Security review: digital contact tracing

Jonathan Lam

09/22/21

1 Overview

Contact tracing is a method to identify individuals who have been in contact with people known to be infected. This technique came to prominence during the COVID-19 pandemic, primarily through the use of (non-mandatory) government- and privately-owned smartphone applications. Digital contact tracing is highly desirable because manual contact tracing uses a large number of human resources, and relies on people known to have COVID-19 to immediately report to a health authority who they have been in contact with recently. This process is not very accurate, as the infected person may not remember everyone they have been in contact with or may have been around unidentified strangers. Digital contact tracing aims to (semi-)automate the process of collecting information about who an individual has been in proximity with so that this process is carried out with greater speed and accuracy, using commonly-available smart devices (smartphones), and potentially offering better anonymity (in the case of decentralized networks). Governments of various scale have adopted official (but non-mandatory) digital contact tracing applications, but there are also non-government-sanctioned apps that exist as well.

Most contact tracing applications work using Bluetooth (e.g., BlueTrace [1]) or GPS (e.g., TraceTogether [4]), which are technologies available on most modern smartphones. (One of the newer systems, NOVID, uses ultrasound.) A user's smartphone generally shares anonymized, time-shifting tokens (Ephemeral ID's) with the other users in their proximity and keeps a local log of the interactions. Several governments (notably in Malaysia, Australia, and New Zealand) have also adopted QR code tagging associated with certain locations. In some systems there may still be some human interaction, such as to filter out likely false positives, but some systems attempt to completely automate the process. The reporting systems associated with

these techniques can be either centralized or decentralized; the latter are more recent (stemming from a MIT paper in May 2020 [3]) and arose due to privacy concerns.

2 Assets

Data assets:

- **User data**: This includes personal information (e.g., contact info) about users, where they have been, and what people they have been in contact with. Most of the security concerns are relevant here. **Confidentiality** (privacy) is the major concern here: we want to make sure that adversaries, or other parties in general (such as the government or organization that may have access to the location data) do not have access to this data. **Authorization**: the only people who should access this data are the health officials who are administering manual parts of the contact tracing. **Authenticity** (users should not be able to spoof their identity as someone else) and **integrity** (contact and location data should not be tampered with) also ensure that the data in the system is correct; loss of data or incorrect data would cause the contact tracing to be less effective.

Hardware assets:

- **User smartphones**: Vulnerabilities in the implementation of wireless protocols may result in the compromise of the smartphone. **Confidentiality** may be a concern: in Bluetooth an RF signal is emitted every 200ms, which can alert others of the user's presence. Confidentiality may also be compromised if the wireless protocol can be fingerprinted.
- **Centralized servers**: If the contact and location information is stored on a centralized server, then we may have to worry about **availability** (due to DoS attacks) or **tampering** by on-site workers. Decentralized networks are less at risk of these.

3 Adversaries/Threats

- **Government spying and tampering**: If the **government** has access to the (centralized) database on which the location and contact records are stored, then they can spy on user whereabouts and contact behavior. This would threaten **confidentiality** of user data. If they

are also given authorization to modify records (i.e., to hide the fact that a political official went somewhere), this would threaten **integrity**.

- **Network attacks**: A **tech-savvy COVID-denier** with a few Bluetooth devices at hand may attempt to cause incorrect data or loss of data. A Bluetooth device can plausibly be overloaded by a DoS attack performed by the adversary's Bluetooth devices, compromising **availability** of the contact tracing system.

4 Potential weaknesses/vulnerabilities

- **Bluetooth**: Bluetooth was already mentioned in the previous section, since implementation bugs may cause problems. A recent set of bugs in Bluetooth called Braktooth is known to allow DoS and even the ability to run arbitrary code, which can compromise the user device in general [5].

- **Tracking identifiers shared by clients**: Even if the identifiers shared by users are anonymized, they are still the same for each user. Since a user is continually emitting this identifier, an adversary may be able to identify the device associated with an anonymous ID.

5 Potential defenses

- To mitigate Bluetooth (or other networking) attacks, users should make sure that their devices have the most up-to-date firmware, and app creators should make sure to run their apps with the minimum permissions necessary to function correctly.

- To protect against tracking identifiers, identifiers are made ephemeral, i.e., "Ephemeral ID's" [1]. This mitigates the ability to identify a device ID because the ID is changed after a set interval of time. There is a tradeoff between how often the key changes and storage space. This is implemented in some contact tracing systems, but it is unknown whether all implement this.

6 Risks

The risk of surveillance deterred many people from the use of contact tracing. Many people might feel that the ability to track people (both their location

and who they contact) feels very much *1984*-ish. Decentralized networks were created as a response to decrease the risk. Confidentiality is also put at risk by local adversaries who are tracking static identifiers – this is mitigated by ephemeral identifiers but cannot be avoided completely.

The risk of Bluetooth vulnerabilities or other networking are probably fairly low. Using an established wireless technology is probably fairly robust, and new vulnerabilities are widely publicized. However, technologies that use more obscure or recent technologies (such as NOVID's use of ultrasound) may be more susceptible to implemenation bugs simply due to smaller community and smaller security efforts aimed at the technology.

7 Reflections

The contact tracing technology has rapidly evolved as it became popularized during the COVID-19 pandemic. There have been several variants of this technology: different proximity-detection technologies, decentralized and centralized reporting techniques, and ephemeral vs. non-ephemeral ID's. Future evolutions may involve IoT devices specialized to this, which would introduce a number of new considerations about usability (would the user want to carry around a new hardware token?), anonymity (doesn't require a login or use of a personal smartphone), and security (dependent on the implementation of the IoT device).

Current decentralized systems offer low-risk of surveillance, or any of the other risks associated with a centralized database. This should offer protection against the largest concern users have: privacy of their location data. However, use of contact tracing requires devices in the proximity to be aware of a user's device which (despite being anonymized) may still trigger the irrational fear of being watched.

Despite the advantages digital contact tracing has to offer in terms of accuracy and convenience, it is still not widely adopted during the pandemic, mostly due to surveillance concerns [4]. A team at the Australian National University concluded that the efficacy also relates to a high testing rate that wasn't being actualized [2]. As a result, it is difficult for contact tracing to achieve its maximimal efficacy.

References

[1] Jason Bay et al. "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders". In: *Government Technology Agency-Singapore, Tech. Rep* (2020).

[2] Manuel Cebrian. "The past, present and future of digital contact tracing". In: *Nature Electronics* 4.1 (2021), pp. 2–4.

[3] Ramesh Raskar et al. *Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic*. 2020. arXiv: `2003.08567 [cs.CR]`.

[4] Dewey Sim and Kimberly Lim. "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app". In: *South China Morning Post* 18 (2020).

[5] Satsuki Then. *BrakTooth vulnerability impacts Bluetooth devices*. Aug. 2021. URL: `https://asset-group.github.io/disclosures/braktooth/` (visited on 09/22/2021).