Proximity Tracing in an Ecosystem of Surveillance Capitalism

Joel Reardon, University of Calgary

Abstract:
Proximity tracing apps have been proposed as an aide in dealing with the COVID-19 crisis. Some of those apps leverage attenuation of Bluetooth beacons from mobile devices to build a record of proximate encounters between a pair of device owners. The underlying protocols are known to suffer from false positive and re-identification attacks.

We present evidence that the attacker's difficulty in mounting such attacks has been overestimated. Indeed, an attacker leveraging a moderately successful app or SDK with Bluetooth and location access can eavesdrop and interfere with these proximity tracing systems at no hardware cost and perform these attacks against users who do not have this app or SDK installed. We describe concrete examples of actors who would be in a good position to execute such attacks.

We further present a novel attack, which we call a biosurveillance attack, which allows the attacker to monitor the exposure risk of a smartphone user who installs their app or SDK but who does not use any contact tracing system and may falsely believe they have opted out of the system.

Through traffic auditing with an instrumented testbed, we characterize precisely the behaviour of one such SDK that we found in a handful of apps---but installed on more than one hundred million mobile devices. Its behaviour is functionally indistinguishable from a
re-identification or biosurveillance attack and capable of executing a false positive attack with minimal effort.

We also describe how the implementation of the system logged sensitive data to the system log, where they could be accessed by system and pre-installed apps. We show what data was logged and how this data can result in deanonymization and biosurveillance attacks on users of
such contact tracing systems.

Bio:
Joel Reardon is an Assistant Professor of Computer Science and Parex Innovations Fellow at the University of Calgary and has received the Casper Bowden Award for Outstanding Research in Privacy Enhancing Technologies. He is also a co-founder of Appcensus, Inc., which provides privacy analytics as a service in the mobile world. He studies systems security at all software layers, and has particular interest in mobile security and privacy, tools for privacy compliance, and secure storage.