sPECTRA: a Precise framEWork for analyzing CrypTographic vulneRabies in Android apps

Jyoti Gajrani*, Meenakshi Tripathi*, Vijay Laxmi*, M.S. Gaur*, Mauro Conti†, Muttukrishnan Rajarajan‡

*MNIT, Jaipur, INDIA, {2014rcp9542, mtripathi.cse, vlaxmi, gaurms}@mnit.ac.in
†University of Padua, Italy, conti@math.unipd.it
‡City University London, R.Muttukrishnan@city.ac.uk

Abstract—The majority of Android applications (apps) deals with user’s personal data. Users trust these apps and allow them to access all sensitive data. Cryptography, when employed in an appropriate way, can be used to prevent misuse of data. Unfortunately, cryptographic libraries also include vulnerable cryptographic services. Since Android app developers may not be cryptographic experts, this makes apps become the target of various attacks due to cryptographic vulnerabilities.

In this work, we present sPECTRA: an automated framework for analyzing wide range of cryptographic vulnerabilities in Android apps at large scale. sPECTRA is more precise and accurate in comparison to state-of-the-art approaches as it reduces both false negatives and false positives. The inclusion of Intelligent UI exploration during dynamic analysis makes sPECTRA deployable to analyze apps at large scale. Moreover, sPECTRA works on apk files without the need of any source code.

We evaluate sPECTRA on 7,000 apps collected from 7 most popular Android app stores. Results indicate that 90% of apps are exploitable because of cryptographic vulnerabilities. We made sPECTRA available as an open source1.

Index Terms—cryptographic, APIs, vulnerabilities, Android, attacks.

I. INTRODUCTION

With the rapid growth of smartphone technology, our daily life is becoming more dependent on smartphones. Among various smartphone technologies, Android share is worth 84.1% by Q1 2016 [1]. Users trust mobile apps and grant them access to their personal information. Therefore, all the private data that is taken by these apps either for storage on the device or for transmission out of the device must be secured with strong cryptographic services.

Cryptographic providers like Java Cryptographic Architecture (JCA) [7], BouncyCastle [14] and SpongyCastle [12] provide a set of cryptographic APIs (Application Program Interface) for developers. These cryptographic APIs and associated parameters must be used in the correct way to provide strong security guarantees otherwise the incorrect way may lead to attacks such as Man-in-the-mobile (MitMo) attacks, Brute-force attacks, and Dictionary attacks. In [19], researchers shown the first key recovery attack on full AES-128 with computational complexity 2^{26}.1.

Android has become the preferred target for financial malware due to large market coverage and plenty of reported attacks. Cryptographers know what are the most secure parameters to be used with these APIs in the way to ensure strong security guarantee however, may not be the same for software developers. Developers may invoke a wrong API function, set incorrect parameters, and check the return values improperly and so on. Therefore, not only the developers but app distributors must check for vulnerabilities in apps before publishing them to markets to prevent any loss of end-user. Correct usage of cryptographic primitives (low-level cryptographic algorithms) such as strong encryption algorithms, random keys, key-length, padding with block ciphers, validation of SSL/TLS certificates, digital signature algorithms, salts, and iteration count ensures resilience against cryptographic exploits.

In this paper, we propose sPECTRA, an automated framework using hybrid analysis for detection of such vulnerabilities in Android apps to provide high-security guarantees to app users. The main contributions of sPECTRA are summarized as follows:

- sPECTRA analyzes a wide range of cryptographic vulnerabilities in comparison to state-of-the-art approaches.
- sPECTRA includes intelligent techniques to enable automated vulnerability analysis at large scale. We show the efficacy of sPECTRA by analyzing of 7000 Android apps collected from 7 different app repositories. The results show that almost 90% of the apps using cryptographic features are vulnerable.
- sPECTRA includes lightweight approaches to speedup the analysis.

We release sPECTRA as open source1 to drive research in this direction. sPECTRA will be made available as web-based analysis service to benefit developers and app stores.

II. CRYPTOGRAPHIC PRIMITIVES AND ASSOCIATED VULNERABILITIES

This section briefly covers cryptographic primitives and the inappropriate usage of these primitives which makes the apps vulnerable to various cryptographic attacks.

A. Cryptographic APIs

Listing 1 shows the code that implements encryption of IMEI number using Password-Based Encryption (PBE). This code contains a set of cryptographic vulnerabilities.
SecureRandom class provides a cryptographically strong pseudo-random number generator unfortunately, this is seeded with constant Seed (Line 4). Use of static value for seeding may completely replace the cryptographically strong default seed causing it to generate an anticipated sequence of salts (Line 7) which are unfit for secure use. Random salt restricts the attackers from pre-computing a dictionary of derived keys.

TABLE I: Cryptographic Primitives and Associated Vulnerabilities

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Use/Focus</th>
<th>Vulnerabilities</th>
<th>Implemented Attacks</th>
<th>Few Relevant APIs Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric Encryption</td>
<td>Securely storing data/keys.</td>
<td>Chosen-plaintext attacks.</td>
<td>ivParameterSpec.init()</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure transmission of sensitive data.</td>
<td>Brute-force attacks.</td>
<td>KeyGenerator.init()</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cipher.getInstance()</td>
<td></td>
</tr>
<tr>
<td>Digital Signature</td>
<td>Digitally Signing certificates</td>
<td>Hash Collision</td>
<td>Signature.getInstance()</td>
<td></td>
</tr>
<tr>
<td>Padding</td>
<td>NoPadding</td>
<td>Collision-based attacks.</td>
<td>PBEKeySpec.init()</td>
<td></td>
</tr>
<tr>
<td>Message Digest</td>
<td>Hashes of user credentials.</td>
<td>Length Extension attacks.</td>
<td>SecretKeyFactory.generateSecret()</td>
<td></td>
</tr>
<tr>
<td>Key Derivation</td>
<td>Random Key generation using secure PRNG</td>
<td>Static key Material.</td>
<td>SecretKeySpec.init()</td>
<td></td>
</tr>
<tr>
<td>Key Generation</td>
<td></td>
<td>Collision-based attacks.</td>
<td>SecretKeyFactory.generateSecret()</td>
<td></td>
</tr>
<tr>
<td>Pseudo-Random Number Generation</td>
<td>Random Salt</td>
<td>Constant Seed</td>
<td>SecureRandom.random.setSeed()</td>
<td></td>
</tr>
<tr>
<td>SSL/TLS protocol</td>
<td>Communication Security</td>
<td>HostnameVerifier, TrustManager</td>
<td>File.init()</td>
<td></td>
</tr>
<tr>
<td>On-Device Storage</td>
<td>Storing data in shared storage</td>
<td>Writing to &quot;sdcard/*&quot;.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Listing 1: Vulnerable use of cryptographic Primitives

PBEKeySpec Spec (Line 9) used for generating KeySpec is vulnerable due to use of static salt (second parameter of PBEKeySpec API) and iteration count (IC) (third parameter of PBEKeySpec API) with value 256 (must be minimum 1000 [11]). Larger IC complicates the key derivation function and increases the difficulty of brute force attack. Further, it performs encryption using AES algorithm in ECB mode (Line 14) which has proven vulnerable. This is because this mode will generate the same cipher-text if the same plain-text is encrypted with the same key. The code specifies NoPadding as Padding Scheme (Line 14). However, Padding must be present with ciphers to prevent the cryptanalyst in predicting plain-text message length.

Table I summarizes various cryptographic primitives used by Android apps, associated vulnerabilities based on National Institute of Standards and Technology (NIST) and Federal Office for Information Security (BSI) recommendations, and the attacks that can exploit these vulnerabilities. To prevent Android apps from these attacks, all the cryptographic APIs must be critically analyzed. For each primitive mentioned in Table I, column 1, we exhaustively identified all APIs provided by at least three libraries SunJCE, BouncyCastle and SpoonsyCastle. Further, we analyzed all vulnerable values for each of these APIs and prepared vulnerability database. Table I, last column include some of these APIs from SunJCE.

B. SSL/TLS Connection Validation

Apps use SSL/TLS protocols with the goal to securely transmit sensitive data to the server. During SSL connection establishment, two conditions are validated:

- Hostname of the server must match CommonName mentioned in certificate presented by server.
- There must exist trust chain between the certificate presented by the server and the root CA certificates pre-installed on mobile.

Two JCA classes HostnameVerifier and X509TrustManager are used to validate above conditions respectively but vulnerability in custom implementation of validation methods may lead to MiTM attacks. Listings 2-3 shows code snippet with HostnameVerifier vulnerability. HostnameVerifier's verify() method always returns true as shown in Listing 2 (Line 3) which means even if Hostname does not match CommonName, it returns true. This makes the code vulnerable. In Listing 3, SSLSocketFactory create SSL socket but it allows all hostnames (Line 2) through setHostnameVerifier API.

Listing 2: Vulnerable HostnameVerifier

Listing 3: Vulnerable HostnameVerifier

Listing 4 shows code snippet with TrustManager vulnerability. Here, SSLSocketFactory accept all certificates irrespective of its signer as shown by blank overridden checkServerTrusted() method without any exception.
Vulnerability Report

C. Vulnerable On-device Storage

External storage is shared in Android and must not be used for storing any private data of an app. Even encrypted storage is also vulnerable through covert and overt channels.

III. METHODOLOGY AND DESIGN

Figure 1 shows overall work-flow of framework. sPECTRA is designed to work in two phases. Phase 1 prepares the set of all cryptographic APIs used by app. The app using cryptographic primitives is potentially sensitive app. Section III.1 covers the detail of this phase. Phase 2 performs precise vulnerability analysis of only sensitive apps. This phase comprises four major functions: SSL/TLS Vulnerability Identification, App Hooking and Repackaging, Intelligent UI Exploration and Log Parsing. Section III.2 covers the details of Phase 2.

1. Phase 1

Implementation of this phase is done using Androguard framework [2]. A method descriptor represents the type of parameters that the method takes and the value that it returns. Method descriptors extracted from app using Androguard (get_descriptors() utility) are used to filter sensitive apps. The four primary packages, relevant to crypto APIs are javax.crypto, javax.crypto.spec, java.security and javax.net.ssl. Therefore, all methods that make use of cryptographic APIs have patterns “crypto”, “security” or “ssl”, in their descriptors. All methods having any of above descriptor pattern are filtered in Step 2, Figure 1 (using get_methods() utility). Next step constructs the set \( \xi_A \) (the set of all cryptographic sensitive APIs used by the app \( A \)) using filtered methods (Step 3, Figure 1). It is done by finding actual APIs used in source code, with the help of get_source() method of Androguard.

As shown in Equation 1, empty set \( \xi_A \) indicates that the app is Non-Sensitive app. App with Non-Empty set \( \xi_A \) is marked as a potentially sensitive app.

\[
\text{App} = \begin{cases} 
\text{Non - Sensitive,} & \text{if } \xi_A = \emptyset \\
\text{Sensitive,} & \text{otherwise}
\end{cases}
\]  

Listing 5 shows the result of Phase 1 analysis for Mobikwik app\(^2\). As shown in result, few of the arguments can be checked for vulnerability directly but for others, vulnerability identification require actual run-time values. Moreover, it is observed that for obfuscated apps, the vulnerable arguments can not be inferred from phase 1. The parameter declaration, definition and API using it may all be distributed over different components. The asynchronous nature and presence of multiple components in Android makes static backward slicing imprecise to find arguments. Therefore, to obtain vulnerabilities precisely, sensitive app is further analyzed by Phase 2. The set \( \xi_A \) is input for next phase.

2. Phase 2

The details of four major modules of this phase are as follows:

A. SSL/TLS Certificate Validation

The module identifies vulnerable implementations of SSL/TLS certificate validation using static analysis. The analysis is implemented on top of Soot library [23]. Soot’s tagging feature is employed to tag apps as “Vulnerable” or “Non-Vulnerable”. Initially, tags are set to “Non-Vulnerable”. The analysis utilizes Soot’s Points-To analysis, Control Flow Graph (CFG) and Data-Flow analysis features. Point-To analysis is a static analysis techniques that aims to find objects, a pointer/reference may point during execution of program. For e.g. if \( p = \& x; \ p = \& y; \) then \( p \) may points to \( x \) or \( y \) during execution. Therefore Points-To analysis of \( p \) gives set Points-To(\( p \)) = \( \{x, y\}\) . sPECTRA first generate intermediate representations (IRs) in form of CFG, Points-To set and then apply following checks on IRs:

a) The module analyze exit nodes in CFG of class containing HostnameVerifier interface for return value. Vulnerability is reported if it always returns a true value.

Listing 6 shows the source code snippet. Whenever verify method of HostnameVerifier class is called (Line 4), UnitGraph is constructed for the class (Line 5). The state

is marked as VULNERABLE if all the tails (Line 6) of graph return value of 1 (True) (Line 12).

b) For listing 3, to find whether HostnameVerifier is vulnerable or not. Points-To set of SSLSocketFactory is calculated. If the set contains AllowAllHostnameVerifier then it is marked as vulnerable.

c) sPECTRA mark the absence of an exception in custom implementations of X509TrustManager as vulnerable.

The absence of exception means not generating alerts in the case of non-validation of signing authority.

In all above cases, before reporting vulnerability, sPECTRA confirms that vulnerable instantiations of HostnameVerifier and TrustManager are used in any SSL connection using Data-Flow analysis. For e.g. vulnerabilities are reported for Listing 2 and 4 because vulnerable instantiation of HostnameVerifier in Listing 2-Line 1 is used at Line 6 and vulnerable TrustManager in Listing 4-Line 3 is used at Line 6. The Data-Flow analysis approach helps sPECTRA in addressing false positives.

Algorithm 1 covers the approach in more detail. UI Exploration begins by first finding all activities in the app A (app to test) and setting the corresponding flag as unexplored (Line 1). Exploration starts with Launcher Activity (Line 2). It finds all type of views in current activity if this activity is being loaded the first time and set the respective flags as false initially (Lines 7-11). Next, it performs zoom, scroll and click events on respective views in Depth-First order with all input type of views intelligently filled. An input value is provided based on the nearest placeholder of view. E.g., a placeholder with values “Number”, “Contact Number”, “Mobile”, “cell” is given a valid mobile number as input. After performing event on any view, the flag associated with that view is set. A delay is added to load the activity fully (Lines 13-23), and the process is repeated with loaded activity. Once all views of activity are explored, the activity’s explored flag is set (Lines 25-26) and ensured that this activity is not considered again (Line 6). App Exploration continues in this case by loading previous activity. It ensures that previous activity is not loaded if the current activity is Launcher Activity (Lines 25-31).

D. Log Parsing
The module exhaustively finds the vulnerabilities from the logs collected during app execution in the emulator. The logs collection is made using logcat utility of adb in parallel of UI Exploration by running both in separate subprocesses. sPECTRA maintains a database of cryptographic APIs along with vulnerable arguments and return values of all APIs of 3 crypto libraries. After the app exploration finishes, Parser module intelligently processes the collected logs. The module identifies vulnerabilities by testing each argument and the return value of the API against the database. If the app uses primitives like salt, key-material then the app exploration and log collection modules are executed second time. From processing both the logs it is ensured that multiple runs of app use the different values.

IV. Evaluation
sPECTRA’s evaluation is done on three fronts:
EMMA requires source code to find code coverage of Monkey. Intelligent UI Exploration module and Android's Monkey tool is used to obtain code coverage of both sPECTRA’s to the monkey tool due to the use of complete and deterministic exploration. EMMA [6], a code coverage measurement tool is used to obtain code coverage of both sPECTRA’s Intelligent UI Exploration module and Android’s Monkey. EMMA requires source code to find code coverage of Monkey.

Therefore, we downloaded 40 apps belonging to various categories from F-Droid\(^3\) and modified them by adding code coverage code. EMMA generates % code coverage in terms of Class, Method, Block and Line. Figure 2 shows the mean coverage (Class, Method, Block and Line) for both sPECTRA and Monkey for 14 representative apps (out of 40 measured). In the experiments, the Monkey is set to execute 5000 events that is quite a large number. Results for all 40 apps confirm that sPECTRA performs better than Monkey. This is attributed to following reasons:

1) sPECTRA includes context aware input generation for TextViews. A set of predefined inputs is maintained for different placeholders. E.g., a placeholder with values “Number,” “Contact Number,” etc. is given a valid mobile number as input. In this way, sPECTRA address the problem of Monkey which terminates the app on invalid input.

2) sPECTRA handles advanced UI elements like swipes, Long Press, tabs, spinners, etc. which are missing in Monkey.

3) The systematic handling of explored and unexplored views in each activity makes sPECTRA more complete system for code coverage.

Not only code coverage but sPECTRA also improves over Monkey and MonkeyRunner in other regards as mentioned in Table III.

![Fig. 2: UI Exploration Comparison](image)

<table>
<thead>
<tr>
<th>Property</th>
<th>sPECTRA</th>
<th>Monkey</th>
<th>Property</th>
<th>sPECTRA</th>
<th>MonkeyRunner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeatable Events</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Intelligent Text Input</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Crash Handling</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Scalability</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Effective Exploration</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Coordinate based UI Interaction</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Code Coverage</td>
<td>High</td>
<td>Low</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

False Negatives SMV-HUNTER [24] propose a hybrid approach for detection of SSL/TLS vulnerabilities where static analysis first marks the app as vulnerable if overriding of default validation methods is done. Then the dynamic phase performs actual Man-in-the-middle (MITM) attack for the marked app to confirm the vulnerability. But, due to reported crashes of MITM proxies in processing large number of requests, sPECTRA develop static analysis approach as detailed in Section III.2.A. For HostnameVerifier vulnerability, sPECTRA considers both the cases of Listing 2 and 3 while SMV-HUNTER only considers the case of Listing 3. This

\(^3\)https://f-droid.org/repository/browse/
leads to considerable number of false negatives by SMV-HUNTER. The popular playstore apps like BuzzWidget, SMS Blocker, OneDrive are found to be vulnerable by sPECTRA while SMV-HUNTER does not report the same.

In dynamic analysis based approach, a critical step in reducing false negatives is to trigger the vulnerable behavior by simulating the user interaction that leads to vulnerability. sPECTRA’s handling of advance views like tabs, long presses, spinners, valid inputs for textviews reduces the false negatives.

V. Results

Table IV shows the market-wise statistics of analyzed apps. We use Google-Play citegcrawler and Third-Party crawlers [10] to collect the samples for analysis. Out of these apps, 107 apps failed during analysis. Some of the apps failed as Soot was not able to analyze them, some failed during repackaging and some during exploration (not compatible with emulator).

### Table IV: Sample’s Statistics

<table>
<thead>
<tr>
<th>Domain/Market-Name</th>
<th>#Apps</th>
<th>Domain/Market-Name</th>
<th>#Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>google playstore</td>
<td>800</td>
<td>gfan</td>
<td>6000</td>
</tr>
<tr>
<td>nduoa</td>
<td>700</td>
<td>androidpur</td>
<td>366</td>
</tr>
<tr>
<td>mobomarket</td>
<td>58</td>
<td>appsapk</td>
<td>82</td>
</tr>
<tr>
<td>apkfun</td>
<td>31</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability report (partial) for mobikwik app after Phase 2 is as shown in Listing 7. The Listing shows that same salt (Vulnerable 1), same key-material (Vulnerable 2) and same IV (Vulnerable 3) is used in two runs. Iteration count value is only 4 as shown in vulnerability 1. HostnameVerifier vulnerability is also present. It uses AES algorithm in ECB mode and signing algorithm is SHA1WithRSA (Phase 1 report).

```java
1 //Vulnerable 1 -> Same Password and Salt is used in multiple (4) runs. Low Iteration Count
2 PBEKeySpec;-><init>(c, o, m, .. m, o, b, i, k, w, i, k, .. n, o, m, j, y, o, c, i, .. g, a, j, r, a, n, i, o, m, n, i, t, .. a, c, i, .. i, n)
3 A2 (Salt) {-46, 90, -68, -128, -103, 57, -74, -64, 88, -95, -65, 77, -117, -36, -113, -1, 32, -64, 89}
4 A3 (Iteration-Count) | 1 | 4 |
5 //Vulnerable 2 -> Same Key material used in 4 instances for generation of secret key
6 SecretKeySpec;-><init>(c, o, m, .. m, o, b, i, k, w, i, k, .. n, o, m, j, y, o, c, i, .. g, a, j, r, a, n, i, o, m, n, i, t, .. a, c, i, .. i, n)
7 SecretKeySpec;-><init>(c, o, m, .. m, o, b, i, k, w, i, k, .. n, o, m, j, y, o, c, i, .. g, a, j, r, a, n, i, o, m, n, i, t, .. a, c, i, .. i, n)
8 //Vulnerable 3 -> Same Initialization Vector 2 times
9 IVParameterSpec;-><init>(c, o, m, .. m, o, b, i, k, w, i, k, .. n, o, m, j, y, o, c, i, .. g, a, j, r, a, n, i, o, m, n, i, t, .. a, c, i, .. i, n)
10 A2 (Salt) {-46, 90, -68, -128, -103, 57, -74, -64, 88, -95, -65, 77, -117, -36, -113, -1, 32, -64, 89}
11 A3 (Iteration-Count) | 1 | 4 |
12 //Vulnerable 4 -> HostnameVerifier always returning true
13 Class Path : org/apache/cordova/filetransfer
14 final class FileTransfer implements HostnameVerifier{prerequisites: }
15 public boolean verify(String urlString, SSLSession paramSSLSession) { return true; }
```

Listing 7: Precise Report of Analysis for Mobikwik App

Table V shows detailed results for some of the highest downloaded apps of Google-playstore from various categories. The name of banking app is not disclosed for privacy reasons. The analysis shows that even the most popular Android apps are vulnerable due to improper use of cryptographic primitives.

![Vulnerability by Primitive](image)

**Fig. 3: Vulnerability by Primitive**

<table>
<thead>
<tr>
<th>App/Category/Download in 10^3</th>
<th>Vulnerabilities Identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking App/Banking/1-5</td>
<td>MessagesDigest algorithm is SHA-1</td>
</tr>
<tr>
<td>AES in ECB Mode</td>
<td></td>
</tr>
<tr>
<td>Signature Algorithm is SHA1WithRSA</td>
<td></td>
</tr>
<tr>
<td>HostnameVerifier always return TRUE</td>
<td></td>
</tr>
<tr>
<td>TrustManager does not throw any exception</td>
<td></td>
</tr>
<tr>
<td>Mobikwik/LifeStyle/10-50</td>
<td>MessagesDigest algorithm is MD5</td>
</tr>
<tr>
<td>AES in ECB mode</td>
<td></td>
</tr>
<tr>
<td>Signature Algorithm is SHA1WithRSA</td>
<td></td>
</tr>
<tr>
<td>SSL TrustManager Vulnerability</td>
<td></td>
</tr>
<tr>
<td>Password Notes/Tools/5-1</td>
<td>Iteration Count in PBE is 100</td>
</tr>
<tr>
<td>AES in ECB mode</td>
<td></td>
</tr>
<tr>
<td>Key Length (32 bit) in PBE</td>
<td></td>
</tr>
<tr>
<td>TaxiForSure/Transport/1-5</td>
<td>AES in ECB mode</td>
</tr>
<tr>
<td>AES in ECB mode</td>
<td></td>
</tr>
<tr>
<td>Snapdeal/Shopping/10-50</td>
<td>AES in ECB mode</td>
</tr>
<tr>
<td>Signal/Communication/1-5</td>
<td>Iteration Count in PBE is 100</td>
</tr>
</tbody>
</table>

VI. Related Work

**Static Analysis** Egele et al. developed CryptoLint to statically analyze cryptographic vulnerabilities based on misuse of symmetric and PBE in Google playstore apps [22]. Additionally, sPECTRA analyze other vulnerabilities as detailed in Table II. The critical observations show that CryptoLint being the pure static approach, may not determine vulnerability for obfuscated, run-time dependent or logical condition.
based parameters. Moreover, the security prerequisites put necessity on using non-unique and non-predictable values for critical security parameters like Initialization Vector, Salts, etc. Static analysis can only infer that these critical parameters are derived from static components or not while sPECTRA reports the vulnerability on the use of same values for critical parameters in different executions. The comparison of results of sPECTRA is not done with CryptoLint due to it’s unavailability.

**Hybrid Analysis** CMA uses hybrid approach for analysis [27]. However, the approach relies on manual analysis which limits it’s scalability for large app stores. Specifically, the aim of sPECTRA is to enable the automatic large scale analysis. Moreover, sPECTRA covers the wider range of vulnerabilities compared to CMA as shown in Table II. Overall, sPECTRA's approach makes it a lightweight framework compared to CMA. Mauro et al. proposed a lightweight, system MITHYS for protecting against SSL vulnerabilities [20]. Steven et al. propose OpenCCE system which provides developers with cryptographically correct code blueprint based on their requirement [16]. However, our focus is to verify the apps after development.

**Automated Analysis** Dynodroid [25] is an automatic input generation system that instruments the Android SDK for capturing system events. On average, it achieves a code coverage of 55%. Dynodroid’s results show that monkey also performs comparable code coverage, but Monkey requires nearly 20X more input events for same code coverage. However, Dynodroid is only supported for Android version 2.3 while sPECTRA is tested till version 5.1.1. Appsplayground’s [26] UI exploration is closely related to sPECTRA. However, it works on modified Android software stack while sPECTRA works on unmodified software stack. This restricts Appsplayground current implementation applicable only for single API level. The critical issue of emulator fails in loading snapshot with exception “savevm: unable to load section RAM” is observed during experiments with Appsplayground.

A$E^3$ [17] constructs a high-level CFG that captures legal transitions among activities (app screens). This graph is then used to develop an exploration strategy. The time of exploration modules are more than hour which is very high and create the problem in scaling. It does not handle multi-touch gestures such as pinching and zooming and only tested for Android version 2.3.4.

**References**

[23] Arni Einarsen and Janus Dam Nielsen. A survivor’s guide to java program analysis with soot. BRICS, Department of Computer Science, University of Aarhus, Denmark, 2008.