XXXXX

Daniel E. Krutz, Hussein Talib and Samuel A. Malachowsky
Software Engineering Department
Rochester Institute of Technology
1 Lomb Memorial Drive
Rochester, NY, USA
{dxkvse,hat6622,samvse}@rit.edu

ABSTRACT

Categories and Subject Descriptors

K.X.X [**Computers and Education**]: XXXXX—*XXXXXX*

Keywords

XXXX, XXXX

1. INTRODUCTION

Android is the world's most popular mobile OS [2] with over 1.8 million apps available from Google Play alone [1]. Unfortunately, this popularity comes at a steep cost, since Android is the most frequent target of security related attacks, and whose apps routinely suffer from serious security vulnerabilities.These vulnerabilities can range from

small leaks insignificant data, to the user to....

[**?**]

[cite] Understanding proper protection methods, and defensive coding practices is paramount for any developer in creating apps which are secure and better protect the user's privacy [cite].

A primary driving factor of the mobile revolution is the fact that anyone with basic programming experience can create an app, upload it to their platform's app store, and have it used by millions. However, this is a double edge sword since inexperienced developers can make mistakes which can seriously impact the security of an app. In fact, even the most experienced mobile developers can make mistakes which hinder an app's security as well [cite].

In order to help address this shortfall for both abuse and misuse cases, we can created a publicly available, educational oracle of Android vulnerabilities. Each example contains the following:

1. A clear example of how to re-create the vulnerability.
2. A definition of why the vulnerability is detrimental to an app along with background about the issue.
3. Clear steps of how to repair the vulnerability.
4. Steps of how to demonstrate that the vulnerability has been successfully repaired.

Our goal for the project is for other instructors to use these activities in both their mobile and security related courses. Instructors may choose to use all components, or even only a single component in their course. Each example or module is independent of one another, and vary from basic vulnerabilities, to ones which are oriented to more advanced developers. Since each activity contains robust instructions for its use, individuals who are hoping to learn more about mobile development and security may use these activities as well.

2. ORACLE CREATION

3. CREATED VULNERABLE APPS

We currently have [XXX] apps in our oracle, although we expect this list to grow on a regular basis.

[**update & expand this list**]

1. **AdLibraries:** XXXX
2. **Android Javascript:** XXXX
3. **Broadcast:** XXXX
4. **Activities Access:** XXXX
5. **Content Providers:** XXXX
6. **Data Storage:** XXXX
7. **DataOverHTTP:** XXXX
8. **DOS: Denial of Service:** XXXX
9. **Intent** XXXX
10. **XML:** XXXX

3.1 Sample App: XXXX

In order to best demonstrate our set of vulnerable apps and how it may be best used, we will provide information on one of the apps created our oracle.

4. USAGE INSTRUCTIONS

5. FUTURE GROWTH

ACM ISBN 978-1-4503-2138-9.
DOI: 10.1145/1235

6. RELATED WORK

7. LIMITATIONS & FUTURE WORK

8. CONCLUSION

We have created a publicly available instruction set of vulnerable Android apps which includes 10 groups of vulnerabilities. Our goal is for instructors to use these activities in a diverse set of courses, and may be used by a diverse set of skill levels ranging from beginning level developers, to more advanced levels. All course material may be found on our project website: **XXXXX**

Acknowledgements

This work is partially sponsored by a SIGCSE Special Projects Grant.

9. REFERENCES

[1] Number of apps available in leading app stores as of november 2015. http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/.

[2] J. Edwards. iphone lost market share to android in every major market except one. http://www.businessinsider.com/apple-ios-v-android-market-share-2016-1?r=UK&IR=T, January 2016.