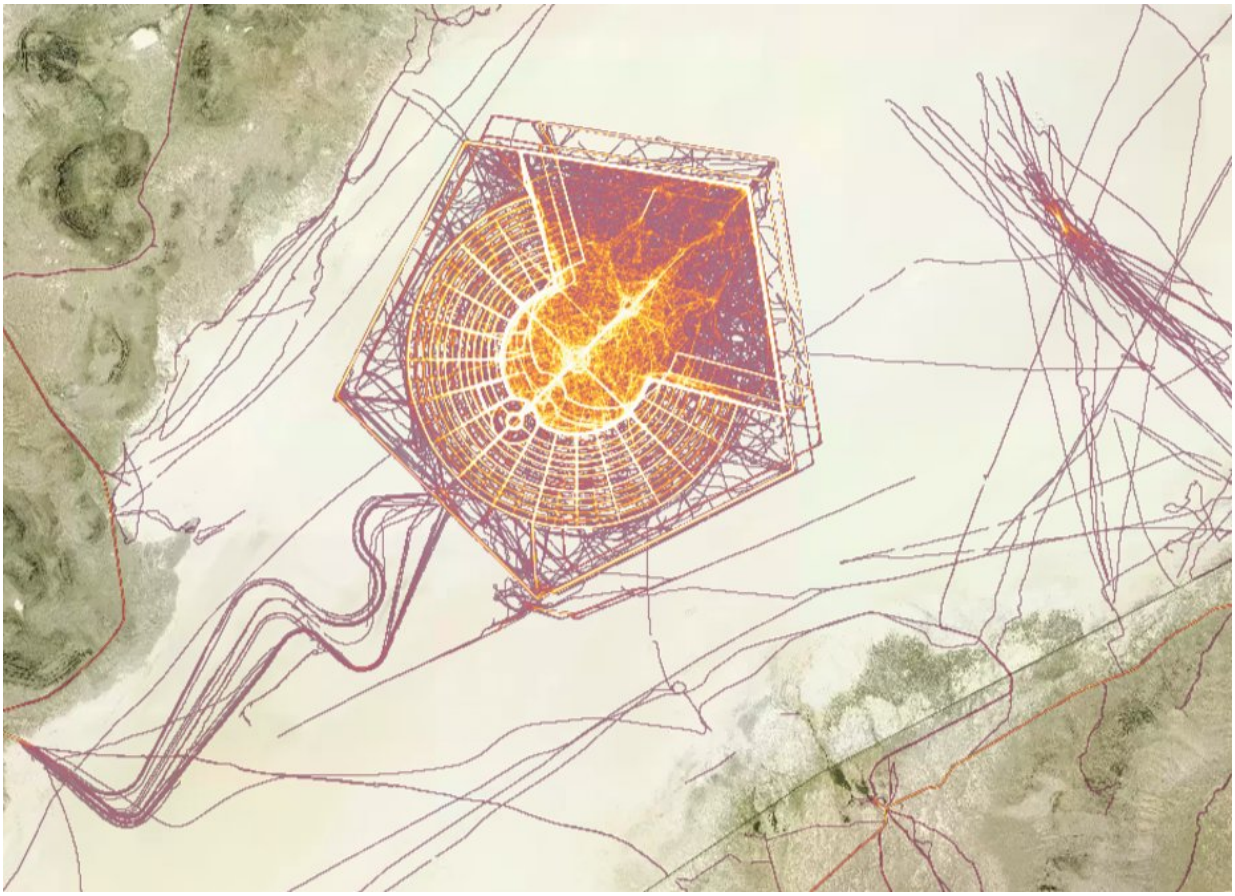
Your mobile phone can give away your location, even if you tell it not to

February 6 2018, by Guevara Noubir



Fitness trackers report their location and map the Burning Man festival in the Nevada desert. Screenshot of Strava Heat Map

U.S. military officials were recently caught off guard by revelations that

servicemembers' digital fitness trackers were storing the locations of their workouts – including at or near military bases and clandestine sites around the world. But this threat is not limited to Fitbits and similar devices. My group's recent research has shown how mobile phones can also track their users through stores and cities and around the world – even when users turn off their phones' location-tracking services.

The vulnerability comes from the wide range of sensors phones are equipped with – not just GPS and communications interfaces, but gyroscopes and accelerometers that can tell whether a phone is being held upright or on its side and can measure other movements too. Apps on the phone can use those sensors to perform tasks users aren't expecting – like following a user's movements turn by turn along city streets.

Most people expect that turning their phone's location services off disables this sort of mobile surveillance. But the research I conduct with my colleagues Sashank Narain, Triet Vo-Huu, Ken Block and Amirali Sanatinia at Northeastern University, in a field called "side-channel attacks," uncovers ways that apps can avoid or escape those restrictions. We have revealed how a phone can listen in on a user's finger-typing to discover a secret password – and how simply carrying a phone in your pocket can tell data companies where you are and where you're going.

Making assumptions about attacks

When designing protection for a device or a system, people make assumptions about what threats will occur. Cars, for instance, are designed to protect their occupants from crashes with other cars, buildings, guardrails, telephone poles and other objects commonly found in or near roads. They're not designed to keep people safe in cars driven off a cliff or smashed by huge rocks dropped on them. It's just not cost-effective to engineer defenses against those threats, because they're

assumed to be extremely uncommon.

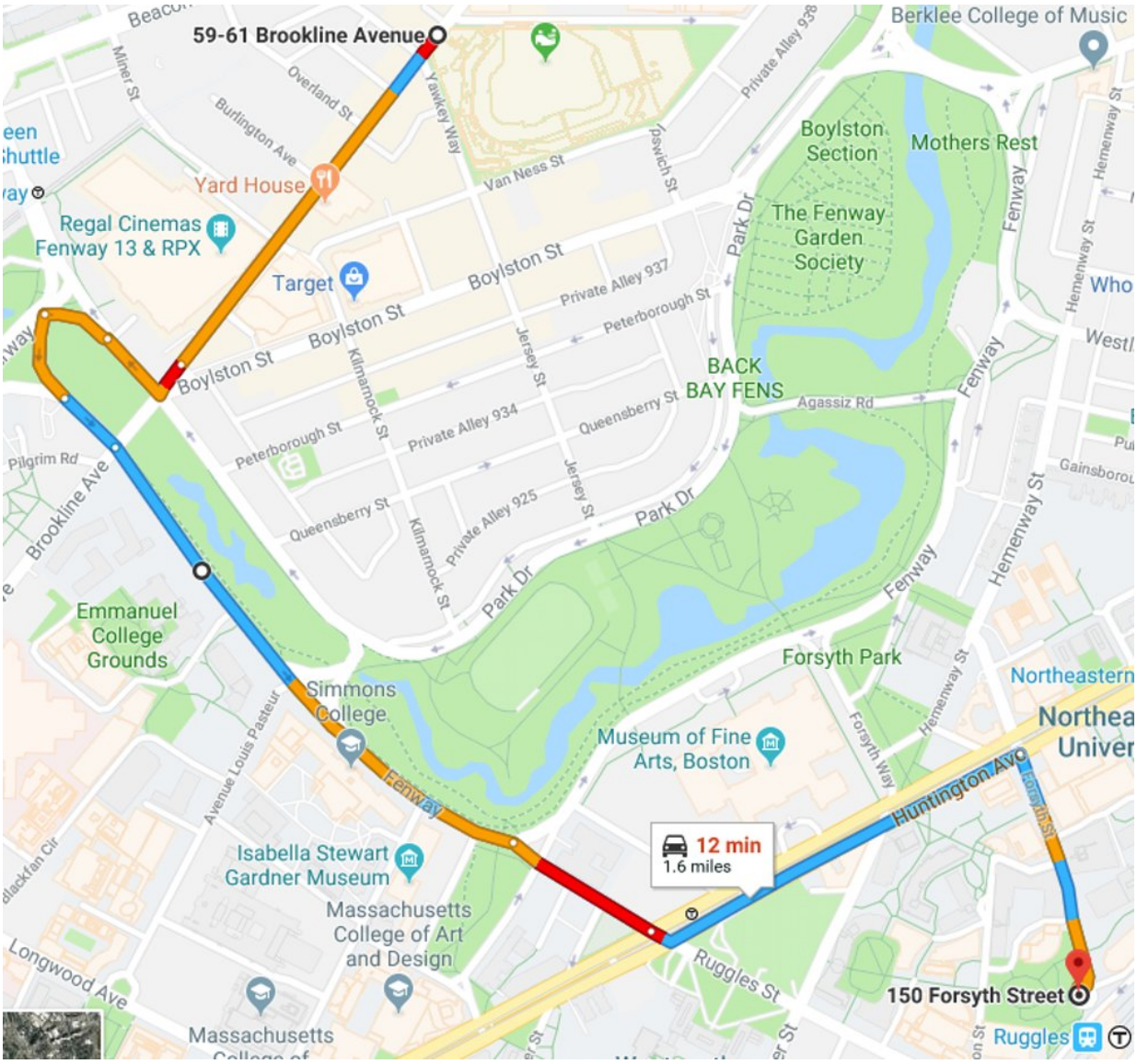
Similarly, people designing software and hardware make assumptions about what hackers might do. But that doesn't mean devices are safe. One of the first side-channel attacks was identified back in 1996 by cryptographer Paul Kocher, who showed he could break popular and supposedly secure cryptosystems by carefully timing how long it took a computer to decrypt an encrypted message. The cryptosystem designers hadn't imagined that an attacker would take that approach, so their system was vulnerable to it.

There have been many other attacks through the years using all sorts of different approaches. The recent Meltdown and Spectre vulnerabilities that exploit design flaws in computer processors, are also side-channel attacks. They enable malicious applications to snoop on other applications' data in the computer memory.

Monitoring on the go

Mobile devices are perfect targets for this sort of attack from an unexpected direction. They are stuffed with sensors, usually including at least one accelerometer, a gyroscope, a magnetometer, a barometer, up to four microphones, one or two cameras, a thermometer, a pedometer, a light sensor and a humidity sensor.

Apps can access most of these sensors without asking for permission from the user. And by combining readings from two or more devices, it's often possible to do things that users, phone designers and app creators alike may not expect.



Matching the route of a smartphone with a trip through Boston. Credit: Google Maps, CC BY-ND

In one recent project, we developed an app that could determine what letters a user was typing on a mobile phone's on-screen keyboard – without reading inputs from the keyboard. Rather, we combined information from the phone's gyroscope and its microphones.

When a user taps on the screen in different locations, the phone itself rotates slightly in ways that can be measured by the three-axis micromechanical gyroscopes found in most current phones. Further, tapping on a phone screen produces a sound that can be recorded on each of a phone's multiple microphones. A tap close to the center of the screen will not move the phone much, will reach both microphones at the same time, and will sound roughly the same to all the microphones. However, a tap at the bottom left edge of the screen will rotate the phone left and down; it will reach the left microphone faster; and it will sound louder to microphones near the bottom of the screen and quieter to microphones elsewhere on the device.

Processing the movement and sound data together let us determine what key a user pressed, and we were right over 90 percent of the time. This sort of function could be added secretly to any app and could run unnoticed by a user.

Identifying a location

We then wondered whether a malicious application could infer a user's whereabouts, including where they lived and worked, and what routes they traveled – information most people consider very private.

We wanted to find out whether a user's location could be identified using only sensors that don't require users' permission. The route taken by a driver, for instance, can be simplified into a series of turns, each in a certain direction and with a certain angle. With another app, we used a phone's compass to observe the person's direction of travel. That app also used the phone's gyroscope, measuring the sequence of turn angles of the route traveled by the user. And the accelerometer showed whether a user was stopped, or moving.

By measuring a sequence of turns, and stringing them together as a

person travels, we could make a map of their movements. (In our work, we knew which city we were tracking people through, but a similar approach could be used to figure out what city a person was in.)

Imagine we observe a person in Boston heading southwest, turning 100 degrees to the right, making a sharp U-turn to the left to head southeast, turning slightly to the right, continuing straight, then following a shallow curve to the left, a quick jog to the right, bumping up and down more than usual on a road, turning 55 degrees right, and turning 97 degrees left and then making a slight curve right before stopping.

We developed an algorithm to match those movements up against a digitized map of the streets of the city the user was in, and determined which were the most likely routes a person might take. Those movements could identify a route driving from Fenway Park, along the Back Bay Fens, past the Museum of Fine Arts and arriving at Northeastern University.

We were even able to refine our algorithm to incorporate information about curves in roads and speed limits to help narrow options. We produced our results as a list of possible paths ranked by how likely the algorithm thought they were to match the actual route. About half the time, in most cities we tried, the real path a user followed was in the top 10 items on the list. Further refining the map data, sensor readings and the matching algorithm could substantially improve our accuracy. Again, this type of capability could be added to any app by a malicious developer, letting innocent-appearing apps snoop on their users.

Our research group is continuing to investigate how side-channel attacks can be used to reveal a variety of private information. For instance, measuring how a phone moves when its owner is walking could suggest how old a person is, whether they are male (with the phone in a pocket) or female (typically with the phone in a purse), or even health

information about how steady a person is on his feet or how often she stumbles. We assume there is more your phone can tell a snoop – and we hope to find out what, and how, to protect against that sort of spying.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Your mobile phone can give away your location, even if you tell it not to (2018, February 6) retrieved 9 April 2024 from https://techxplore.com/news/2018-02-mobile.html