CENSA® Council for Emerging National Security Affairs

CENSA Report:
Coronavirus Contact Tracing Applications – A Technical Analysis

June 2020
Miguel Guevara

BACKGROUND

The Coronavirus spread has brought the entire world to a halt with no end in sight besides the development of a vaccine, still potentially a year away. As countries face the dilemma of how to open up their economies while reducing the harm of exposure, contact tracing apps have emerged as an important component to a solution. The principle behind these apps is simple: track the set of individuals with whom a person has been in contact. If an individual tests positive for Coronavirus and authorizes the application on their phone, then everyone that has been in contact with them who also has authorized the application will be notified.

This report presents an overview of current contact-tracing applications and the three challenges they mainly present: maximizing adoption, reducing power consumption, and ensuring privacy and security. Countries, like China, are developing their own national applications, not without sacrifices to elements like privacy. Alternative solutions, proposed by cooperative partnerships like Apple-Google, seek to address many of these challenges while ensuring privacy.

In this paper we attempt to highlight the tradeoffs of these competing strategies, examining international attempts to develop an application, and highlighting where these challenges were not met, lead to an adoption of the Apple-Google protocol. We then examine the security mechanisms currently in development within the Apple-Google protocol and conclude with implications for future contact tracing application development and future recommendations for implementation.

PRECEDENT USE-CASES

Singapore and South Korea are recognized by many for their rapid deployment of contact-tracing applications. These applications are attributed as one of the largest reasons for these countries success in halting the spread of COVID-19. The Australian government, a country that recently eased restrictions, has also similarly launched their own applications. These applications all use the Singaporean standard launched in late April, which were separately developed efforts from the Apple-Google protocol.

A major difference between these standards relates to their usage of core system resources like Bluetooth access. By design, iOS does not allow developers to create applications that regularly access some system resources such as Bluetooth. Therefore, for an application to be able to do contact tracing effectively, it needs to stay open while the phone is unlocked. This, in turn, creates a usability problem as the battery drains quickly which causes users to less likely use the applications.

The Australian application overcame this challenge by continually pushing notifications to its users to remind them to open the application. Admittedly, this isn't the most user-friendly solution and therefore reduces the application's effectiveness. The University of Oxford estimated that at least sixty percent of individuals with smartphones would need to opt-in to these applications for them to be effective. This clearly poses a challenge when use of the applications require these opt-ins or "always on" systems.

More recently Japan, Poland, and Germany launched apps using the Apple-Google mechanism. By utilizing the built-in system resources of Android and iOS in the Apple-Google protocols, applications are able to utilize features like Bluetooth in the background to track interactions with other users which eliminates the power consumption challenges. In the case of the United Kingdom, while they originally sought to develop their own application, they instead reversed that decision and switched to the Apple-Google protocol given the technical difficulties that their homegrown solution faced.

In the United States there is no national standard being pursued, different states are taking individual approaches with some using the Google/Apple protocol.

PRIVACY AND SECURITY MECHANISMS

The protocol that Google and Apple announced in April relies on a host of cryptographic methods. By design it has a decentralized approach to data collection. Both of these points constitute the critical security and privacy aspects of the system.

A core method that Apple and Google are using to ensure privacy is to generate two constantly changing "keys" - one to identify a user's unique device and the other to identify on what day the device interacts with other devices. These keys are randomly generated using high-level encryption so only the user's phone stores the keys of other devices in proximity. The current protocol makes it technologically infeasible for Apple, Google, or any government agencies to track individuals.

These keys provide one of the most crucial security aspects in the system: since they are kept on the device, it becomes computationally infeasible for an attacker to *stitch-together* all the rolling proximity identifiers and attribute them to one device. In practice, it will be very hard for an attacker to sit and collect rolling proximity identifiers and derive meaningful information from these keys. Moreover, these keys only cover the last fourteen days in time—older data is automatically deleted—which enhances the privacy protection.

If a user is diagnosed with COVID-19, they can opt-in to upload all of the keys they generated during the last fourteen days to a central server. Other users in the same region can download those keys in the last fourteen days that are labeled as COVID positive. A users' phone searches for matches of those keys that it came in contact with and alerts users if they have been exposed to someone who tested positive. Data on the centralized servers are deleted when it is older than fourteen days. All of the aspects above relate to the core 'plumbing' of the Apple-Google standard. This ‘plumbing’ addresses many of the pitfalls that the Australian and Singaporean applications have reported.

CONCLUSION AND RECOMMENDATIONS

The success of these apps will highly depend on whether people opt-in to them. People might only do so if they feel that the tradeoff between utility, privacy, and security is favorable in their view. The cryptographical aspects of any application must consider this to ensure maximum participation.

Several states, most notably China, have taken a centralized approach to managing COVID locational based data. Some notable western democracies like France are also advocating a centralized approach to maintaining COVID locational data in order to help epidemiologists to refine their mathematical models. It is our opinion, and that of most privacy advocates, that this is a dangerous precedent that puts too much user information in one location, making it vulnerable to government abuse or cyber-attacks.

The cryptographical aspects being examined in the Apple-Google protocol seem to follow the principle of data minimization—collecting only essential information, decentralizing the locations it is stored at, and deleting the information once it is no longer useful for its limited purposes.

To increase the usage of these apps, governments will need to create an incentive structure for user adoption. In China, citizens’ COVID risk is ranked in terms of colors and to gain access to most buildings they must show their COVID risk on their phone. While these measures might seem excessive in the West, governments will need to use other tools, such as public information campaigns to raise awareness. Workplaces or private businesses could also require employees or customers to install the applications to enter their premises.

If the applications are not widely adopted, governments may need to do an analysis of what aspects need to be changed. In absence of mandated usage, these applications will only succeed if they are easy to use and provide users with the right expectation of privacy and appropriate security guarantees. While this is an open question, we believe that the existing protections in development are a promising start.

This report is the product of a policy working group sponsored by the Council for Emerging National Security Affairs. The views and policy recommendations are the authors’ own and do not reflect an official position of CENSA or its board members. The author is a policy and technical expert affiliated with the companies mentioned in this report.