SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Android 用ファジングツールの適用及びその性能評価
Application of fuzzing tool for Android and its performance evaluation

佐久間耀大朗* 高橋寿一† 加藤雅彦*
Yotaro Sakuma Juichi Takahashi Masahiko Kato

キーワード Android, ファジング, ソフトウェアテスト

あらまし

現在，世界規模で Android が広く普及し，2018 年時点では約320万を超える数のAndroidアプリケーションが作成されている．それに伴いスマートフォンアプリ向けテストツールも開発されており，アプリを自動操作してテストするものなどがある．また，ツールを使用せずに，多数の人員を用いてアプリを操作し，しらみつぶしにバグを見つける方法もある．それらのツールや方法を用いる際は，ボタン等をタップしたときの反応や画面遷移など，アプリが想定通りに動作するかが重要視され，入力値を重要視することは少ない．そのため，入力欄を持つ全ての Android アプリに適用でき，さらに入力値に着目して従来のテストツールでは発見できなかったバグを見つけられるテスト方法が必要である．

本論文では，上記の課題を解決するためにファジングを用いた Android アプリのテスト方法を提案する．提案手法としては，既存のツールを用いて予測不可能な入力データ(ファズ)を生成し，生成したファズを検査対象アプリに自動入力することでエラーの有無の確認を行う．提案手法の全体像を図 1 に示す．

ファズの生成には JQF を利用する．生成するファズは，検査対象アプリによって数字や，文字列と数字を組み合わせたものなど，種類を変えることが可能である．生成したファズはファイルとして保存し，本研究で新たに作成したファジングツールで読み込みを行う．読み込んだデータは，実機のスマートフォンを PC 経由で自動操作することが出来るソフトウェアである Appium を用いて，検査対象アプリへ自動入力を行う．

* 長崎県立大学 〒851-2195 長崎県西彼杵郡長与町まなび野 1-1-1.
University of Nagasaki, 1-1-1, Manabino, Nagayotyo, Nisisonogigunn, Nagasaki, 851-2195, Japan
† 株式会社ロジギアジャパン 〒151-0061 東京都渋谷区初台 1-51-1 初台センタービル 407
LOGIGEAR JAPAN CORPORATION, 1-51-1 Hatsudai, Shibuya-ku, Tokyo, 151-0061, Japan Hatsudai Center Building 407

次に評価として，以下のアプリを用いて動作検証を行う．

- 数値の入力欄を持つ，脆弱性を仕込んだアプリ
- 標準インストールされている Gmail アプリ
- 設定アプリの Wi-Fi 検索機能

検証環境として，Android スマートフォンが接続された PC を用意し，それぞれ次の項目に対してファジングを行う．値の自動入力が出来るか，エラーを検知するかを検証する．

- 脆弱性を仕込んだアプリの数値入力欄
- Gmail の新規メール作成画面の件名と本文
- Wi-Fi 設定の SSID 入力欄

その結果，脆弱性を仕込んだアプリは想定した通りにエラーを起こし，エラー内容やエラー発生時の入力値が確認できた．また Gmail アプリと設定アプリの Wi-Fi 検索機能の検証でも，値が自動入力されたが，エラーは発生しなかった．また，1 項目あたりの入力時間は 2 秒から 3 秒程度を要した．

検証結果から，自動入力の速度が遅いという点と，よりバグを発見しやすくするためにファズの質を上げる必要があるという課題が得られた．速度の解決策として今後は，テスト用端末を複数用意し，自動入力を並列化して行うことを検討する．加えて，生成するファズの質を向上させるために，ファジングツールを複数種類用いるなどにより，より高精度のファズを生成できることを目指す．

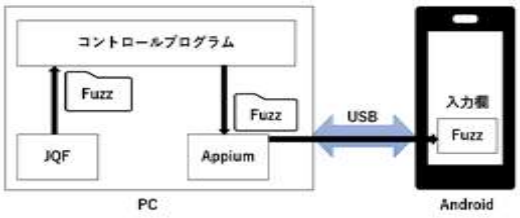

図 1 提案手法の全体像