IOTSPOTTER ONLINE APPENDIX

B.1 Rulesets for CryptoGuard and CogniCrypt

Table 9 and Table 11 show the complete rule sets of CryptoGuard and CogniCrypt.

Table 9: CryptoGuard's Complete Rule Set.

ID	Rule	Severity
1	Predictable/constant cryptographic keys	High
2	*Predictable/constant passwords for PBE	High
3	Predictable/constant passwords for KeyStore	High
4	Custom Hostname verifiers to accept all hosts	High
5	Custom TrustManager to trust all certificates	High
6	Custom SSLSocketFactory without verification	High
7	Occasional use of HTTP	High
8	Predictable/constant PRNG seeds	Medium
9	Cryptographically insecure PRNGs (e.g., java.util.Random)	Medium
10	*Static Salts in PBE	Medium
11	*ECB mode in symmetric ciphers	Medium
12	Static IVs in CBC mode symmetric ciphers	Medium
13	Fewer than 1,000 iterations for PBE	Low
14	*64-bit block ciphers (e.g., DES, IDEA, Blowfish, RC4, RC2)	Low
15	Insecure asymmetric ciphers (e.g, RSA, ECC)*	Low
16	Insecure cryptographic hash (e.g., SHA1, MD5, MD4, MD2)	High

* = Rules that are merged, i.e., checked and reported together, in the CryptoGuard tool; specifically, rule ID's [2,10] and [11,14].

B.2 Details of the Vulnerability Disclosure

We reported the confirmed vulnerabilities from the case study (Section 8) to 12/18 vendors in April 2022, and are in the process of reporting to the remaining 6 vendors. As of August 2022, we have received two responses: HubbleConnected created a ticket and is investigating our reported vulnerability, while we received an automated response with FAQ information from Amazon Alexa. The template used in our vendor disclosure is available in Listing 1. Particularly, we crafted our email based on the findings for each vendor. Listing 1 presents the generic outline of how we informed vendors about different findings reported in this paper.

```
1
2  Subject: Security Vulnerabilities identified in <app_name>
3
4  To Whom It May Concern:
5
6  We are a team of security researchers from <XYZ> at <ABC>. We
    performed a systematic study to analyze the security issues for
    mobile-IoT apps i.e., mobile apps that connect to IoT devices.
7
8  We found the following vulnerabilities in the app <app_name> <
    app_link> <version_number> published in Google Play:
9
10         1. <Security Finding>
11         2. <Security Finding>
12
13 Any additional information that you think that causes the
    vulnerabilities would be extremely helpful.
14
15 If you have recently patched your app, kindly let us know in which
     version you address the issue.
16
17 Thank you!
18
19 <Email_Signature>
```

Listing 1: Email Template used to inform the vendors

B.3 List of Apps for Case Study

Table 12 lists the set of apps analyzed in Section 8.

Table 10: IoT Product Entities clustered using GSDMM

Product Types	Example Product Entities
TV	tv, tv remote, vizio tv, philips tv, roku tv, hisense tv, hitachi tv
Remote Control	universal remote control, remote control, ac remote control
Security Camera	ip camera, wifi camera, cctv, security cameras, ptz cameras
Light	light, led, lamp, bulb, led lights, led light, rgb led

B.4 Sampling non-IoT apps for library and crypto-API misuse analysis

To ensure a comparable sample of non-IoT apps for the library and crypto-API analyses, we used the following approach: we randomly sampled non-IoT apps repeatedly until we found a set with the same popularity distribution (as indicated by its CDF of installs) as the mobile-IoT apps, for each case (*i.e.*, the 913 apps for crypto-API analysis, and 5,380 for library analysis). For example, for the library analysis, we first randomly sample 5,380 apps from all non-IoT apps with more than 50k installs, and then, plot the CDF using install-count ranges reported by Google Play, *i.e.*, 50 - 100k, 100 - 500k, and so on, until 500 million, redoing the sample for a specific range if the difference is greater than 0.5%. Our online appendix [39] shows the equivalent install distributions of the sets of mobile-IoT

Table 11: CogniCrypt's Complete Rule Set

ID	Rule SPEC
1	javax.net.ssl.TrustManagerFactory
2	javax.crypto.Cipher
3	java.security.AlgorithmParameters
4	java.security.KeyPairGenerator
5	java.security.cert.TrustAnchor
6	java.security.spec.DSAParameterSpec
7	javax.crypto.SecretKey
8	javax.net.ssl.SSLParameters
9	Stopwatch
10	javax.net.ssl.SSLContext
11	javax.net.ssl.CertPathTrustManagerParameters
12	SSLSocketFactory
13	java.security.spec.DSAGenParameterSpec
14	javax.crypto.spec.DHGenParameterSpec
15	java.security.DigestOutputStream
16	javax.crypto.SecretKeyFactory
17	java.security.DigestInputStream
18	java.security.Key
19	javax.crypto.spec.DHParameterSpec
20	java.security.KeyPair
21	javax.net.ssl.KeyManagerFactory
22	java.security.KeyStore
23	com.amazonaws.services.kms.model.GenerateDataKeyRequest
24	javax.crypto.KeyGenerator
25	javax.crypto.Mac
26	SSLSocket
27	java.security.cert.PKIXBuilderParameters
28	SSLServerSocket
29	javax.net.ssl.KeyStoreBuilderParameters
30	javax.crypto.CipherOutputStream
31	java.security.SecureRandom
32	javax.crypto.spec.IvParameterSpec
33	java.security.spec.RSAKeyGenParameterSpec
34	javax.crypto.spec.SecretKeySpec
35	javax.crypto.spec.PBEParameterSpec
36	MessageDigest
37	javax.crypto.CipherInputStream
38	javax.net.ssl.SSLEngine
39	javax.crypto.spec.PBEKeySpec
40	SSLServerSocketFactory
41	javax.crypto.spec.GCMParameterSpec
42	javax.xml.crypto.dsig.spec.HMACParameterSpec
43	java.security.Signature
44	java.security.cert.PKIXParameters

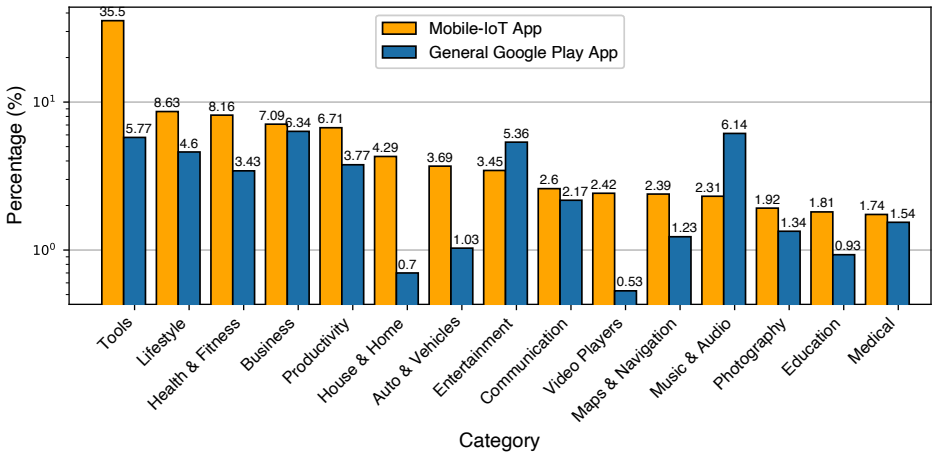

Figure 6: Top categories of that mobile-IoT apps and general Google Play apps belong to. We sort the x-axis based on the popularity of categories in mobile-IoT apps.

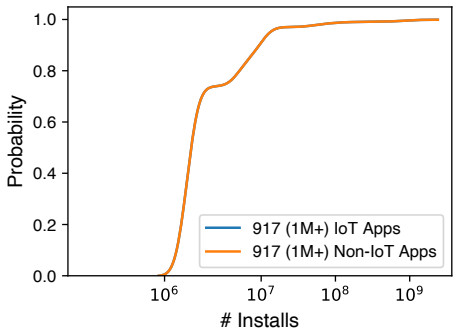

Figure 8: CDF of the popularity distribution (using install count) of top IoT and non-IoT apps for crypto-API misuse analysis. The overlapping lines show their popularity distribution equivalence.

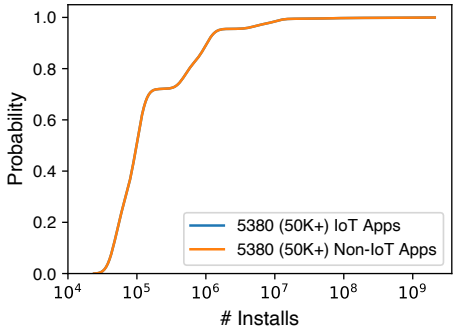

Figure 7: CDF of the popularity distribution (using install count) of IoT and non-IoT apps for library-use analysis. The overlapping lines show their popularity distribution equivalence.

and non-IoT apps used in both the library and crypto-API misuse analysis, respectively.

Table 12: List of apps selected for case-study in Section 8

ID	App Name	APK
1	CetusPlay	com.cetusplay.remotephone
2	LG ThinQ	com.lgeha.nuts
3	Amazon Fire TV	com.amazon.storm.lightning.client.aosp
4	Remote for Samsung TV	wifi.control.samsung
5	JBL Music	com.harman.jblmusicflow
6	Harmony	com.logitech.harmonyhub
7	Eye4	vstc.vscam.client
8	Hubble Connected for Motorola	com.blinkhd
9	IP Pro (VR Cam, EseeCloud)	com.specialyg.ippro
10	SURE	com.tekoia.sure.activities
11	EagleEyes(Lite)	push.lite.avtech.com
12	Amazon Alexa	com.amazon.dee.app
13	ANT+ Plugins Service	com.dsi.ant.plugins.antplus
14	Samsung Health	com.sec.android.app.shealth
15	Vestel Smart Center	com.vestel.smartcenter
16	Sricam	com.xapcamera
17	Realme Link	com.realme.link
18	LinkSys	com.cisco.connect.cloud