“Supporting Education Using a Public Oracle of Vulnerable Mobile Apps”

Daniel E. Krutz
Software Engineering Department
Rochester Institute of Technology
dxkvse@rit.edu

I would like to start this report by first thanking SIGCSE for giving me the opportunity to conduct this work.

Over the last several months, I worked with a graduate student, Hussein Talib, to create a set of vulnerable Android apps. Each vulnerability example contains:

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.

Although several more examples will be added in the next few weeks, we currently have the vulnerability examples:

1. **AdLibraries:** Ad library could use the permissions that given to the app which contains the Ads library, even the people did not give this permission to Ads library. This can open up various security and privacy issues within the app.
2. **Android Javascript:** This demonstrates the negative implications of using Javascript in Webview to pass data from an Android app to a server. This is considered bad practice because anyone could use malicious Javascript code on their website to gain private user information within the app.
3. **Broadcast:** Broadcast data sent by the app is easy to access by any app in the system, so when we do Broadcast to specific apps, we have to encrypt the data. Unencrypted data could be accessed by unintended apps, which could lead to serious security and privacy issues within the app.
4. **Activities Access:** Security issues arise when people try to access specific unauthorized activity. An example could be like in bank app, where users try to access a balance management activity without ever logging to the system.
5. **Content_Providers:** Content providers share data between apps, and any app in the system can access the Content_Providers database. This means that data stored here must be kept secure and encrypted so that it can only be read only from an authorized app.
6. **Data Storage:** When an app does not secure storage data like Files, Shared references, SQLite, it could be read very easy from anyone. This means that important information stored in these files like, such as a database connection, must also be encrypted.
7. **DataOverHTTP:** Data that moves over an HTTP connection which is not encrypted is vulnerable to Man in the Middle attacks. One example of this is credit card information. Information passed over an HTTP connection must be encrypted to remain secure from unintended listeners.

8. **DOS:** Denial of Service (DoS) attacks is a common problem with Android, because an adversary could create many HTTP requests going to a specific server. These requests must be managed to make them less vulnerable to these types of attacks.
9. **Intent:** Android uses Intents to pass data between apps. Examples include Facebook and Facebook Messenger. Passing data between these apps may be easily ready by hacker apps. This module explains how to protect information being sent via Intents between apps.
10. **XML:** XML is very easy to read using reverse engineering , so we have to avoid saving important information like Ads code, or Map Code

Each example contains a Word docx file which walks the user through the vulnerability, along with all relevant artifacts for the app and exercise. All project artifacts are located at: https://github.com/dan7800/VulnerableAndroidAppOracle

Based on this work, I will soon begin writing a full paper to be submitted to either SIGCSE, ITiCSE or ICER. I plan on concluding this paper by the end of the summer. I will also begin to hold free workshops for local students where they will work through several of the provided examples. I will especially focus in providing these sessions to underrepresented groups in computing, with a specific emphasis on encouraging young women to become active in computing. I've also begun to collaborate with instructors at other institutions who have already expressed great interest in using these activities in their classrooms.

Thank you very much for giving me this opportunity, and please let me know of any questions that you have.

-Daniel Krutz