Privacy Issues for Apple-Google Exposure Notification Mechanism

Adam Bobowski, Jacek Cichoń, Mirosław Kutyłowski
Department of Fundamentals of Computer Science, Wrocław University of Science and Technology

Exposure notification. One of the key means for limiting the spread of contagious diseases is to follow potential infection chains and quarantine the suspect persons. Unfortunately, an infected person may become infectious before any symptoms occur. This is the case for COVID-19 and isolation of diagnosed patients is not sufficient: at the moment when symptoms appear for a patient A, then not only A could have already infected a person B, but the person B could already transmit the illness to a third person C. For this reason it is crucial to trace quickly the contacts and impose appropriate contact limitation measures. It has been reported that manual contact tracing takes a long time and a limited capacity leads to a processing bottleneck in case of an epidemic.

One of the ideas to speed-up contact tracing and made it more reliable is to use a smart phone app and a short range Bluetooth Low Energy channel (BLE). A smart phone continuously sends its identifiers over BLE. On the other hand, it records all identifiers sent by the other smartphones in its vicinity – the distance between the smartphones is estimated based on the signal strength.

Once a person is diagnosed to be infected, the app can send appropriate data to a Diagnosis Server where a list of diagnosis keys is composed for all reported cases of a given period. After downloading this list an app can check whether a person holding the smart phone has been exposed to infection by comparing the identifiers derived from the diagnosis keys with the identifiers recorded on the smart phone.

Privacy issues. From the point of view of effectiveness the best solution would be to upload all contact data in real time to a central server. Then the relevant epidemic data might be derived immediately. However, in practice such a system is doomed to fail. First, the data collected could be misused to create a state surveillance system. Even if this is not the case, the citizens may fear such a situation and refuse to join the system.

The exposure notification system developed by Apple and Google takes privacy issues very seriously and, in contrast to some European proposals, strictly follows the paradigms of GDPR. In our talk we provide a map of possible attacks on such systems and analyze how far they create real threats for the Apple-Google mechanism. Moreover, despite that security depends critically on a cryptographic random number generator implemented on the operating system level, we show that it is possible to make the system immune against backdoors installed by the provider of the hardware and the operating system. End-to-end security can be achieved by combining the ideas of a watchdog and subversion resilience techniques.

Keywords: exposure notification, contact tracking, privacy, CPRNG, verifiability