

# CRYPTOGERD: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects

Sazzadur Rahaman<sup>1</sup>, Ya Xiao<sup>1</sup>, Sharmin Afrose<sup>1</sup>, Fahad Shaon<sup>2</sup>, Ke Tian<sup>1</sup>, Miles Frantz<sup>1</sup>, Danfeng (Daphne) Yao<sup>1</sup>, Murat Kantarcioglu<sup>2</sup>

<sup>1</sup>Computer Science, Virginia Tech, Blacksburg, VA

<sup>2</sup>Computer Science, University of Texas at Dallas, Dallas, TX

{sazzad14,yax99,sharminaafrose,ketian,frantzme,danfeng}@vt.edu,{Fahad.Shaon,muratk}@utdallas.edu

## ABSTRACT

Cryptographic API misuses, such as exposed secrets, predictable random numbers, and vulnerable certificate verification, seriously threaten software security. The vision of automatically screening cryptographic API calls in massive-sized (e.g., millions of LoC) Java programs is not new. However, hindered by the practical difficulty of reducing false positives without compromising analysis quality, this goal has not been accomplished. State-of-the-art crypto API screening solutions are not designed to operate on a large scale.

Our technical innovation is a set of fast and highly accurate slicing algorithms. Our algorithms refine program slices by identifying language-specific irrelevant elements. The refinements reduce false alerts by 76% to 80% in our experiments. Running our tool, CRYPTOGERD, on 46 high-impact large-scale Apache projects and 6,181 Android apps generate many security insights. Our findings helped multiple popular Apache projects to harden their code, including Spark, Ranger, and Ofbiz. We also have made substantial progress towards the science of analysis in this space, including: *i*) manually analyzing 1,295 Apache alerts and confirming 1,277 true positives (98.61% precision), *ii*) creating a benchmark with 38-unit basic cases and 74-unit advanced cases, *iii*) performing an in-depth comparison with leading solutions including CrySL, SpotBugs, and Coverity. We are in the process of integrating CRYPTOGERD with the Software Assurance Marketplace (SWAMP).

## KEYWORDS

accuracy, cryptographic API misuses, static program analysis, false positive, benchmark

## 1 INTRODUCTION

Cryptographic algorithms offer provable security guarantees in the presence of adversaries. However, vulnerabilities and deficiencies in low-level cryptographic implementations seriously reduce the guarantees in practice [15, 24, 27, 35, 36]. Researchers also found misusing cryptographic APIs is not unusual in application-level code [31]. Causes of these vulnerabilities are multi-fold, which include complex APIs [12, 55], the lack of cybersecurity training [52], the lack of tools [14], and insecure and misleading forum posts (such as on StackOverflow) [13, 52]. Some aspects of security libraries (such as JCA, JCE, and JSSE<sup>1</sup>) are difficult for developers

to use correctly, e.g., certificate verification [37] and cross-language encryption and decryption [52].

In this work, we focus on the goal of screening massive-sized Java projects for cryptographic API misuses. Specifically, we aim to design a static analysis tool that has no or few false positives (i.e., false alarms) and can be routinely used by developers.

Efforts to screen cryptographic APIs have been previously reported in the literature, including static analysis (e.g., CrySL [44], FixDroid [57], CogniCrypt [43], CryptoLint [31]) and dynamic analysis (e.g., SMV-Hunter [65], and AndroSSL [34]), as well as manual code inspection [37]. Static and dynamic analyses have their respective pros and cons. Static methods do not require the execution of programs. They scale up to a large number of programs, cover a wide range of security rules, and are unlikely to have false negatives (i.e., missed detections). Dynamic methods, in comparison, require one to trigger and detect specific misuse symptoms at runtime (e.g., misconfigurations of SSL/TLS). The advantage of dynamic approaches is that they tend to produce fewer false positives (i.e., false alarms) than static analysis. Deployment-grade code screening tools need to be scalable with wide coverage. Thus, static program analysis approach is favorable. However, existing static analysis-based tools (e.g., [31, 43, 44, 57]) are not optimized to operate on the scale of massive-sized Java projects (e.g., millions of LoC), which we explain later.

Existing static analysis tools are also limited in detecting SSL/TLS API misuses and are not designed to detect complex misuse scenarios. For example, MalloDroid [33] uses a list of known insecure implementations of HostnameVerifier and TrustManager to screen apps. Google Play recently deployed an automatic app checking mechanism for SSL/TLS hostname verifier and certificate verification vulnerabilities [11]. However, the inspection appears to only target obvious misuse scenarios, e.g., return true in verify method or an empty body in checkServerTrusted [4].

We made substantial progress toward building a high accuracy and low runtime static analysis solution for detecting cryptographic and SSL/TLS API misuse vulnerabilities. Our tool, CRYPTOGERD, is built on specialized forward and backward program slicing techniques. These slicing algorithms are implemented by using flow-, context- and field-sensitive data-flow analysis.

Although program slicing is a well-known technique for identifying the set of instructions that influence or are influenced by a program variable, its direct application to screening cryptographic implementations has several problems, which are explained next.

<sup>1</sup>JCA, JCE, and JSSE stand for Java Cryptography Architecture, Java Cryptography Extension, and Java Secure Socket Extension, respectively.

*Detection accuracy.* A challenging problem that has not been solved by prior work is the excessive number of false positives that basic static analysis (including slicing) generates. Several types of detection require one to search for constants or values from predictable APIs, e.g., passwords, seeds, or initialization vectors (IVs). However, benign constants or irrelevant parameters may be mistaken as violations (e.g., array/collection bookkeeping constants). Another source of detection inaccuracy comes from the assumption that all the system and runtime libraries are present during the analysis. This assumption holds for Android apps (e.g., CrySL [44], CryptoLint [31]), but not necessarily for Java projects.

A feature of our solution CRYPTOGUARD is a set of refinement algorithms that systematically discard false alerts. These refinement insights are derived from empirical observations of common programming idioms and language restrictions to remove irrelevant resource identifiers, arguments about states of operations, constants on infeasible paths, and bookkeeping values. For eight of our rules, these refinement algorithms reduce the total number of alerts by 76% in Apache and 80% in Android (Figure 3). Our manual analysis shows that CRYPTOGUARD has a precision of 98.61% on Apache.

*Runtime overhead and coverage.* Existing flow-, context- and field-sensitive analysis techniques build a super control-flow graph of the entire program, which has a significant impact on runtime. In contrast, our on-demand slicing algorithms run much faster, which start from the slicing criteria and only propagate to the methods that have the potential to impact security. Hence, a large portion of the code base is not touched. For the Apache projects we evaluated, CRYPTOGUARD took around 3.3 minutes on average.

More importantly, our lightweight analysis building blocks enable us to address complex API misuse scenarios. CRYPTOGUARD covers more cryptographic properties than CrySL [44], Coverity [1], and SpotBugs [2] combined. Our most complex analysis (for Rule 15 on insecure RSA/ECC key sizes) involves multiple rounds of forward and backward slicing.

Our technical contributions are summarized as follows.

- We designed and implemented a set of new analysis algorithms for detecting cryptographic and SSL/TLS API misuses. Our static code checking tool, CRYPTOGUARD, is designed for developers to use routinely on large Java projects. Besides open-sourcing CRYPTOGUARD<sup>2</sup>, we are currently integrating it with the Software Assurance Marketplace (SWAMP) [30], a well-known free software security analysis platform.
- We gained numerous security insights from screening 46 Apache projects. For 15 of our rules, we observed violations in Apache projects (Table 6). 39 out of the 46 projects have at least one type of cryptographic misuses, and 33 projects have at least two. We reported our security findings to Apache, some of which have been promptly fixed. In Section 7, we share our experience of interacting with Apache teams and their pragmatic constraints e.g., backward compatibility, operation in humanless settings.
- Our evaluation on 6,181 Android apps shows that around 95% of the total vulnerabilities come from libraries that are packaged with the application code. Some libraries are from Google,

Facebook, Apache, Umeng, and Tencent (Table 5). We observe violations in most of the categories, including hardcoded keyStore passwords, e.g., `notasecret` is used in multiple Google libraries (Table 4). We also detected multiple SSL/TLS (MitM) vulnerabilities that Google Play’s automatic screening seemed to have missed.

- We created a benchmark named CRYPTOAPI-BENCH with 112 unit test cases.<sup>3</sup> CRYPTOAPI-BENCH contains basic intra-procedural instances, inter-procedural cases, field sensitive cases, false positive tests, and correct API uses. Our evaluation on CRYPTOAPI-BENCH shows that CRYPTOGUARD achieves higher precision and recall than Coverity, SpotBugs and CrySL [44], which is the state-of-the-art research solution. The benchmark also reveals false negatives that CRYPTOGUARD needs to improve on in the future.

Our key technical novelty and significance are summarized as follows. **[Formulation of problems]** We present the mappings between a number of cryptographic abstractions to concrete Java programming elements that can be statically enforced. The mapping strategy (including specific slicing criteria) is useful beyond CRYPTOGUARD (in Section 3). **[Methodology development]** We specialize program slicing with new language-based contextual refinement algorithms and successfully show a significant reduction of false alarms (related to constants and predictable values). It is a substantial advancement over general-purpose slicing and state-of-the-art solutions (in Section 5). **[New security capabilities]** Our lightweight algorithm design enables CRYPTOGUARD to check more rules than existing solutions, while maintaining high precision. **[New security findings]** CRYPTOGUARD enables us to report a number of alarming cryptographic coding issues in open source Apache projects and Android (in Sections 6.1 and 6.2). **[Science of security]** Our CRYPTOAPI-BENCH will motivate researchers to improve the accuracy, coverage, scalability, and transparency of their tools, collectively advancing the science of security (in Section 6.3).

## 2 THREAT MODEL, CHALLENGES, AND OVERVIEW

We describe our threat model and discuss the technical challenges associated with detecting these threats with static program analysis. For each challenge, we briefly overview our solution.

### 2.1 Threat Model

We summarize the vulnerabilities that CRYPTOGUARD aims to detect below and in Table 1. We also rank their severity.

**1. Vulnerabilities due to predictable secrets.** Software with predictable cryptographic keys and passwords are inherently insecure [31]. Here, we consider the use of any constants, as well as values that are derived from constants or API calls with predictable outputs (e.g., DeviceID, Timestamps) to be insecure.

**2. Vulnerabilities from MitM attacks on SSL/TLS.** Improper customization of Java Secure Socket Extension (JSSE) APIs may result in man-in-the-middle (MitM) vulnerabilities [33, 37]. CryptoLint [31] does not detect these vulnerabilities.

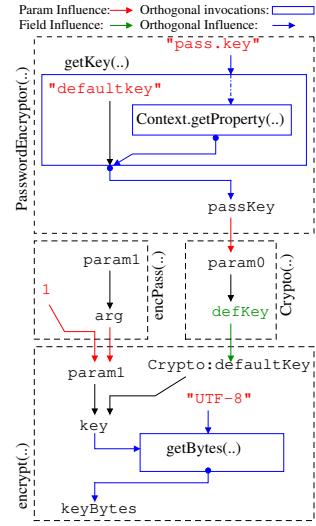
<sup>2</sup>Available at <https://github.com/CryptoGuardOSS/cryptoguard> under GPL v3.0.

<sup>3</sup>Our benchmark is available at <https://github.com/CryptoGuardOSS/cryptoapi-bench>.

```

1 class PasswordEncryptor {
2
3     Crypto crypto;
4
5     public PasswordEncryptor() {
6         String passKey = PasswordEncryptor
7             .getKey("pass.key"); (P)
8         crypto = new Crypto(passKey); (P)
9     }
10    byte[] encPass(String [] arg){
11        return crypto.encrypt(arg[0], arg[1]); (P)
12    }
13
14    static String getKey(String src){
15        String key = Context.getProperty(src);
16        if (key == null) {
17            key = "defaultkey";
18        }
19        return key;
20    }
21 }
22 class Crypto {
23
24     String ALGO = "AES";
25     String ALGO_SPEC = "AES/CBC/NoPadding";
26     String defaultKey;
27     Cipher cipher;
28
29     public Crypto(String defKey){
30         cipher = Cipher.getInstance(ALGO_SPEC);
31         defaultKey = defKey; // assigning field
32     }
33
34     byte[] encrypt(String txt, String key){(f)
35         if (key == null){
36             key = defaultKey; (f)
37         }
38         byte[] keyBytes = key.getBytes("UTF-8");
39         byte[] txtBytes = txt.getBytes();
40         SecretKeySpec keySpc =
41             new SecretKeySpec(keyBytes, ALGO);
42         cipher.init(Cipher.ENCRYPT_MODE, keySpc);
43         return cipher.doFinal(txtBytes);}}
```

(a)



(b)

**Figure 1:** (a) An example demonstrating various features of CRYPTOGUARD. `Crypto` class is used for generic AES encryption and `PasswordEncryptor` class uses `Crypto` for password encryption. (f) indicates influence through the fields and (P) indicates influence through the method parameters. (b) Partial data dependency graph for `keyBytes` variable.

**3. Vulnerabilities from predictable PRNGs.** The predictability of pseudorandom number generators (PRNGs) has been a major source of vulnerabilities [19, 38, 39]. The use of `java.util.Random` as a PRNG is insecure [6, 42]. In addition, seeds for `java.security.SecureRandom` [7] should not be predictable.

**4. Vulnerabilities from CPA.** Ciphertexts should be indistinguishable under chosen plaintext attacks (CPA) [31]. Static salts make dictionary attacks easier on password-based encryption (PBE). In addition, static initialization vectors (IVs) in cipher block chaining (CBC) and electronic codebook (ECB) modes are insecure [18, 46].  
**5. Vulnerabilities from feasible bruteforce attacks.** MD5 and SHA1 are susceptible to hash collision [66, 67] and pre-image [8, 26] attacks. In addition, bruteforce attacks are feasible for 64-bit symmetric ciphers (e.g., DES, 3DES, IDEA, Blowfish) [20]. 1024-bit RSA/DSA/DH and 160-bit ECC are also weak [3]. RFC 8018 recommends at least 1000 iterations for PBE [53].

*How severe are these vulnerabilities?* Each case has specific attack scenarios documented in the literature. To prioritize alerts, we categorize their severity into high, medium, and low, based on *i*) attacker's gain and *ii*) attack difficulty. Vulnerabilities from predictable secrets and SSL/TLS MitM are immediately exploitable and substantially benefit attackers. In Android, an application can only access its own KeyStore. Hence, hard-coded passwords are less harmful in Android. However, privilege escalation attacks bypass this restriction, which has been demonstrated [69]. Commercially available rainbow tables allow attackers to easily obtain pre-images of MD5 and SHA1 hashes for typical passwords [9]. Hash collisions for these algorithms enable attackers to forge digital signatures or break the integrity of any messages [21, 66]. Therefore, these vulnerabilities are classified as high risks. Vulnerabilities from predictability and CPA provide substantial advantages to attackers by significantly

reducing attack efforts. They are medium-level risks. Brute-forcing ciphers, requiring non-trivial effort, is low risk.

## 2.2 Technical Challenges and Solution Overview

The task of screening millions of lines of code for cryptographic API misuses poses a set of technical challenges.

### Technical Challenge I: False positives.

*1. False positives due to phantom methods.* A method is phantom if its body is not available during analysis. Unlike Android, Java web applications have phantom libraries. A non-system library that is not packaged with the project binaries is referred to as a phantom library. Existing cryptographic misuse vulnerability solutions (e.g., CryptoLint [31], CrySL [44]) are not designed to handle phantom libraries, which may cause false positives. For example, in Figure 1(a) if the class `Context` is a member of a phantom library, then `getProperty` method (Line 15) is a phantom method. The data-flow diagram in Figure 1(b) shows that a straightforward def-use analysis would likely report `pass.key` as a hard-coded key, since it cannot explore `getProperty` method at Line 15.

Our solution is a set of new algorithms to refine slicing outputs (Section 5). For example, examining the context reveals that `pass.key` is used as an identifier of a key and has no security influence on `keyBytes`. Thus, it can be safely discarded.

*2. False positives due to data structures.* Constants for bookkeeping data structures are another major source of false positives that are largely uncovered in the existing literature (e.g., [31, 44]). Most frequently used data structures include lists, maps, and arrays. For example, a data-structure-unaware analysis would likely report `1` from Line 11 (Figure 1(a)) as a hard-coded key, as it influences the `key`

parameter of `encrypt` method (Figure 1(b)). Our refinement algorithms track and discard any kinds of data-structure-bookkeeping constants (Section 5).

*Technical Challenge II: precision vs. runtime tradeoff.* For a project with millions LoC (e.g., Apache Hadoop has 2.5 million LoC), building a super-CFG is costly and unnecessary. Cryptographic functionality is often confined within a small fraction of the project. However, most flow-, context- and field-sensitive analysis based tools (e.g., [31, 44]) appear to build a super control-flow graph, e.g., by superimposing the project’s call graph over control-flow graphs of methods, adding call edges between `invoke` instructions, method entries, and exits.

In contrast, we adopt the following more scalable approaches.

*1. Demand-driven analysis.* Our flow- and context- sensitive analysis is demand driven. Initially, it only creates a call graph. During the analysis, it performs on-demand inter-procedural backward data flow analysis to perform backward slicing where the analysis starts from the slicing criteria and propagates *upward* and *orthogonally* on-demand. For example, in Figure 1(a), a propagation from `encrypt` method to `encPass` method, is an upward propagation. A propagation to orthogonal method invocations at Line 6 and 38 are orthogonal propagation. Our field sensitivity is also demand driven. Field sensitivity is applied to a field if the field is directly or indirectly used in our inter-procedural backward slices. A field’s influence is considered indirect if the field is accessed using orthogonal method invocations (i.e., getter methods). We refer to this field sensitivity as *data-only class field-sensitivity*.

*2. Control the depth of orthogonal explorations.* Most of our cryptographic vulnerabilities involve finding constants. A distinguishing feature of constants is that they require no or few processing before use. Generally, processing is done by orthogonal method invocations. Thus, we explore the trade-off between the depth of orthogonal explorations and the runtime/accuracy of the analysis, by clipping orthogonal explorations up to a predetermined level with a low likelihood of causing false negatives. (We set the depth to 1 in our experiments.) We then use similar techniques as in phantom methods handling to reduce the false positives introduced by clipping.

*3. Subproject awareness.* Code in large Java projects is usually organized into reusable subprojects, packaged as separate .jars. One may create a *fat jar* by including all subprojects to resolve inter-subproject dependencies, which would unnecessarily increase the call graph generation time and size. In contrast, CRYPTO GUARD creates and consults a directed acyclic graph (DAG) representing subproject dependencies. It helps *i*) exclude unnecessary subprojects and *ii*) analyze independent sub-projects concurrently.

### 3 MAPPING VULNERABILITIES TO PROGRAM ANALYSIS

It is important to map cryptographic properties to concrete Java programming elements that can be statically enforced. We break the detection plan into one or more abstract steps so that each step can be mapped to a single round of static analysis.

In this section, we illustrate the process of mapping cryptographic vulnerabilities to concrete program analysis tasks. This mapping process is manual and only needs to be performed once for each

vulnerability. In what follows, we use rule *i* to refer to the detection of vulnerability *i* in Table 1.

For example, in Rule 4 we detect the abuse of `HostnameVerifier` interface. Ideally, an implementation of `HostnameVerifier` must use the `javax.net.ssl.SSLSession` parameter `verify` method to verify the hostname. Using the return statement as the slicing criterion, we perform intra-procedural backward slicing of `verify` method to implement this rule.

Rule 5 is to detect the abuse of the `X509TrustManager` interface. We reduce the task to detecting 3 concrete cases: *i*) throwing no exception after validating a certificate in `checkServerTrusted`, *ii*) unpinned self-signed certificate with an expiration check, and *iii*) not providing a valid list of certificates in `getAcceptedIssuers`. For Case *i*), intuitively, our program analysis needs to search for the occurrences of `throw` or propagated exception. `throw` is the slicing criterion in the (intra-procedural) backward slicing. Simple parsing is inadequate, as the analysis needs to learn the type of the thrown exception.

Rule 6 is to detect whether any method uses `SSLocket` directly without performing hostname verification. Intuitively, to detect this vulnerability, we need to track whether an `SSLocket` created from `SSLocketFactory` influences the `SSLSession` parameter of a `verify` method (of a `HostnameVerifier`) invocation. In addition, we also need to check whether the return value of the `verify` method is used in a condition checking statement (e.g., `if`). For detection, we use forward program slicing to identify all the instructions that are influenced by the `SSLocketFactory` instance. Among these instructions, we examine three cases *i*) an `SSLocket` is created, *ii*) an `SSLSession` is created and used in `verify`, and *iii*) the return value of `verify` method is used to make decisions. These three cases represent a correct use of `SSLocket` with proper hostname verification.

Rule 15 is to detect insecure asymmetric cipher configurations (e.g., 1024-bit RSA). A more concrete goal is to detect an insecure default key size use and an explicit definition of insecure key size. The tasks of program analysis are to determine *a*) whether the key size is defined explicitly or by default, *b*) the statically defined key size, and *c*) the key generation algorithm. For Task *a*), our analysis uses forward slicing to determine whether the `initialize` method is invoked to set the key size of a key-pair generator. For Tasks *b*) and *c*), we use two rounds of backward program slicing to determine the key size and algorithm, respectively. We also employ on-demand field sensitivity for data-only classes in Task *b*). The analyses for Rule 15 are the most complex in CRYPTO GUARD.

Mappings for other rules are relatively straightforward and can be deduced from Table 1. For example, ↑ in Rule 1 & 2 means these rules are implemented using inter-procedural backward slicing and ↓ indicates inter-procedural forward slicing is used for on-demand data-only class field sensitivity. We also list the slicing criteria used for each rule in Tables 8, 9 and 10 in Appendix.

### 4 CRYPTO-SPECIFIC SLICING

We specialize static def-use analysis [71] and forward and backward program slicings [49] for detecting Java cryptographic API misuses. We break the detection strategy into one or more steps, so that a

**Table 1: Cryptographic vulnerabilities, properties, and static analysis methods used.** High, medium, and low risk levels are denoted by H/M/L, respectively. CPA stands for chosen ciphertext attack, MitM for man-in-the-middle, C/I/A for confidentiality, integrity, and authenticity, respectively.  $\uparrow$  means backward slicing and  $\downarrow$  means forward slicing. Slicing is inter-procedural unless otherwise specified (e.g., intra, both). Refinement insights are applied for all the inter-procedural backward slicing.

No	Vulnerabilities	Attack Type	Crypto Property	Severity	Our Analysis Method
1	Predictable/constant cryptographic keys.	Predictable Secrets	Confidentiality	H	$\uparrow$ slicing & $\downarrow$ slicing
2	Predictable/constant passwords for PBE		Confidentiality	H	$\uparrow$ slicing & $\downarrow$ slicing
3	Predictable/constant passwords for KeyStore		Confidentiality	H	$\uparrow$ slicing & $\downarrow$ slicing
4	Custom Hostname verifiers to accept all hosts	SSL/TLS MitM	C/I/A	H	$\uparrow$ slicing (intra)
5	Custom TrustManager to trust all certificates		C/I/A	H	$\uparrow$ slicing (intra)
6	Custom SSLSocketFactory w/o manual Hostname verification		C/I/A	H	$\downarrow$ slicing (intra)
7	Occasional use of HTTP		C/I/A	H	$\uparrow$ slicing
8	Predictable/constant PRNG seeds	Predictability	Randomness	M	$\uparrow$ slicing & $\downarrow$ slicing
9	Cryptographically insecure PRNGs (e.g., java.util.Random)		Randomness	M	Search
10	Static Salts in PBE	CPA	Confidentiality	M	$\uparrow$ slicing & $\downarrow$ slicing
11	ECB mode in symmetric ciphers		Confidentiality	M	$\uparrow$ slicing
12	Static IVs in CBC mode symmetric ciphers		Confidentiality	M	$\uparrow$ slicing & $\downarrow$ slicing
13	Fewer than 1,000 iterations for PBE	Brute-force	Confidentiality	L	$\uparrow$ slicing & $\downarrow$ slicing
14	64-bit block ciphers (e.g., DES, IDEA, Blowfish, RC4, RC2)		Confidentiality	L	$\uparrow$ slicing
15	Insecure asymmetric ciphers (e.g., RSA, ECC)		C/A	L	$\uparrow$ slicing & $\downarrow$ slicing (both)
16	Insecure cryptographic hash (e.g., SHA1, MD5, MD4, MD2)		Integrity	H	$\uparrow$ slicing

step can be realized with a single round of program slicing. After performing the slicing, each program slice is analyzed to find the presence of a vulnerability. Our 16 categories of vulnerabilities require different program analysis methods for detection. Table 1 summarizes slicing techniques to detect each of the vulnerabilities. General-purpose slicing alone is inadequate. Thus, we explain our solution for overcoming the accuracy challenge in Section 5.

A definition of variable  $v$  is a statement that modifies  $v$  (e.g., declaration, assignment). A use of variable  $v$  is a statement that reads  $v$  (e.g., a method call with  $v$  as an argument). Def-use data-flow analysis or def-use analysis identifies the definition and use statements and describes their dependency relations. Given a slicing criterion, which is a statement or a variable in a statement (e.g., a parameter of an API), backward program slicing is to compute a set of program statements that affect the slicing criterion in terms of data flow. Given a slicing criterion, forward program slicing is to compute a set of program statements that are affected by the slicing criterion in terms of data flow. Given a program and a slicing criterion, a program slicer returns a list of program slices. Intra-procedural program slicing mechanisms use def-use analysis to compute slices.

To confine inter-procedural backward slicing within security code regions, the analysis starts from cryptographic APIs and follows their influences recursively. This approach effectively skips the bulk of the functional code and substantially speeds up the analysis.

## 4.1 Slicing Criteria and Backward Slicing

We give the intuition behind selecting slicing criteria and then present our backward slicing techniques. The complete list of our slicing criteria and corresponding APIs are shown in Tables 8, 9, and 10 in Appendix.

*Slicing criteria.* The choice of slicing criterion directly impacts the analysis outcomes. We choose slicing criteria based on several factors, including relevance to the vulnerability, simplicity of checking rules, shared across multiple projects.

For inter-procedural backward slicing, the slicing criteria are defined as the parameters of a target method’s invocation. For example, to find predictable secrets (in Rules 1-3), we use the key parameter of the constructors of `SecretKeySpec` as the slicing criterion. For intra-procedural backward slicing, we define three types of slicing criteria: *i*) parameters of a method, *ii*) assignments, and *iii*) `throw` and `return`. For example, to detect insecure hostname verifiers that accept all hosts (in Rule 4), we use the `return` statement in the `verify` method as the slicing criterion.

*Intra-procedural backward slicing.* The purpose of intra-procedural backward slicing is two-fold. It is used independently to enforce security as well as a building block of inter-procedural back program slicing. The intra-procedural program slicing utilizes the def-use property of a statement to decide whether a statement should be included in a slice or not. Our implementation utilizes the worklist algorithm from the intra-procedural data-flow analysis framework of Soot. During this process, if any orthogonal method invocations are encountered, it recursively slices them to collect the arguments and statements that influence any field or return statements within that orthogonal methods. To reduce runtime overhead, such orthogonal method explorations are clipped at a pre-configurable depth (1 in our experiments). In this procedure, we use refinement insights presented in Section 5 to exclude security irrelevant instructions that basic use-def analysis cannot identify.

*On-demand Inter-procedural backward slicing.* The main responsibility of this algorithm is the upward propagation of the analysis. Our inter-procedural backward slicing builds on intra-procedural backward slicing. Major steps of the algorithm are as follows. *i*) We build a caller-callee relationship graph of all the methods of the

```

,,

$rl.setText("mytext");
$rl.setKey("mykey");
...
key = $rl.getKey();

```

**Figure 2: Indirect field access using orthogonal invocations on data-only class object \$rl.**

program. The call-graph construction uses class-hierarchy analysis. *ii*) We identify all the callsites of the method specified in the slicing criterion. A callsite refers to a method invocation. *iii*) For all the callsites, we obtain all the inter-procedural backward slices by invoking intra-procedural slicing recursively to follow the caller chain. *iv*) Our procedure is field sensitive. Typical field initialization statements are assignments. After encountering a field assignment, the analysis follows the influences through fields, recursively.

## 4.2 Forward Slicing

Some of our analysis demands forward slicing, which inspects the statements occurring after the slicing criterion.

*Intra-procedural forward slicing.* We design intra-procedural forward slicing for Rules 6 (SSLocketFactory w/o Hostname verification) and 15 (Weak asymmetric crypto). The operation of intra-procedural forward slicing is similar to that of intra-procedural backward slicing. In forward slicing, we choose assignments as the slicing criteria. The traversal follows the order of the execution, i.e., going forward. Because problematic code regions for Rules 6 and 15 are confined within a method, their forward slicing analyses do not need to be inter-procedural.

*Inter-procedural forward slicing.*

Given an assign instruction or a constant as the slicing criterion, we perform the inter-procedural forward slicing to identify the instructions that are influenced by the slicing criterion in terms of def-use relations. Our version of inter-procedural forward slicing operates on the slices obtained from inter-procedural backward program slicing. Our inter-procedural backward slicing produces an ordered collection of instructions combined from all visited methods.

We define a class as a data-only class, if the fields of the class are only visible within orthogonal method invocations. We use inter-procedural forward slicing for on-demand field sensitivity of data-only classes, as the field sensitivity during upward propagation (inter-procedural backward slicing) does not cover them. In Figure 2, \$rl is an object of data-only class, where its fields are accessed indirectly with an orthogonal method (i.e, getKey) invocation. Given a constant, using inter-procedural forward slicing, CRYPTOGUARD determines whether the constant influences any field of a data-only class object and records it. Later on, when it encounters an assign invocation on the same object and observes that the previously recorded field influences the return statement, then it reports the constant. Through this on-demand field sensitivity for data-only class, CRYPTOGUARD knows that constant mytext (Figure 2) is not a hard-coded key. ↓ in Table 1 represents the use of forward slicing for on-demand data-only class field sensitivity.<sup>4</sup>

<sup>4</sup>Current prototype uses this field sensitivity for 8 rules.

## 5 REFINEMENT FOR FP REDUCTION

We design a set of refinement algorithms to exclude security irrelevant instructions to reduce false alarms. These *refinement insights* (*RI*) are deduced by observing common programming idioms and language restrictions. We also discuss the possibility of false negatives (i.e., missed detection).

### 5.1 Overview of Refinement Insights (RI)

Eight of our rules (1, 2, 3, 8, 10, 12, 13 and 15) require identifying constants/predictable values in a program slice. The purpose is to ensure that no data (e.g., cryptographic keys, passwords, IVs, and seeds) is hardcoded or solely derived from any hardcoded values. Use of any predictable values (e.g., Timestamp, DeviceID) is also insecure for Rules 1, 2, 3 and 8. However, there are many constant/predictable values that do not impact security. We refer to them as *pseudo-influences*. Pseudo-influences are a major source of false positives.

Based on empirical observations of common programming idioms and language restrictions, we invent five strategies to systematically remove irrelevant constants/predictable values from slices and reduce pseudo-influences, which are summarized next. For eight of our rules, these refinement insights yield a 76% reduction in total alerts for Apache projects and 80% reduction for Android applications (Section 5.4). In CRYPTOGUARD, rule checkers apply these refinements on constants/predictable values in program slices to remove pseudo-influences.

- *RI-I: Removal of state indicators.* We discard constants/predictable values that are used to describe the state of a variable during an orthogonal method invocation.
- *RI-II: Removal of resource identifiers.* We discard constants/predictable values that are used as the identifier of a value source during an orthogonal method invocation.
- *RI-III: Removal of bookkeeping indices.* We discard constants/predictable values that are used as the index or size of any data structures. Specifically, RI-III discards any influences on i) size parameter of an array or a collection instantiation, ii) indices of an array, iii) indices of a collection.
- *RI-IV: Removal of contextually incompatible constants.* We discard constants/predictable values, if their types are incompatible with the analysis context. For example, a boolean variable cannot be used as a key, IV, or salt.
- *RI-V: Removal of constants in infeasible paths.* Some constant initializations are updated along the path to the slicing criterion. We need to discard the initializations that do not have a valid path of influence to the criterion.

RI-I, RI-II and RI-IV are used to handle the clipping orthogonal method explorations, which can occur due to phantom method invocations or pre-configured clipping at a certain depth. RI-III is used to achieve data structure awareness and RI-V are used to compensate path insensitivity. The breakdown of the total reduction of false alarms in our experiment shows that RI-II and RI-III are most effective in Apache and Android apps (Figure 4). In the next two subsections, we highlight the details of two refinement insights based on removing state indicators and resource identifiers. Details for other RIs can be found in Section 10.1 of Appendix.

## 5.2 RI-I: Removal of State Indicators

Clipping of orthogonal method exploration can cause false positives if the arguments of method is used to describe the state of a variable. Consider `UTF-8` in Line 38 of Figure 1(a). Its Jimple<sup>5</sup> representation is as follows, where `$r2` represents variable key, `$r4` represents `keyBytes`, and `virtualinvoke` is for invoking the non-static method of a class.

```
$r4 = virtualinvoke $r2.<java.lang.String: byte[]
getBytes(java.lang.String)>("UTF-8")
```

If the analysis is clipped so that it cannot explore the `getBytes` method, then a def-use analysis shows that constant `UTF-8` influences the value of `$r4` (i.e., `keyBytes`). Thus, a straightforward detection method would report `UTF-8` as a hardcoded key. However, `UTF-8` is for describing the encoding of `$r2` and can be safely ignored. We refer to this type of constants as *state indicator pseudo-influence*.

The use of refinement insights have direct impact on analysis outcomes. For example, discarding arguments of `virtualinvoke` may generate false negatives. Suppose `virtualinvoke` is used to set a key in a `KeyHolder` instance with some constant: `virtualinvoke $r5.<KeyHolder: void setKey(java.lang.String)>("abcd")`. Constant `abcd` needs to be flagged. On the contrary, we observe that arguments of `virtualinvoke` appearing in assign statements are typically used to describe the state of a variable and can be ignored. In summary, RI-I states that *i*) arguments of any `virtualinvoke` method invocation in an assignment instruction can be regarded as pseudo-influences, and *ii*) any constants that influence these arguments can also be discarded.

## 5.3 RI-II: Removal of Source Identifiers

Another type of pseudo-influences due to the clipping of orthogonal method exploration is the identifiers of value sources. We use an example to illustrate the importance of this insight. For the code below, a straightforward analysis would flag constant `ENCRYPT_KEY`. However, it is an identifier for retrieving a value from a Java Map data structure, and thus a false positive.

```
$r30 = interfaceinvoke r29.<java.util.Map:
java.lang.Object get(java.lang.Object)>("ENCRYPT_KEY")
i) Retrieving values from an external source. Static method invocations (staticinvoke in Jimple) in assign statements are typically used to read values from external sources, e.g., Line 15 in Figure 1(a):
```

```
$r4 = staticinvoke <Context: java.lang.String
getProperty(java.lang.String)>(src)
```

Variable `src` refers to the identifier, not the actual value of the key. Thus, it is a pseudo influence. To avoid such pseudo-influences, RI-II discards any arguments of `staticinvoke` that appear in an assignment. Although `staticinvoke` may be used to transform a value from one representation to another, it is unlikely to use `staticinvoke` to transform a constant.

<sup>5</sup>Jimple is an intermediate representation (IR) of a Java program.

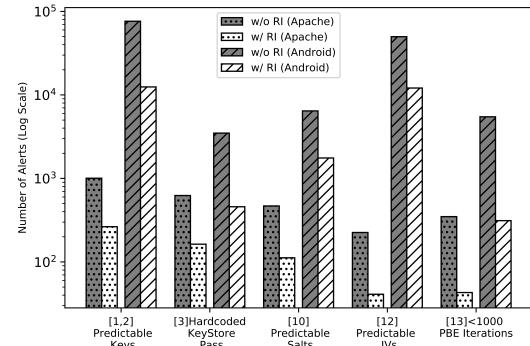


Figure 3: Reduction of false positives with refinement insights in 46 Apache projects (94 root-subprojects) and 6,181 Android apps. Top 6 rules with maximum reductions are shown.

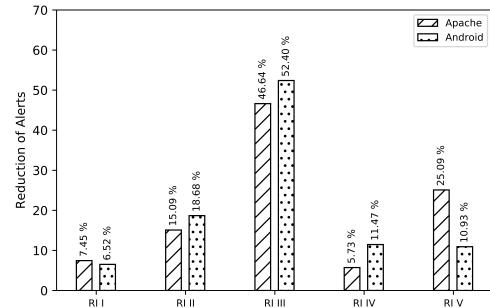


Figure 4: Breakdown of the reduction of false positives due to five of our refinement insights.

## 5.4 Evaluation of Refinement Methods

We compared the numbers of reported alerts before and after employing the five refinement algorithms for 46 Apache projects and 6,181 Android apps. Our experiments show that refinement algorithms reduce the total alerts by 76% in Apache and 80% in Android. For Apache projects, we manually confirmed that all the removed alerts are indeed false positives<sup>6</sup>. All constant-related rules (including 1, 2, 3, and 12) greatly benefit from the refinements and have significant reduction of irrelevant alerts. Results for top six rules with maximum reductions are shown in Figure 3. The detailed breakdown is shown in Figure 4. The most effective refinement insight for Apache and Android are RI-III (removal of array/collection bookkeeping information).

With refinements enabled, there are a total of 1,295 alerts for the 46 Apache projects. Our careful manual source-code analysis confirms that 1,277 alerts are true positives, resulting in a precision of 98.61%. Out of the 18 false positives, 1 case is due to path insensitivity and 17 to clipping orthogonal explorations (discussed in Section 7). All experiments reported in the next section were conducted with refinements enabled.

<sup>6</sup>Regarding the validity of the manual analysis, the manual confirmation of alerts was conducted by a second-year Ph.D. student with a prior Master degree in cybersecurity (the second author), under the close guidance of a professor and a senior Ph.D. student (the first author).

## 6 SECURITY FINDINGS AND BENCHMARK EVALUATION

Our experimental evaluation aims to answer the following questions.

- What are the security findings in Apache Projects? Do Apache projects have too many high-risk vulnerabilities such as hardcoded secrets or MitM vulnerabilities? (Section 6.1)
- What are the security findings in Android Apps? Do third-party libraries have high-risk vulnerabilities? (Section 6.2)
- How does CRYPTOGRAPH compare with CrySL, SpotBugs, and the free trial version of Coverity on benchmarks or real-world projects? (Section 6.3)

*Selection and pre-processing of programs.* We selected 46 popular Apache projects that have crypto API uses. The popularity is measured with the numbers of stars and forks in Github. The maximum, minimum and average Line of Code (LoC) are around 2,571K (Hadoop), 1.1K (Commons Crypto) and 402K, respectively. We perform subproject dependency analysis to build DAGs by parsing build scripts. Subproject dependency analysis was automated for *gradle* and *maven*, and was manual for *Ant*. We identified the root-subprojects, which are sub-projects that have no incoming edges on the subproject dependency DAG. We analyzed 94 root-subprojects in total<sup>7</sup>. We downloaded 6,181 high popularity Android apps from the Google app market covering 58 categories. The median value of the number of apps per category is 120. We used Soot to decompile .apk files to Java bytecode in order to interface with CRYPTOGRAPH. We use online APK decompiler<sup>8</sup> to obtain human-readable source code for manual verification.

*CRYPTOGRAPH runtime.* We ran 4 concurrent instances of CRYPTOGRAPH in an Intel Xeon(R) X5650 server (2.67GHz CPU and 32GB RAM). Runtime increases with the use of cryptography APIs. For Apache projects, the average runtime was 3.3 minutes with a median of around 1 minute. For Android apps, we terminated unfinished analysis after 10 minutes. The average runtime was 3.2 minutes with a median of 2.85 minutes, including the cutoff ones. 552 (9%) of 6,181 app's analysis did not finish within 10 minutes, on which CRYPTOGRAPH generated partial results.<sup>9</sup>

### 6.1 Security Findings in Apache Projects

Out of the 46 Apache projects, 39 projects have at least one type of cryptographic misuses and 33 projects have at least two types. Table 6 summarizes our security findings in screening Apache projects. Predictable keys (Rules 1 and 2), HTTP URL (Rule 7), insecure hash functions (Rule 16), and the insecure PRNGs (Rule 9) are the most common types of vulnerabilities in Apache. As predictable values, we only observed constants for all these rules. We did not observe any predictable seeds under Rule 8.

**6.1.1 Vulnerabilities from Predictable Secrets.** 16 Apache projects (37 sub-rootprojects) have hardcoded keys (Rule 1, 2). Three (Meecrowave, Kylin, and Cloudstack) of them use hardcoded symmetric keys (Rule 1). Meecrowave uses *DESede* (i.e., Triple DES)<sup>10</sup>

<sup>7</sup>We exclude 15 test root-subprojects.

<sup>8</sup><http://www.javadecompilers.com/apk>

<sup>9</sup>Most of them missed results from Rule 7, which CRYPTOGRAPH runs the last.

<sup>10</sup>Triple DES itself is considered insecure. OpenSSL removed the support of Triple DES. NIST recommended moving to AES as soon as possible [68].

**Table 2: Breakdown of Accuracy in Apache Projects. Duplicates are handled at root-subproject level (total 82 root-subprojects) level. For Rules 1, 2, 3, 8, 10, 12, each constant/predictable value of an array/collection is considered as an individual violation.**

Rules	Total Alerts	# True Positives	Precision
(1,2) Predictable Keys	264	248	94.14 %
(3) Hardcoded Store Pass	148	148	100 %
(4) Dummy Hostname Verifier	12	12	100 %
(5) Dummy Cert. Validation	30	30	100 %
(6) Used Improper Socket	4	4	100 %
(7) Used HTTP	222	222	100 %
(8) Predictable Seeds	0	0	0%
(9) Untrusted PRNG	142	142	100 %
(10) Static Salts	112	112	100 %
(11) ECB mode for Symm. Crypto	41	41	100 %
(12) Static IV	41	40	97.56 %
(13) <1000 PBE iterations	43	42	97.67 %
(14) Broken Symm. Crypto Algorithm	86	86	100 %
(15) Insecure Asymm. Crypto	12	12	100 %
(16) Broken Hash	138	138	100 %
<b>Total</b>	<b>1,295</b>	<b>1,277</b>	<b>98.61 %</b>

```
1 <http:tlsClientParameters disableCNCheck="true">
2 ...
3 </http:tlsClientParameters>
```

**(a) A portion of https-cfg-client.xml**

```
1 ...
2 } else if (tlsClientParameters.isDisableCNCheck ()) {
3 verifier = new AllowAllHostnameVerifier ();
4 }
```

**(b) A portion of SSLUtils.java**

**Figure 5: Example code in Apache Cxf that disables hostname verification checks by default.**

```
1 public static String sendUpsRequest (...) {
2 ...
3 http.setAllowUntrusted(true);
4 ... }
```

**(a) A portion of UpsServices.java**

```
1 SSLContext getSSLContext (String alias, boolean trustAny) {
2 ...
3 TrustManager[] tm;
4 if (trustAny) {
5 tm = SSLUtil.getTrustAnyManagers(); } ... }
```

**(b) A portion of SSLUtil.java**

**Figure 6: Example code in Apache Ofbiz that enables trusting all certificates by default while invoking UPS service.**

for obfuscation purpose. Unfortunately, deterministic keys make it trivial to break the obfuscation. Kylin (635 Forks, 1325 Stars) uses AES to encrypt user passwords. However, using hardcoded keys make these passwords vulnerable. In Apache Cloudstack, it appears that hardcoded keys are used in test code, which is accidentally packaged with the production code.

For Rule 2, we found that most of the hardcoded passwords in PBE serve as the default. The most common default password

for PBE is masterpassphrase (e.g., Ambari and Knox). Manifoldcf uses NowIsTheTime. Setting PBE code to take the default hardcoded passwords without sufficient warnings are risky. Distributions using the default configuration are susceptible to the recovery of the plaintext password by an attacker who has the access to the PBE ciphertext. Apache Ranger (165 forks, 155 stars) uses a hardcoded password as default for PBE for all distributions. Its installation Wiki does not mention anything about it. System administrators unaware of this setup are likely not to change the default. This coding practice significantly weakens the security guarantee of PBE.

For Rule 3, most common hardcoded passwords for KeyStores (for storing private keys) are changeit (e.g., Tomcat, Knox, Judi, Ofbiz and Wss4j) and none (e.g., Knox, Hive and Hadoop). Most of them are set as default. There are 9 projects that have both predictable keys (Rule 1, 2) and hardcoded KeyStore passwords (Rule 3), indicating persistent insecure coding styles.

**Insecure common practices.** During manual analysis, we found three types of insecure common practices in Apache projects for storing secrets: *i*) hard-coding default keys or passwords in the source code, *ii*) storing plaintext keys or passwords in configuration files, *iii*) storing encrypted passwords in configuration files with decryption keys in plaintext in source code or configuration. Java provides a special security APIs (e.g., Callback and CallbackHandler) to prompt users for secrets (e.g., passwords). However, none of these projects provides any code to support this option.

Sysadmins are forced to store plaintext passwords in the filesystem unless they personally modify the code. The biggest danger that these insecure secret-storage practices bring to users is probably the inflated sense of security and not being able to see the actual risks.

**6.1.2 Vulnerabilities from SSL/TLS MitM.** Man-in-the-Middle (MitM) vulnerabilities are high risk in our threat model. 5 Apache projects (8 root-subprojects) have dummy hostname verifiers that accept any hostnames (Rule 4), including Spark (15086 forks, 16324 stars), Ambari (814 forks, 778 stars), Cxf (706 forks, 398 stars), Ofbiz, and Mecrowave. 6 Apache projects have dummy trust managers that trust any certificates (Rule 5), including Spark, Ambari, Cloudstack, Qpid-broker, Jclouds, and Ofbiz. It appears that most projects offer them as an additional connectivity option.

Our manual analysis reveals that some projects set this insecure implementation as default (e.g., Figure 5 and Figure 6). In Figure 6, we see that Ofbiz uses insecure SSL/TLS configurations by default while using UPS (a shipping company) service. When plain sockets are used, it is recommended to verify the hostname manually. We found 3 projects that do not follow this rule and accept any arbitrary hostnames. We also found 7 projects (24 root-subprojects) that occasionally use the HTTP protocol for communication.

#### Listing 1: A vulnerable code snippet from Apache Ranger to demonstrate various security issues

```

1 PBEKeySpec getPBEParameterSpec(String password) throws Throwable {
2     MessageDigest md = MessageDigest.getInstance(MD_ALGO); // MD5
3     byte[] saltGen = md.digest(password.getBytes());
4     byte[] salt = new byte[SALT_SIZE];
5     System.arraycopy(saltGen, 0, salt, 0, SALT_SIZE);
6     int iteration = password.toCharArray().length + 1;
7     return new PBEKeySpec(password.toCharArray(), salt, iteration);
8 }
```

**6.1.3 Medium and Low Severity Vulnerabilities.** It is important to be aware of the medium and low-risk vulnerabilities in the system and to recognize that the risk levels may increase under different adversarial models.

We found hardcoded salts in 4 projects including Apache Ranger, Manifoldcf, Juddi, and Wicket. We also observe the use of ECB mode in AES in 5 projects and predictable IVs in 2 projects with a total of 40 occurrences. We found 5 projects that use PBE with less than 1,000 iterations (Rule 13). Ranger and Wicket projects use 17 iterations for PBE; and Incubator-Taverna-Workbench and Juddi projects use 20 iterations, much fewer than the required 1,000.

Listing 1 shows a code snippet from Ranger, which has multiple issues. The number of iterations is proportional to the password size (Line 6), which is far less than 1,000. In addition, this code offers a timing side-channel. An adversary capable of measuring PBE execution time (e.g., in multi-tenant environments) may learn the length of the password. This information can substantially decrease the difficulty of dictionary attacks. Another issue is that the salt is computed as the MD5 hash of the password (Lines 2-3). An adversary obtaining the salt may quickly recover the password. The salt's dependence on the password itself also breaks the indistinguishability requirement of PBE under chosen plaintext attack.

We found various occurrences of Blowfish, DES, and RC4 ciphers for Rule 14. Under Rule 15, we found 3 occurrences of using default key size of 1024 and 9 other occurrences that explicitly initialize the key size to 1024. 23 projects use java.util.Random as a PRNG (Rule 9), where two of them set static seeds to java.util.Random. We do not observe any deterministic seed to a java.security.SecureRandom (Rule 8).

**Listing 2: An example of only checking the expiration (checkValidity) of self-signed certificates in Yahoo Finance (TWStock) Android app.** The base package name (`com.softmobile`) of this class indicates that the vulnerable code comes from a third-party library.

```

1 void checkServerTrusted(X509Certificate[] chain, String str){
2     if (chain == null || chain.length != 1) {
3         this.f7654a.checkServerTrusted(chain, str);
4     } else {
5         //Lack of signature verification and others
6         chain[0].checkValidity();}}
```

**Listing 3: An example of ignoring exceptions in checkServerTrusted in Sina Finance Android app.**

```

1 void checkServerTrusted(X509Certificate[] chain, String str){
2     try {
3         this.f7427a.checkServerTrusted(chain, str);
4     } catch (CertificateException e) {} //Ignores exception
```

**Listing 4: The use of SSLSocket without manual hostname verification in ProTaxi Driver Android app.**

```

1 try {
2     SSLContext instance = SSLContext.getInstance("TLS");
3     ...
4     this.webSocketClient
5         .setSocket(instance.getSocketFactory().createSocket());
6 } catch (Throwable e) { ... }
7 this.webSocketClient.connect();
```

**Table 3: Experimental results on the CRYPTOAPI-BENCH basic and CRYPTOAPI-BENCH advanced benchmarks with CrySL, Coverity, SpotBugs and CRYPTOGUARD.** GTP stands for the ground truth positives. TP, FP, and FN are the number of true positives, false positives, false negatives in a tool’s output, respectively. Pre. and Rec. represent precision and recall, respectively. Tools are evaluated on 6 common rules (out of our 16 rules), i.e., the maximum common subset of all tools. For these 6 rules, there are 6 correct cases (i.e., true negatives) in basic and 3 correct cases in advanced, which are used for computing FPRs. Total alerts = TP + FP.

Tools	CRYPTOAPI-BENCH: Basic						CRYPTOAPI-BENCH: Advanced																
	GTP:14			Summary			Inter-Proce. (Two) GTP: 13			Inter-Proce. (Multiple) GTP: 13			Field Sensitive GTP: 13			FP Test/ Correct Uses GTP: 3			Summary				
	TP	FP	FN	FPR	FNR	Pre.	Rec.	TP	FP	FN	TP	FP	FN	TP	FP	FN	TP	FP	FN	FPR	FNR	Pre.	Rec.
CrySL[44]	10	4	4	40.00	28.57	71.43	71.43	10	3	3	0	12	13	0	1	13	0	2	3	85.71	76.19	35.71	23.81
Coverity[1]	13	0	1	0.00	7.14	100.0	92.86	3	0	10	3	0	10	1	0	12	0	0	3	0.00	83.33	100.0	16.67
SpotBugs[2]	13	0	1	0.00	7.14	100.0	92.86	0	0	13	3	10	10	0	0	13	0	0	3	76.92	92.86	23.08	7.14
CRYPTOGUARD	14	0	0	0.00	0.00	100.0	100.0	13	0	0	13	0	0	13	0	0	3	0	0	0.00	0.00	100.0	100.0

## 6.2 Security Findings in Android Apps

*Violations in apps or in libraries?* We distinguished app’s own code from libraries by using the package information from `AndroidManifest.xml`.<sup>11</sup> Android also uses it during `R.java` file generation (robust against obfuscation). We found that on average **95% of the detected vulnerabilities come from libraries** (Table 4). This result extends the observation from 7 types of vulnerabilities (reported in [17]) to 16.

Table 4 shows the distribution of vulnerability sources for each rule. For hardcoded KeyStore passwords (Rule 3), all violations come from libraries. Most frequent hardcoded KeyStore password is `notasecret`, which is used to access certificates and keys in Google libraries (e.g., `*.googleapis.GoogleUtils`, `*.googleapis.*.GoogleCredential`).

**Table 4: Distribution of vulnerabilities in Android apps.**

	Library (Total)	Library (Unique)	App Itself	Total
(1,2) Predictable Keys	11,634 (93.4%)	5,940	823 (6.6%)	12,457
(3) Hardcoded Store Password	431 (94.1%)	170	27 (5.8%)	458
(4) Dummy Hostname Verifier	1,148 (99.3%)	51	7 (0.7%)	1,155
(5) Dummy Cert. Validation	3,715 (96.3%)	1,317	141 (3.7%)	3,856
(6) Used Improper Socket	270 (99.6%)	13	1 (0.4%)	271
(7) Used HTTP	7,687 (92.5%)	2,105	623 (7.5%)	8,321
(8) Predictable Seeds	522 (96.0%)	101	22 (4.0%)	544
(9) Untrusted PRNG	26,312 (91.7%)	8,679	2,393 (8.3%)	36,223
(10) Predictable Salts	1,638 (93.2%)	774	119 (6.8%)	1,757
(11) ECB in Symm. Crypto	16,577 (93.1%)	682	123 (6.9%)	1,780
(12) Predictable IVs	11,357 (94.2%)	6,048	692 (5.8%)	12,089
(13) <1000 PBE iterations	294 (94.2%)	129	18 (57.8%)	312
(14) Broken Symm. Crypto	1,668 (95.8%)	753	74 (4.2%)	1,742
(15) Insecure Asymm. Crypto	4 (3.6%)	3	107 (96.4%)	111
(16) Broken Hash	49,257 (99.0%)	7509	496 (1.0%)	49,769
<b>Total</b>	<b>117,594 (95.40%)</b>	<b>34,274</b>	<b>5,666 (4.60%)</b>	<b>130,845</b>

Besides Google, other high-profile library sources include Facebook, Apache, Umeng, and Tencent (Table 5). These libraries frequently appear in different applications. We distinguished these libraries using base packages and ignored obfuscations.

*Overview of other Android findings.* We found exposed secrets, similar to Apache projects. Table 6 summarizes the discovered vulnerabilities in Android applications. The categories of untrusted PRNG (Rule 9) and broken hash (Rule 16) have the most violations. Interestingly, we observed 544 cases of predictable seeds (Rule 8). 13 cases of them used time-stamps from `<java.lang.System: long currentTimeMillis ()>` API calls.

<sup>11</sup>An .apk contains both the app code and the libraries.

**Table 5: Violations in 5 popular libraries (manually confirmed).**

Package name	Violated rules
com.google.api	3, 4, 5, 7
com.umeng.analytics	7, 9, 12, 16
com.facebook.ads	5, 9, 16
org.apache.commons	5, 9, 16
com.tencent.open	2, 7, 9

**Compared with Apache projects, Android apps have higher percentages of SSL/TLS API misuses (Rules 4, 5 and 6) and HTTP use (Rule 7).** For example, 25.30% of Android apps have dummy trust manager (Rule 5), which is more than 2 times of the number in Apache (11.70%) as shown in Table 6 in Appendix.

Our analysis can detect sophisticated cases that Google Play’s built-in screening is likely to miss. We give code snippets for such cases (Listing 2, 3, 4). CRYPTOGUARD detects a case where developers allow unpinned self-signed certificates with a mere expiration check, as shown in Listing 2. Another case is where developers ignore the exception in `checkServerTrusted` method as shown in Listing 3. In addition, CRYPTOGUARD detects 271 occurrences of improper use of `SSLocket` without manual Hostname verification in 210 apps. One such example is shown in Listing 4, where `SSLocket` is used in `WebSocketClient` without manually verifying the hostname<sup>12</sup>. In comparison, Google Play’s inspection appears to only detect obvious misuses [4].

Grouping security violations by app popularity or category did not show substantial differences across groups.

## 6.3 Comparison with Existing Tools

We compare the accuracy and runtime of CRYPTOGUARD with three existing tools, i.e., CrySL [44], Coverity [1], and SpotBugs [2]<sup>13</sup>. During our experiments, we use CrySL 1.0 (commit id `10e86fdb`), SpotBugs 3.0.1 (from SWAMP) and the results from Coverity was obtained before Jan 07, 2019.

**Benchmark preparation.** First, we<sup>14</sup> had to construct CRYPTOAPI-BENCH, a comprehensive benchmark for comparing the quality of cryptographic vulnerability detection tools. Regarding the existing

<sup>12</sup>Guide for the correct use can be found at <https://developer.android.com/training/articles/security-ssl#WarningsSslSocket>.

<sup>13</sup>CryptoLint’s code is unavailable.

<sup>14</sup>The person (third author) who led the benchmark design is different from the person (first author) who implemented CRYPTOGUARD.

benchmark DroidBench [16], *i*) DroidBench does not cover cryptographic APIs, *ii*) the free web version of Coverity requires source code, however DroidBench only contains APK binaries.

CRYPTOAPI-BENCH covers all 16 cryptographic rules specified in Table 1. There are 38 basic test cases and 74 advanced test cases. The basic benchmark contains 25 straightforward API misuses and 13 correct API uses (i.e., true negative cases). The advanced cases have more complex scenarios, including 42 inter-procedural cases<sup>15</sup>, 20 field-sensitive cases, 9 false positive test cases (for evaluating the ability of recognizing irrelevant elements), and 3 correct API uses (i.e., true negative cases). Figures 7 and 8 in Appendix show the distributions of test cases per rule and per API, respectively. Augmenting the benchmark with more test cases is our ongoing work. See Github for the most updated version <https://github.com/CryptoGuardOSS/cryptoapi-bench>.

**Benchmark comparison.** To maintain fairness in our comparison, we only report the benchmark results for the six shared rules (1, 2, 3, 11, 14, 16) that are covered by all the tools, CrySL [44], Coverity [1], SpotBugs [2], and ours. Due to the lack of documentation, we had to infer a tool’s coverage based on whether or not it ever generates any alert in that category. We show the results in Table 3.

For the basic benchmark, SpotBugs and Coverity perform well, but not CrySL. Our investigation reveals that CrySL’s false positives are mainly due to their rules being overly strict. For example, CrySL would raise an alert if the password for PBE is derived from a `String` typed variable, or a symmetric key is not generated by a key generator. It cannot recognize 4 correct API uses in the evaluation (out of 9). The root cause for this overly specific definitions of security is likely the CrySL’s language restrictions on constraint definitions. For the advance benchmark, both CrySL and SpotBugs generate false positives, when a variable is passed through multiple methods. For all cases, Coverity has zero false positives, likely because of the use of symbolic execution and/or path-sensitive analysis<sup>16</sup>. However, Coverity misses multiple advanced vulnerability scenarios (for rules that it does cover in the basic benchmark).

Table 7 in Appendix presents the comparison for all 16 rules (not just the 6 common rules as in above). When testing all 16 rules, CRYPTOGERD failed to report 11 misuses (i.e., false negatives). We discuss the causes in Section 7.

**Runtime comparison.** We ran CrySL and CRYPTOGERD on 10 randomly selected Apache root-subprojects. Unfortunately, CrySL crashed and exit prematurely for 7 of them. For the 3 completed projects, CrySL is slower, but comparable on 2 projects (5 vs. 3 seconds, 25 vs. 19 seconds). However, it is 3 orders of magnitude slower than CRYPTOGERD on `kerberos-codec`.<sup>17</sup>

We choose not to compare with SpotBugs – the comparison would not be meaningful, because its analysis is mostly based on the syntactical matching of source code to known bug patterns [40, 62]. For the free web version of Coverity, we are unable to obtain its runtime. *Summary of experimental findings.*

- Our refinement algorithms are effective. They bring an 76% reduction in alarms for Apache projects and an 80% reduction for Android applications. We manually confirmed that all the

removed alerts are indeed false positives. Manually examining the remaining 1,295 Apache alerts (after refinements) confirms our precision of 98.61%.

- 39 out of the 46 Apache projects have at least one type of cryptographic misuses and 33 have at least two types. There is a widespread insecure practice of storing plaintext passwords in code or in configuration files. Insecure uses of SSL/TLS APIs are set as the default configuration in some cases.
- 5,596 (91%) out of the 6,181 Android apps have at least one type of cryptographic misuses and 4,884 (79%) apps have at least two types. 95% of the vulnerabilities come from the libraries that are packaged with the applications. Some libraries are from large software firms. CRYPTOGERD’s detection for SSL/TLS API misuses is more comprehensive than the built-in screening offered by Google Play.
- In terms of detecting complex misuses, CRYPTOGERD outperforms all leading solutions (in Table 3). It substantially outperforms CrySL in terms of robustness and runtime.

## 7 DISCUSSION

**Code correction.** Most of the Apache developers’ responses to our vulnerability disclosure reports were prompt and insightful. We highlight the feedback from some projects. Apache Spark promised to remove the support of dummy hostname verifier and trust store. Ofbiz promised to fix the reported issues of constant IVs and KeyStore passwords. Apache Ranger already fixed our report of constant default values for PBE [10] and insecure cryptographic primitives [5]. Regarding MD5, Apache Hadoop justifies that its MD5 use is for the per-block checksums for Hadoop file systems (HDFS)’s consistency and the setup does not assume the presence of active adversaries.

For some cases, developers explained that certain operational constraints (e.g., backward compatibility for clients) prevent them from fixing the problems. For example, Apache Tomcat server has to use MD5 in its digest authentication code, because major browsers do not support secure hash functions (as defined in RFC 7616). However, digest authentication is rarely used in the wild<sup>18</sup>.

The thorniest issue is secret storage. One justification for developers’ choice of storing plaintext passwords or keys in file systems is for supporting humanless environments (e.g., automated scripts to manage services). However, first, not all deployment scenarios are server farms in a humanless environment. Projects should also provide the secure option, which is to use Java callback to prompt human operators for passwords which can be used to unlock/generate other passwords or keys on the fly. Second, not properly disclosing and documenting the insecure configurations does a great disservice to the project’s users.

**Our limitations.** No static analysis tool is perfect. CRYPTOGERD is no exception. We discuss the detection limitations of CRYPTOGERD and future improvements.

**False positives.** One source of false positives comes from the path insensitivity. For example, CRYPTOGERD raises an alert if the variable `iteration` is assigned with a value of 0 for the following code snippet (from project `jackrabbit-oak`). However, this alert is a false positive, since this assignment is on an infeasible path.

<sup>15</sup>21 cases involve two methods and 21 cases involve more than two methods.

<sup>16</sup>Coverity is close sourced, so we are unable to confirm.

<sup>17</sup>Reported runtime is the average of three runs.

<sup>18</sup><https://security.stackexchange.com/questions/152935/why-is-there-no-adoption-of-rfc-7616-http-digest-auth>

```

    ,
    ,

int iteration = 0;
...
if (iteration < NO_ITERATION) { // NO_ITERATION = 1
    iteration = DEFAULT_ITERATION;
}

```

Another source of false positives is the clipping of orthogonal exploration, which can be substantially reduced by re-configuring the prototype to explore deeper. However, this will impact the runtime. In addition, CRYPTOGUARD detects the existence of API misuses in a code base but does not verify that the vulnerable code will be triggered at runtime. This issue is a general limitation of static program analysis. Apache Spark confirmed insecure PRNG uses, but stated that the affected code regions are not security critical.<sup>19</sup> However, eliminating this type of alerts is difficult, if possible at all, as the analysis needs to be aware of custom defined security criteria (e.g., what constitutes critical security) with in-depth knowledge about project semantics.

*False negatives.* For the full benchmark evaluation in Table 7 in Appendix, CRYPTOGUARD has 11 false negatives (i.e., missed detection). All these cases are due to our refinements after clipping orthogonal explorations. For example, RI-II would ignore 6A5B7C8A as a pseudo-influence from the following instruction, if orthogonal explorations are clipped to explore *parseHexBinary* method. `byte[] key = DatatypeConverter.parseHexBinary("6A5B7C8A")`.

These false negatives can be avoided by increasing the depth of the orthogonal exploration. However, these conversions are mostly required to absorb values from external sources (e.g., file system, network). Any such conversions of static values under the rules of Table 1 are highly unlikely. Outside the benchmark, we did not observe any such cases during our manual investigation of Apache alerts. We also manually investigated 5 randomly selected Apache projects for false negatives from within orthogonal invocations (due to clipping) and did not observe any.

CRYPTOGUARD runs the intra-procedural forward slicing for Rules 6 and 15, where an inter-procedural forward slicing could potentially improve the coverage. For Rule 15, this change might not make much difference, as *KeyPairGenerator* creation and its initialization usually occur in the same method. For Rule 6, our current implementation ignores the direct sub-classes of *SSLSocketFactory* to avoid false positives. Inter-procedural slicing could extend the analysis to the sub-classes.

Another limitation of our work is that the coverage of our benchmark needs further improvement, in terms of incorporating path sensitive test cases and increasing the diversity of APIs involved. Our ongoing work includes enhancing CRYPTOAPI-BENCH.

## 8 RELATED WORK

*Tools to detect cryptographic misuses.* Cryptographic misuse detection tools are typically constructed into two broad groups, i.e., static analysis (e.g., CryptoLint [31], MalloDroid [33], FixDroid [57], CogniCrypt [43] and CrySL [44]) and dynamic analysis (e.g., SMV-Hunter [65], AndroSSL [34] and K-Hunt [47]). For example, MalloDroid [33] uses a list of known insecure implementations of *HostnameVerifier* and *TrustManager* to screen Android apps. In [41], authors showed that generating false positives is one of the most significant barrier to adopt static analysis tools. This

<sup>19</sup>It is unclear why Spark chose to use insecure PRNG, even for non-security purposes.

false positive problem also exists in anomaly and intrusion detection systems [48, 72]. When screening large projects, virtually all static slicing solutions in this space (e.g., [31]) might generate a non-negligible amount of false positives. Contextual refinements similar to CRYPTOGUARD’s is necessary to achieve high precision in practice. In terms of the coverage, CRYPTOGUARD covers more rules than CryptoLint [31], CrySL [44] and MalloDroid [33] combined.

Other misuse detection tools (e.g., FixDroid [57] and CogniCrypt [43]) were mainly built for the user-experience study with the goal of making detection tools developer-friendly, as opposed to a deployment-quality screening solution. For example, FixDroid focuses on providing real-time feedback to developers. CogniCrypt’s [43] focus is on code generation (in Eclipse IDE) for several common cryptographic tasks (e.g., data encryption).

Dynamic analysis tools are complementary to static analysis ones. Most of them use a simple static analysis to first narrow-down the number of potential apps for dynamic analysis. For example, SMV-Hunter [65] looks for apps that contain any custom implementation of *X509TrustManager* or *HostNameVerifier* for initial screening.

*Other static analysis tools.* TaintCrypt [61] uses static taint analysis to discover library-level cryptographic implementation issues in C/C++ cryptographic libraries (e.g., OpenSSL). It uses symbolic execution based path exploration to reduce false alarms, which is usually costly. Researchers found that misusing non-cryptographic APIs in Android also have serious security implications. These APIs include APIs to access sensitive information (such as location, IMEI, and passwords) [56], APIs for fingerprint protection [23], and cloud service APIs for information storage [74]. The methodology described in this paper can be applied to address these APIs. Recently, data driven techniques to identify API misuses have been proposed [58, 73]. These techniques uses lightweight static analysis to infer rules from examples that can be used for detection. In [54], authors proposed a Bayesian framework for automatically learning correct API uses that can be used for anomaly-based API misuse detection. Efforts on automatically repairing insecure code have also been reported [50, 51, 60]. Static code analysis has been extensively used for other related software problems as well, including malware analysis and detection [32, 59, 70], vulnerability discoveries [22, 45], and data-leak detection [25]. In [28], Chi *et al.* presented a system to infer client behaviors by leveraging symbolic executions of client-side code. They used such knowledge to filter anomalous traffic. Fuzzing has been demonstrated to automatically discovering software vulnerabilities [29, 63, 64]. These techniques aim to find input guided vulnerabilities that result in immediately observable behaviors (e.g., triggering program crashes [64] or anomalous protocol states [29, 63]). It is unclear how to use fuzzing to detect cryptographic vulnerabilities (e.g., predictable IVs/secrets, legacy primitives) that do not exhibit easily observable anomalous behaviors.

## 9 CONCLUSIONS AND AN OPEN PROBLEM

We described our effort of producing a deployment-quality static analysis tool CRYPTOGUARD to detect cryptographic misuses in Java programs that developers can routinely use. This effort led to significant new technical contributions, including language-specific

contextual refinements for FP reduction, on-demand flow-sensitive, context-sensitive, and field-sensitive program slicing, and benchmark comparisons of leading solutions. We also obtained a trove of security insights into Java secure coding practices. An **open research problem** is designing a compiler that automatically transforms a cryptographic vulnerability or rule into a static-analysis-based code-screening algorithm, similar to what CrySL partially provides, but with much higher expressiveness, precision, and recall.

## REFERENCES

- [1] Coverity Static Application Security Testing (SAST).
- [2] Spotbugs: Find Bugs in Java Programs.
- [3] Cryptographic Key Length Recommendation. <https://www.keylength.com/en/4/>, 2016. [Online; accessed 29-Jan-2018].
- [4] Google Play Warning: How to fix incorrect implementation of HostnameVerifier? <https://stackoverflow.com/questions/41312795/google-play-warning-how-to-fix-incorrect-implementation-of-hostnameverifier>, 2016. [Online; accessed 29-Jan-2018].
- [5] Change the default Crypt Algo to use stronger cryptographic algo. "<https://issues.apache.org/jira/browse/RANGER-1644>", 2017. [Online; accessed Jan 26, 2018].
- [6] Class Random. <https://docs.oracle.com/javase/8/docs/api/java/util/Random.html>, 2017. [Online; accessed 29-Jan-2018].
- [7] Class SecureRandom. <https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html>, 2017. [Online; accessed 29-Jan-2018].
- [8] Lifetimes of cryptographic hash functions. <http://valerieaurora.org/hash.html>, 2017. [Online; accessed 29-Jan-2018].
- [9] List of Rainbow Tables. <http://project-rainbowcrack.com/table.htm>, 2017. [Online; accessed 29-Jan-2018].
- [10] Update Doc/Wiki to provide details on using custom encryption key and salt for encryption of credentials. <https://issues.apache.org/jira/browse/RANGER-1645>, 2017. [Online; accessed Jan 26, 2018].
- [11] Google rejected app because of HostnameVerifier issue. "<https://stackoverflow.com/questions/48420530/google-rejected-app-because-of-hostnameverifier-issue>", 2018. [Online; accessed Jan 26, 2018].
- [12] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky. Comparing the Usability of Cryptographic APIs. In *IEEE S&P'17*, pages 154–171, 2017.
- [13] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky. You Get Where You're Looking for: The Impact of Information Sources on Code Security. In *IEEE S&P'16*, pages 289–305, 2016.
- [14] Y. Acar et al. Developers Need Support, Too: A Survey of Security Advice for Software Developers. In *IEEE Secure Development Conference SecDev*, 2017.
- [15] D. Adrian et al. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In *ACM CCS'15*, pages 5–17, 2015.
- [16] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. L. Traon, D. Oeteau, and P. D. McDaniel. FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. In *ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '14*, pages 259–269, 2014.
- [17] M. Backes, S. Bugiel, and E. Derr. Reliable Third-Party Library Detection in Android and its Security Applications. In *ACM CCS'16*, pages 356–367, 2016.
- [18] G. V. Bard. The Vulnerability of SSL to Chosen Plaintext Attack. *IACR Cryptology ePrint Archive*, 2004:111, 2004.
- [19] D. J. Bernstein, Y. Chang, C. Cheng, L. Chou, N. Heninger, T. Lange, and N. van Someren. Factoring RSA Keys from Certified Smart Cards: Copersmith in the Wild. In *ASIACRYPT'13*, pages 341–360, 2013.
- [20] K. Bhargavan and G. Leurent. On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. In *ACM CCS'16*, pages 456–467, 2016.
- [21] K. Bhargavan and G. Leurent. Transcript Collision Attacks: Breaking Authentication in TLS, IKE and SSH. In *NDSS'16*, 2016.
- [22] A. Bianchi, Y. Fratantonio, A. Machiry, C. Kruegel, G. Vigna, S. Chung, and W. Lee. Broken Fingers: On the Usage of the Fingerprint API in Android. In *NDSS'18*, 2018.
- [23] A. Bianchi, Y. Fratantonio, A. Machiry, C. Kruegel, G. Vigna, S. P. H. Chung, and W. Lee. Broken Fingers: On the Usage of the Fingerprint API in Android. In *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*, 2018.
- [24] D. Boneh. Twenty Years of Attacks on the RSA Cryptosystem. *NOTICES OF THE AMS*, 46(2), 1999.
- [25] A. Bosu, F. Liu, D. D. Yao, and G. Wang. Collusive Data Leak and More: Large-scale Threat Analysis of Inter-app Communications. In *ACM AsiaCCS'17*, pages 71–85, 2017.
- [26] D. Chang, A. Jati, S. Mishra, and S. K. Sanadhya. Cryptanalytic Time-Memory Tradeoff for Password Hashing Schemes. *IACR Cryptology ePrint Archive*, 2017:603, 2017.
- [27] S. Checkoway, J. Maskiewicz, C. Garman, J. Fried, S. Cohney, M. Green, N. Heninger, R. Weinmann, E. Rescorla, and H. Shacham. A Systematic Analysis of the Juniper Dual EC Incident. In *ACM CCS'16*, pages 468–479, 2016.
- [28] A. Chi, R. A. Cochran, M. Nesfield, M. K. Reiter, and C. Sturton. A System to Verify Network Behavior of Known Cryptographic Clients. In *USENIX NSDI'17*, pages 177–195, 2017.
- [29] J. de Ruiter and E. Poll. Protocol State Fuzzing of TLS Implementations. In *USENIX Security'15*, pages 193–206, 2015.
- [30] Welcome to the SWAMP. <https://continuousassurance.org>, 2018.
- [31] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel. An empirical study of cryptographic misuse in Android applications. In *ACM CCS'13*, pages 73–84, 2013.
- [32] K. O. Elish, X. Shu, D. D. Yao, B. G. Ryder, and X. Jiang. Profiling user-trigger dependence for Android malware detection. *Computers & Security*, 49:255–273, 2015.
- [33] S. Fahl, M. Harbach, T. Muders, M. Smith, L. Baumgärtner, and B. Freislenben. Why Eve and Mallory love Android: an analysis of Android SSL (in)Security. In *ACM CCS'12*, pages 50–61, 2012.
- [34] F. Gagnon, M. Ferland, M. Fortier, S. Desloges, J. Ouellet, and C. Boileau. AndroSSL: A Platform to Test Android Applications Connection Security. In *FPS'15*, pages 294–302, 2015.
- [35] C. P. García, B. B. Brumley, and Y. Yarom. "Make Sure DSA Signing Exponentiations Really are Constant-Time". In *ACM CCS'16*, pages 1639–1650, 2016.
- [36] C. Garman, M. Green, G. Kaptchuk, I. Miers, and M. Rushanan. Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage. In *USENIX Security'16*, pages 655–672, 2016.
- [37] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov. The most dangerous code in the world: validating SSL certificates in non-browser software. In *ACM CCS'12*, 2012.
- [38] I. Goldberg and D. Wagner. Randomness and the Netscape browser. *Dr Dobb's Journal-Software Tools for the Professional Programmer*, 21(1):66–71, 1996.
- [39] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. In *USENIX Security'12*, pages 205–220, 2012.
- [40] D. Hovemeyer and W. Pugh. Finding bugs is easy. *SIGPLAN Notices*, 39(12):92–106, 2004.
- [41] B. Johnson et al. Why don't software developers use static analysis tools to find bugs? In *ICSE'13*, pages 672–681, 2013.
- [42] H. Krawczyk. How to Predict Congruential Generators. In *CRYPTO'89*, pages 138–153, 1989.
- [43] S. Krüger et al. CogniCrypt: supporting developers in using cryptography. In *IEEE/ACM ASE'17*, pages 931–936, 2017.
- [44] S. Krüger, J. Späth, K. Ali, E. Bodden, and M. Mezini. CrvSL: An Extensible Approach to Validating the Correct Usage of Cryptographic APIs. In *ECOOP'18*, pages 10:1–10:27, 2018.
- [45] Y. Kwon, B. Saltzman, I. L. Kim, K. H. Lee, X. Zhang, and D. Xu. A2C: Self destructing exploit executions via input perturbation. In *NDSS'17*, 2017.
- [46] D. Lazar, H. Chen, X. Wang, and N. Zeldovich. Why does cryptographic software fail?: A case study and open problems. In *APSYS'14*, 2014.
- [47] J. Li, Z. Lin, J. Caballero, Y. Zhang, and D. Gu. K-Hunt: Pinpointing Insecure Cryptographic Keys from Execution Traces. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 412–425, 2018.
- [48] R. Lippmann and R. K. Cunningham. Improving intrusion detection performance using keyword selection and neural networks. *Computer Networks*, 34(4):597–603, 2000.
- [49] A. D. Lucia. Program Slicing: Methods and Applications. In *IEEE International Workshop on Source Code Analysis and Manipulation SCAM'01*, pages 144–151, 2001.
- [50] S. Ma, D. Lo, T. Li, and R. H. Deng. CDRep: Automatic Repair of Cryptographic Misuses in Android Applications. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2016*, pages 711–722, 2016.
- [51] S. Ma, F. Thung, D. Lo, C. Sun, and R. H. Deng. VuRLE: Automatic Vulnerability Detection and Repair by Learning from Examples. In *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security*, pages 229–246, 2017.
- [52] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G. A. Argoty. Secure Coding Practices in Java: Challenges and Vulnerabilities. In *ACM ICSE'18*, Gothenburg, Sweden, May 2018.
- [53] K. Moriarty, B. Kaliski, and A. Rusch. PKCS# 5: Password-Based Cryptography Specification Version 2.1. 2017.
- [54] V. Murali, S. Chaudhuri, and C. Jermaine. Bayesian specification learning for finding API usage errors. In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, ESEC/FSE 2017, Paderborn, Germany*, 2017.

- September 4-8, 2017, pages 151–162, 2017.
- [55] S. Nadi, S. Krüger, M. Mezini, and E. Bodden. Jumping Through Hoops: Why Do Java Developers Struggle with Cryptography APIs? In *ICSE’16*, pages 935–946, 2016.
- [56] Y. Nan, Z. Yang, X. Wang, Y. Zhang, D. Zhu, and M. Yang. Finding Clues for Your Secrets: Semantics-Driven, Learning-Based Privacy Discovery in Mobile Apps. In *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*, 2018.
- [57] D. C. Nguyen et al. A Stitch in Time: Supporting Android Developers in Writing Secure Code. In *ACM CCS’17*, pages 1065–1077, 2017.
- [58] R. Paletov, P. Tsankov, V. Raychev, and M. T. Vechev. Inferring crypto API rules from code changes. In *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2018*, pages 450–464, 2018.
- [59] X. Pan, X. Wang, Y. Duan, X. Wang, and H. Yin. Dark Hazard: Learning-based, Large-Scale Discovery of Hidden Sensitive Operations in Android Apps. In *NDSS’17*, 2017.
- [60] N. H. Pham, T. T. Nguyen, H. A. Nguyen, and T. N. Nguyen. Detection of recurring software vulnerabilities. In *ASE 2010, 25th IEEE/ACM International Conference on Automated Software Engineering*, pages 447–456, 2010.
- [61] S. Rahaman and D. Yao. Program Analysis of Cryptographic Implementations for Security. In *IEEE Secure Development Conference (SecDev)*, 2017, pages 61–68, 2017.
- [62] N. Rutar, C. B. Almazan, and J. S. Foster. A comparison of bug finding tools for Java. In *15th International Symposium on Software Reliability Engineering (ISSRE 2004)*, pages 245–256, 2004.
- [63] S. Sivakorn, G. Argyros, K. Pei, A. D. Keromytis, and S. Jana. HVLearn: Automated Black-Box Analysis of Hostname Verification in SSL/TLS Implementations. In *IEEE S&P’17*, pages 521–538, 2017.
- [64] J. Somorovsky. Systematic Fuzzing and Testing of TLS Libraries. In *ACM CCS’16*, pages 1492–1504, 2016.
- [65] D. Souonthiraj, J. Sahs, G. Greenwood, Z. Lin, and L. Khan. SMV-Hunter: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps. In *NDSS’14*, 2014.
- [66] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. The First Collision for Full SHA-1. In *CRYPTO’17*, 2017.
- [67] M. Stevens, A. K. Lenstra, and B. de Weger. Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities. In *EUROCRYPT’07*, pages 1–22, 2007.
- [68] Update to Current Use and Deprecation of TDEA, 2017. <https://csrc.nist.gov/ncw/2017/update-to-current-use-and-deprecation-of-tdea>.
- [69] V. van der Veen et al. Drammer: Deterministic Rowhammer Attacks on Mobile Platforms. In *ACM CCS’16*, pages 1675–1689, 2016.
- [70] K. Xu, D. Yao, B. Ryder, and K. Tian. Probabilistic Program Modeling for High-Precision Anomaly Classification. In *CSF’15*, July 2015.
- [71] H. Y. Yang, E. D. Temporo, and H. Melton. An Empirical Study into Use of Dependency Injection in Java. In *Australian Software Engineering Conference ASWEC’08*, pages 239–247, 2008.
- [72] D. Yao, X. Shu, L. Cheng, and S. J. Stolfo. *Anomaly Detection as a Service: Challenges, Advances, and Opportunities*. In *Information Security, Privacy, and Trust Series*. Morgan & Claypool, 2017.
- [73] T. Zhang, G. Upadhyaya, A. Reinhardt, H. Rajan, and M. Kim. Are code examples on an online Q&A forum reliable?: a study of API misuse on stack overflow. In *Proceedings of the 40th International Conference on Software Engineering, ICSE 2018*, pages 886–896, 2018.
- [74] C. Zuo, Z. Lin, and Y. Zhang. Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps. In *IEEE S&P’16*, 2019.

## 10 APPENDIX

### 10.1 Other Refinement insights

#### RI-III: Removal of bookkeeping indices.

```
1 byte[] iv = new byte[] {0x0, 0x0, 0x0,
2   0x0, 0x0, 0x0, 0x0}
```

Consider the Java statement above. After transforming into jimple representation, this statement looks like the following list of instructions.

```
1   $r15 = newarray (byte) [8]
2   $r15[0] = 0
3   $r15[1] = 0
4   $r15[2] = 0
5   $r15[3] = 0
6   $r15[4] = 0
```

```
7   $r15[5] = 0
8   $r15[6] = 0
9
10  $r2 = $r15
```

The hard coded size and the indices of an array can be regarded as pseudo-influences. To address this false positives, we discard all the constants that influences an array index. Also, any constant that influences the size or the index parameter of a collection can also be regarded as pseudo-influences. We regard List, Set as collections.

#### RI-IV: Removal of contextually incompatible constants.

Clipping of orthogonal invocations that doesn’t appear in an assign statement can also cause false positives. To reduce false alarms further, we also discard some constants constants based on its type and context. Let’s consider, a class named PBEInfo is used to store iteration count and salt and the analysis cannot explore PBEInfo class. A basic use-def analysis will report 5 as a salt from the following invoke instruction: `specialinvoke r1.<KeyHolder: void <init>(Integer, String)>(5, "5341453")`. However, a standalone Boolean or Integer constant is unlikely to be used as a key, IV or salt, since their corresponding APIs only allow byte arrays. Also, any hard-coded size parameter (e.g., number of iterations in PBE (Rule 13), key size for insecure asymmetric crypto (Rule 15)) is unlikely to have any type other than `Integer`. Therefore, it is possible to discard some of the pseudo-influences by considering the types of a constant based on its context.

#### RI-V: Removal of constants in infeasible paths.

Some constant initializations are overwritten along the path to the point of interest. Counting such constants with infeasible influences will result in false positives. Since, empty strings and `null`s are used for initialization purpose and most often, these initialization are replaced with other values. To avoid false positive for this case, depending on rules and the slicing criteria we discard `null` and empty strings. For example, `SecretKeySpec` prohibits keys to be `null` or empty. `IvParameterSpec` does not allow `null` as IV. Also, `PBEParameterSpec` does not allow the salt to be `null`.

## 10.2 Other Evaluation Results

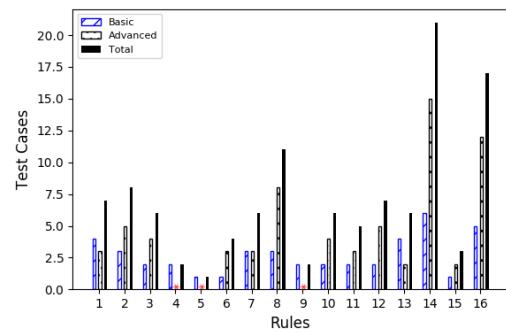


Figure 7: Test cases per Rule in CRYPTOAPI-BENCH.

**Table 6: The number of alerts in Apache (total 94 root-subprojects) and Android applications (6,181). For Rules 1, 2, 3, 8, 10, 12, each constant/predictable value of an array/collection is considered as an individual violation.**

Rules	Apache		Android	
	# of Root-subprojects	# of Alerts Per Rule	# of Applications	#of Alerts Per Rule
(1,2) Predictable Keys	37 (39.36%)	264	1,617 (26.16%)	12,457
(3) Hardcoded Store Password	29 (30.85%)	148	218 (3.52%)	458
(4) Dummy Hostname Verifier	8 (8.51%)	12	800 (12.94%)	1,155
(5) Dummy Cert. Validation	11 (11.70%)	30	1,564 (25.30%)	3,856
(6) Used Improper Socket	4 (4.25%)	4	210 (3.39%)	271
(7) Used HTTP	24 (29.62%)	222	2,486 (40.22%)	8,321
(8) Predictable Seeds	0 (0%)	0	80 (1.29%)	544
(9) Untrusted PRNG	33 (35.10%)	142	5,194 (84.03%)	36,223
(10) Static Salts	21 (22.34%)	112	199 (3.21%)	1,757
(11) ECB mode for Symm. Crypto	16 (17.02 %)	41	882 (14.26%)	1,780
(12) Static IVs	4 (4.25 %)	41	913 (14.77%)	12,089
(13)<1000 PBE Iterations	25 (26.59 %)	43	151 (2.44%)	312
(14) Broken Symm. Crypto Algorithms	29 (30.85 %)	86	701 (11.34%)	1,742
(15) Insecure Asymm. Crypto	9 (10.98 %)	12	108 (1.74%)	111
(16) Broken Hash	42 (44.68 %)	138	5,272 (85.29%)	49,769

**Table 7: Benchmark comparison of CrySL, Coverity, SpotBugs, and CryptoGuard on all 16 rules with CRYPTOAPI-BENCH’s 112 test cases. There are 16 secure API use cases (13 in basic and 3 in advanced), which a tool should not raise any alerts on. CRYPTOGERD successfully passed these 16 test cases. GTP stands for ground truth positive, which is the number of positives in the benchmark. CRYPTOGERD has 11 false negatives, which we reported in Section 6 and discussed in Section 7.**

No.	Rules	GTP	CrySL		Coverity		SpotBugs		CryptoGuard	
			TP	FP	TP	FP	TP	FP	TP	FP
1	Predictable Cryptographic Key	5	0	4	3	0	2	0	5	0
2	Predictable Password for PBE	6	0	2	5	0	3	0	6	0
3	Predictable Password for KeyStore	5	0	5	3	0	2	0	5	0
4	Dummy Hostname Verifier	1	—	—	1	0	1	0	1	0
5	Dummy Cert. Validation	1	—	—	1	0	1	0	1	0
6	Used Improper Socket	4	—	—	4	0	—	—	4	0
7	Use of HTTP	4	—	—	—	—	—	—	4	0
8	Predictable Seed	10	—	—	1	0	—	—	5	0
9	Untrusted PRNG	1	—	—	—	—	1	0	1	0
10	Static Salt	5	5	1	—	—	—	—	3	0
11	ECB in Symm. Crypto	4	2	1	1	0	1	1	4	0
12	Static IV	6	0	6	—	—	6	0	4	0
13	<1000 PBE Iteration	5	2	1	—	—	—	—	4	0
14	Broken Symm. Crypto	20	10	5	4	0	5	5	20	0
15	Insecure Asymm. Crypto	3	2	1	—	—	0	1	2	0
16	Broken Hash	16	8	4	4	0	4	4	16	0
Total		96	29	30	27	0	26	11	85	0

**Table 8: Rules that use intra-procedural backward program slicing to slice implemented methods of standard Java APIs and their corresponding slicing criteria.**

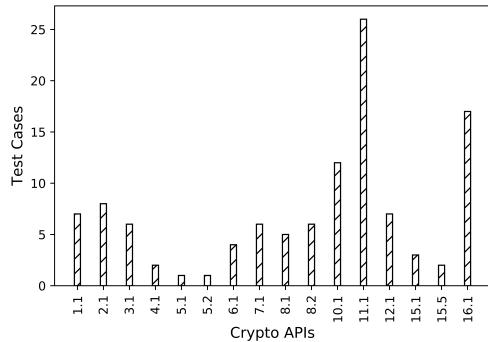
No.	Method to Slice	Rule	Criterion
4.1	javax.net.ssl.HostnameVerifier: boolean verify(String, SSLSession)	4	return
5.1	void checkServerTrusted(X509Certificate[], String)	5	checkValidity()
5.2	void checkServerTrusted(X509Certificate[], String)	5	throw
5.3	java.security.cert.X509Certificate[] getAcceptedIssuers()	5	return

**Table 9: Java APIs used as slicing criteria in our intra-procedural forward program slicing and their corresponding security rules.**

No.	Slicing Criterion for Intra Procedural Forward Program Slicing	Rule	Semantic
6.1	javax.net.ssl.SSLSocketFactory: SocketFactory getDefault()	6	Create SocketFactory
6.2	javax.net.ssl.SSLContext: SSLSocketFactory getSocketFactory()	6	Create SocketFactory
15.1	java.security.KeyPairGenerator: KeyPairGenerator getInstance(java.lang.String)	15	Create KeyPairGenerator
15.2	java.security.KeyPairGenerator: KeyPairGenerator getInstance(String, String) >	15	Create KeyPairGenerator
15.3	java.security.KeyPairGenerator: KeyPairGenerator getInstance(String, Provider)	15	Create KeyPairGenerator

**Table 10: Java APIs used as slicing criteria in our inter-procedural backward slicing and their corresponding security rules. Boldface indicates the parameter of interest.**

No.	API	Rule	Semantic
1.1	javax.crypto.spec.SecretKeySpec: void <init>( <b>byte</b> [], String)	1	Set key
1.2	javax.crypto.spec.SecretKeySpec: void <init>( <b>byte</b> [], int, int, String)	1	Set key
2.1	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [])	2	Set password
2.2	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [], <b>byte</b> [], int, int)	2	Set password
2.3	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [], <b>byte</b> [], int)	2	Set password
3.1	java.security.KeyStore: void load(InputStream, <b>char</b> [])	3	Set password
3.2	java.security.KeyStore: void store(OutputStream, <b>char</b> [])	3	Set password
3.3	java.security.KeyStore: void setKeyEntry(String, Key, <b>char</b> [], Certificate[])	3	Set password
3.4	java.security.KeyStore: Key getKey(String, <b>char</b> [])	3	Set password
7.1	java.net.URL: void <init>( <b>String</b> )	7	Set URL
7.2	java.net.URL: void <init>( <b>String</b> , String, String)	7	Set URL
7.3	java.net.URL: void <init>( <b>String</b> , String, int, String)	7	Set URL
7.4	okhttp3.Request\$Builder: Request\$Builder url ( <b>String</b> )	7	Set URL
7.5	retrofit2.Retrofit\$Builder: Retrofit\$Builder baseUrl( <b>String</b> )	7	Set URL
8.1	java.security.SecureRandom: void <init>( <b>byte</b> [])	8	Set seed
8.2	java.security.SecureRandom: void setSeed( <b>byte</b> [])	8	Set seed
8.3	java.security.SecureRandom: void setSeed( <b>long</b> )	8	Set seed
10.1	javax.crypto.spec.PBESpecParameterSpec: void <init>( <b>byte</b> [], int)	10	Set salt
10.2	javax.crypto.spec.PBESpecParameterSpec: void <init>( <b>byte</b> [], int, AlgorithmParameterSpec)	10	Set salt
10.3	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [], <b>byte</b> [], int, int)	10	Set salt
10.4	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [], <b>byte</b> [], int)	10	Set salt
11.1	javax.crypto.Cipher: Cipher getInstance( <b>String</b> )	11, 14	Select cipher
11.2	javax.crypto.Cipher: Cipher getInstance( <b>String</b> , String)	11, 14	Select cipher
11.3	javax.crypto.Cipher: Cipher getInstance( <b>String</b> , Provider)	11, 14	Select cipher
12.1	javax.crypto.spec.IvParameterSpec: void <init>( <b>byte</b> [])	12	Set IV
12.2	javax.crypto.spec.IvParameterSpec: void <init>( <b>byte</b> [], int, int)	12	Set IV
13.1	javax.crypto.spec.PBESpecParameterSpec: void <init>( <b>byte</b> [], int)	13	Set iterations
13.2	javax.crypto.spec.PBESpecParameterSpec: void <init>( <b>byte</b> [], int, AlgorithmParameterSpec)	13	Set iterations
13.3	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [], <b>byte</b> [], int, int)	13	Set iterations
13.4	javax.crypto.spec.PBEKeySpec: void <init>( <b>char</b> [], <b>byte</b> [], int)	13	Set iterations
15.1	java.security.KeyPairGenerator: KeyPairGenerator getInstance( <b>String</b> )	15	Select generator
15.2	java.security.KeyPairGenerator: KeyPairGenerator getInstance( <b>String</b> , String) >	15	Select generator
15.3	java.security.KeyPairGenerator: KeyPairGenerator getInstance( <b>String</b> , Provider)	15	Select generator
15.4	java.security.KeyPairGenerator: void initialize(int)	15	Set key size
15.5	java.security.KeyPairGenerator: void initialize(int, java.security.SecureRandom)	15	Set key size
15.6	java.security.KeyPairGenerator: void initialize(AlgorithmParameterSpec)	15	Set key size
15.7	java.security.KeyPairGenerator: void initialize(AlgorithmParameterSpec, SecureRandom)	15	Set key size
16.1	java.security.MessageDigest: MessageDigest getInstance( <b>String</b> )	16	Select hash
16.2	java.security.MessageDigest: MessageDigest getInstance( <b>String</b> , String)	16	Select hash
16.3	java.security.MessageDigest: MessageDigest getInstance( <b>String</b> , Provider)	16	Select hash



**Figure 8:** Test cases per API in CRYPTOAPI-BENCH. A test case can cover one or more APIs (e.g., test cases for Rule 15). APIs corresponding to the labels can be found in Tables 10, 8, and 9.