An Empirical Study of the Robustness of Google Play Store Applications Using Fuzzing Techniques

Kiran Chandrapaul[1], Harrison Fernandez[1], Aleksey Kravtsov[1], and Mevin Thomas[1]
John Jay College of Criminal Justice (CUNY), New York, NY.
[1] firstname.lastname@jjay.cuny.edu

Introduction

What is fuzzing?

- Automated input of invalid/random data to find bugs, i.e. crashes, ANR messages, or unauthorized access.

Why is it important?

- Android powers 80% devices worldwide [5].
- Mobile devices are heavily trusted to hold personal information: emails, banking, web browsing. If these are susceptible to fuzzing, the application should not be trusted.

Why Intent Fuzzing?

- An intent is simply a message to transfer data from one activity to another. Random intent fuzzers such as DoApp [2] are useful for the discovery of software bugs.

Research Question

How robust* are Google Play store applications?

*Robustness referring to the ability of the app to handle errors during execution, including invalid or unexpected input.

Artifact Collection

- Top 100 Google Play Store apps as of 10/9/18
- Average rating: 4.7/5
- 1 million to 500 million+ downloads across apps

Experimental Setup

- NOX App Player [4] - Virtual machine used to test applications
- ADB [1] - Android Debug Bridge, used to hook into VM and run Logcat.
- Logcat [1] - ADB module for logging android operating system.
- DoApp [2] - Application that scans for intents in target application, dynamically analyze target application for execution paths.

Results

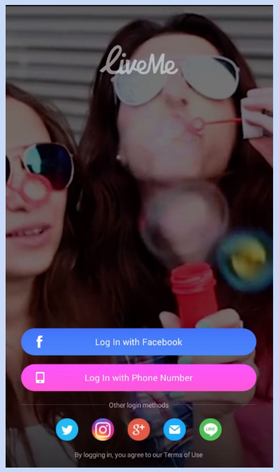

Figure 1A. LiveMe Default Login Screen, Requires User Authentication

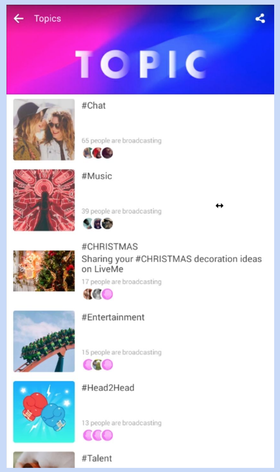

Figure 1B. LiveMe Fuzzing Intent allows attacker to bypass authentication.

- Out of the top 100 apps, only 61 apps were able to be tested. Out of these, 17 apps were found to have software bugs.
- Bugs vary across all categories of apps.
- All apps are rated 4.0 or greater.
- Out of 17 apps that were not robust, 12 apps crashed where input could not be handled. The remaining 5 apps could be exploited to bypass different forms of authentication including email, and phone number.

```
android.content.ActivityNotFoundException: Unable to find explicit activity class
{com.snapchat.android/com.snap.mushroom.MainActivity}; have you declared this activity in
your AndroidManifest.xml?
```

Figure 1C. SnapChat - Example of a crash.

Conclusion

We find that most Google Play Store apps are robust as only 17/61 were found to have bugs.

Future Work

- Use of latest Android Operating System.
- Test fuzzers on physical devices.
- Analysis of the relationship between software bugs and developer's access to capital.
- Further experimentation consisting of more applications, fuzz testers, and emulators.

Acknowledgements

- Mathematics and Computer Science Department
- Professor Sven Dietrich
- CSCI 400 Peers
- John Jay College of Criminal Justice (CUNY)

References

1. Android website: https://www.android.com/
2. DoApp Android Fuzzer: https://github.com/lmartire/DoApp
3. Google Play Store: https://play.google.com/store/
4. Nox Android Emulator: https://downloadnox.onl/
5. S. Kovach, "How Android Grew to be More Popular Than the Iphone," Business Insider, 2013.