Rayhunter

At EFF we spend a lot of time thinking about Street Level Surveillance technologies—the technologies used by police and other authorities to spy on you while you are going about your everyday life—such as automated license plate readers, facial recognition, surveillance camera networks, and cell-site simulators (CSS). Rayhunter is a new open source tool we've created that runs off an affordable mobile hotspot that we hope empowers everyone, regardless of technical skill, to help search out CSS around the world.

CSS (also known as Stingrays or IMSI catchers) are devices that masquerade as legitimate cell-phone towers, tricking phones within a radius into connecting to the device instead of a tower.

CSS operate by conducting a general search of all cell phones within the device's radius. Law enforcement use CSS to pinpoint the location of phones often with greater accuracy than other techniques such as cell site location information (CSLI) and without needing to involve the phone company at all. CSS can also log International Mobile Subscriber Identifiers (IMSI numbers) unique to each SIM card, or hardware serial numbers (IMEIs) of all of the mobile devices within a given area. Some CSS may have advanced features allowing law enforcement to intercept communications in some circumstances.

What makes CSS especially interesting, as compared to other street level surveillance, is that so little is known about how commercial CSS work. We don't fully know what capabilities they have or what exploits in the phone network they take advantage of to ensnare and spy on our phones, though we have some ideas.

We also know very little about how cell-site simulators are deployed around the world. But we know that CSS are used by law enforcement, spies, and scammers. We want to find out if they are being used to violate human rights. Much of these gaps in our knowledge are due to a lack of solid, empirical evidence about the function and usage of these devices. Police departments are resistant to releasing logs of their use, even when they are kept. The companies that manufacture CSS are unwilling to divulge details of how they work.

EFF

Introducing Rayhunter

To fill these gaps in our knowledge, we have created an open source project called Rayhunter. It is developed to run on a variety of mobile hotspots. We have tried to make Rayhunter as easy as possible to install and use, regardless of your level of technical knowledge. We hope that activists, journalists, and others will run these devices all over the world and help us collect data about the usage and capabilities of cell-site simulators.

Rayhunter works by intercepting, storing, and analyzing the control traffic (but not user traffic, such as web requests) between the mobile hotspot Rayhunter runs on and the cell tower to which it's connected. Rayhunter analyzes the traffic in real-time and looks for suspicious events, which could include unusual requests like the base station (cell tower) trying to downgrade your connection to 2G, which is vulnerable to further attacks, or the base station requesting your IMSI under suspicious circumstances.

Rayhunter notifies the user when something suspicious happens and makes it easy to access those logs for further review, allowing users to take appropriate action to protect themselves, such as turning off their phone and advising other people in the area to do the same. The user can also download the logs (in PCAP format) to send to an expert for further review.

Installing Rayhunter is simple: After buying the necessary hardware, download the latest release package, unzip the file, plug the device into your computer, and run an install script.

We have a few goals with this project. An overarching goal is to determine conclusively if CSS are used to surveil free expression such as protests or religious gatherings, and if so, how often it's occurring. We'd like to collect empirical data (through network traffic captures, i.e. PCAPs) about what exploits CSS are using in the wild so the community of cellular security researchers can build better defenses. We also hope to get a clearer picture of the extent of CSS usage inside and outside of the U.S., especially in countries that do not have legally enshrined free speech protections. We already have hundreds of people using Rayhunter all over the world, but we want more. So far we have found some evidence of active CSS, but no evidence of such devices being used at protests in the U.S. But we want to know if this ever changes.

Once we have gathered this data, we hope we can help folks more accurately engage in threat modeling about the risks of cell-site simulators, and avoid the fear, uncertainty, and doubt that comes from a lack of knowledge. We hope that any data we do find will be useful to those who are fighting through legal process or legislative policy to rein in CSS usage where they live.

To find out more go to https://rayhunter.eff.org

Currently we are seeking partner organizations and individuals to help us run this project in the U.S. and around the world. In short, we want to collect more data, but especially from areas which are overpoliced or from communities subject to increased surveillance. You can start right now by getting a device, installing Rayhunter, and sending us info about any alerts you receive. If you want to get more involved or have questions reach out to info@eff.org !

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org