

μ SE: Mutation-based Evaluation of Security-focused Static Analysis Tools for Android

Amit Seal Ami, Kaushal Kafle, Adwait Nadkarni, Denys Poshyvanyk

Computer Science Department

College of William & Mary

Williamsburg, VA, USA

{aami@email., kkafle@email., apnadkarni@, denys@cs.}wm.edu

Kevin Moran

Computer Science Department

George Mason University

Fairfax, VA, USA

kpmoran@gmu.edu

Abstract—This demo paper presents the technical details and usage scenarios of μ SE: a mutation-based tool for evaluating security-focused static analysis tools for Android. Mutation testing is generally used by software practitioners to assess the robustness of a given test-suite. However, we leverage this technique to systematically evaluate static analysis tools and uncover and document soundness issues. μ SE’s analysis has found 25 previously undocumented flaws in static data leak detection tools for Android. μ SE offers four mutation schemes, namely Reachability, Complex-reachability, TaintSink, and ScopeSink, which determine the locations of seeded mutants. Furthermore, the user can extend μ SE by customizing the API calls targeted by the mutation analysis. μ SE is also practical, as it makes use of filtering techniques based on compilation and execution criteria that reduces the number of ineffective mutations.

Website: <https://muse-security-evaluation.github.io>

Video URL: <https://youtu.be/Kfkzi57gYys>

Index Terms—Security, Software, Java, Testing strategies, Security and privacy

I. INTRODUCTION

Software practitioners use different analysis tools from both academia and industry in order to guarantee a variety of security-related application properties, such as compliance, assurance, and safety. Static analysis tools, also known as Static Application Security Testing (SAST) tools are often favored due to their provided soundness guarantees and performance, as dynamic analysis tools can suffer from issues such as state explosion or succumb to techniques for evading detection.

Because of the importance and impact of these SASTs, they are often evaluated by using custom benchmarks [1], [2]. By measuring precision and recall of detected security-related issues, the practicality and soundness of SASTs can be estimated. However, such custom curated benchmarks may not represent the diverse programming habits of developers. Furthermore, due to the evolving nature of APIs and frameworks, such benchmarks quickly become obsolete due to new practices and considerations. Unintentional introduction of unsound design/implementation choices further jeopardizes the security guarantees offered by such tools by making them *soundy* in practice. That is, these tools may make unsound design assumptions, either knowingly or unknowingly, that can impact the accuracy of their analyses. Given the importance of

SASTs in modern development workflows, there is a need for automated techniques that can help to uncover and document potential unsound properties that affect SAST efficacy.

In this paper, we describe μ SE (pronounced as “muse”), a mutation-based tool for evaluating security-focused static analysis tools for the Android platform. μ SE seeds mutants into applications that are analyzed by static analysis tools. Then, the tools are run on the mutated applications, and any undetected mutants are analyzed to uncover flaws in the tools. In μ SE, we define *security operators* based on security goals, instead of tool-specific properties (e.g., unwanted behaviors). As a result, entire classes of tools can be analyzed using the same security operator(s). The effectiveness of these operators in finding unsound assumptions is enhanced through the introduction of *mutation schemes* – strategies that define *where* to apply security operators to seed mutants in applications.

μ SE is implemented using Java and uses the Eclipse Abstract Syntax Tree (AST) framework to inject mutations. To reduce manual effort, it applies several techniques such as checking the syntax of security operators to add necessary *try-catch* blocks and removing mutations that might lead to compilation issues. An optional execution engine can be used with μ SE (e.g., based on CrashScope [3], [4]) that helps to filter non-executable mutations specifically in Android apps. The source code of μ SE and its documentation are publicly available [5]. The full details of μ SE are available in research papers [6]. This paper makes the following contributions:

- We provide a description of techniques that underlie μ SE, a tool used for evaluating security-focused static analysis tools (SASTs) for Android [6];
- We discuss how μ SE can be used in practice;
- We describe experiments on existing SASTs for data leak detection to find previously undocumented soundness issues in tools;
- We provide an open-source version of μ SE complete with documentation [5].

II. μ SE: MUTATION BASED SOUNDNESS EVALUATION

We provide an overview of the design of μ SE in Fig. 1. The specifications related to security operators and choice of mutation scheme strategy are provided through the configuration file. Furthermore, relevant properties, such as a

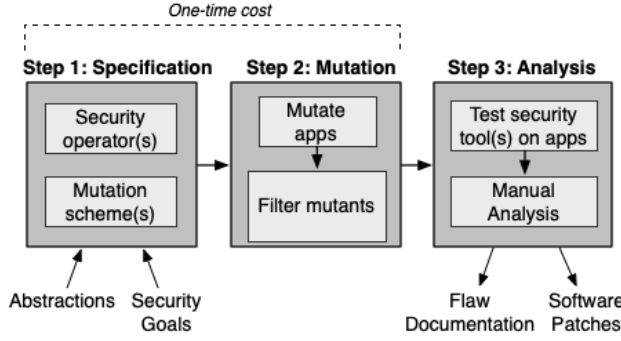


Fig. 1. The components and process of the μ SE.

software system to mutate and output paths are required to be provided. Once these are specified, μ SE starts by analyzing the given project to identify the application Java source files while creating a model based on the Eclipse AST framework. Based on the selected mutation scheme, μ SE identifies locations where security operators can be injected. When all these locations are identified, the security operators are introduced. Mutations are inserted and checked for syntax issues through *Java Compiler Diagnostics* to kill error-prone mutations preemptively. Furthermore, the mutated applications can optionally be executed by an execution engine to filter source-sink type mutations which may not result in data leaks. The analysis of SASTs is done manually by applying them to detect mutants. Logs of results from tool analysis and inserted mutations are then compared to understand what mutations were not detected by the SASTs. Finally, undetected mutations are analyzed to determine soundness issues in SASTs.

A. Security Operators

```

Inject:
String dl##
= java.util.Calendar.getInstance().getTimeZone().
  getDisplayName();
android.util.Log.d("leak-##", dl##);

```

Listing 1. Security operator that injects a data leak from the Calendar API to the device log

Security Operators (SO) are manifestations of unwanted behaviors with respect to a security goal. For example, in a data leak detection tool, a security operator defines a source of sensitive information, such as IMEI or location, which is exported to a public sink, such as a device log or storage. As a result, the same operator can be used for all the data leak detectors (e.g. FlowDroid, HornDroid, and BlueSeal [7]–[9]). We use the Calendar and Log APIs as example of sensitive data source and sink respectively throughout this document (Listing 1). Similarly, a security operator can be defined for evaluating SASTs that detect vulnerable SSL use, or crypto API misuse as well. μ SE makes this process easier by allowing the user to define custom security operators where the user needs to specify the API of source and sink as well as the variable name to be used through a configuration file.

B. Mutation Schemes

Mutation schemes define *where* to apply or introduce security operators within applications. μ SE can be used to choose

```

String dl0 =
    java.util.Calendar.getInstance().getTimeZone().
        getDisplayName();
String[] lr0 = new String[] {"n/a", dl0};
String dlp0 = lr0[lr0.length - 1];
android.util.Log.d("leak-0", dlp0);

```

Listing 2. Complex Path Operator Placement

```

public class ParentClass {
    String dl = "";
    int methodA() {
        android.util.Log.d("leak-0-1", dl);
        return 1; }
    class ChildClass {
        int childMethodA() {
            dl = java.util.Calendar.getInstance().
                getTimeZone().
                getDisplayName();
            android.util.Log.d("leak-0-0", dl);
            return 1; } }
}

```

Listing 3. ScopeSink scheme based operator placement at different levels of inheritance

one of four pre-defined mutation schemes each of which serves a different goal.

1) *Reachability Mutation Scheme*: The reachability mutation scheme is a simple and important mutation scheme that is used for evaluating the reachability of SASTs. The reachability scheme creates mutants by injecting security operators at every reachable location, such as methods, anonymous inner class object declarations, and class level declarations. Because of the evolving nature of APIs and frameworks, such as newly introduced lifecycle callbacks in Android frameworks as well as interfaces and abstractions, this approach is necessary to evaluate reachability.

2) *Complex-Reachability Mutation Scheme*: SASTs often improve runtime by preventing analysis after an arbitrary number of hops in a program call graph. The complex reachability mutation scheme makes the path from source to sink complex by inserting pre-defined hops in between source and sink. For our implementation of μ SE, we defined the complex-reachability for String variable that stores sensitive information as shown in Listing 2. To introduce complexity, it then converts it to a String Array with garbage value *StringBuilder*, which is converted back to a String with the sensitive value. The sensitive information is then leaked to a public sink.

3) *TaintSink Mutation Scheme*: The TaintSink mutation scheme aids in evaluating asynchronous actions in SASTs by placing the source and sink in different locations that are called asynchronously. For example, in Android applications, *onStart()* is always called before *onResume()* lifecycle method. This can be exploited by a malicious entity that collects and stores sensitive information in a variable in *onStart()*, and then leaks it in the *onResume()* callback.

4) *ScopeSink Mutation Scheme*: The ScopeSink mutation scheme takes the concept of a visibility scope from object oriented principles into consideration when seeding mutants. As shown in Listing 3, μ SE analyzes the visibility scope and determines that *childMethodA* is visible from both

ChildClass and ParentClass. As a result, it creates a variable at ParentClass - making it visible to both ParentClass and ChildClass. Next, sensitive information is stored in the variable childMethodA. Because this variable dl is visible in both childMethodA in ChildClass and methodA in ParentClass, it is leaked in both locations.

C. Syntax Requirements Checker

A user may define custom sources and sinks using μ SE while specifying the fully qualified name of relevant APIs. However, some APIs also require fulfilling syntax requirements to be used properly which the user may not be aware of or simply does not want to be concerned about. For example, accessing system storage requires the relevant functions to be placed within try-catch blocks as the methods throw an exception in case of uncommon situations. To handle this, method invocations used in both source and sink, including the method chains, are checked and put inside try-catch blocks as required.

D. Filtering Mutants

The number of mutants can grow quickly depending on project size. This leads to two potential issues: placing mutations in locations that result in compilation errors and placing source and sinks in locations that are never actually executed by a given application. As a result, the analysis of μ SE's mutants becomes more difficult if mutations are not filtered. We discuss two filtering techniques to reduce the number of mutations to further facilitate the analysis. The first, compilability-based filter, is built-in to μ SE, whereas the latter can be achieved through an external tool such as CrashScope [3], [4].

1) *Compilability of Mutations*: As explained in Section II-C, some API calls may require placement inside try-catch blocks in order to fulfill syntax requirements. However, this means that such API calls enclosed in try-catch block will result in compilation issues if these are placed in class declaration locations (i.e. outside any method), even though API calls that do not require such try-catch blocks to be placed at those same locations. To handle this, and other similar corner-cases, we leverage the javax.tools.JavaCompiler API from the Java Development Kit (JDK) to check for compilation issues on a per case basis. This helps remove mutations which may result in compilation issues for most, if not all, corner cases.

2) *Executability of Mutants*: Because the TaintSink mutation scheme distributes sources and sinks across method calls, it may result in having mutations that are compilable but that may not lie upon an executable program path when the mutated program is run. For example, if the source is placed in onResume method and sink in onStart method, these could not be feasibly executed in sequence during runtime. Tools that explore as many states of a given app as possible, such as CrashScope, can be used as an execution engine to explore mutant executability. By processing those results, mutations that are not executable can be removed.

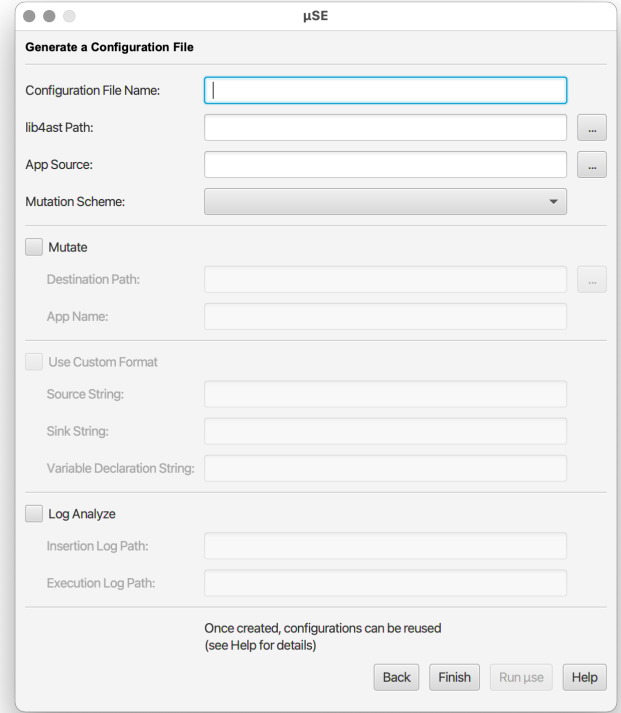


Fig. 2. Screenshot of μ SE - Creating New Configuration File

```
lib4ast: libs4ast/
appSrc: /tmp/AppFoo/src/
appName: AppFoo
output: /tmp/mutants/
operatorType: SCOPESINK
//optional customization
varDec: Type var%d = "";
source: var%d = api.method_value()
sink: api.method("value_%d-used_%d: " + var%d.toString())
```

Listing 4. Sample Configuration File for μ SE

III. USAGE

μ SE can be used through both a Command Line Interface (CLI) and a Graphical User Interface (GUI). This allows μ SE to be used as both standalone software as well as a component of other software. μ SE relies on Java LTS 11.0 for compilation and runtime. In addition, the GUI depends on OpenJFX version 11.0.2. Furthermore, a JAVA_HOME is required to be declared as an environment variable as it is required for checking compilation issues. To get started with mutation either through CLI or GUI, a configuration file (Listing 4) is required which specifies:

- **lib4ast path** - contains definition libraries required for AST, such as android.jar
- **Mutation Scheme** - Choice of mutation scheme, currently available choices are Reachability, Complex-Reachability, TaintSink, and ScopeSink
- **App source Location** - Path of project that is to be mutated

```
java -jar muse.jar configuration.properties
```

Listing 5. Sample usage of μ SE CLI

```
In file: BMIMain.java
Mutation Scheme: TAINTSINK
mutation-3-0: BMIMain.onCreate
mutation-2-0: BMIMain.onCreate
mutation-1-0: BMIMain.onCreate
mutation-0-0: BMIMain.onCreate
...
```

Listing 6. Example Output from μ SE

- **Destination Path** - Path where mutated project will be saved
- **App Name** - Name of the project

By default, μ SE uses `java.util.Calendar`, and `android.util.Log` APIs for creating source and sink related calls. However, this can be customized by the user by specifying the variable format and involved APIs in a configuration file as shown in Listing 4. Because of the configuration file, using μ SE is simple. Only the path to the configuration file is required as a parameter for the CLI as shown in Listing 5. Alternatively, the user can use the GUI as shown in Fig. 2 which will walk the user through different configuration settings, helping the user to save/load a configuration file for use. When μ SE is executed, it creates mutants while creating logs as shown in Listing 6. Finally, the mutants are analyzed by SASTs, the results of which are analyzed with the μ SE’s log as reference to identify undetected mutants for finding flaws.

IV. EVALUATION

We used μ SE to evaluate FlowDroid [7], a static analysis based data leak detection tool (full details are available in [6]) by mutating open-source Android apps. For this, we defined a security operator that represents a data leak by collecting information related to Location and leaking it to an insecure Sink. By systematically analyzing the results, we were able to find 13 previously documented flaws. For example, we found that Android Fragments [10] were incorrectly modeled in FlowDroid v2.0, and the tool could not trace data leaks in Fragments. Furthermore, FlowDroid missed the `onCreate` callback of classes extending `Android SQLiteOpenHelper`. Then, we studied additional tools, namely BlueSeal [8], IccTA [11], HornDroid [9], Argus (also known as AmanDroid [12]), DroidSafe [13], and DidFail [14] to find whether the soundness issues of FlowDroid also exists for these tools. We found that these flaws propagated to tools that were based on FlowDroid. Furthermore, at least one of each of the FlowDroid soundness issues is applicable to each of these tools. We later studied HornDroid and Argus using similar methodology while increasing the number of base apps for mutation (submission currently under minor acceptance review) and found 12 additional, previously undocumented flaws. All of these flaws were communicated with the authors

of these tools. This demonstrates that μ SE can be used to evaluate a family of Android focused SASTs for finding soundness issues. These flaws were discoverable because of the combination of mutation augmented by the diverse practices adopted by app development practitioners.

V. CONCLUSION

In this paper, we discussed the technical approach, implementation, and usage details of the mutation based soundness evaluation framework, namely μ SE. Our approach helps detect previously undocumented soundness issues in Android focused SASTs [6] by leveraging mutation testing techniques while assimilating the diversity of real, open-source applications. As a result, developers of static analysis tools can improve soundness by applying techniques demonstrated by μ SE.

ACKNOWLEDGMENT

The authors acknowledge the contributions from Richard Bonett for building the initial version of μ SE, and from the following undergraduate students from William & Mary: Liz Weech, Yang Zhang, John Clapham, Kevin Cortright, Nicholas di Mauro, Michael Foster, Pablo Solano, Phillip Watkins, Ian Wolff, Scott Murphy, Kyle Gorham, Will Elliott & Jeff Petit-Freres for improving μ SE.

REFERENCES

- [1] “ICC-Bench,” <https://github.com/fgwei/ICC-Bench> last accessed on June 27, 2020.
- [2] “DroidBench 2.0,” <https://github.com/secure-software-engineering/DroidBench> last accessed on June 27, 2020.
- [3] K. Moran, M. L. Vásquez, C. Bernal-Cárdenas, C. Vendome, and D. Poshyvanyk, “Automatically discovering, reporting and reproducing android application crashes,” in *ICST’16*, 2016, pp. 33–44.
- [4] K. Moran, M. Linares-Vasquez, C. Bernal-Cardenas, C. Vendome, and D. Poshyvanyk, “Crashscope: A practical tool for automated testing of android applications,” in *ICSE’17-C*, May 2017, pp. 15–18.
- [5] μ SE Developers. (2020, Nov) μ SE sources and data. [Online]. Available: <https://muse-security-evaluation.github.io>
- [6] A. S. Ami, K. Kafle, K. Moran, A. Nadkarni, and D. Poshyvanyk, “Systematic mutation-based evaluation of the soundness of security-focused android static analysis techniques,” *ACM Transactions on Privacy and Security*, vol. 24, no. 3, Feb. 2021. [Online]. Available: <https://doi.org/10.1145/3439802>
- [7] L. Qiu, Y. Wang, and J. Rubin, “Analyzing the analyzers: FlowDroid/IccTA, AmanDroid, and DroidSafe,” in *ISSTA’18*. Amsterdam, Netherlands: ACM Press, pp. 176–186.
- [8] F. Shen, N. Vishnubhotla, C. Todarka, M. Arora, B. Dhandapani, S. Y. Ko, and L. Ziarek, “Information Flows as a Permission Mechanism,” in *ASE’14*.
- [9] S. Calzavara, I. Grishchenko, and M. Maffei, “HornDroid: Practical and Sound Static Analysis of Android Applications by SMT Solving,” in *EuroS&P’16*, March, pp. 47–62.
- [10] Android Developers, “Fragments,” <https://developer.android.com/guide/components/fragments.html>
- [11] L. Li, A. Bartel, T. F. Bissyandé, J. Klein, Y. Le Traon, S. Arzt, S. Rasthofer, E. Bodden, D. Outeau, and P. McDaniel, “IccTA: Detecting inter-component privacy leaks in android apps,” in *ICSE’15*, pp. 280–291.
- [12] X. O. Fengguo Wei, Sankardas Roy and Robby, “Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps,” in *CCS’14*, Nov.
- [13] M. I. Gordon, D. Kim, J. Perkins, L. Gilham, N. Nguyen, and M. Rinard, “Information Flow Analysis of Android Applications in DroidSafe,” in *NDSS’15*, Feb.
- [14] W. Klieber, L. Flynn, A. Bhosale, L. Jia, and L. Bauer, “Android Taint Flow Analysis for App Sets,” in *SOAP’14*, pp. 1–6.