BRIEFING NOTES

#BN-49-COVID19-Feb2021

SECURITY AND PRIVACY RISKS AND CONSIDERATIONS IN DEVELOPING COVID-19 CONTACT TRACING MOBILE APPS

Authors: Mehdi Taheri[1] and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- As multiple new waves of COVID-19 pandemic are emerging, governments are developing contingency plans to protect individuals and further contain the virus outbreak while reopening the economy.
- Several countries such as South Korea, Singapore, Norway, UK, and Canada have been developing contact tracing mobile apps that can measure the proximity of users from one another to identify potential COVID-19 patients. A user with prolonged close contacts with confirmed patients will be notified by the app and will be asked to take a test for COVID-19.
- Besides the benefits of the COVID-19 contact tracing apps, they have raised concerns regarding the privacy and security of users on the cyberspace. Governments and service providers need to take steps to ensure that the users' privacy is protected, thus encouraging individuals to use the apps more commonly.

CONTEXT

- Artificial intelligence (AI) has recently been utilized to develop services that can assist governments and societies in their combat against the COVID-19 outbreak. For instance, chatbots have been designed that provide useful and trustworthy information about the virus, AI-based technologies have been employed to diagnose the disease and predict whether a patient will develop severe symptoms or not, development of drugs and finding a cure for this lethal disease is another application of AI.
- AI has also been utilized in monitoring crowds and identifying potential COVID-19 patients by measuring the proximity of users from one another [1]. Personal user information is required to be collected, processed, and stored to develop contact tracing apps that measure proximity of users. Hence, privacy and security concerns regarding utilization of mobile apps have been raised.
- Since traditional contact tracing methods that are carried out manually by humans are not adequate and cannot keep up with the rapid spread of the virus, there is a need to develop COVID-19 contact tracing technologies by utilizing machines and smartphones. Moreover, contact tracing technologies can help health organizations to control and contain spread of the virus in a large scale.
- Among the first initiatives in Canada to develop COVID-19 contact tracing, Public Health Ontario launched a campaign to recruit volunteers in April 2020 as "a process that is used to identify, educate and monitor individuals who have had close contact with someone who is infected with a virus" [2]. The COVID-19 contact tracing app in Ontario has been developed with a feature that allows users to voluntarily declare if their COVID-19 test results are positive, which helps to protect user's privacy [3].
- It has been discovered that the contact tracing app developed in Alberta can be a security threat to Apple cellphones [4]. Office of the Information and Privacy Commissioner of Alberta (OIPC) has announced that since the developed contact tracing app in Alberta

requires Apple devices to be unlocked while using the app, it "significantly increases risk in case of theft or loss" [4].

- MIT researchers have initiated Private Automated Contact Tracing (PACT) as an effort to design and develop an exposure detection technology for digital communication devices [5]. The PACT protocol was released in April 2020. This protocol proposes a decentralized method for data usage and storage and uses Bluetooth Low Energy signals to measure the proximity of users. One of the main objectives of PACT is to preserve individual's privacy by generating a random string of numbers on each phone as its identification number that other nearby devices can receive and store.
- A peer-to-peer contact tracing approach has been proposed in [6], and a prototype app has been developed. This method is based on an anonymized graph that illustrates the interaction among users. Users can check their risk of being infected and anonymously report if they have been diagnosed positive. Moreover, a simulation result that indicates the effectiveness of the proposed app in [6] has been provided.
- Effectiveness of contact tracing apps in monitoring the outbreak massively depends on the number of users and widespread use of them to identify other nearby devices [7]. In addition to the trade-off between privacy of users and effectiveness of apps, one can consider security risks as a discouraging factor in usage of contact tracing apps. Augmentation of traditional manual contact tracing and app-based tracing is an approach that may help to leverage the advantages of contact tracing methodologies [7].
- In Iceland, only 35 percent of the country's population started using their contact tracing app, also in UK, a small percentage of people used their apps. Therefore, the developed apps in above countries were not useful [3]. On the contrary, in Germany, they have succeeded in containing the spread of the virus by utilizing a combination of contact tracing apps and direct contact and calling potential COVID-19 cases [3].
- A malicious adversary is capable of injecting false positive cases or false negative cases into the contact tracing apps if security measures are not employed in design and development stages of the apps. Moreover, denial of service cyber attacks can be performed on contact tracing apps [8]. Types of cyber attacks vary based on the structure of the data storage system, server of an app, and encryption methods that are utilized.
- There are several cyber attack strategies, for instance, replay attack in which an adversary first stores received messages or signals from other users and then forwards the recorded signals to other users in different locations such as hospitals. Moreover, wireless device tracking where an adversary's objective is to trace routes and locations of a contact tracing app user, location confirmation that is performed by an adversary to discover and disclose a user's presence in an area, enumeration attack in which adversaries try to count the number of positive cases that use a tracing app, denial of service (DoD) attacks that consume device battery, bandwidth, and processing power, de-anonymizing the users or linkage attacks which intend to identify a user's identity, and disclosure of social graph that illustrates individuals by nodes and their proximity by edges of the graph [8].

CONSIDERATIONS

Developers require a framework and an architecture that preserves users' privacy and guarantee their security to create a COVID-19 contact tracing app according to that. Characteristics of centralized and decentralized architectures are described in the following.

- Centralized architecture: In the first step, a user is required to register in the central server to get its Temporary ID (TempID). The TempID is encrypted with a secret key that is stored in the server. The encrypted TempID will be exchanged with devices that are close to one another by utilizing Bluetooth signals. Since the server encrypts the TempIDs, the identity of a user and their personal information cannot be discovered by other users. A user with positive test results can voluntarily upload its received encounter messages to the server, following that a map of encountered TempIDs will be generated to identify potential patients.
- Decentralized architecture: The main objective in the decentralized architecture is to have most of the process and tracing process on the user device to alleviate privacy concerns [8]. Hence, anonymous identifiers will be generated on the user device, and exposure encounters will be processed on that device instead of a central server. Each device generates its random identifier that is changed in a short amount of time to a new identifier, and other nearby devices can receive and store these identifiers. A confirmed COVID-19 patient can voluntarily upload its encounter messages, which consist of received nearby identifiers to a central server. Finally, the server provides the recorded identifiers by a patient's device for other devices to download and match them with their received identifiers. As a significant advantage of this approach, neither the server nor other users can identify the infected user.
- From the security point of view, each architecture has its advantages and disadvantages. In a centralized architecture, the server can be compromised by adversaries and is prone to data theft. Information exchanges among devices can be compromised by replay attacks to spread incorrect encounter information. A malicious hacker can discover location of a user. The server can be subject to DoS attacks, and adversaries can discover a part of the social graph.
- A decentralized architecture is prone to replay attacks if the expiry time of generated identifiers on a device is not short. Moreover, in a decentralized architecture, adversaries can perform DoS attacks, they can enumerate the number of infected users from the list of infected identifiers that the server provides, and the social graph among patients and their nearby users can be discovered.

RECOMMENDATIONS

- The COVID-19 contact tracing apps on smartphones have been useful tools in countries such as South Korea, Singapore, and Germany to monitor and contain the spread of the

virus. These apps are required to be developed in a manner that individuals privacy are preserved and their security is ensured.

- Among centralized and decentralized architectures, it is evident that the decentralized design alleviates privacy concerns since the identity of an infected user is unknown to health authorities and other users. Moreover, an infected user can voluntarily disclose its encounter messages to a server that is managed by health authorities.
- A centralized architecture has a simple structure and is easier to implement since the encryption and most of the process is carried out on a central server. Furthermore, health authorities have access to more information about an infected user that can be utilized to trace other risky individuals that do not use the app. However, it could cause some privacy concerns and may result in disclosing the patient's personal information.
- A decentralized architecture is more secure in comparison with a centralized one. An adversary's capability is limited by the randomly generated identifiers in the decentralized architecture. Also decreasing the expiry time of identifiers improves the security of users. However, it results in more process and battery consumption on cellphone devices.

REFERENCES

[1] B. Sookman, "AI and contact tracing: How to protect privacy while fighting the COVID- pandemic," 2020.

[2] "National COVID-19 Volunteer Recruitment Campaign," [Online]. Available: https://emploist psjobs.cfp-psc.gc.ca/psrs-srfp/applicant/page1800?toggleLanguage=en&poster=1437722. [Accessed August 2020].

[3] "Can contact-tracing apps really help us beat COVID-19?," 10 July 2020. [Online]. Availab https://www.cbc.ca/radio/whitecoat/can-contact-tracing-apps-really-help-us-beat-covid-19 1.5643163. [Accessed August 2020].

[4] K. Slugoski, "Alberta's COVID-19 contact-tracing app a 'security risk' on Apple devices: priva commissioner," 10 July 2020. [Online]. Availab https://globalnews.ca/news/7159859/alberta-covid-19-coronavirus-tracking-app-risks/. [Accessed August 2020].

[5] R. L. Rivest, D. J. Weitzner, L. C. Ivers, I. Soibelman and M. A. Zissman, "PACT: Private Automat Contact Tracing," MIT, 2020.

[6] T. M. Yasaka, B. M. Lehrich and R. Sahyouni, "Peer-to-Peer Contact Tracing: Development o Privacy-Preserving Smartphone App," *JMIR Mhealth Uhealth,* vol. 8, 2020.

[7] R. A. Kleinman and C. Merkel, "Digital contact tracing for COVID-19," *CMAJ,* vol. 192, pp. E65 -E656, 2020.

[8] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, Janicke and S. Jha, "A survey of covid-19 contact tracing apps," *IEEE Access,* 2020.