

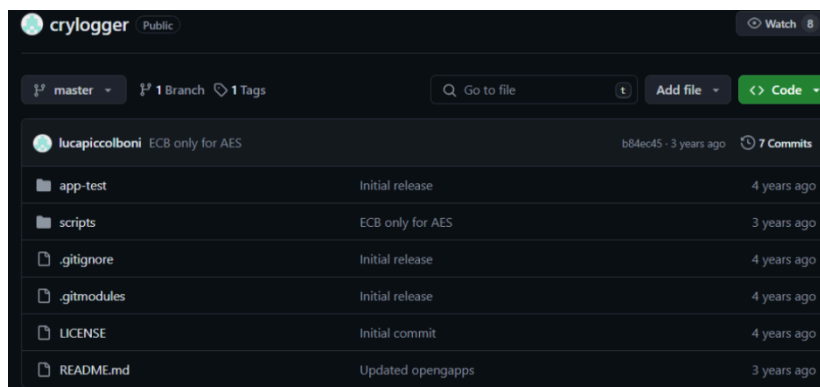
## Dynamic Analysis Tool –Crylogger

Aakash R  
CB.SC.P2CYS23011

CRYLOGGER detects cryptographic (crypto) misuses in Android apps. A crypto misuse is an invocation to a crypto API that does not respect common security guidelines, such as those suggested by cryptographers or organizations.

CRYLOGGER detects crypto misuses for you automatically, without requiring to analyse a single line of your code.

First, CRYLOGGER runs your Android app on the official Android **Emulator**. **CRYLOGGER** runs your app by using Monkey or the user-interface events you send to the emulator.



***adb shell monkey -p your.package.name -v 500***

For ex, as shown above frameworks and libcore can be changed accordingly to create a new android distribution and to have our emulator a different logging functionality.

Likewise many changing logging functionality of the open source android OS and making it their own Android distributions.

```

crylogger / scripts / deltas / libcore / ojluni / src / main / java / javax / crypto / spec / PBEKeySpec.java
Code Blame 263 lines (244 loc) · 9.55 KB Code 55% faster with GitHub Copilot
69 public class PBEKeySpec implements KeySpec {
117 public PBEKeySpec(char[] password, byte[] salt, int iterationCount,
126 "must be non-null");
127 } else if (salt.length == 0) {
128 throw new IllegalArgumentException("the salt parameter " +
129 "must not be empty");
130 } else {
131 this.salt = salt.clone();
132 }
133 if (iterationCount <= 0) {
134 throw new IllegalArgumentException("invalid iterationCount value");
135 }
136 if (keyLength <= 0) {
137 throw new IllegalArgumentException("invalid keyLength value");
138 }
139 this.iterationCount = iterationCount;
140 this.keyLength = keyLength;
141
142 /* CRYLOGGER */
143 CRYLogger.write("[PBEKeySpec] PBEKeySpec(char[], byte[], int, int) called\n");
144 CRYLogger.write("[PBEKeySpec] salt: ", this.salt);
145 CRYLogger.write("[PBEKeySpec] password: " + String.valueOf(this.password) + "\n");
146 CRYLogger.write("[PBEKeySpec] iteration: " + this.iterationCount + "\n");
147 CRYLogger.write("[PBEKeySpec] keylength: " + this.keyLength + "\n");

```

It will make logs and specifies the analysis made upon cryptographic functionalities of the application.

## AndroidXRef

<p><b>ANDROID SOURCE</b></p> <ul style="list-style-type: none"> <li>Pie - 9.0.0_r3</li> <li>Oreo - 8.1.0_r33</li> <li>Oreo - 8.0.0_r4</li> <li>Nougat - 7.1.2_r36</li> <li>Nougat - 7.1.1_r6</li> <li>Nougat - 7.0.0_r1</li> <li>Marshmallow - 6.0.1_r10</li> <li>Marshmallow - 6.0.0_r5</li> <li>Marshmallow - 6.0.0_r1</li> <li>Lollipop - 5.1.1_r6</li> <li>Lollipop - 5.1.0_r1</li> <li>Lollipop - 5.0.0_r2</li> <li>KitKat - 4.4.4_r1</li> <li>KitKat - 4.4.3_r1.1</li> <li>KitKat - 4.4.2_r2</li> <li>KitKat - 4.4.2_r1</li> <li>KitKat - 4.4</li> <li>JellyBean - 4.3</li> <li>JellyBean - 4.2.2</li> <li>JellyBean - 4.2</li> <li>JellyBean - 4.1.2</li> <li>JellyBean - 4.1.1</li> <li>ICS - 4.0.4</li> <li>ICS - 4.0.3</li> <li>Gingerbread - 2.3.7</li> <li>Gingerbread - 2.3.6</li> </ul>	<p><b>News</b></p> <ul style="list-style-type: none"> <li>• 2018-08-11 - New Index: Pie - 9.0.0_r3</li> <li>• 2018-06-19 - New Index: Oreo - 8.1.0_r33</li> <li>• 2017-12-22 - New Index: Nougat - 7.1.2_r36</li> <li>• 2017-09-19 - New Index: Oreo - 8.0.0_r4</li> <li>• 2016-12-22 - New Index: Nougat - 7.1.1_r6</li> <li>• 2016-08-24 - New Index: Nougat - 7.0.0_r1</li> <li>• 2016-01-08 - New Index: Marshmallow - 6.0.1_r10</li> <li>• 2016-01-07 - New Index: Marshmallow - 6.0.0_r5</li> <li>• 2015-10-07 - New Index: Marshmallow - 6.0.0_r1</li> <li>• 2015-07-03 - New Index: Lollipop - 5.1.1_r6</li> <li>• 2015-03-13 - New Index: Lollipop - 5.1.0_r1</li> <li>• 2014-09-06 - New Index: Lollipop - 5.0.0_r2</li> <li>• 2014-07-14 - New Index: KitKat - 4.4.4_r1</li> <li>• 2014-06-06 - New Index: KitKat - 4.4.3_r1.1</li> <li>• 2014-03-25 - New Index: KitKat - 4.4.2_r2</li> <li>• 2014-01-08 - New Index: KitKat - 4.4.2_r1</li> <li>• 2013-11-01 - New Index: KitKat - 4.4</li> <li>• 2013-10-31 - New Index: Gingerbread - 2.3.7</li> <li>• 2013-09-30 - New Index: ICS - 4.0.3</li> <li>• 2013-07-25 - New Index: JellyBean - 4.3</li> <li>• 2013-04-22 - New Index: JellyBean - 4.1.2</li> <li>• 2013-02-25 - New Index: JellyBean - 4.2.2</li> <li>• 2012-11-21 - New Index: JellyBean - 4.2</li> <li>• 2012-08-22 - New Index: Froyo - 2.2.3</li> <li>• 2012-08-22 - New Index: Eclair - 2.1</li> <li>• 2012-08-22 - New Index: Donut - 1.6</li> </ul>	<p><b>KERNEL SOURCE</b></p> <ul style="list-style-type: none"> <li>Kernel - 3.18</li> <li>Kernel - 3.14</li> <li>Kernel - 3.10</li> <li>Kernel - 3.4</li> <li>Kernel - 3.3</li> <li>Kernel - 3.0</li> <li>Kernel - 2.6.39</li> </ul> <div style="text-align: center;">  </div> <p><b>CONTACT</b></p> <p>Rodrigo Chiossi  <a href="mailto:contact(at)androidxref.com">contact(at)androidxref.com</a></p>
---	--	--

Above is the repositories that contains source codes of the released android versions and by changing the logging functionality of the desired version of android, new distribution is created on our own.

### **Benefits of Using Crylogger:**

- **Automatic Detection:** Crylogger automates the detection of cryptographic misuse, making it easier and faster to identify security issues compared to manual code reviews.
- **Runtime Analysis:** By analysing the app's behaviours at runtime, Crylogger can detect issues that may not be apparent through static analysis alone.
- **Focused on Cryptography:** The tool is specialized for cryptographic API misuse, providing in-depth insights and recommendations specific to cryptographic security.