Security Vulnerabilities and Privacy Posture of Contact Tracing Applications

Authored by

Md Nizam Uddin

Research Project

Submitted to the Faculty of Graduate Studies

Concordia University of Edmonton

In Partial Fulfillment of the Requirements for the

Final Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

Advisor: Dr Sergey Butakov (sergey.butakov@concordia.ab.ca)

December 2022

Security Vulnerabilities and Privacy Posture of Contact Tracing Applications

Authored by

Md Nizam Uddin

Approved:

Sergey Butakov [Original Approval on File]

Sergey Butakov Date: December 09, 2022

Primary Supervisor

Dr.Patrick Kamau [Original Approval on File]

Dr. Patrick Kamau Date: December 09, 2022

Dean, Faculty of Graduate Studies

Table of Contents

I. Introduction 4
II. related works on contact tracing security 4
A. Background 4
B. Related Research on COVID-19 Contact Tracing Applications 5
III. Assessment of Applications 5
A. Objectives of the Research 5
B. Methodology 5
C. Testbed 6
IV. Results 7
A. Application Security Score 7
B. Vulnerability Analysis 7
C. Privacy Policy Analysis 8
D. Backend Server Location Analysis 9
V. Conclusion 10
VI. References 10

List of Tables

Table 1 Samples of the vulnerabilities discovered in the applications. 7
Table 2 PIPEDA Parameters conformance 9
Table 3 Geolocation of Backend Server 10
Table 4 List of Applications 12
Table 5 Potential security issues of the reviewed applications 14
Table 6 List of tools 16

List of Figures

Figure 1 Steps for static analysis 6
Figure 2 Steps for dynamic analysis 6
Figure 3 Application security score by MobSF 7

Security Vulnerabilities and Privacy Posture of Contact Tracing Applications.

Md Nizam Uddin
Master of Information Systems Security Management
Concordia University of Edmonton
Edmonton,Canada
nizamuddnin.missm@gmail.com

***Abstract*—This research analyzed selected contact tracing applications to identify potential vulnerabilities and geolocation of services used by these applications. MobSF framework and Android emulators were used to perform static and dynamic analysis of the applications. Security policies of applications were analyzed to check conformance with selected parameters outlined in personal information protection regulations. Results obtained from analysis revealed that some of the applications had vulnerabilities which could be exploited by bad actors endangering users' personal information The findings from the study can be useful to privacy researchers and mobile applications developers.**

Keywords—contact tracing, application vulnerabilities, privacy, location-based services .

I. INTRODUCTION

During COVID-19 pandemic, many health authorities around the world introduced mobile applications for COVID-19 contact tracing purposes. These applications were developed to reduce workload on manual contact tracing imposed by the drastic growth of COVID-19 cases. As these applications deal with sensitive personal data and medical information, adequate protection mechanisms are required to protect user privacy. There were concern from various stakeholders about the privacy and effectiveness of these applications for reliable contact tracing. In their paper [1] authors identified potential limitations in terms of neighbor discovery, smartphone based tracing was the the only option for a quick deployment of contact tracing automation. As many quick solutions for emerging problems these deployed apps came with significant risks. In an open letter[2], 300 scientists expressed their concern about the implementation of tools that collects and processes mass-scale personal data. As this data is vulnerable to cyberattack and this data could be misused for the unprecedented surveliilence of public. Governments might use these data to track location of citizens and use for law enforcement purposes.Although COVID-19 pandemic is over now, contact tracing applications may be deployed to mass public under some other circumstances. This leads to the necessity to have a deep understading of security and privacy problems with the current set of contact tracing apps.

This research analyzed vulnerabilities and privacy characteristics of selected COVID-19 applications by performing static and dynamic analysis onto these selected applications. The results from static and dynamic analysis and privacy policy review revealed related vulnerabilities, privacy issues and mechanism for handling sensitive user data by these applications. The research aimed to provide insight into privacy concerns of intended users, application developers and other stakeholders about potential shortcomings of these applications which could lead to sensitive data breach. The research has analyzed COVID-19 contact tracing applications from diverse geographic locations around the world particularly applications from North America (USA and Canada). This research has investigated vulnerabilities related to these applications against OWASP TOP-10 and OWASP Mobile Application Security Verification Standard (OWASP-MASVS) [3].Communication between applications and backend servers has been reviewed using dynamic analysis to identify servers' location. Using dynamic analysis, it was reviewed whether user data was processed outside of the respective country or jurisdiction of the application.

Static analysis was carried out by Mobile Security Framework (MobSF) tool. Dynamic analysis was performed by installing applications on Android emulator and proxying by Burp suite to find server IP address to determine whether user data were processed outside of respective application's country or jurisdiction. Application's privacy policy was reviewed against a few selected criteria from CANADA's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA) [4].

As stated in [5] newer operating systems from Google and Apple have embedded capacity to utilize decentralized protocol of Google Apple Exposure Notification (GAEN) which provides strong security architecture for contact tracing, but it cannot protect users' data if applications have severe vulnerabilities, GAEN also does not control the way how users' data are being handled on the third-party servers. Although applications typically being sandboxed by an operating system , there is a potential for invasive features of the application to use other applications permission to access sensitive data of user device and exfiltrate them to a third party.

Although COVID-19 pandemic seems to be ending, findings from this research could be useful for general users and application developers dealing with mobile applications using location tracking features and processing sensitive personal information.

II. RELATED WORKS ON CONTACT TRACING SECURITY

A. Background

The COVID-19 pandemic, which creates severe contagious respiratory infection by the virus, spread rapidly throughout the world. Many health authorities around the world have

developed and released their own COVID-19 contact tracing applications to contain and mitigate the spread of COVID-19 [6]. Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission [7]. To provide privacy-friendly platform for contact tracing applications, Google and Apple Jointly developed Google Apple Exposure Notification in April 2020[8].Mobile applications had been used to contain and contact tracing of infectious diseases before COVID-19 pandemic hit. Mobile applications were used to mitigate the spread of Ebola virus in Africa [9].Functionalities ranged from contact tracing and case management by mobile applications during Ebola outbreak. Mobile applications were also successful in the case of mitigating the spread of tuberculosis in Botswana in the use of public health intervention [10].Manual contact tracing process is labor-intensive and consumes a lot of resources. Manual contact tracing found insufficient during COVID-19 pandemic, especially during peak infection. There was extensive interest in development and implementation of digital COVID-19 tracing applications to overcome shortcomings of manual contact tracing. Because of the urgency of developing contact tracing applications, many applications have been produced at a rapid speed. Many of these applications were deployed without extensive testing making these applications vulnerable to cybercriminals.

B. *Related Research on COVID-19 Contact Tracing Applications*

Launching of the COVID-19 contact tracing applications was the first attempt to use smartphone contact tracing in a large scale. Even thoughCOVID-19 pandemic seemed to be over contact tracing applications have potential to help with the outbreak of some other contagious diseases. The research paper by [9] evaluated 13 applications from 10 countries based on technology used. This study found that most used technology for application was Bluetooth, followed by Global Positioning System (GPS). The study revealed that some applications (The Norwegian, Singaporean and New Zealand applications) collected most personal information from users and some applications (Swiss application and Italian application) did not collect any user information. The research completed by [11] conducted multilateral analysis of 28 selected COVID-19 tracing applications of Android platform. This study analyzed privacy policies of each app, conducted dynamic application behavior analysis and security analysis of each program code to identify vulnerabilities. Most of the applications (17 out of 20) were found to be accessing user's geolocation. Almost one-third (31%) of applications seek dangerous category permission, 66% of applications seek normal permission and 3% required signature permissions. This research identified some vulnerabilities related to contact tracing applications. Researchers found that, none of the evaluated applications fulfilled privacy breach notice principle. The research conducted by [12] studied ethical and deployment challenges of COVID-19 contact tracing applications. The study revealed that deployment of tracing applications poses challenge of effectiveness, technical issues and risks to privacy and equity. This research revealed that the elderly who may not access to smartphones are excluded from the use of contact tracing applications. Another study conducted by [13] analyzed 28 Contact tracing applications from North America (US & Canada). The study analyzed permission required by these applications to function. Server location of these applications were identified by static analysis conducted with Mobile Security Framework (MobSF). This study is focused on static analysis.

The proposed research analyzed COVID-19 contact tracing applications from diverse geographic locations around the world with main focus on applications from North America (USA and Canada). The proposed reach will investigate vulnerabilities related to these applications and map these vulnerabilities into OWASP Mobile Application Security Verification Standard (OWASP- MASVS). This research investigated communication between applications and backend servers using dynamic analysis to identify servers' location. Using dynamic analysis, it was verified whether user data is processed outside of the respective country or jurisdiction of the application.

III. Assessment of Applications

A. *Objectives of the Research*

To access privacy and security posture of the contact tracing application this research aims at the following research objectives.

- To analyze vulnerabilities of contact tracing applications and summarize them under OWASP top 10 mobile and OWASP Mobile Application Security Verification Standard (MASVS).
- To analyze privacy policies of selected applications for verifying degree of compliance with some chosen criteria from Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
- To analyze whether user data is processed outside of the application's designated country/jurisdiction by determining server locations.

B. *Methodology*

After reviewing available COVID-19 contact tracing applications on Google Play, android package kit (.apk) files of 28 applications were obtained based on active status, number of installs and applications from diverse locations. Mobile Security Framework (MobSF) was installed as a docker image to perform static analysis on selected applications. Static analysis was performed by uploading .apk files into MobSF framework. Privacy policy of each application was reviewed against chosen parameters from PIPEDA to analyze whether privacy policies conform with those parameters. Applications were installed on an Android emulator created by Genymotion to intercept communication with backend server. Once installed applications were run on the virtual device and communication was intercepted using Burp Suite proxy server community edition. After getting IP address of the

server, physical locations of server were obtained from two sources, “IP2LOCATION” and “dbip”

C. Testbed

There are many tools available to get comprehensive analysis report of mobile applications. This research used Open-source tool called Mobile Security Framework (MobSF) for static analysis for its popularity, scalability, and effectiveness in identifying vulnerabilities within applications very quickly. For dynamic analysis, Genymotion was used to create Android emulator to simulate real Android devices. A proxy, Burp Suite community edition was used to intercept traffic between device and servers to trace server’s location. To perform static analysis MobSF was installed on windows machine as a Docker image. APK file of selected applications were downloaded from google play store. For preliminary research purpose static analysis was performed on application named “"ABTraceTogether” by uploading AKP file of this application onto MobSF. MobSF performs static analysis by accessing compiled source code and manifest. Research process for static analysis is summarized as below figure

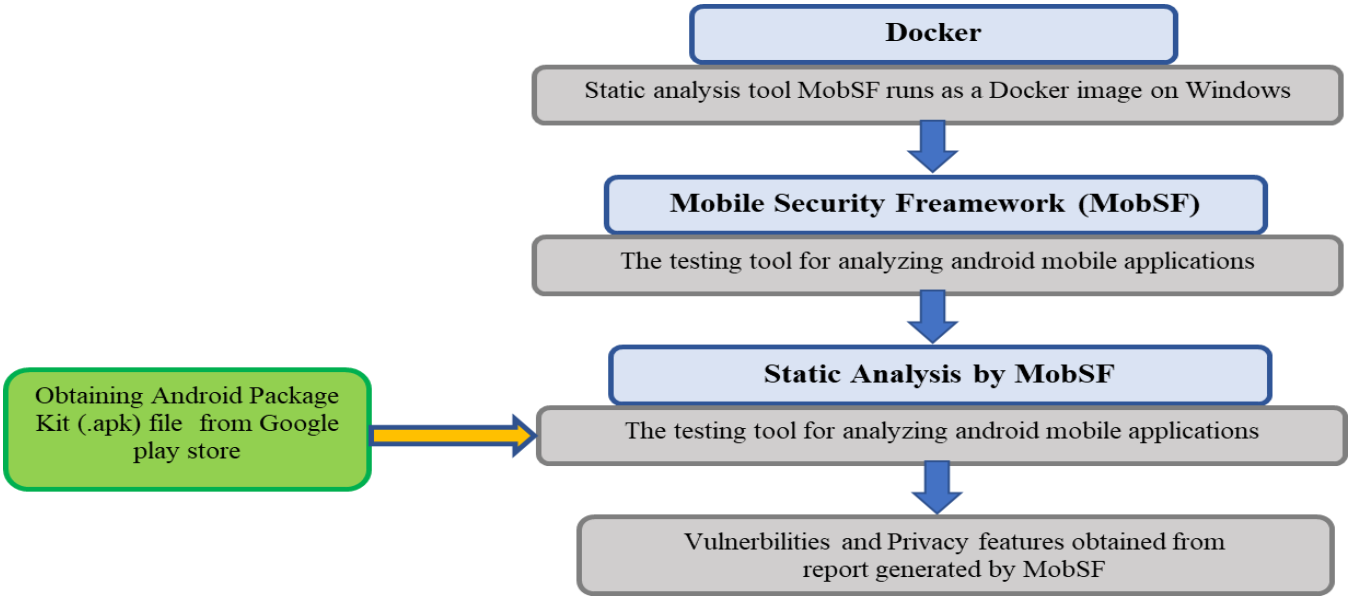

Figure 1 Steps for static analysis

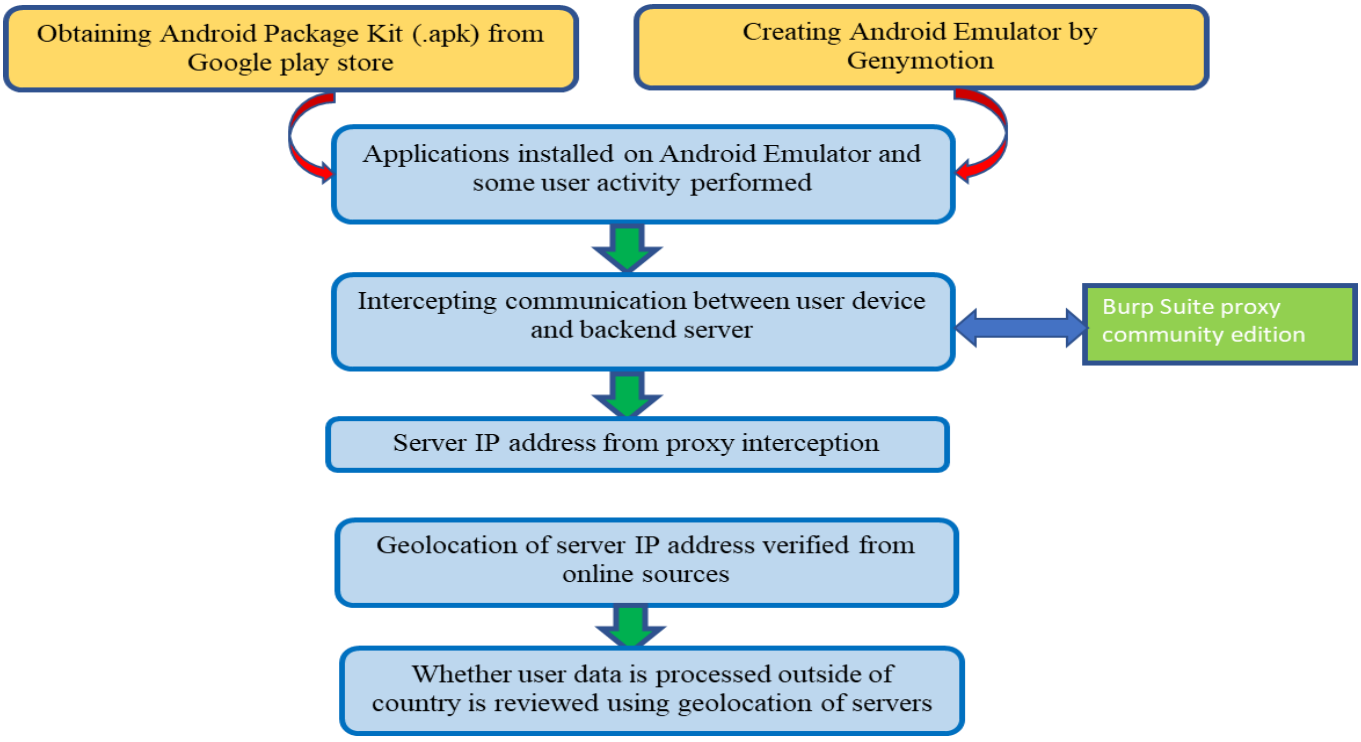

Figure 2 Steps for dynamic analysis

Dynamic analysis was conducted by installing application on Android emulator. Genymotion was used to create Android emulator and some tasks were performed to simulate communication between user device and backend server of the applications. To determine server location, communication between user device and back-end server was intercepted by Burp suite proxy. Once server IP addresses were found, geolocation of the server IP addresses were verified by two different online sources. Research process for dynamic analysis is summarized in figure 2.

IV. Results

A. Application Security Score

MobSF framework assigns an application security score in the range of zero to 100. For every identified high severity finding and warning severity finding 15 and 10 points are reduced from initially assigned 100 points respectively. For every identified good severity 5 points are added to the score.

Most of the applications (23 out 26) applications were assigned a perfect security score of 100 by MobSF. Three applications (ABTraceTogether, Care19_Alert and Covid Alert DE) were assigned security score of 75,60 and 30 respectively. For example, COVID Alert DE has 6 warning severity, 1 high severity and 4 mild severities.

B. Vulnerability Analysis

Static analysis has been conducted for the contact tracing application named "ABTraceTogether" using Mobile Security Framework (MobSF). MobSF performs vulnerability analysis based on the information data contained application's APK file including the source code and the manifest file. Common Vulnerability Scoring System (CVSS) is an open framework for rating vulnerabilities. Report generated by MobSF contains a handful number of vulnerabilities associated with selected applications. However, vulnerabilities with high CVSS score have been considered for mapping to OWASP top 10 and OWASP-MASVS. MobSF conducted manifest analysis on applications to identify vulnerabilities. Static analysis listed vulnerabilities on three applications of selected application for this research. MobSF analysis revealed application "Covid Alert DE" as most vulnerable amongst selected applications for the research. One "high" severity and six "warning" severity vulnerabilities were identified on "Covid Alert DE" App. Several "high" and "warning" severity vulnerabilities were identified on ABTraceTogether, Care19_Diary, and Care19_Alert applications.

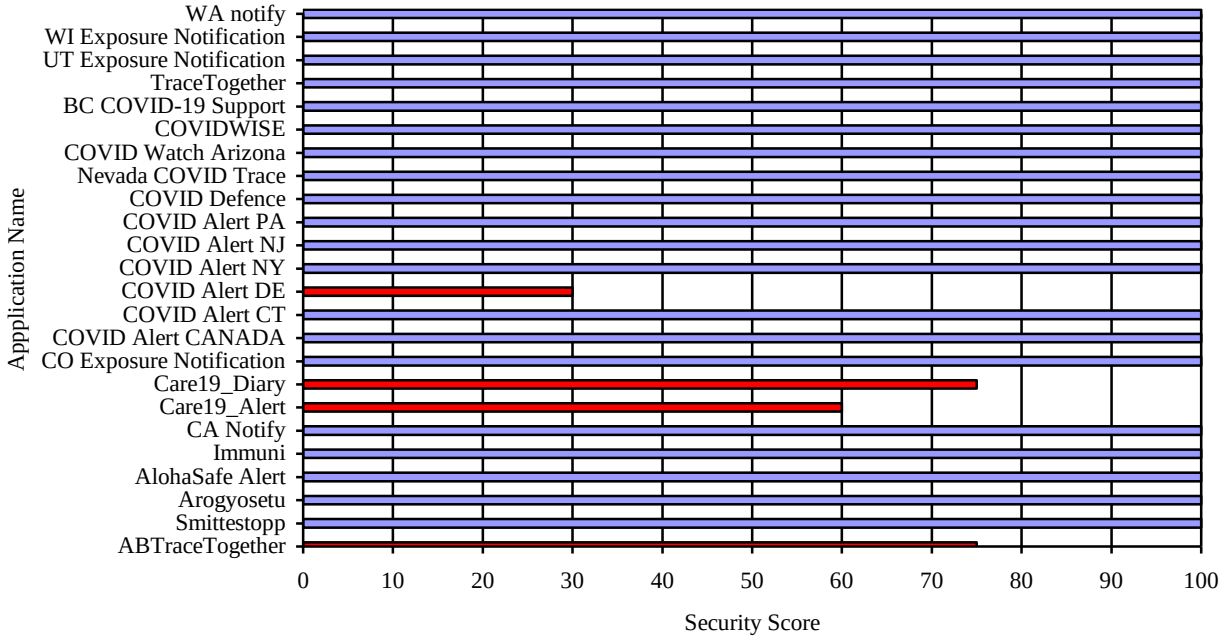

Figure 3 Application security score by MobSF

Table 1 Samples of the vulnerabilities discovered in the applications.

App Name	Vulnerability	Severity	Standards			
			CVVS-V2	CWE	OWASP-TOP10	OWASP-MASVS
ABTraceTogether	The application uses an insecure Random Number Generator.	Warning	7.5(High)	CWE-330 Use of Insufficiently Random Values	M5: Insufficient Cryptography	MSTG-CRYPTO-6
	The application uses the encryption mode	High	7.4(High)	CWE-649 Reliance on	M5: Insufficient	MSTG-CRYPTO-3

	CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks			Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking	Cryptography	
Care19_Alert	App can read/write to External Storage. Any App can read data written to External Storage.	High	5.5 (Medium)	CWE-276 Incorrect Default Permission	OWASP Top 10: M2: Insecure Data Storage	MSTG-STORAGE-2
	The App uses an insecure Random Number Generator.	Warning	7.5(High)	CWE-330 Use of Insufficiently Random Values	OWASP Top 10: M5: Insufficient Cryptography	OWASP MASVS: MSTG-CRYPTO-6
Care 19 Diary	The application logs information.	High	7.5 (High)	CWE-532 Insertion of Sensitive Information into Log File		OWASP MASVS: MSTG-STORAGE-3
	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	High		CWE-312 Cleartext Storage of Sensitive Information	OWASP Top 10: M9: Reverse Engineering	OWASP MASVS: MSTG-STORAGE-14

C. Privacy Policy Analysis

A privacy policy is a legal document which must disclose how an application gathers, stores and uses personally identifiable information it collects from its users. Privacy policy is a basic requirement to upload new applications and updates to the platforms like Google Play store and Apple's App Store.

Canadian federal privacy regulation – PIPEDA [1] was used as to evaluate the major aspects of policy coverage. Although authors understood that not all the reviewed applications were subject to Canadian regulations, it was used as a common ground as it covers the most common aspect of privacy policies. Application's privacy policy will be assessed against the following criteria selected from PIPEDA.

- **User Consent** This parameter mentioned in article 6.1 of PIPEDA states that, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.
- **Data Collection** Data collection framework is covered by articles 4.3 and 7.1 of PIPEDA.
  Although it is clearly mentioned in PIPEDA that information must be collected with user consent, information may be collected without individual consent if the collection is clearly in the interests of the individual and consent can be obtained in a timely way.
- **Record Retention** Personal information shall be retained if necessary for the declared purpose. This principle is covered by article 4.5.2 and 4.5.3. Article 4.5.2 states that organization should develop guidelines for maximum and minimum retention period for personal information. Once the personal information is no longer required for the purpose should be destroyed, erased, or made anonymous as stated by article 4.5.3.
- **Third Party Sharing** Legal base is set in principle 4.9 which states that an individual shall be informed of the existence, use and disclosure of his or her personal information upon request by that individual. As stated in principle 4.9.3 an organization should provide a list of organizations to which organization has disclosed information about an individual.
- **Data Protection** As required in principle 4.1.3 an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.
- **Data Protection** As required in principle 4.1.3 an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.
  Contact Information As stated in article 4.8 of PIPEDA, an organization shall make available about their policies and practices including-the name or title, and the address of the person who is accountable for the organizations policies and procedures.

Analysis of privacy policy revealed that most of the privacy had no clear mentioning of privacy breach notification parameter.

Table 2 summarizes results of privacy policy analysis, green color indicates clear mention of the parameter, Amber color indicates indirect mention and red color indicates no mention of that specific parameter o the application privacy policy.

Table 2 PIPEDA Parameters conformance

Application Name	User Consent	Data Collection	Record Retention	3rd Party Sharing	Data Protection	User Control	Privacy Breach Notification	App Focused	Contact Info
ABTraceTogether									
BCCOVID-19 Support									
Smittestopp									
TraceTogether									
Aarogya Setu									
Immuni									
AlohaSafe Alert									
CA Notify									
CO Exposure Notifications									
COVID Alert-CANADA									
COVID Alert DE									
COVID Alert NJ									
COVID Alert NY									
COVID Alert PA									
COVID Defense									
COVIDWISE									
UT Exposure Notification									
WI Exposure Notification									
WA Notify									
COVID Alert CT									

D. Backend Server Location Analysis

Once installation of applications on Android emulator, some user activity has been performed to simulate real-time activities of the application. As the traffic between user device and back-end server has been intercepted with burp proxy, IP address of respective could be found on proxy. Geolocation of IP address has obtained using free tools available online namely “iplocation” and “geolocation”

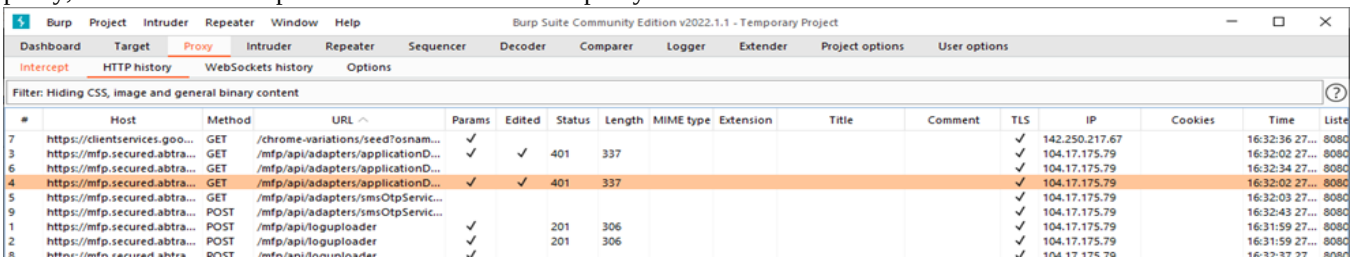

Figure 4 . Intercepted traffic between “ABTraceTogether” application and responding server IP.

Server IP address (104.17.175.79) found on response against request from user device. There are many online sources available to verify IP geolocation. Below are the results found from two websites named “iplocation” and “dbip”

Table 3 Geolocation of Backend Server

Server IP	Protocol	Verification Source	Geolocation of IP
104.17.175.79	https	"IP2LOCATION" https://www.ip2location.com/	California, United States of America
		"dbip" https://db-ip.com/?refid=dck	Ontario, Canada

V. Conclusion

The research looked at the security posture of COVID-19 contact tracing applications. The goal of the screening was to find vulnerabilities that can potentially endanger the privacy of users who install these applications. Since these applications were intended to be used by public and assume sharing personal information, there could be serious implications if any vulnerability was successfully exploited by malicious actors.

The research findings indicate that some of the contact tracing applications had vulnerabilities which are present in CWE, OWASP-TOP 10 and OWASP-MASVS lists. These vulnerabilities were discovered during the static analysis phase of the application screening.

PIPEDA was used to test applications for compliance with privacy regulations. Of course, many of the reviewed applications formally did not need to comply with the PIPEDA as it is a Canadian regulation, but the Act was used as common ground of comparison and only basic privacy related requirement from the Act were reviewed. Only a few (3 out of 20) of the studied applications were found to follow one of the selected PIPEDA parameters – privacy breach notification which left a loophole for the users in in the case of a data breach.

Conducted review of the applications clearly indicated not only issues with the software vulnerabilities but also the fact that many basic privacy requirements were not embedded in these applications privacy policy. Developers should consider proper security screening before deploying applications that are handling highly sensitive information. Contact tracing is not limited to COVID, it can be expected similar technologies can be used for other purposes. Google and Apple support development effort in many countries with GAEN protocols to release express application into their later OS releases leaving older version OS's potentially incompatible with this protocol thus leaving gaps in the accessibility of the technology. Reliance of these advanced protocols smartphones raises the concern of equity and accessibility in the future.

All the extended reports for all applications can be viewed on the following web site:
https://github.com/nizamRM/MobSF
https://github.com/nizamRM/List-of-table

VI. References

[1] P. H. Kindt, T. Chakraborty and S. Chakraborty, "How reliable is smartphone-based electronic contact tracing for COVID-19?," *Association for Computing Machinery*, vol. 65, no. 1, pp. 56-67, 2021.

[2] Open Letter, "Joint Statement on Contact Tracing," 19 April 2020. [Online]. Available: https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view. [Accessed 10 January 2022].

[3] OWASP, "OWASP Mobile Application Security," 07 March 2020. [Online]. Available: https://mas.owasp.org/MASVS/. [Accessed 15 November 2021].

[4] Office of the Privacy Commissioner of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)," 13 April 2005. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/. [Accessed 7 February 2022].

[5] ECDC, " Contact tracing for COVID-19: current evidence, options for scale-up and an assessment of resources needed," 05 May 2020. [Online]. Available: https://www.ecdc.europa.eu/en/publications-data/contact-tracing-covid-19-evidence-scale-up-assessment-resources. [Accessed 10 January 2022].

[6] L. Du, V. L. Raposo and M. Wang, "COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the," *The Journal of Medical Internet Research*, vol. 8, no. No 11(2020), 2020.

[7] J.-H. Hopeman, "A Critique of the Google Apple Exposure Notification," *Researchgate*, no. +0100 / arXiv / gaen-critique.tex, 09 December 2020.

[8] D. Tom-Aba, P. M. Nguku, C. C. Arinze and G. Krause, "Assessing the Concepts and Designs of 58 Mobile Apps for the Management of the 2014-2015 West Africa Ebola Outbreak:Systematic Review," *JMIR Public Health & Surveillance* , vol. Vol 4, no. No 4 (2018): Oct-Dec, pp. 2-3, 2018.

[9] M. Elkhodr, O. Mubin, Z. Iftikhar, M. Masood, B. Alsinglawi, S. Shahid and F. Alnajjar, "Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search and Content Analysis," *J Med Internet Res.*, no. 2021 Feb; 23(2): e23467.doi: 10.2196/23467, 2021.

[10] R. Klar and D. Lanzerath, "The ethics of COVID-19 tracking apps – challenges and voluntariness," *Research Ethics*, vol. Vol. 16, no. 3-4, 2020.

[11] T. A. Danish and S. Butakov, "Study of the Privacy Preserving Mechanism in the COVID-19 Contact Tracing Applications," 2021.

[12] C. Troncoso, D. Bogdanov, E. Bugnion, S. Chatel, S.

Gürses, J.-P. Hubaux, D. Jackson, J. R. Larus, W. Lueks, R. Oliveira, M. Payer, B. Preneel, A. Pyrgelis, M. Salathé, T. Stadler and M. Veale, "Deploying decentralized, privacy-preserving proximity tracing," *Communications of the ACM*, vol. 65, no. 9, pp. 48-57, 2022.

[13] M. Hatamian, S. Wairimu, N. Momen and L. Fritsch, "A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps.," *Empirical Software Engineering*, vol. 26, no. 3, 2021.

Table 4 List of Applications

No	Application Name	Country/ Jurisdiction	Google Play Store Link	Status	Number of Installs
1	Smittestopp	Norway	https://play.google.com/store/apps/details?id=no.fhi.smittestopp_exposure_notification&hl=en_CA&gl=US	Active Updated on October. 20,2021	100,000+
2	TraceTogether	Singapore	https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace&hl=en_CA&gl=US	Active Updated on January 24,2022	1,000,000+
3	Aarogya Setu	India	https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_CA&gl=US	Active Updated on January 12 ,2022	100,000,000+
4	Immuni	Italy	https://play.google.com/store/apps/details?id=it.ministerodellasalute.immuni&hl=en_CA&gl=US	Active Updated on January 21 ,2022	10,000,000+
5	ABTraceTogether	Alberta	https://play.google.com/store/apps/details?id=ca.albertahealthservices.contacttracing&hl=en_CA&gl=US	Active Updated on January 12 ,2022	100,000+
6	AlohaSafe Alert	Hawaii	https://play.google.com/store/apps/details?id=org.alohasafe.alert&hl=en_CA&gl=US	Active Updated on May, 25 ,2021	100,000+
7	BC COVID-19 Support	British Columbia	https://play.google.com/store/apps/details?id=ca.bc.gov.health.hlbc.COVID19&hl=en_CA&gl=US	Active Updated on January 26, 2022	100,000+
8	CA Notify	California	https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 28, 2022	1,000,000+
9	Care19 Alert	North Dakota and Wyoming	https://play.google.com/store/apps/details?id=com.proudcrowd.exposure&hl=en&gl=US	Active Updated on November 27, 2020	10,000+
10	Care 19 Diary	North Dakpta/South Dakota/Wyoming (US)	https://play.google.com/store/apps/details?id=com.proudcrowd.care&hl=en_CA&gl=US	Active Updated on June 26, 2020	50,000+

11	CO Exposure Notifications	Colorado	https://play.google.com/store/apps/details?id=gov.co.cdphe.exposurenotifications&hl=en_CA&gl=US	Active Updated on December 21, 2021	100,000+
12	COVID Alert - Let's protect each other	Canadian Federal	https://play.google.com/store/apps/details?id=ca.gc.hcsc.canada.stopcovid&hl=en_CA&gl=US	Active Updated on August 9, 2021	1,000,000+
13	COVID Alert CT	Connecticut	https://play.google.com/store/apps/details?id=gov.ct.covid19.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 28, 2022	100,000+
14	Covid Alert DE	Delaware	https://play.google.com/store/apps/details?id=gov.de.covidtracker&hl=en_CA&gl=US	Active Updated on March 6, 2021	50,000+
15	COVID Alert NJ	New Jersey	https://play.google.com/store/apps/details?id=com.nj.gov.covidalert&hl=en_CA&gl=US	Active Updated on June 14, 2021	500,000+
16	COVID Alert NY	New York	https://play.google.com/store/apps/details?id=gov.ny.health.proximity&hl=en_CA&gl=US	Active Updated on November 11, 2021	500,000+
17	COVID Alert PA	Pennsylvania	https://play.google.com/store/apps/details?id=gov.pa.covidtracker&hl=en_CA&gl=US	Active Updated on February 23, 2021	500,000+
18	COVID Defense	Louisiana	https://play.google.com/store/apps/details?id=org.pathcheck.la.bt&hl=en_CA&gl=US	Active Updated on January 19, 2021	100,000+
19	Nevada COVID Trace	Nevada	https://play.google.com/store/apps/details?id=gov.nv.dhhs.en&hl=en_CA&gl=US	Active Updated on January 30, 2022	100,000+
20	WeHealth Arizona	Arizona	https://play.google.com/store/apps/details?id=gov.azdhs.covidwatch.android&hl=en_CA&gl=US	Active Updated on January 20, 2022	100,000+
21	COVIDWISE	Virginia	https://play.google.com/store/apps/details?id=gov.vdh.exposurenotification&hl=en_CA&gl=US	Active Updated on January 18, 2022	500,000+
22	CRUSH COVID RI (401Health)	State of Rhode Island	https://play.google.com/store/apps/details?id=com.ri.crushcovid&hl=en_CA&gl=US	Active Updated on December 10,	10,000+

				2021	
23	GuideSafe	Alabama	https://play.google.com/store/apps/details?id=gov.adph.exposurenotifications&hl=en_CA&gl=US	Active Updated on February 3, 2021	100,000+
24	MD COVID Alert	Maryland	https://play.google.com/store/apps/details?id=gov.md.covid19.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 28, 2022	100,000+
25	MI COVID Alert	Michigan	https://play.google.com/store/apps/details?id=gov.michigan.MiCovidExposure&hl=en_CA&gl=US	Active Updated on August 24, 2021	100,000+
26	NM Notify	New Mexico	https://play.google.com/store/apps/details?id=gov.nm.covid19.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 28, 2022	100,000+
27	PunchAlert	Georgia	https://play.google.com/store/apps/details?id=in.punch.alert&hl=en_CA&gl=US	Active Updated on August 30, 2020	5,000+
28	UT Exposure Notifications	Utah (US)	https://play.google.com/store/apps/details?id=gov.ut.covid19.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 30, 2022	100,000+
29	WA Notify	Washington	https://play.google.com/store/apps/details?id=gov.wa.doh.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 28, 2022	500,000+
30	WI Exposure Notification	Wisconsin	https://play.google.com/store/apps/details?id=gov.wi.covid19.exposurenotifications&hl=en_CA&gl=US	Active Updated on January 28, 2022	100,000+

Table 5 Potential security issues of the reviewed applications

Applications	Security Issues	Severity
Smittestopp	One Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked.	**High**
	Broadcast Receiver (androidx. work.impl.diagnostics.DiagnosticsReceiver) is protected by a permission, but the protection level of the permission should be checked.	**High**
	One service named (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected.	**High**

Arogyosetu	Broadcast Receiver (nic.goi.aarogyasetu.background.BootReceiver) is not Protected.	**High**
Immuni	Broadcast Receiver (it.ministerodellasalute.immuni.receivers.UpdateReceiver) is not Protected.	High
AlohaSafe Alert	The activity (org.pathcheck.covidsafepaths.MainActivity) is not Protected. [android:exported=true]	High
	Broadcast Receiver (org.matomo.sdk.extra.InstallReferrerReceiver) is not Protected.	High
BC COVID-19	Application Data can be Backed up (This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	Medium
	Service (com.getcapacitor.CapacitorFirebaseMessagingService) is not Protected.	High
CA Notify	Application Data can be Backed up.	Medium
	Service(com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked.	High
CO Exposure Notification	Application data can be backed up	Medium
	Broadcast Receiver (com.google.android.apps.exposurenotification.nearby.SmsVerificationBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.	High
COVID Alert Canada	Broadcast Receiver (com.transistorsoft.tsbackgroundfetch.BootReceiver) is not Protected.	High
COVID Alert CT	Application data can be backed up.	Medium
COVID Alert NJ	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected.	High
COVID Alert NY	A Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected.	High
COVID Alert PA	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected.	High
COVID Defence	An Activity (org.pathcheck.covidsafepaths.MainActivity) is not Protected.	High
	Broadcast Receiver (org.matomo.sdk.extra.InstallReferrerReceiver) is not Protected.	High
COVID Watch Arizona	Service(com.google.android.gms.nearby.exposurenotification.WakeUpService) is protected by a permission, but the protection level of the permission should be checked.	High
COVIDWISE	An Activity-Alias (gov.vdh.exposurenotification.ENNotifyOthers) is not Protected.	High
Nevada COVID Trace	A broadcast Receiver (com.transistorsoft.tsbackgroundfetch.BootReceiver) is not Protected.	High
	Application Data can be Backed up.	Medium

Table 6 List of tools

Resource	Purpose	Description	Source
Android Package Kit (apk) file of COVID-19 contact tracing applications	To perform vulnerability analysis and permission analysis of selected applications using apk files.	APK or Android Package Kit is an extension for the Android Package files that are used for distributing applications on Android OS from Google.	**https://www.apkmirror.com/** **https://m.apkpure.com/**
Mobile Security Framework **(MobSF)**	To perform static analysis of selected COVID-19 contact tracing applications	Mobile Security Framework (MobSF) is an automated, all-in-one mobile application pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.	**https://mobsf.github.io/docs/**
Genymotion Emulator	To create virtual Android device for installing COVID-19 contact tracing applications and perform dynamic analysis	Genymotion Desktop is an Android emulator which includes a complete set of sensors and features to interact with a virtual Android environment.	**https://www.genymotion.com/**
Burp Suite-Application Security Testing Software (Community Edition)	To intercept and analyze traffic between user device and application server	Burp Suite is an integrated platform/graphical tool for performing security testing of web and mobile applications.	**https://portswigger.net/burp/communitydownload**