Table 8: The number of violations of CogniCrypt's rules in mobile-IoT and non-IoT apps (*sorted by # violations in mobile-IoT apps*).

CogniCrypt's Rules (IDs as per [46])		# Violations	
ID	**Rule SPEC**	**Mobile-IoT**	**Non-IoT**
36	MessageDigest	1743	2571
10	javax.net.ssl.SSLContext	1160	661
2	javax.crypto.Cipher	485	303
1	javax.net.ssl.TrustManagerFactory	257	238
43	java.security.Signature	236	140
39	javax.crypto.spec.PBEKeySpec	140	75
34	javax.crypto.spec.SecretKeySpec	133	82
16	javax.crypto.SecretKeyFactory	132	87
32	javax.crypto.spec.IvParameterSpec	78	56
12	SSLSocketFactory	66	5
22	java.security.KeyStore	47	42
4	java.security.KeyPairGenerator	33	17
25	javax.crypto.Mac	33	25
21	javax.net.ssl.KeyManagerFactory	23	1
26	SSLSocket	23	1
24	javax.crypto.KeyGenerator	21	10
30	javax.crypto.CipherOutputStream	17	8
37	javax.crypto.CipherInputStream	17	16
35	javax.crypto.spec.PBEParameterSpec	11	5
15	java.security.DigestOutputStream	8	8
31	java.security.SecureRandom	8	6
41	javax.crypto.spec.GCMParameterSpec	6	3
8	javax.net.ssl.SSLParameters	3	0
5	java.security.cert.TrustAnchor	2	1
17	java.security.DigestInputStream	2	2
3	java.security.AlgorithmParameters	1	0
27	java.security.cert.PKIXBuilderParameters	1	0
-	**TOTAL Violations**	4,686	4,363

Table 7: Number of violations of CryptoGuard's rules in mobile-IoT and non-IoT apps (*sorted by # violations in mobile-IoT apps*). CryptoGuard assigns *severity* to rules, as we annotate in the table (high severity= [H], medium severity= [M], low=unmarked).

CryptoGuard's Rules (IDs as per [55])		# Violations	
ID	**Rule Name**	**Mobile-IoT**	**Non-IoT**
9	Insecure PRNGs (e.g., java.util.Random) [M]	15573	16778
16	Insecure cryptographic hash (e.g., SHA1, MD5) [H]	13297	16365
7	Occasional use of HTTP	2298	1593
1	Predictable/constant cryptographic keys [H]	2271	2359
5	Custom TrustManager to trust all certificates [H]	1931	910
14,11	*64-bit block ciphers (e.g., DES, RC4), ECB mode [M]	1311	1087
12	Static IVs in CBC mode symmetric ciphers [M]	716	467
4	Custom Hostname verifiers to accept all hosts [H]	293	269
3	Predictable/constant passwords for KeyStore [H]	100	
6	SSLSocketFactory w/o hostname verification [H]	186	86
13	Fewer than 1,000 iterations for PBE	104	32
2,10	*Predictable passwords, static salts in for PBE [H/M]	85	62
15	Insecure asymmetric cipher use	71	27
8	Predictable/constant PRNG seeds [M]	67	83
-	**TOTAL Violations**	38,486	40,218

* = CryptoGuard reports combined results for certain rules.

IOTSPOTTER ONLINE APPENDIX

A INTUITION BEHIND SELECTING SPECIFIC DECISION BOUNDARY VALUES

The decision boundary (μ) of 44 was chosen with an intuition to balance identification of IoT library package names with high precision and relatively less false positive cases. For this, we randomly sampled a set of 20 library package names (starting with a decision boundary of 60). We observed that the false positive cases continue to rise as we decreased the decision boundary. We found 44 to reasonably fit our goal i.e., our sample contained less false positive cases but were 44x more popular in IoT than non-IoT apps. We used a different decision boundary (ϵ) to identify library package names that were only available in IoT apps and unavailable in non-IoT apps (as we elaborate in Fig 4(a). This allows us to identify instances similar to the ones explained in the example (i.e., 10 apps calls a given library but non of of the non-IoT apps call a given package)

B CRYPTO-API MISUSE DETECTED BY CRYPTOGUARD AND COGNICRYPT

Table 7 and Table 8 show the mapping of different rules with their respective flaws and severity of violation.

C RULESETS FOR CRYPTOGUARD AND COGNICRYPT

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

o

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

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].

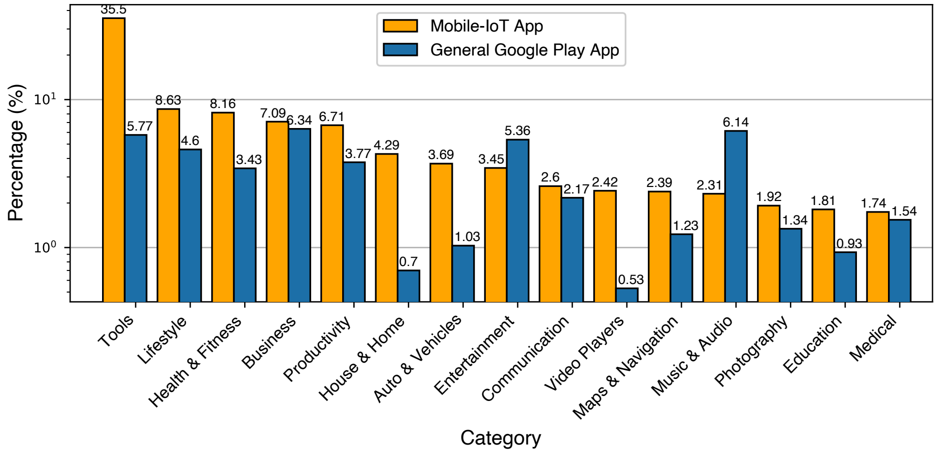

Figure 6: Top categories of that mobile-IoT apps and general Google Play apps belong to. We sort the x-axis based on the popularity of categories in mobile-IoT apps.

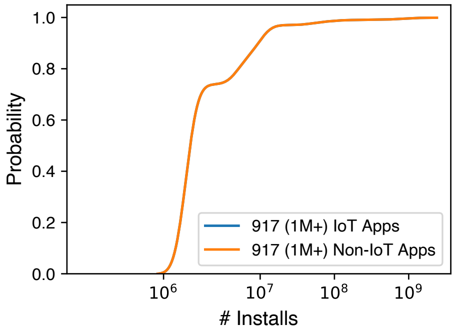

Figure 8: CDF of the popularity distribution (using install count) of top IoT and non-IoT apps for crypto-API misuse analysis. The overlapping lines show their popularity distribution equivalence.

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

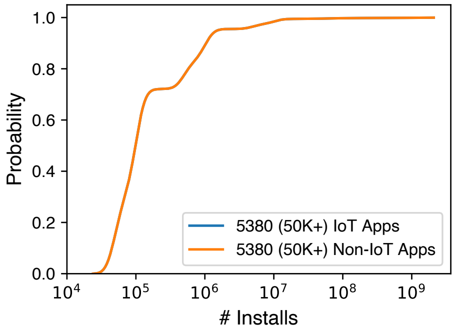

Figure 7: CDF of the popularity distribution (using install count) of IoT and non-IoT apps for library-use analysis. The overlapping lines show their popularity distribution equivalence.

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

E 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.

```

Subject: Security Vulnerabilities identified in <app_name>

To Whom It May Concern:

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.

We found the following vulnerabilities in the app <app_name> <
 app_link> <version_number> published in Google Play:

        1. <Security Finding>
        2. <Security Finding>

Any additional information that you think that causes the
 vulnerabilities would be extremely helpful.

If you have recently patched your app, kindly let us know in which
  version you address the issue.

Thank you!

<Email_Signature>
```

Listing 1: Email Template used to inform the vendors

F LIST OF APPS FOR CASE STUDY

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

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