How Apple and Google will let your phone warn you if you've been exposed to the coronavirus

May 1 2020, by Johannes Becker

Credit: CC0 Public Domain

On April 10, Apple and Google announced a coronavirus exposure notification system that will be built into their smartphone operating systems, iOS and Android. The system uses the ubiquitous Bluetooth short-range wireless communication technology.

There are dozens of apps being developed around the world that alert people if they've been exposed to a person who has tested positive for COVID-19. Many of them also report the identities of the exposed people to public health authorities, which has raised privacy concerns. Several other exposure notification projects, including PACT, BlueTrace and the COVID Watch project, take a similar privacy-protecting approach to Apple's and Google's initiative.

So how will the Apple-Google exposure notification system work? As researchers who study security and privacy of wireless communication, we have examined the companies' plan and have assessed its effectiveness and privacy implications.

Recently, a study found that contact tracing can be effective in containing diseases such as COVID-19, if large parts of the population participate. Exposure notification schemes like the Apple-Google system aren't true contact tracing systems because they don't allow public health authorities to identify people who have been exposed to infected individuals. But digital exposure notification systems have a big advantage: They can be used by millions of people and rapidly warn those who have been exposed to quarantine themselves.

Bluetooth beacons

Because Bluetooth is supported on billions of devices, it seems like an obvious choice of technology for these systems. The protocol used for this is Bluetooth Low Energy, or Bluetooth LE for short. This variant is optimized for energy-efficient communication between small devices, which makes it a popular protocol for smartphones and wearables such as smartwatches.

Bluetooth LE communicates in two main ways. Two devices can communicate over the data channel with each other, such as a smartwatch synchronizing with a phone. Devices can also broadcast useful information to nearby devices over the advertising channel. For example, some devices regularly announce their presence to facilitate automatic connection.

To build an exposure notification app using Bluetooth LE, developers could assign everyone a permanent ID and make every phone broadcast it on an advertising channel. Then, they could build an app that receives the IDs so every phone would be able to keep a record of close encounters with other phones. But that would be a clear violation of privacy. Broadcasting any personally identifiable information via Bluetooth LE is a bad idea, because messages can be read by anyone in range.

Anonymous exchanges

To get around this problem, every phone broadcasts a long random number, which is changed frequently. Other devices receive these numbers and store them if they were sent from close proximity. By using long, unique, random numbers, no personal information is sent via Bluetooth LE.

Apple and Google follow this principle in their specification, but add some cryptography. First, every phone generates a unique tracing key that is kept confidentially on the phone. Every day, the tracing key generates a new daily tracing key. Though the tracing key could be used to identify the phone, the daily tracing key can't be used to figure out the phone's permanent tracing key. Then, every 10 to 20 minutes, the daily tracing key generates a new rolling proximity identifier, which looks just like a long random number. This is what gets broadcast to other devices via the Bluetooth advertising channel.

When someone tests positive for COVID-19, they can disclose a list of their daily tracing keys, usually from the previous 14 days. Everyone else's phones use the disclosed keys to recreate the infected person's rolling proximity identifiers. The phones then compare the COVID-19-positive identifiers with their own records of the identifiers they received from nearby phones. A match reveals a potential exposure to the virus, but it doesn't identify the patient.

Most of the competing proposals use a similar approach. The principal difference is that Apple's and Google's operating system updates reach far more phones automatically than a single app can. Additionally, by proposing a cross-platform standard, Apple and Google allow existing apps to piggyback and use a common, compatible communication approach that could work across many apps.

No plan is perfect

The Apple-Google exposure notification system is very secure, but it's no guarantee of either accuracy or privacy. The system could produce a large number of false positives because being within Bluetooth range of an infected person doesn't necessarily mean the virus has been transmitted. And even if an app records only very strong signals as a proxy for close contact, it cannot know whether there was a wall, a window or a floor between the phones.

However unlikely, there are ways governments or hackers could track or identify people using the system. Bluetooth LE devices use an advertising address when broadcasting on an advertising channel. Though these addresses can be randomized to protect the identity of the sender, we demonstrated last year that it is theoretically possible to track devices for extended periods of time if the advertising message and advertising address are not changed in sync. To Apple's and Google's credit, they call for these to be changed synchronously.

But even if the advertising address and a coronavirus app's rolling identifier are changed in sync, it may still be possible to track someone's phone. If there isn't a sufficiently large number of other devices nearby that also change their advertising addresses and rolling identifiers in sync—a process known as mixing—someone could still track individual devices. For example, if there is a single phone in a room, someone could keep track of it because it's the only phone that could be broadcasting the random identifiers.

Another potential attack involves logging additional information along with the rolling identifiers. Even though the protocol does not send personal information or location data, receiving apps could record when and where they received keys from other phones. If this was done on a large scale—such as an app that systematically collects this extra information—it could be used to identify and track individuals. For example, if a supermarket recorded the exact date and time of incoming rolling proximity identifiers at its checkout lanes and combined that data with credit card swipes, store staff would have a reasonable chance of identifying which customers were COVID-19 positive.

And because Bluetooth LE advertising beacons use plain-text messages, it's possible to send faked messages. This could be used to troll others by repeating known COVID-19-positive rolling proximity identifiers to many people, resulting in deliberate false positives.

Nevertheless, the Apple-Google system could be the key to alerting thousands of people who have been exposed to the coronavirus while protecting their identities, unlike contact tracing apps that report identifying information to central government or corporate databases.

Provided by The Conversation

Citation: How Apple and Google will let your phone warn you if you've been exposed to the coronavirus (2020, May 1) retrieved 3 April 2024 from https://techxplore.com/news/2020-05-apple-google-youve-exposed-coronavirus.html