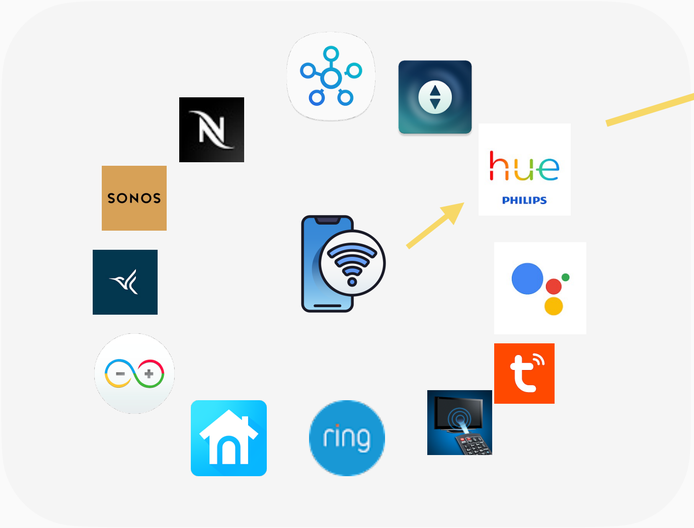
Understanding IoT Security from a Market-Scale Perspective

Xin Jin[1], Sunil Manandhar[2*], Kaushal Kafle[3], Zhiqiang Lin[1], Adwait Nadkarni[3]

[1]The Ohio State University
[2]IBM T.J. Watson Research Center
[3]William & Mary

*This work was completed when the author was at William & Mary.

IoT Security



Mobile-IoT Apps

IoT Devices

- Automations
- Firmwares
- Cloud Backends
- IoT Libraries

Attack Surface

IoT Security

Hacker spoke to baby, hurled obscenities at couple using Nest camera, dad says

Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs

Home › News › Hackers take over Smart Home

NEWS THREATS

Hackers take over Smart Home

By CISOMAG - September 26, 2019

Consumer Tech • Perspective

Alexa has been eavesdropping on you this whole time

When Alexa runs your home, Amazon tracks you in more ways than you might want.

TECHNOLOGY

Is your Christmas present spying on you? How to assess gifts' privacy risks

Siemens SIMATIC PLCs (Security Bug Reveals Hardcoded Universal Key)

Cyber Security Today, Oct. 26 2022 – American schools increasingly hit by ransomware, an event ticket agency is hacked and more

Yes, Your Video Baby Monitor Can Be Hacked. No, You Don't Have to Stop Using It

By Jack Busch

Last Updated on June 24, 2021

New PoC Shows IoT Devices Can Be Hacked to Install Ransomware on OT Networks

Bluejacking: How Bluetooth Can Be Used to Hack Your Devices

Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

European Police Arrest a Gang That Hacked Wireless Key Fobs to Steal Cars

Critical Amazon Ring Vulnerability Could Expose Camera Recordings

Public electric car chargers are an 'open door' to drivers being hacked – urgent warning

Buggy software in off-brand smart home devices is a hacker's playground

Samsung SmartThings Hub Vulnerable to Hacks: Check Yours Now

Crooks are jamming security cameras — Protect yours now!

SMART HOME TECH CYBERSECURITY

Your Philips Hue light bulbs can still be hacked — and until recently, compromise your network

Might want to check if you've got firmware 1935144040

Police dismantles criminal ring that hacked keyless cars

Wisconsin couple describe the chilling moment that a hacker cranked up their heat and started talking to them through a Google Nest camera in their kitchen

IoT Security Challenges

Secure IoT Products at scale → **Triaging?**

We do not know what products constitute IoT Ecosystem!

Mobile-IoT Apps

Unique features for **Identification**

Metadata to build **understanding of IoT Market**

Critical **Attack Surface**

Security ramifications of vulnerabilities **beyond Mobile Space**

IoT Security Challenges

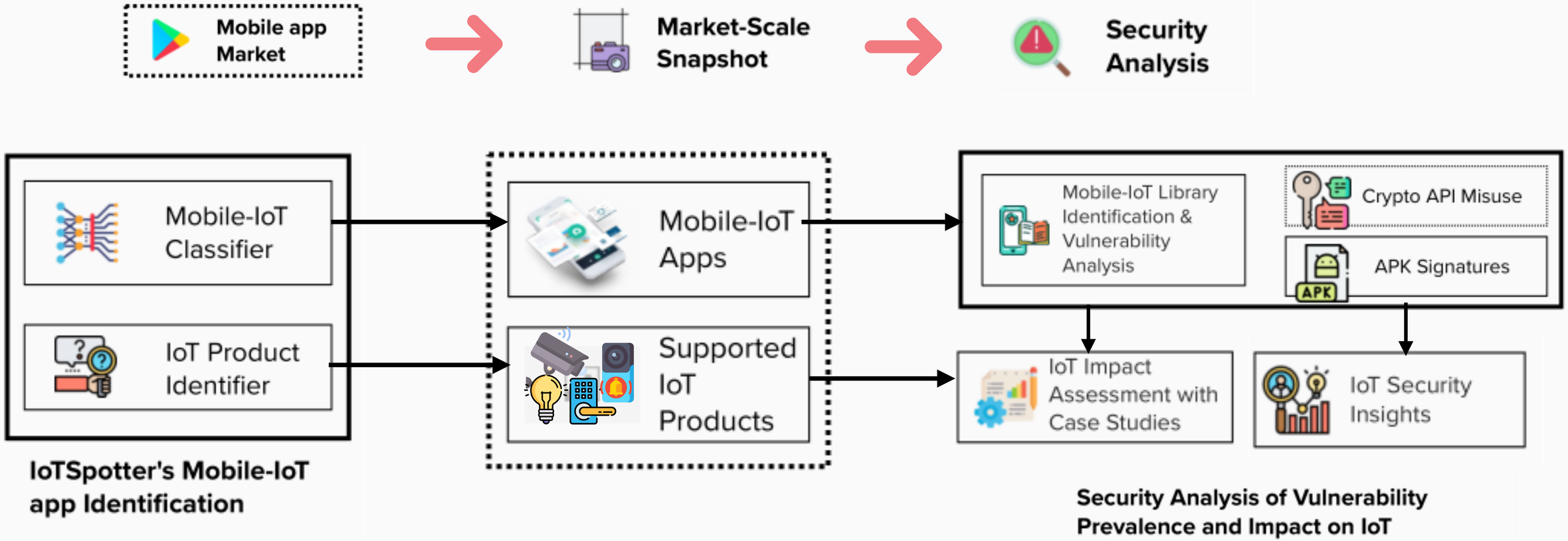
We do not know what products constitute IoT Ecosystem!

Research Questions

RQ1: How can we automatically ***develop a market-scale snapshot*** of mobile-IoT apps from markets containing heterogeneous apps?

RQ2: How can we ***make the snapshot useful for security***?

IoTSpotter Framework



Mobile-IoT App Identification

Methodology

Step 1: Building Train/Test Set

(a) Preliminary analysis of Mobile-IoT apps
- App Descriptions
- App UI
- Reviews
- Permissions

(b) Heuristics Based Identification Device Types (e.g., Security Camera)
- IoT Keywords (e.g., IoT)
- Device Keywords (e.g., smart device)
- IoT Protocols (e.g., Zigbee)
- Platforms (e.g., SmartThings)
- Regex patters (remotely control..)

(c) Pattern Matches:
- 1 Keyword Match: **89,508 apps**
- 2 Keyword Match: 8,467 apps
- 3+ Keyword Match: 1758 apps

Step 2: Manual Labeling

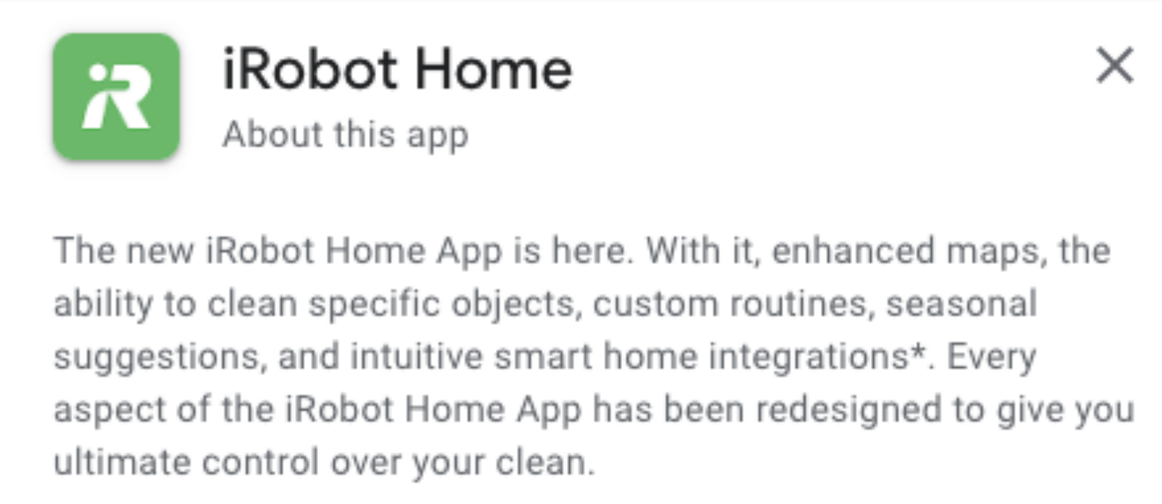
(a) 7196 Labeled Apps
- 4,123 IoT apps
- 3,073 non-IoT apps

(b) Cohen Kappa: 0.976

Step 3: Build Classifier Model

(a) Run different Learning algorithms for description:
- Stratified train-test set

(b) Evaluate Performance



Mobile-IoT App Identification

Results

Performance	Description							
	LR	SVM	NB	RF	RNN	LSTM	BiLSTM	BERT
Accuracy	0.927	0.916	0.914	0.926	0.947	0.946	0.952	0.957
Precision	0.932	0.897	0.909	0.929	0.925	0.957	0.962	0.949
Recall	0.896	0.908	0.889	0.896	0.954	0.915	0.925	0.951
F1-Score	0.914	0.902	0.899	0.913	0.939	0.936	0.943	0.950

*Ran the model (with hard voting) on the entire market with **2 Million Apps!***

Result 1: Identified **37,783 Mobile-IoT apps.**

Results 2: Manual validation of 2,250 mobile-IoT apps showed **88% are indeed IoT.**

IoT Product Identification

Methodology

Step 1: Building Train/Test Set

(a) Select 600 Random Mobile-IoT Apps
(b) Manually labeled 3961 statements to identify IoT_Product Entities

Step 2: Train Named Entity Recognition (NER) Model

(a) 82.84% Precision
(b) 83.04% Recall

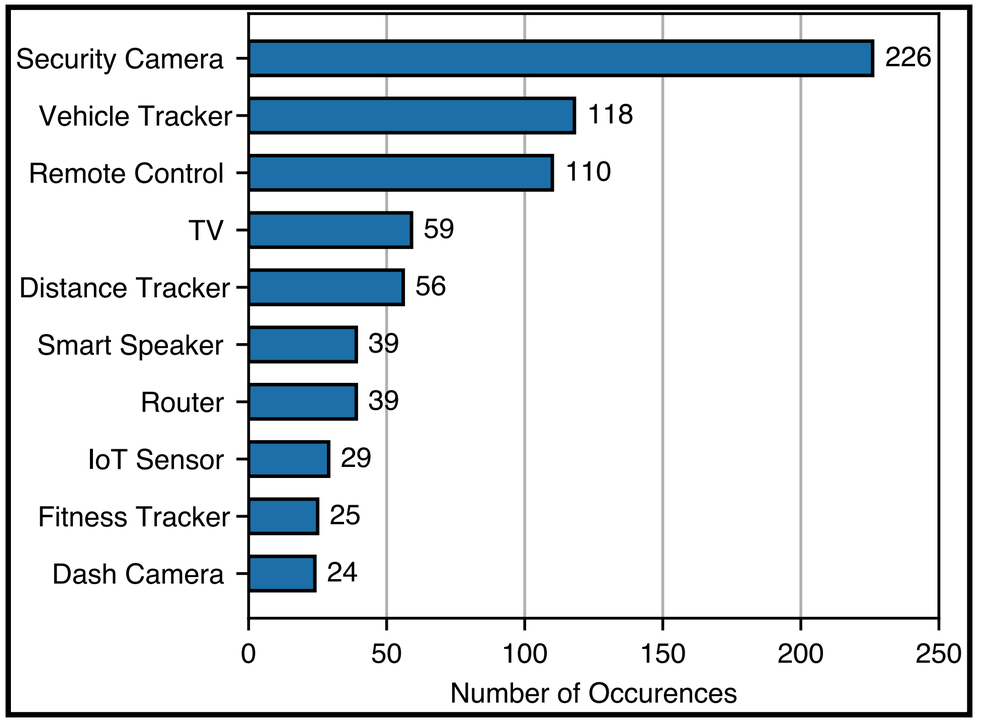
Our first product was the trendsetting Wyze Cam **IOT_PRODUCT** :
a multi-purpose indoor smart camera **IOT_PRODUCT** that helped
our users keep an eye on what matters most without a hefty price tag.

IoT Product Identification

Results

Result 3: Identified **65,676 unique product entities — 917 clusters** of device types

Result 4: Security sensitive devices are most common devices supported by mobile-IoT apps.



Security Analysis: IoT Library

Methodology

Identifying IoT Libraries

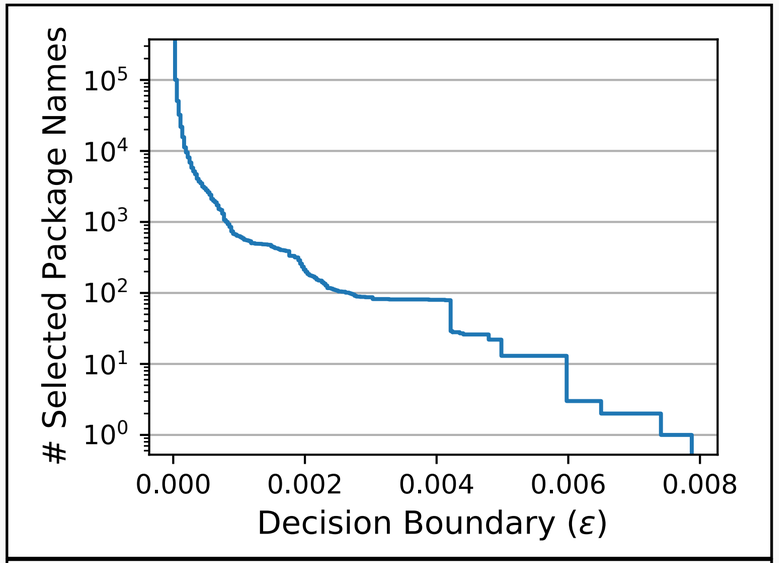
Identified 522,285 third-party library package names from the mobile-IoT snapshot

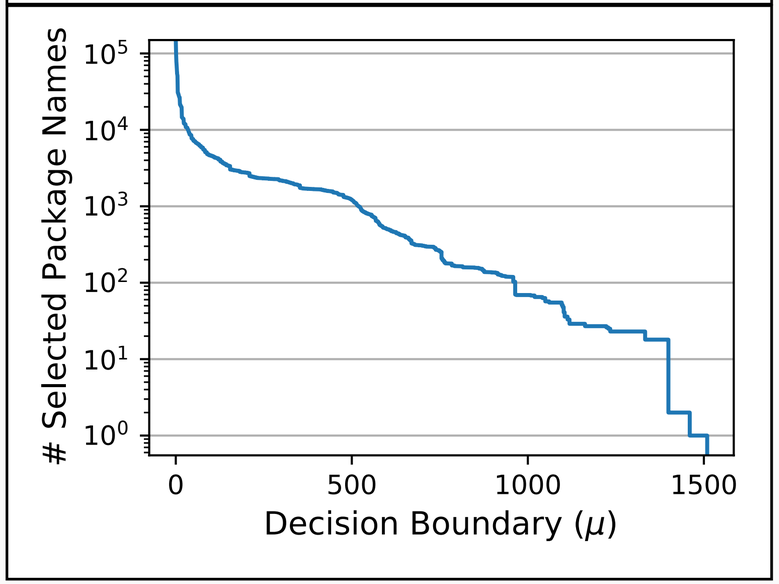
- **Popular third-party libraries only found in IoT**

  $\epsilon = \frac{\text{no. of apps using the library}}{\text{total no. of mobile-IoT apps}}$

- Third-Party libraries **more popular in mobile-IoT snapshot than non-IoT set**

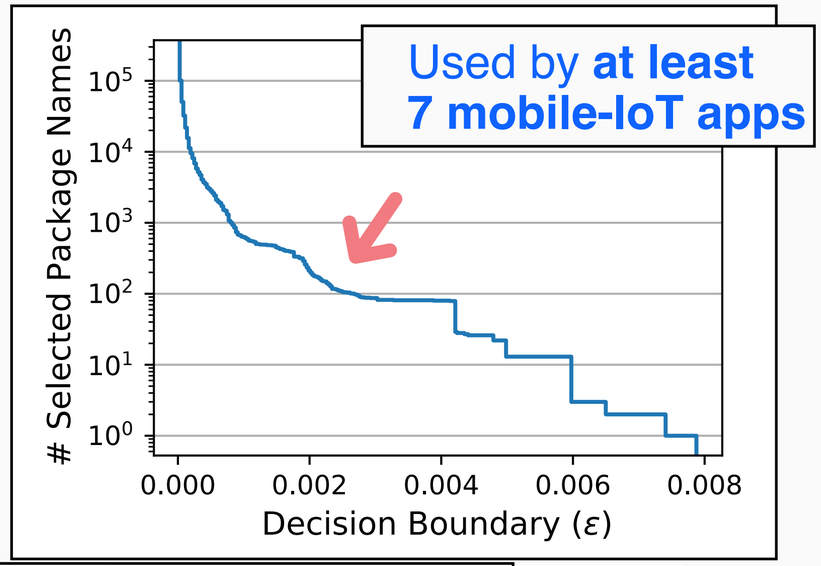
  $\mu = \frac{\text{Popularity in Mobile-IoT}}{\text{Popularity in Non-IoT}}$

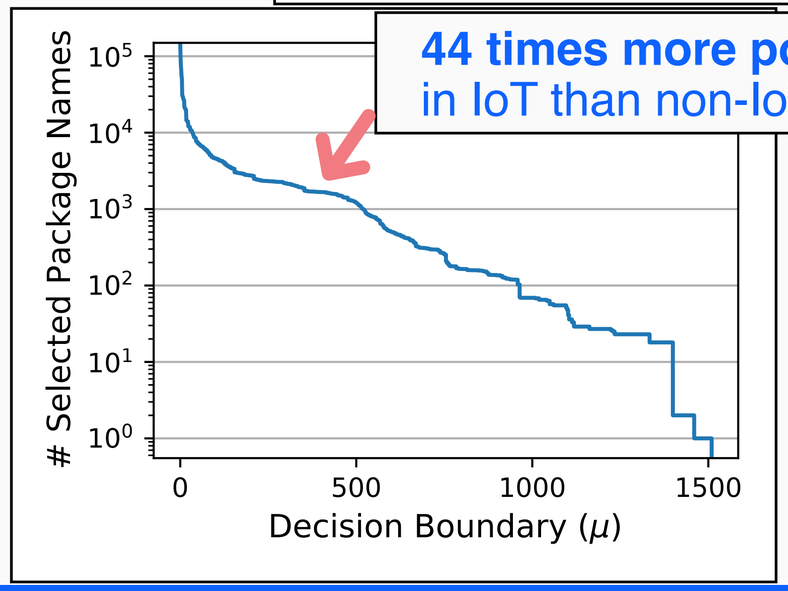




Security Analysis: IoT Library

Results





Result 5: Identified **19,939 IoT library package names**.

Analysis of 50 library package names.

Library Family	Functionality	# Apps
com.tuya	IoT framework	1,362
no.nordicsemi.android	BLE & firmware services	1,097
javax.jmdns	DNS services	852
com.amazonaws.mobileconnectors	IoT cloud services	751
com.connectsdk	Device control	378
com.inuker.bluetooth	BLE services	358
com.clj.fastble	BLE services	333
com.hiflying	Device control	285
com.telink	Device control	250
com.hikvision	Device control	191
org.fourthline.cling	Device control	187

Results 6: Identified 11 library families; 10 provide functionalities associated with IoT

Security Analysis: IoT Library

Findings

Vulnerabilities in IoT libraries

Finding 1: 65 IoT Libraries (481 unique versions) are subject to **79 CVEs**

Finding 2: IoT libraries are less vulnerable relative to non-IoT libraries; Out of 2500 samples:

- **Non-IoT:** 193 CVEs, 63 libraries, 7,105 versions
- **IoT:** 7CVEs, 10 libraries, 98 versions

Use of Vulnerable IoT Libraries

Finding 3: 40 popular mobile-IoT apps are vulnerable because of vulnerable **IoT library usage.**

Finding 4: Vulnerable library usage in non-IoT is 12.7X (507/40) more than in IoT.

MVN REPOSITORY

Categories	Android Packages
Tags	panel aar android
Date	Jan 08, 2021
Files	aar (90 KB) View All
Repositories	JCenter
Ranking	#405161 in MvnRepository (See Top Artifacts) #56265 in Android Packages
Vulnerabilities	Vulnerabilities from dependencies: CVE-2022-25845 CVE-2022-24329 CVE-2021-36090 View 5 more ...

Security Analysis: Crypto APIs

Findings

Flaws detected by CryptoGuard

Finding 5: 94.11% apps contain at least 1 Crypto-API misuse according to CryptoGuard out of *917 apps with 1M+ installs (96.29% non-IoT).*

Finding 6: 82.5% high severity violations detected by CryptoGuard is true positive.

CryptoGuard's Rules (IDs as per [55])		# Vulnerable Apps	
ID	**Rule Name**	**Mobile-IoT**	**Non-IoT**
9	Insecure PRNGs (e.g., java.util.Random) [M]	842	870
16	Insecure cryptographic hash (e.g., SHA1, MD5) [H]	825	865
1	Predictable/constant cryptographic keys [H]	577	669
7	Occasional use of HTTP [H]	438	441
14,11	*64-bit block ciphers (e.g., DES, RC4), ECB mode [M]	406	376
5	Custom TrustManager to trust all certificates [H]	380	302
4	Custom Hostname verifiers to accept all hosts [H]	293	269
12	Static IVs in CBC mode symmetric ciphers [M]	239	208
6	SSLSocketFactory w/o hostname verification [H]	186	86
3	Predictable/constant passwords for KeyStore [H]	142	60
13	Fewer than 1,000 iterations for PBE	70	26
15	Insecure asymmetric cipher use	66	19
2,10	*Predictable passwords, static salts in for PBE [H/M]	63	47
8	Predictable/constant PRNG seeds [M]	50	23
-	**Number of apps that violated at least one rule**	863	883

* = CryptoGuard reports combined results for rules indicated by combined rule IDs.

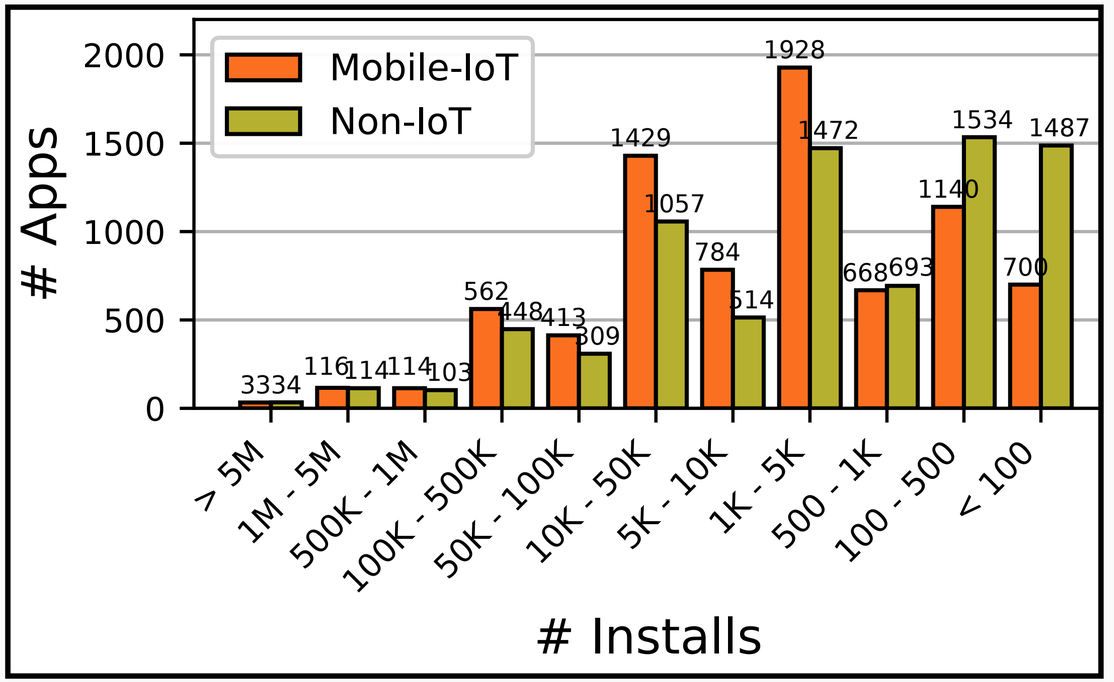
Security Analysis: App Signatures

Findings

Janus Vulnerability in Apps

Finding 7: 7,887 (20.87%) mobile-IoT apps are susceptible to Janus Vulnerability
- 263 with 1M+ download and 33 have 50M+ download

Finding 8: Non-IoT are similarly vulnerable (7765 apps).



Case Study: Contextual Analysis

Findings

Contextualization

Finding 9: Every class of vulnerability impacts critical IoT functions.

Finding 10: Vulnerable IoT apps support security/privacy critical devices.

IoT Impact	Vulnerabilities	Devices Affected
Firmware (Malicious Modification)	Crypto (HTTP, no integrity checks)	Camera JBL Speaker IP Camera
App/Device Functions (hijack, code execution)	IoT Libraries (multiple CVEs)	PTZ Camera Smart TV Vestel Smart TV IP Camera Wi-Fi Routers
User Credentials, Authentication	Crypto (MD5, TrustManager, HTTP)	IP Camera, NVR TVs, Chromecast Camera
Admin Password Leakage	Crypto (constant password, HTTP)	IP Camera
App Integrity (Malware)	Janus	Activity trackers Echo Devices
General Data Security	Crypto (DES, MD5, ECB mode)	Smart TV Washer, AC, TV Lights, Blinds, TV

Lessons

- Focused Effort on Mobile-IoT Apps
- Precise Exploration of Mobile-IoT Security
- Contextualized, Automated, Security Analysis for Mobile-IoT