10-2021

COVID-19 one year on: Security and privacy review of contact tracing mobile apps

Wei Yang ANG
Singapore Management University, weiyang.ang.2019@mais.smu.edu.sg

Lwin Khin SHAR
Singapore Management University, lkshar@smu.edu.sg

Citation

ANG, Wei Yang and SHAR, Lwin Khin. COVID-19 one year on: Security and privacy review of contact tracing mobile apps. (2021). *IEEE Pervasive Computing*. 20, (4), 61-70.
Available at: https://ink.library.smu.edu.sg/sis_research/6437

COVID-19 One Year On – Security and Privacy Review of Contact Tracing Mobile Apps

Ang Wei Yang
Singapore Management University

Dr Lwin Khin Shar
Singapore Management University

***Abstract*— The ongoing COVID-19 pandemic caused 3.8 million deaths since December 2019. At the current vaccination pace, this global pandemic could persist for several years. Throughout the world, contact tracing (CT) apps were developed, which play a significant role in mitigating the spread of COVID-19. This work examines the current state of security and privacy landscape of mobile CT apps. Our work is the first attempt, to our knowledge, which provides a comprehensive analysis of 70 CT apps used worldwide as of year Q1 2021. Among other findings, we observed that 80% of them may have handled sensitive data without adequate protection, 70% of them uses weak cryptographic algorithms and 35% of them embeds data trackers. We also observed key developments in app privacy protection and security assurance initiatives. Our findings provide useful insights to the design and deployment of more secure and privacy preserving CT apps moving forward.**

Keywords: mobile software security and data security, government contact tracing

■ **INTRODUCTION** Coronavirus Disease 2019 (COVID-19) is an infectious disease that was first identified in December 2019 and has resulted in an ongoing pandemic. As of 19 June 2021, more than 177 million cases have been reported globally, resulting in more than 3.8 million deaths [1].

In response to the pandemic, governments and organizations around the world have developed and continue to improve contact tracing (CT) solutions to speed up CT and exposure notification efforts to contain the spread of disease. The widespread use of mobile phones globally has allowed CT via mobile apps to be the most expedient way to track and notify people on potential exposures.

After one year into the pandemic, there has been significant developments to the COVID-19 CT app solution landscape. The number of CT apps has increased. A new wave of apps is rolled out recently both in the US and globally [2]. This is partly facilitated by the availability of Apple-Google Exposure Notification (GAEN) system which allows public health authorities to launch apps with little coding requirement and encourage broader rollouts [3]. At the current vaccination pace and the

uncertainty of emerging COVID-19 virus variants, this global pandemic could persist for several years, and such apps continue to play an important role to minimize the risks of community spread and facilitate a new norm as countries prepare to open borders, emerge, and recover from the pandemic.

The security and privacy of these apps are of interest to our work as they are rolled out on a national scale and in some countries are mandatory to use. This new breed of apps collects personal identifiable information (PII) and user location details. The pandemic situation also introduces potential new threats and risks that could undermine governments' effort to protect the confidentiality, integrity, and availability of CT systems and data. The stakes are high as security breaches could impact the pandemic containment effort, people's movement, lifestyle as well as public confidence.

Our paper is organized as follows. Section 2 presents the scope. Section 3 discusses the app design trade-offs. Section 4 identifies the threat landscape. Section 5 describes our analysis methodology. Section 6 presents our results. Section 7 provides further observations. Section 8 discusses implications to future apps. Section 9 presents related work. Section 10 concludes the paper.

2. SELECTION OF CONTACT TRACING (CT) APPS

The selection of CT apps in our work is based on the following criteria and considerations:

a) The app must be sanctioned, endorsed, and supported by national/state government or equivalent authority for CT purpose.

b) The app must be widely used and active, i.e., has a minimum download of 5,000, is last updated within the past 8 months, and is not on early/beta release.

c) The app must be primarily designed to perform core CT function.

The download count may not be an accurate reflection of the "take-up/penetration" rate, which is measured by the total number of downloads against the total population size of the country/region. However, we consider that since the apps are in different maturity stages with some only recently rolled out by state or federal governments, the take-up rate could vary and increase drastically over time and circumstances in tandem with government initiatives, regulations, and outreach campaign efforts.

Table 1 shows our selected 70 apps from 47 countries including 20 US states. These apps were identified from the MIT CT App Database [4] and expanded further. The app sources are verified from Google Play Store as well as the official app websites. To the best of our knowledge, this is the most comprehensive collation of global CT apps that fits our selection criteria.

Our review is limited to Android, the leading mobile operating system with 71.9% market share in Q1 2021 [5].

Our work did not consider apps used by China for CT as they adopt a central health code QR system, and this feature is delivered and serviced through a super-app model whose primary function is not designed for CT. The key super-apps used in China for CT are Alipay by Alibaba and WeChat by Tencent [6]. The availability and use of super apps for CT may have shorten the time to develop and launch a separate app and eased the roll out and adoption of CT solution for China. However, as the super apps are owned and managed by non-government entities, there may be implications on data privacy and app security issues.

South Korea adopts a data-surveillance approach to perform CT [7]. Instead of using a dedicated app, the system gathers tracking information from a variety of sources including mobile device tracking data from telco companies, CCTVs and card transaction data from banks, and these are collated to generate notifications via text messages to potentially infected individuals.

Table 1. Summary of CT Apps considered in our Analysis.

S/No	Name of Mobile App	Installs	Country
1	Aarogya Setu	100M+	India
2	ALHOSN UAE	1M+	UAE
3	AlohaSafe Alert	5000+	U.S (Hawaii)
4	Beat Covid Gibraltar	10K+	Gibraltar
5	BeAware Bahrain	500K+	Bahrain
6	BlueZone	10M+	Vietnam
7	CA Notify	500K+	US (California)
8	Care19 Alert	10K+	US (WY and SD)
9	careFIJI	50K+	FIJI
10	CG Covid-19 ePass	1M+	India

11	CO Exposure Notifications	100K+	US (Colorado)
12	COCOA	5M+	Japan
13	Coronalert – Belgium	1M+	Belgium
14	CoronaMelder	1M+	Netherlands
15	Coronavírus - SUS	5M+	Brazil
16	Coronavirus Algérie	100K+	Algeria
17	Corona-Warn-App	5M+	Germany
18	COVA Punjab	1M+	India
19	COVID Alert - Let's protect each other	1M+	Canada
20	Covid Alert CT	50K+	US (Connecticut)
21	Covid Alert DE	10K+	U.S (Delaware)
22	COVID Alert NJ	100K+	US (New Jersey)
23	COVID Alert NY	500K+	US (New York)
24	COVID Alert PA	100K+	US (PA)
25	COVID Alert South Africa	1M+	South Africa
26	Covid Trace Nevada	100K+	US (Nevada)
27	COVID Tracker Ireland	500K+	Ireland
28	COVIDaware MN	100K+	US (Minnesota)
29	COVIDSafe	1M+	Australia
30	COVIDWISE	100K+	US (Virginia)
31	CRUSH COVID RI	100K+	US (RI)
32	DC CAN	10K+	US (D.C.)
33	E7mi	50K+	Tunisia
34	EHTERAZ	1M+	Qatar
35	eRouška	1M+	Czech Republic
36	GH Covid-19 Tracker	5K+	Ghana
37	Guam Covid Alert	10K+	U.S (Guam)
38	GuideSafe	100K+	US (Alabama)
39	HaMagen	1M+	Israel
40	Hayat Eve Sığar	10M+	Turkey
41	Hoia	100K+	Estonia
42	Immuni	1M+	Italy
43	Koronavilkku	1M+	Finland
44	MD Covid Alert	100K+	US (Maryland)
45	MI COVID Alert	100K+	US (Michigan)
46	MorChana	1M+	Thailand
47	MySejahtera	10M+	Malaysia
48	MyTrace	100K+	Malaysia
49	NCOVI	1M+	Vietnam
50	NHS COVID-19	1M+	UK
51	NZ COVID Tracer	1M+	New Zealand
52	PeduliLindungi	1M+	Indonesia
53	Protect Scotland	100K+	Scotland
54	Radar COVID	1M+	Spain
55	RADAR covid	1M+	Mexico
56	Rakning C-19	100K+	Iceland
57	Shlonik	100K+	Kuwait
58	SlowCOVIDNC	100K+	US (N. Carolina)
59	Smittestopp	100K+	Norway
60	StaySafe PH	500K+	Philippines
61	STOP COVID - ProteGO Safe	1M+	Poland
62	StopCOVID NI	100K+	Northern Ireland
63	StopKorona!	50K+	North Macedonia
64	Stopp Corona	100K+	Austria
65	SwissCovid	500K+	Switzerland
66	Tabaud (COVID-19 KSA)	5M+	Saudi Arabia
67	TousAntiCovid	5M+	France
68	TraceTogether	1M+	Singapore
69	VirusRadar	100K+	Hungary
70	WA Notify	100K+	US (Washington)

3. CT APP DESIGN APPROACHES

The CT apps reviewed are generally designed using either a centralized or decentralized approach. There are also hybrid implementation and several privacy-preserving frameworks such as the Apple-Google Exposure Notification (GAEN) framework and DP-3T used by Radar COVID in Spain and SwissCovid in Switzerland.

The design trade-offs and adoption are dependent on factors such as the overall CT strategy, requirement on data collection, privacy regulations and technology policies.

GAEN is one of the widely adopted frameworks designed with strong controls and protections for user privacy. It can be deployed without the need to manually develop an app using the "Exposure Notifications Express" (EN Express) mode. Under such implementation, the country's health authority only needs to provide information to the backend infrastructure which will generate an app on Android. On iOS, the functionality is integrated directly at the native OS without a dedicated app. This helps countries expedite the roll out of the CT solution.

However, the GAEN privacy-by-design approach limits the amount of information to be collected and this poses a challenge for CT efforts to quickly identify how, when and whom the person was infected by or passed the infection to. Some countries such as Singapore decided against using the GAEN framework because it was considered not as effective in the local context.

4. THREATS TO CT MOBILE APPS

We identified the following threat scenarios relevant to CT apps and this serve as a reference to contextualize our subsequent security and user data privacy assessment.

- **Falsified CT Records:** If the integrity of data collected by the app is not adequately secured, an adversary could compromise the CT details. When exploited at massive scale, this could undermine the CT efforts [8].
- **Incorrect/Misconfigured Permissions:** An insecure app granted with excessive privileged permissions could lead to exploitation of hardware components such voice recorder leading to risks of spying or invasion of privacy without users' knowledge. It is reported that the Australia's intelligence agencies have been "incidentally" collecting data from the country's COVIDSafe app [9]. In the middle east, CT apps from Kuwait and Bahrain were criticized for invasion of privacy as they were tracking users' live locations [10].

- **Network and Man in the Middle (MITM) Attacks:** If the app adopts a centralized architecture and sends data to a server, the communication channel could be compromised if there is inadequate defense method to protect against exploits on malicious proxies, compromised certificates, and reuse of stale sessions. This could lead to exposure of sensitive information (e.g. UK's NHS CT app was found to transmit unencrypted sensitive interaction logs [11]).
- **Sensitive Data Leakage and Compromise:** The design of CT app may involve handling of sensitive data such as PII, location and health records and if without adequate measures to protect and delete them, there could be risk of data leakage and compromise. For example, in Qatar, researchers found a vulnerability in their Covid-19 app that allows hackers to obtain people's national ID numbers and health status [12]. The Dutch CT System suffered cyber breaches twice, first in Apr 2020 when the app (i.e. CoronaMelder) source code was exposed resulting in leakage of PII and in Jan 2021 where the backend system was breached and thousands of citizens PII including Dutch social security number were stolen and put-on sale on dark web [13].
- **Malware Infection:** With the ongoing proliferation of CT apps, malware could find their way in to contaminate legitimate apps that are vulnerable or imitate official apps. Such malicious app could steal data or compromise the CT system.
- **Vulnerable Third-Party Dependencies:** The apps with dependency on third-party libraries should isolate their code from untrusted third-party code to avoid data leaks, such as leaking PII details without user's consent. These libraries could also be vulnerable over time and requires timely patching and it is crucial to manage such dependencies.
- **Code Injection and Input Validation:** Code injection occurs when an adversary adds malicious code through a GUI, data connection point or other vector that provides access to application code. For example, if a login form field does not have any proper input validation, this presents an opportunity for adversary to enter a malicious JavaScript code snippet to compromise user data. In May 2020, NIST reported that COVIDSafe had a Denial-of-Service vulnerability, allowing an adversary to remotely crash the app if they are within Bluetooth handshake distance. This is due to an erroneous subroutine call which does not perform proper input validation [14].
- **Insecure Cryptography:** Cryptography is used to protect confidentiality of payload and communication channels as well as facilitate secure authentication and authorization of transactions. Insecure implementation or use of weak/broken cryptography suites will pose risks for adversary to exploits these vulnerabilities.
- **Phishing:** During the early phase of the pandemic, there have been a rising trend of fake CT apps, emails, QR codes and websites that attempt to phish user's data and credentials [15].

5. SECURITY AND PRIVACY ANALYSIS METHODOLOGY

Figure 1 illustrates the overall framework and summarizes our analysis approach and scope of security vetting. We extracted the Android Package (APK) binary files of the 70 apps from Google Play Store and then de-compiled the APK of each app to its corresponding class and xml files. We then utilized the Mobile Security Framework (MobSF) and Falcon Sandbox for static analysis. In addition, we also performed manual code inspection to validate findings to minimize false positives to the best of our knowledge. For the dynamic analysis, we scanned for presence of malware in the APK using MetaDefender, VirusTotal and APKiD which checks if the APK had been modified, injected with malware, and recompiled by dexlib.

Static Code Analysis (MobSF, Falcon Sandbox and Manual Review)
- Check Restricted Permissions - Check Protections (NIAP Analysis) - Check Manifest Weakness and Vulnerabilities (i.e. OWASP MASVS TOP10) - Shared Library Binary Analysis
Dynamic and Malware Analysis (MetaDefender, VirusTotal and APKiD)
- Check For APK Tampering and Recompilation - Scan For Malware
Privacy Analysis (MobSF and Manual Review)
- Identify Trackers

Figure 1. Mobile Security Vetting Framework

6. SECURITY AND PRIVACY ANALYSIS RESULTS

In this section, we present the results of 70 CT apps. Our technical analyses were conducted between 10 Dec 2020 and 8 Feb 2021.

6.1 Manifest Weakness and Code Analysis

Our results show that there are several manifest weakness and vulnerabilities in the apps. Figure 2 highlights a summary of key findings.

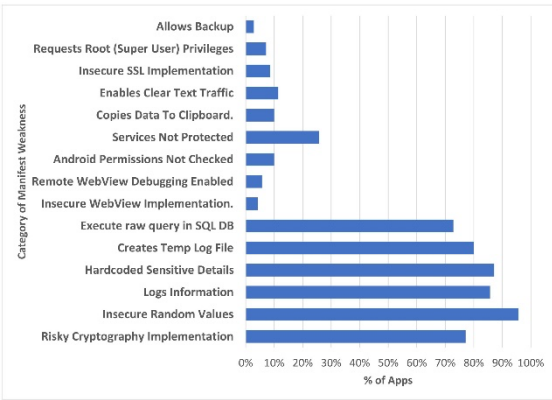

Figure 2. Results (Manifest Weakness)

- **Risky Cryptography Algorithm:** Over 70% of the apps uses at least one of the deprecated cryptographic algorithms (e.g. ECB, MD5 and SHA-1.) with known vulnerabilities. This is flagged as "M5: Insufficient Cryptography" in OWASP where broken cryptography should not be used to protect sensitive payload or channels. For example, NZ COVID Tracer (3.0.2) app uses ECB mode in for its cryptographic function involving secure key store "com/reactlibrary/securekeystore/RNSecure KeyStoreModule.java". The risk here is that ECB mode is known to be weak as it will produce identical encrypted block for equivalent plain text block. This could allow an adversary that is eavesdropping to reverse engineer and recover the original encrypted message. Furthermore, this cipher mode alone does not guarantee integrity.
- **Insecure Random Values:** Over 90% of the apps uses routine in java/koltin that has an insecure random value implementation. Depending on if these routines are used for critical operations or involve sensitive information, this could be a false positive for some of the apps.
- **Hardcoded Sensitive Details:** Over 80% of the apps may have stored sensitive data in cleartext. For example, in CG Covid-19 ePass (34) we found that some sensitive details are stored in "Security.java" such as password key "Sw@pn11". In another app, NZ COVID Tracer (3.0.2) the "PrivateDbEncryptionKey" in BuildConfig.java may also have been hardcoded and exposed.
- **SQLite Database:** The SQLite database is widely used by mobile apps to store user data, and this makes it an attractive target for adversaries. If the app uses dynamic SQL queries using invalidated user inputs, it could cause SQL injection attacks. In addition, the database may not be encrypted and is used to store sensitive information on the client-side app. A recent approach [16] also revealed that it is possible for adversary to hijack queries in an SQLite environment and inject code to trigger errors or to execute malicious actions in applications reading the data. Our static analysis reported that 70% of apps uses SQLite database but we did not discover any risky implementation in our manual inspection.
- **Apps Logs Information and Creates Temporary Log File:** Around 83% of the apps logs information and creates a temporary log file. If sensitive information is involved, it should not be written to a temporary file because the file could then be accessed by another app granted with permission to read logs. For example, StaySafe PH (2.2.4) creates temp log files and contains excessive loggings activities that store sensitive user information. There should also be adequate data protection (i.e., strong encryption) in the client-side app storage to prevent data leakage or compromise.
- **Reverse Engineering**: All apps that we analyzed did not employ sufficient binary code obfuscation techniques or solutions to prevent tools from performing static code analysis and reverse engineering. Code obfuscation is one of the secure coding practices recommended by OWASP to mitigate against malicious reverse engineering.
- **Other Findings:** We also discovered the following cyber hygiene related to secure coding and configuration.

- Around 5% of the apps have insecure web view implementation and remote web view debugging is enabled such as careFIJI (1.0.48) and Shlonik شلونك (2.0.3). This could run the risk of exposing sensitive data if exploited by malicious adversary.
- 7% of the app such as ALHOSN UAE (1.44.248), COVA Punjab (1.3.25) and PeduliLindungi (3.1.2) requests for super root user privileges which may not be a necessary core requirement for CT function. There is a risk that the app may be exploited by other (malicious) apps to execute privilege operations on their behalf. This super user privileges may also be used to determine if the device is rooted. 17% of the apps may have implemented root detection capabilities.
- 11% of the apps has enabled clear text traffic such as Beat Covid Gibraltar (1.0.3) and BeAware Bahrain (0.3.2). We also observed that 39% of the apps uses SSL pinning library to prevent MITM attacks.
- In one finding, the NZ COVID Tracer (3.0.2) app did not protect the Biometric Credential Handler Activity and enabled this to be exported which could result in risk that other services can execute this activity without permission.

6.2 Permissions Analysis

Android framework uses mandatory access control based on app permissions to regulate the capability of apps. It restricts the apps' access to sensitive data such as system state and user's contact information and restrict apps' operations such as recording audio. There are runtime permissions, also known as dangerous or restricted permissions, which grant the app with more privileges to perform restricted actions. In our analysis, we observed the following:

Apps that adopt the GAEN framework do not require any dangerous permissions.

Apps that do not adopt the GAEN framework request at least one dangerous permission. The most requested permissions include:

- ACCESS FINE/COARSE/BACKGROUND LOCATION which is used to determine GPS location.
- ACCESS READ/WRITE_EXTERNAL_STORAGE which may be used for debugging/logging purposes.
- ACCESS CAMERA which may be used for scanning of QR codes to facilitate location check-in.

In addition, several apps request permissions to access restricted data and actions as shown in Figure 3. These maybe unusual or excessive for CT function. For example, the app can record audio, read calendar and contacts as well as access media location. While these permissions require user consent, they are generally considered dangerous permissions and a potential area for adversary to exploit for malicious purposes.

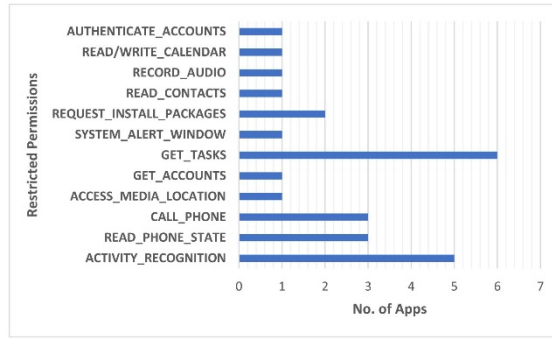

Figure 3. Results (Restricted Permissions)

6.3 Dynamic and Malware Analysis

In our malware analysis, we used MetaDetector, APKiD and VirusTotal to detect if the APKs were malicious or injected with malware. This was achieved by examining the compiler fingerprinting and checking the hash MD5 value against a list of antivirus scanners and URL/domain blacklisting services.

Our scan discovered that the app Canada's "Covid Alert let's protect each other" version 1.1.7 published in 14 Jan 2021 matched a YARA ruleset that detects PlugX malware in memory. This was picked up by MalConfScan, the forensics and incident response tool created by the JPCERT/CC incident response group. PlugX is a remote access tool/trojan (RAT) that uses modular plugins with command-and-control capabilities such as file modification and camera control. However, subsequent scans on a later version 1.1.8 published in 20 Jan 2021 did not reveal any malware presence.

Our results did not find any malware presence for the remaining 69 apps. Google and Apple have taken measures to keep their app store ecosystems a safe

and trusted platform to host COVID-19 themed apps such as ensuring that data sources are reputable and that developers presenting these apps are from recognized entities such as government entities. In the early phase of the pandemic, adversaries were distributing fake android apps themed around official government CT apps to steal PII data and monitor user activities. The family of malwares previously present in the fake apps were predominantly identified as Anubis, Spynote and other malware of Trojan nature [15].

6.4 Privacy Analysis

In our privacy analysis, we observed data trackers embedded within the apps. As shown in Figure 4, over 35% of app uses Google Firebase and ~25% of the apps subscribes to Google Crash Analytics. In an extreme case, we observed that StaySafe PH (2.2.4) uses Facebook trackers that monitor user' logins, places and shares.

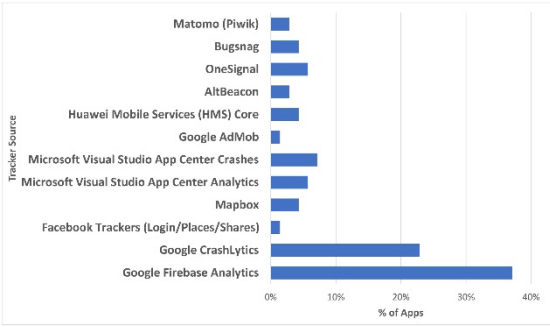

Figure 4. Results (Data Trackers)

The use of Google Analytics has raised concerns for threatening the privacy of users as the data tracked and collected (i.e., PII details) could be used without user's consent to monetize the advertising platforms [17]. Google's parent company Alphabet was found to be the owner of platforms that have data trackers in more than 88% of 1M apps analyzed in 2018 [18].

7. FURTHER INSIGHTS ON APP PRIVACY AND SECURITY ASSURANCE

7.1 Apple Privacy Labels

Apple recently launched it privacy labels as part of its iOS 14.3 update on 14th Dec 2020. This feature will display mandatory privacy labels for iOS apps on Apple app store. The app developer will need to identify all data that they and their third-party partners collect and use. The taxonomy of privacy labels is shown in Figure 5. This provides greater transparency over the data parameters accessed and, helps both users and app developers better understand the security and privacy risks involved regarding accessing and sharing of the data concerned.

Category	Types Of Data	Data Parameters
Data Linked To You	Contact Info	Name
		Email Address
		Phone Number
		Physical Address
		Other User Contact Info
	Health and Fitness	Health
		Fitness
	Financial Info	Payment Info
		Credit Info
		Other Financial Info
	Location	Precise Location
		Coarse Location
	Sensitive Info	Sensitive Info
	Contacts	Contacts
	User Content	Emails or Text Messages
		Photos or Videos
		Audio Data
		Gameplay Content
		Customer Support
		Other User Content
	Browsing History	Browsing History
	Search History	Search History
	Identifiers	User ID
		Device ID
	Purchase History	Purchase History
Data Not Linked To You	Usage Data	Product Interaction
		Advertising Data
		Other Usage Data
	Diagnostics	Crash Data
		Performance Data
		Other Diagnostic Data
	Other Data	Other Data

Figure 5. Taxonomy of Apple App Privacy Labels

Out of the 70 apps we analyzed in Android, we searched for their equivalent iOS version in Apple app store and found that 3 apps are not available in iOS, 19 app adopts the GAEN express framework which only require users to activate the feature on their native iOS instead of downloading a separate app. 20 of remaining 48 iOS apps declared and published the privacy details on Apple app store. However, these declarations have not been verified by Apple. Figure 6 shows the current state of data parameters based on the app developers' declarations.

- In the data that not linked to user category, *product interaction* (7), *crash* (7), and *performance diagnostic* data (4) top the chart.
- In the data linked to user's category, *phone number*. (6), *user id* (6), *health* (6), *location*, and *photo/video* (5) information are among the top details collected.

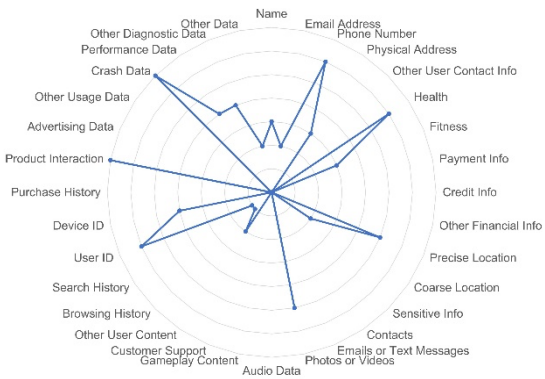

Figure 6. Data Collection Declarations in 20 iOS CT Apps (as at 25 Jan 2021)

Apple has set an exemplary precedence to protect user privacy. On 6th May 2021, Google announced a new safety section in Google Play that will give greater transparency over how apps use its data [19].

7.2 Security Testing and Assurance

Besides secure app coding practices, one of the key security assurance initiatives is also on continuous and rigorous security testing and to this regard, vulnerability disclosures programs (VDP) and bug bounty programs (BBP) have been organized to include CT apps. This could complement existing efforts on vulnerability scans and penetration testing which are usually bounded by time and scope. For example, in Singapore, TraceTogether CT app code is open sourced for the community to validate and improve it and has a link within the app to allow users to report vulnerabilities. Likewise, in the UK, VDP is available for NHS COVID-19 App through HackerOne community. In India, Aarogya Setu App has a public BBP through an independent provider. In France, YesWeHack provides VDP for StopCovid App. In 2020, Google paid $1.74 million in rewards for the Android Vulnerability Reward Program [20] and expanded the criteria to include vulnerabilities on their Exposure Notification API and as well as any governmental apps related to COVID-19 CT function with bounty reward of up to US$20K under Google Play Security Reward Program (GPSRP).

8. IMPLICATIONS FOR FUTURE APPS

CT apps have the potential to expand their use cases beyond contact tracing such as serving as digital health passports to track vaccination and testing records. This increases the risks of data security and privacy. In April 2021, France becomes first EU country to launch digital health passports, and this is facilitated through their TousAntiCovid CT app upgraded to store COVID-19 test results on users' mobile phone [21].

CT app developers should continue to pay attention to the evolving threat landscape, usage pattern and strengthen the rigor of secure coding practices, and vulnerability assessment with close to alignment to OWASP Mobile Security Testing Guide (MSTG) and Mobile AppSec Verification Standard (MASVS). They can also subscribe to and leverage on BBP and VDP programs to encourage and maximize opportunities for early and responsible reporting or disclosure of vulnerabilities.

The new privacy labelling scheme in Android and iOS provides greater transparency and granularity on how app manages data linked to users and this will help prioritize efforts to secure the app, protect sensitive information and build trust with users.

9. RELATED WORKS

There are some studies [22, 23, 17, 24] that have analyzed the security and privacy of CT solutions during the early and mid-phases of the pandemic in 2020. N. Ahmed et al [22] surveyed the CT app attributes and provided early guidance into the various CT solution, architecture design frameworks and approaches. Y. Gvili [23] reviewed the Security Analysis of the COVID-19 CT Specifications by Apple Inc. and Google Inc.

Sun et al. [17] analyzed the security and privacy of 40 CT apps, provided guidance on design principles for secure and privacy preserving apps and recently developed an automated security and privacy assessment tool. He et al. [24] provided a first look and specific analysis on COVID-19 themed mobile malware and threats.

In contrast to these studies, our work is the first attempt to provide a comprehensive security review of the CT app landscape in Q1 2021 covering 70 apps used globally in 47 countries.

10. CONCLUSION

In this work, we analyzed the security and privacy risks of 70 CT apps used globally in 47 countries. Among other findings, we found several manifest weakness/vulnerabilities and excessive permissions requested by the apps. Beyond the rigor of static and dynamic analysis for these apps, we also shared observations and implications on the security and privacy assurance initiatives such as the privacy labelling scheme, vulnerability

disclosure and bug bounty programs which could set a new direction for researchers and practitioners in developing and deploying more secure and privacy preserving CT apps in future.

■ REFERENCES

[1] WHO, "WHO Coronavirus Disease (COVID-19) Dashboard," 31 Jan 2021. [Online]. Available: https://covid19.who.int/. [Accessed 19 Jun 2021].

[2] M. Sato, "Contact tracing apps now cover nearly half of America. It's not too late to use one.," Technology Review, 14 Dec 2020. [Online]. Available: https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/. [Accessed 31 Dec 2020].

[3] P. Dave, "New contact tracing apps stir hope for virus fighters in U.S. states," 20 Nov 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-apps-tracing/new-contact-tracing-apps-stir-hope-for-virus-fighters-in-u-s-states-idUSKBN27Z2SO. [Accessed 27 Dec 2020].

[4] T. Ryan-Mosley, "MIT Technology Review Covid Tracing Tracker," 23 Dec 2020. [Online]. Available: https://public.flourish.studio/visualisation/2241702/. [Accessed 31 Dec 2020].

[5] Statista, "Mobile operating systems' market share worldwide from Jan 2012 to 2021" 8 February 2021. [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/. [Accessed 10 Feb 2021].

[6] F. Liang, "COVID-19 and health code: How digital platforms tackle the Pandemic in China", Soc. Media Soc., vol. 6, no. 3, Jul. 2020.

[7] Mark Zastrow, "South Korea is reporting intimate details of COVID-19 cases: has it helped?" 18 March 2020. [Online]. Available: https://www.nature.com/articles/d41586-020-00740-y. [Accessed 7 Jan 2021].

[8] Li, J., & Guo, X. (2020). COVID-19 Contact-tracing Apps: a Survey on the Global Deployment and Challenges. ArXiv, abs/2005.03599.

[9] Zack Whittaker, "Australia's spy agencies caught collecting COVID-19 app data" 24 November 2020. [Online]. Available: https://techcrunch.com/2020/11/24/australia-spy-agencies-covid-19-app-data/. [Accessed 31 Dec 2020].

[10] Amnesty International, "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy" 16 June 2020. [Online]. Available: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/. [Accessed 17 Dec 2020].

[11] D. Raywood, "NHS Contact Tracing App Security Issues Detailed," 20 May 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/nhs-app-issues/. [Accessed 8 Jan 2021].

[12] Tim Starks, "Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better" 7 June 2020. [Online]. Available: https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601 [Accessed 17 Dec 2020].

[13] K. Loohuis, "Data of thousands of Dutch citizens leaked from government Covid-19 systems," 08 Feb 2021. [Online]. Available: https://www.computerweekly.com/news/252495983/Data-of-thousands-of-Dutch-citizens-leaked-from-government-Covid-19-systems. [Accessed 09 Feb 2021].

[14] NIST National Vulnerability Database (NVD), " CVE-2020-12717" 14 May 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-12717 [Accessed 18 Dec 2020].

[15] Channel News Asia , " SingCERT warns of fake COVID-19 contact tracing apps containing malware" 12 Jun 2020. [Online]. Available: https://www.channelnewsasia.com/news/singapore/covid-19-singcert-fake-contact-tracing-apps-download-privacy-12829624 [Accessed 18 Dec 2020].

[16] J. Vijayan, "Researchers Show How SQLite Can Be Modified to Attack Apps," 8 Dec 2019. [Online]. Available: https://www.darkreading.com/attacks-breaches/researchers-show-how-sqlite-can-be-modified-to-attack-apps/d/d-id/1335500. [Accessed 10 Jan 2021].

[17] Sun, R., Wang, W., Xue, M., Tyson, G., Camtepe, S., & Ranasinghe, D.C. (2020). An Empirical Assessment of Global COVID-19 Contact Tracing Applications. arXiv: Cryptography and Security.

[18] Binns, R., Lyngs, U., Kleek, M.V., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third Party Tracking in the Mobile Ecosystem. Proceedings of the 10th ACM Conference on Web Science.

[19] Android Developer Blog, " New safety section in Google Play will give transparency into how apps use data" 06 May 2021. [Online]. Available: https://android-developers.googleblog.com/2021/05/new-safety-section-in-google-play-will.html [Accessed 10 Jun 2021].

[20] A. Saroha, "Google paid $6.7 million in bug bounty rewards in 2020," TheHindu, 08 Feb 2021. [Online]. Available: https://www.thehindu.com/sci-tech/technology/google-paid-67-million-in-bug-bounty-rewards-in-2020/article33782949.ece. [Accessed 09 Feb 2021].

[21] Jon Henley, "France is first EU member state to start testing digital Covid travel certificate" The Guardian, 20 Apr 2021. [Online]. Available: https://www.theguardian.com/world/2021/apr/20/france-is-first-eu-member-state-to-start-testing-digital-covid-travel-certificate [Accessed 13 Jun 2021].

[22] N. Ahmed et al., "A Survey of COVID-19 Contact Tracing Apps," in IEEE Access, vol. 8, pp. 134577-134601, 2020, doi: 10.1109/ACCESS.2020.3010226.

[23] Y. Gvili, "Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc." Cryptology ePrint Archive, Report 2020/428, April 2020, https://eprint.iacr.org/2020/428.

[24] He, Ren & Wang, Haoyu & Xia, Pengcheng & Wang, Liu & Li, Yuanchun & Wu, Lei & Zhou, Yajin & Luo, Xiapu & Guo, Yao & Xu, Guoai. (2020). Beyond the Virus: A First Look at Coronavirus-themed Mobile Malware.

Ang Wei Yang CISA, CISM, CGEIT, CRISC, CDPSE, QISP is a recent graduate from the School of Computing and Information Systems, Singapore Management University where he received his MSc in Computing (Cybersecurity) under the National Cybersecurity Postgraduate Scholarship Award. He also holds a MSc in Knowledge Management and BEng in Computer Engineering from the Nanyang Technological University of Singapore. He is a member of IEEE and OWASP Foundation. His

research interests include mobile computing, software security and data privacy analysis.

Email: weiyang.ang.2019@mais.smu.edu.sg

Lwin Khin Shar is an Assistant Professor (practice) at School of Computing and Information Systems, Singapore Management University. He received the PhD degree in electrical and electronic engineering from the Nanyang Technological University of Singapore. He was a research associate in software verification and validation at the SnT centre for Security, Reliability, and Trust, University of Luxembourg and a research scientist at Nanyang Technological University. He is a member of IEEE and ACM. His research interests include software security and privacy analysis using program analysis and machine learning techniques.

Email: lkshar@smu.edu.sg