IPA

2019 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当 PM

首藤 一幸（東京工業大学 情報理工学院 准教授）

2. クリエータ氏名

大塚 馨（早稲田大学高等学院）

3. 委託金支払額

2,304,000 円

4. テーマ名

プロセッサトレースを用いた組み込みデバイス向けファザーの開発

5. 関連 Web サイト

検出バグ情報：https://github.com/roppinhoppin/kernel_crashes

6. テーマ概要

ファザー（fuzzer）という、ソフトウェアをテストするソフトウェアを開発する。ファザーは、脆弱性の発見に力を発揮する。開発するファザーの特徴は、ARM プロセッサをターゲットとすること、ソースコードなしでバイナリを扱えること、また、OS のカーネルも扱えること、である。この 3 つの特徴を満たすと、iPhone の OS である iOS や、Android 端末の OS である Android を対象としたテストが可能となる。

7. 採択理由

プログラムのバグやセキュリティ的な問題を発見するツール、ファザー（fuzzer）を開発する。スマートフォンなどの組み込み機器で非常に多く使われている ARM プロセッサを対象とする。開発目標は、対象のソースコードなしでも適用できること、OS に依存しないこと、OS 自体（カーネル）も対象とできること、高速であること、また、カバレッジベースゆえより広範なバグを発見し得ること、である。

2015 年、スマホの OS Android に深刻なバグ Stagefright が見つかり、ある

企業は数カ月間 Android を使用禁止とした。こうしたことが起きているにも関わらず、いまだに ARM プロセッサ上の Android を対象にできるファザーは入手可能となっていない。大塚君がこの状況に一石を投じてくれると確信して採択した。

8. 開発目標

上記のファザーを開発する。さらには、それを使って、iOS や Android の脆弱性を発見する。

9. 進捗概要

ファザーを開発し切った。ただし、目標とするファザーが必要とする機能を備えた ARM マシンがとうとう手に入らなかったため、ARM マシンをソフトウェア（QEMU）でエミュレートしている。必要な機能を備えた ARM マシンが手に入り次第、ソフトウェアエミュレーションではなくハードウェアで高速にテストできるようになる。

開発したファザーを用いて、9 日間で Linux カーネル 4.4.0 を数十万通りの入力でハングアップさせることができた。そのうち 1 万通りの入力はクラッシュを発生させた。これらのクラッシュは 69 個の異なる基本ブロックが引き起こしている。つまり、69 個のバグを発見できた。

今後、これらのバグを辿ることで Android の脆弱性を発見できる可能性がある。ただ、Linux カーネルのバグを Android の脆弱性へと結びつけていく作業は手作業であり、かなりの労力を要する。また、ハードウェア上でのテストが可能となれば、より多くのバグを素早く発見できるようになる。

10. プロジェクト評価

必要なハードウェアがほとんど存在せず、結局手に入らないという逆境も自分の腕で乗り越えて、大変高度なソフトウェアを作り上げた。ARM プロセッサ上の OS カーネル、具体例としては Android の脆弱性発見が、従来より桁違いに効率的になった。その意味で、社会的なインパクトもとても大きい。

11. 今後の課題

- （ハードウェアが利用可能になり次第、）ハードウェア対応
- Android の脆弱性発見
- iOS の脆弱性発見