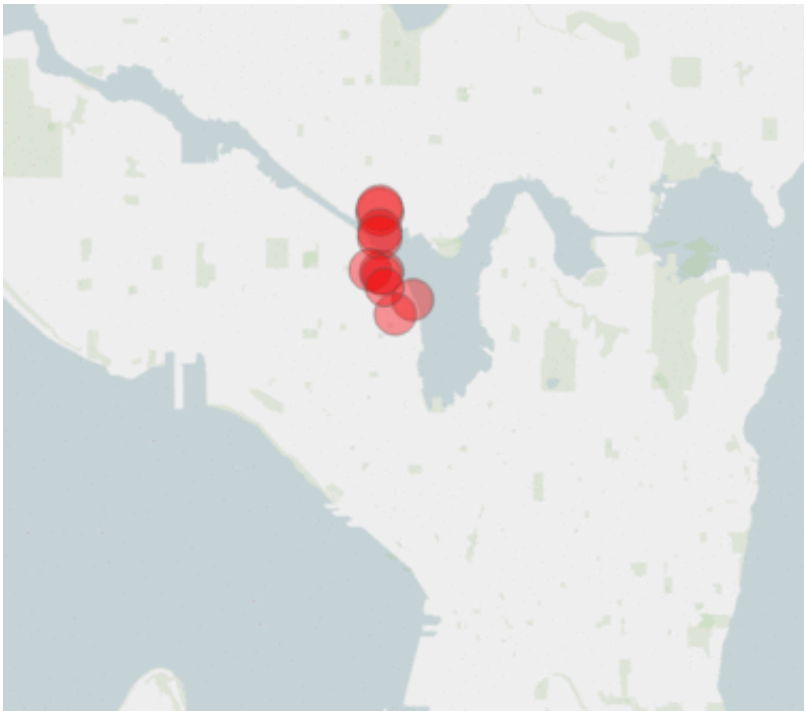
Catching the IMSI-catchers: SeaGlass brings transparency to cell phone surveillance

June 2 2017, by Jennifer Langston



SeaGlass helps detect cell phone surveillance by modeling a city's cellular landscape and identifying suspicious anomalies. This animation shows all measurements captured from a single cell tower near Seattle's Lake Union under "normal" conditions over two months, with stronger signals in red and weaker in blue. Credit: University of Washington

Modern cell phones are vulnerable to attacks from rogue cellular transmitters called IMSI-catchers—surveillance devices that can precisely locate mobile phones, eavesdrop on conversations or send

spam.

Recent leaks and public records requests have revealed that law enforcement in many U.S. cities have used the surveillance devices to locate suspects or hunt for illegal activity. But despite extensive public debate about their use and privacy implications, little is known about how comprehensively International Mobile Subscriber Identity- (IMSI) catchers—also known as cell-site simulators or Stingrays—are being used by governments, hackers or criminals in any given city.

University of Washington security researchers have developed a new system called SeaGlass to detect anomalies in the cellular landscape that can indicate where and when these surveillance devices are being used. The new system is described in a paper to be published in June 2017 in *Proceedings on Privacy Enhancing Technologies*.

"Up until now the use of IMSI-catchers around the world has been shrouded in mystery, and this lack of concrete information is a barrier to informed public discussion," said co-lead author Peter Ney, a doctoral student at the Allen School of Computer Science & Engineering at the UW. "Having additional, independent and credible sources of information on cell-site simulators is critical to understanding how—and how responsibly—they are being used."

During a two-month deployment in which SeaGlass sensors were installed in 15 ridesharing vehicles in Seattle and Milwaukee, researchers identified dozens of anomalies that were consistent with patterns one might expect from cell-site simulators.

University of Washington Security and Privacy Lab researchers Peter Ney (left) and Ian Smith (right) install a SeaGlass sensor in a test vehicle. Credit: Dennis Wise/University of Washington

However, researchers cautioned, without corroborating evidence from public records requests or other documentation about where cell-site simulators are being used—or suspicious activity seen over a longer period of time—they cannot definitively say the signals came from IMSI-catchers.

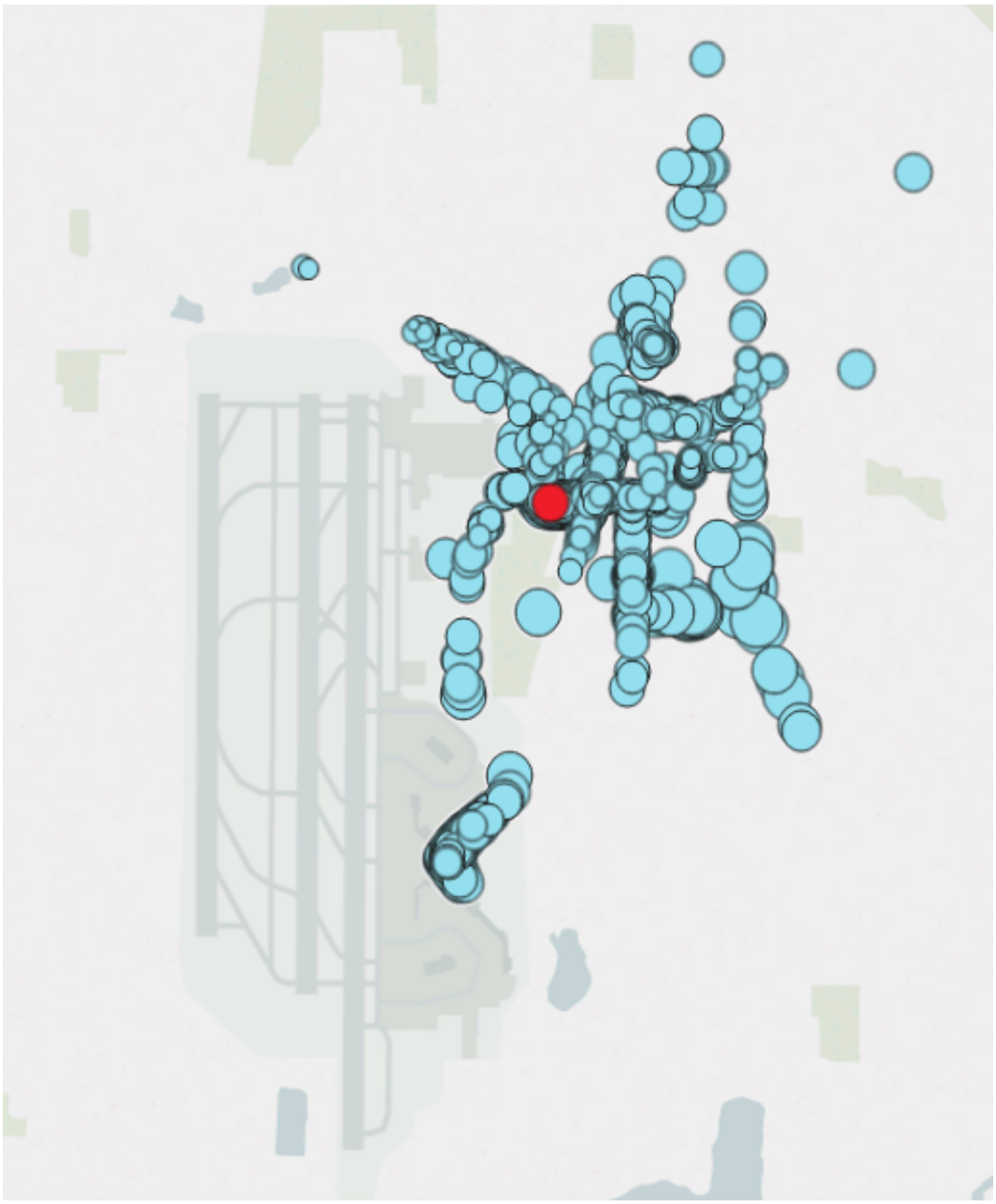
"In this space there's a lot of speculation, so we want to be careful about our conclusions. We did find weird and interesting patterns at certain locations that match what we would expect to see from a cell-site simulator, but that's as much as we can say from an initial pilot study," co-lead author Ian Smith, a former Allen School research scientist. "But we think that SeaGlass is a promising technology that—with wider deployment—can be used to help empower citizens and communities to monitor this type of surveillance."

Cell-site simulators work by pretending to be a legitimate cell tower that a phone would normally communicate with, and tricking the phone into sending back identifying information about its location and how it is communicating. The portable surveillance devices now range in size from a walkie-talkie to a suitcase, and in price from several thousand to hundreds of thousands of dollars.

Law enforcement teams in the U.S. have used the technology to locate people of interest, to find equipment used in the commission of crimes and even to collect massive amounts of cell phone data from airplanes.

Even less is known about how spies or cyber criminals are deploying them worldwide, especially as models become more affordable or able to be built in a hacker's garage.

To catch these IMSI-catchers in the act, SeaGlass uses sensors built from off-the-shelf parts that can be installed in vehicles—ideally ones that drive long hours and to many parts of a city, such as ridesharing vehicles or other fleets. The sensors pick up signals broadcast from the existing cell tower network, which remain fairly constant. Then SeaGlass aggregates that data over time to create a baseline map of "normal" cell tower behavior.



The researchers captured 2000 broadcasts (blue dots) from a cell tower near Sea-Tac airport, which consistently had the same properties. The red dot represents one highly unusual signal - with properties that would be unexpected anywhere in the city - that would be consistent with an IMSI-catcher "pretending" to be that cell tower. Credit: University of Washington

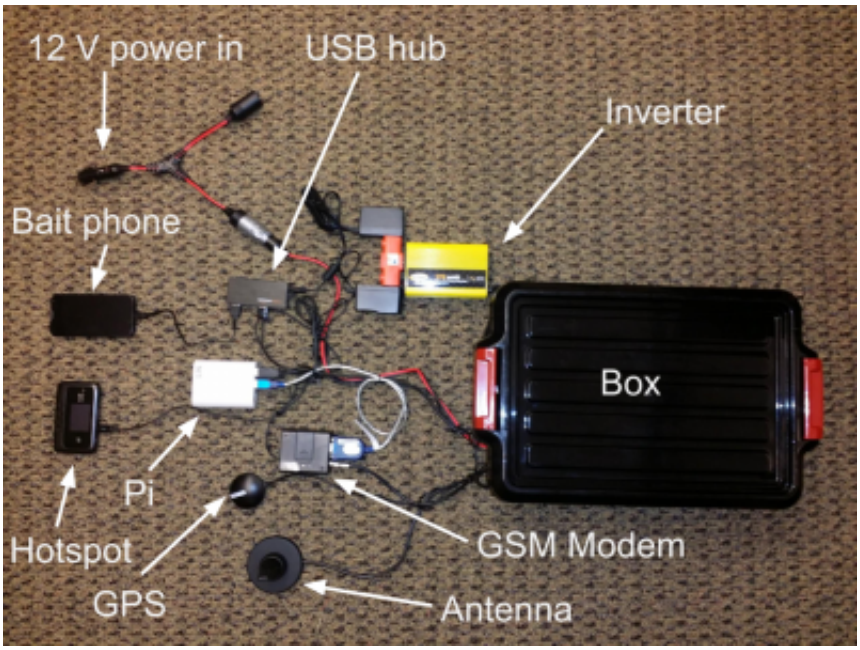
The team from the UW Security and Privacy Research Lab developed algorithms and other methods to detect irregularities in the cellular network that can expose the presence of a simulator. These include a strong signal in an odd spot or at an odd frequency that has never been there before, "temporary" towers that disappear after a short time and signal configurations that are different from what a carrier would normally transmit.

Allen School doctoral student and co-author Gabriel Cadamuro built statistical models to help find anomalies in the data. The team's survey approach differs from existing apps that attempt to detect attacks from a cell-site simulator on an individual's phone.

"We're looking at the whole cellular landscape and pinpointing discrepancies in data, while the apps for the most part are guessing at how a cell-site simulator would act with a phone," said Ney.

Co-author and Allen School professor Tadayoshi Kohno added, "We've demonstrated that SeaGlass is effective in detecting these irregularities and narrowing the universe of things people might want to investigate further."

For instance, around an immigration services building south of Seattle run by the U.S. Department of Homeland Security, SeaGlass detected a cell tower that transmitted on six different frequencies over the two-month period. That was notable because 96 percent of all other base cell towers broadcast on a single channel, and the other 4 percent only used two or three channels.



SeaGlass sensors are made with off-the-shelf parts that are packed into a box and installed in a vehicle's trunk, with antennas placed on or near windows. Credit: University of Washington

The team also detected an odd signal near the Seattle-Tacoma International airport with suspicious properties that were markedly different from those normally used by network providers.

Those patterns would make sense if a mimicking cell-site simulator were operating in those areas, the researchers said, but further investigation would be necessary to definitively reach that conclusion.

"This issue is bigger than one team of researchers," said Smith. "We're eager to push this out into the community and find partners who can crowdsource more data collection and begin to connect the dots in meaningful ways."