CRAB-Droid

AJ Arnold, Matthew Berthoud, Justin Cresent, Ada Rigsby

May 11, 2024

Abstract

Analyzing Android applications for correct security practices such as using permissions, using the SSL API, and potential interface vulnerabilities is a challenging task. This paper presents our tool CRAB-Droid, a python script that builds upon Androguard to carry out a static analysis to identify potential security vulnerabilities in Android applications. We analyzed 100 apps from the Google Play Store with the objective of identifying potential security vulnerabilities. We created 5 experiments to test on our 7 research questions we had outlined in the planning stage of our analysis. Our findings ... #TODO This project shows the significance of developers following best practices when creating Android apps, and the abilities to develop tools to help guide and educate engineers to them. Implementing tools like Androguard and CRAB-Droid to be used in the development process can help to identify potential security vulnerabilities before putting apps into deployment onto the app stores. This can help to save time, money, and most of all, user privacy.

1 Introduction

The Introduction includes references to highly-relevant related work, i.e., state of the art for the problem you are trying to solve.

Note: when writing LaTeX, each paragraph should have a line separated between it and the separate paragraph. This causes proper indentation and makes the document more readable. Do not end paragraphs with \\.

The remainder of this paper proceeds as follows. Section 2 overviews our sample paper. Section 3 describes the design of our sample paper. Section 4 evaluates our solution. Section 5 discusses additional topics. Section 6 describes related work. Section 7 concludes.

2 Methodology

Overview of Approach (a nice and accessible "English" description of your approach). Don't forget a niche high-level figure. Our sample high-level figure is shown in Figure 1.

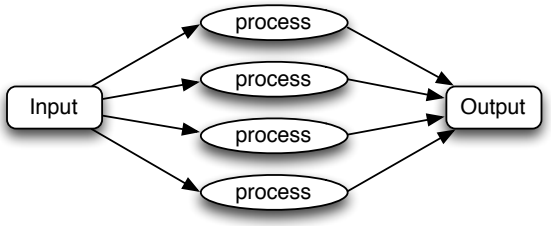

Figure 1: A high-level architecture of our approach

There is sometimes a background section before the overview section. In general, you want to try to get your high level figure somewhere between pages 2 and 4. It is generally bad to have a figure on the first page (but was unavoidable in this sample).

3 Experiments

1. Permissions Misuse Experiment:
2. Trust Managers and Error Handlers Experiment:
3. AllowAllHostnameVerifier Experiment:
4. Mixed use SSL Experiment:
5. addJavascriptInterface Experiment:

4 Evaluation

Evaluation (don't forget to interpret your data)

5 Results

Discussion (discuss some of the important simplifying assumptions, and suggest possibilities for future work)

6 Findings

Related Work ("somewhat related" work goes here; directly related work goes into the Introduction) [**?**].

7 Conclusion

Conclusions (don't summarize your work here. That's what the abstract was for. Instead provide some philosophical ruminations of your work and future possibilities, i.e., conclusions that you have arrived at as a result of your work.)

References

[1] Sebastian Bachmann Anthony Desnos, Geoffroy Gueguen. Androguard. https://github.com/androguard/androguard, 2018.

[2] Erika Chin, Adrienne Porter Felt, Kate Greenwood, and David Wagner. Analyzing inter-application communication in android. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, page 239–252, New York, NY, USA, 2011. Association for Computing Machinery. ISBN 9781450306430. doi: 10.1145/1999995.2000018. URL https://doi.org/10.1145/1999995.2000018.

[3] William Enck, Machigar Ongtang, and Patrick McDaniel. On lightweight mobile phone application certification. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, page 235–245, New York, NY, USA, 2009. Association for Computing Machinery. ISBN 9781605588940. doi: 10.1145/1653662.1653691. URL https://doi.org/10.1145/1653662.1653691.

[4] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. Why eve and mallory love android: an analysis of android ssl (in)security. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, page 50–61, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450316514. doi: 10.1145/2382196.2382205. URL https://doi.org/10.1145/2382196.2382205.

[4] [1] [2] [3]