (2014). Dendroid: A text mining approach to analyzing and classifying code structures in android malware families. *Expert Syst. Appl.*, 41(4):1104–1117.