Issued 2/7/18

Hackers Crack Smartphone Location Tracking – Even if You've Turned Off the GPS

Religiously turning off location services might not save you from having your phone tracked: a paper from a group of IEEE researchers demonstrates tracking when GPS and Wi-Fi are turned off. And, as a kicker: at least some of the data used in the attack, published this week on arXiv, can be collected without permission, because smartphone makers don't consider it sensitive. The researchers from Princeton University tracked smartmobes in an attack they dubbed PinMe, which combined data from the phone and non-phone sources to work out where the user is. In their paper, they explain that PinMe works with “non-sensory/sensory data stored on the smartphone” (the first category includes timezone and network status; the second includes air pressure and heading), and when that's combined with elevation maps, it's able to “estimate the user's location when all location services, eg GPS, are turned off.” The combination of data sources, the paper says, yielded user tracking “comparable to GPS” on their iPhone 6, iPhone 6S and Galaxy S4 i9500 test devices. The paper noted that while an attacker might try to sweep up such data using the well- trodden path of installing a malicious app (after all, user-snooping flashlight apps have been around for years [link]), there are also public sources of data: fitness apps such as Strava. Fitness apps "can, without arousing suspicion, collect and upload a significant amount of valuable non-sensory/sensory data, which can be post- processed to infer critical information about the user". In the PinMe attack, the researchers

found the app doesn't need the user's permission. Timezone, device IP address and network status don't need permission; nor do the accelerometer, magnetometer (which measures the angle between the phone's heading and north), or barometer. The public data PinMe uses includes OpenStreetMap, Google Maps' elevation data fetched through its API, OpenFlights (which maps 9,541 airports); they built a train heading database from Google Maps, and accessed public transport timetables (where possible, from their APIs). As an example of how all this translates to getting a user's location: the IP address can be geolocated to provide a guess at a city; barometer data tells you if the user arrived on an airplane; if the user's heading doesn't change much, they're on a train; travel by car can be correlated to street map data; and so on. In the cities in which the hackers ran their tests (Princeton, NJ, and Trenton, NJ and Philadelphia, PA), the correlation between heading changes and street maps yields a track that gets more accurate the further the trip – because the longer the drive, the fewer the possible paths the user might take. Likewise, you don't need a GPS to work out which airport someone flew into: takeoff and landing times are public, you can grab elevation from the phone, so the "planeTracker" component in PinMe "was able to accurately and uniquely return both departure and destination airports for all four flight routes" in the test.