A Future in Android Application Security with Jeffrey Walley

[JeffreyWalley@student.bpcc.edu](mailto:JeffreyWalley@student.bpcc.edu)

My name is Jeffrey Walley and I am interested in a future in the field of Android Application Security. One of my good friends, Jack, has been working for Bank of America for nearly 20 years in network, and now application security; he has been pushing me towards changing fields and I have finally taken the first steps. I have taken two Java Programming boot camps, they were both Tech Talent South programs, offered through the City of Shreveport. I learned about code development and worked with creating a Node Express MERN stack (MySQL, Express, React, Node) and later a Linux Web LAMP stack server (Linux, Apache, MySQL, PHP). This all made me very interested in learning more about networking and security.

I will need to be comfortable with Java, once the premier language for coding Android applications, because Java still has a strong footprint in Android application development1. In recent years, Kotlin has become the preferred language for many programmers developing applications for Android. Kotlin is a more “concise and secure” language than Java. Many coders find Kotlin has easier syntax than Java and is more secure. In 2019 Kotlin was declared one of Android’s Official languages1.

Python is another language that is very popular in all aspects of coding these days and creating Android applications is no different. Python has become a go to language for building apps, using the “Kivy” library. It is possible to build Android applications with Python, though some developers frown upon it and suggest writing code in Kotlin or Java which are the recommended Android languages1.

While researching I came across a list of many common tools for Android Security Testing, most I don’t understand yet My goal in the next 2 years is to nurture a strong working knowledge of all the tools of the trade. One program, AndroGuard, seemed very popular. AndroGuard is an open-source and well maintained reverse-engineering tool written in Python. The program gives users multiple ways to manipulate the DEX file of Android Applications. It can also check code and diagnose the application for malware2.

The reverse-engineering program, APKTool, seems extremely powerful and I am interested in trying it out someday. You can take a 3rd Party Android application and put it through the APKTool and it will analyze the app, crack it open, then convert the application to it’s near original form. The user can then rebuild the app with custom modifications making reverse-engineering simple and painless. The program will also streamline and remove redundant actions that are involved in the reverse-engineering process2.

Another powerful tool I read about for Android application security is DevKnox, which works well inside the Android Studio IDE (Integrated Development Environment). DevKnox is a tool that assists programmers with improving code by auto-correcting various established security flaws directly in the IDE. This actually brings me to the last major “tool” that I will use, Android Studio2. Android Studio is the official IDE for Android application development. It was created by Google and JetBrains and is based on the JetBrains IDEA platform, but customized for Android3. I have some experience with JetBrains IntelliJ Java IDE, so I am very interested to see if Android Studio will be familiar.

To advance in many Applied Science fields it is important to have certifications and Bossier Parish Community College offers a variety of courses that pair with CompTIA certifications. I am hoping to achieve a voucher for the test for the CompTIA A+ certification from the CTEC-101 course I am enrolled in. I will be working my way towards the Security+, CASP+, and PenTest+ certifications and will work hard to achieve my goals4.

I have quite a lot of studying and reading to do before I am ready for the career that I have chosen, but I believe I made the correct first step by re-enrolling in school and taking these Cyber Security courses. I will continue to further my studies learning Kotlin and successfully developing some applications. The ability to teach myself will be crucial in continuing my education and I will use tools such as Udemy, EdX, and through the official Android coding tutorials3. While reading I also kept coming across the concept of using Virtual Machines for testing an application’s security flaws. I do have VMWare Workstation Pro, but have never used it. I will need to work with that program and get some experience with Virtual Machines5. Another field I am interested in, but have relatively no knowledge of, is the use of Docker, and Dockers. These seem to be deployed applications that are encapsulated with all the dependencies they will need to run on any machine. The benefit is that you can deploy applications in their own contained environment for stability, plus they require very little physical or memory resources due to their small size6.

Sources:

1. <https://techvidvan.com/tutorials/best-programming-languages-for-android-app-development/>

2. https://techbeacon.com/app-dev-testing/16-tools-bulletproof-android-app-security

3. <https://developer.android.com/studio/intro>

4. <https://www.comptia.org/certifications>

5. <https://www.vmware.com/products/workstation-pro.html>

6. https://www.docker.com/