App allows inspectors to find gas pump skimmers faster

August 14 2019


SCANNING

An inspector holds up a phone equipped with Bluetana with a skimmer in the background. The two lines in red are the skimmer's Bluetooth signature. The indentifiers have been blurred on the screen and the skimmer so that criminals can not identify them. Credit: David Baillot/University of California San Diego

A team of computer scientists at UC San Diego and the University of Illinois has developed an app that allows state and federal inspectors to detect devices that steal consumer credit and debit card data at gas pumps. The devices, known as skimmers, use Bluetooth to transmit the data they steal.

"All criminals have to do is download the data from the comfort of their vehicle," said Nishant Bhaskar, a Ph.D. student in computer science at the University of California San Diego and the study's first author.

The app, called Bluetana, detects the Bluetooth signature of the skimmers, and allows inspectors to find the devices without needing to open up the gas pumps.

Bluetana was developed with technical input from the United States Secret Service and is only available to law enforcement officials and gas pump inspectors. It will not be available to the general public. It is now used by agencies in several states.

"Our goal is to give field agents the best tools for the job available today," said Kirill Levchenko, a computer science professor at the University of Illinois who earned his Ph.D. at the Jacobs School of Engineering at UC San Diego. "We've found that Bluetana helps agents find more gas stations with skimmers—and to find more skimmers at those gas stations."

The researchers found that, compared to similar apps currently available for smartphones, Bluetana is likely to discover more skimmers and results in a much lower false positive rate. "Bluetooth technology used in these skimmers are also used for legitimate products commonly seen at and near gas stations such as speed-limit signs, weather sensors and fleet tracking systems," said Bhaskar. "These products can be mistaken for skimmers by existing detection apps."

Bluetana uses an algorithm developed by the researchers to distinguish skimmers from legitimate Bluetooth devices. The researchers designed the algorithm based on the results of a field study during which the researchers analyzed scans of Bluetooth devices taken by officials at 1,185 gas stations in six U.S. states.

"Bluetana extracts more meaningful data from the Bluetooth protocol, such as signal strength, than existing skimmer detection applications. In a few cases, our app was able to find devices missed by visual inspection," said Maxwell Bland, a Ph.D. student in computer science at UC San Diego and study coauthor.

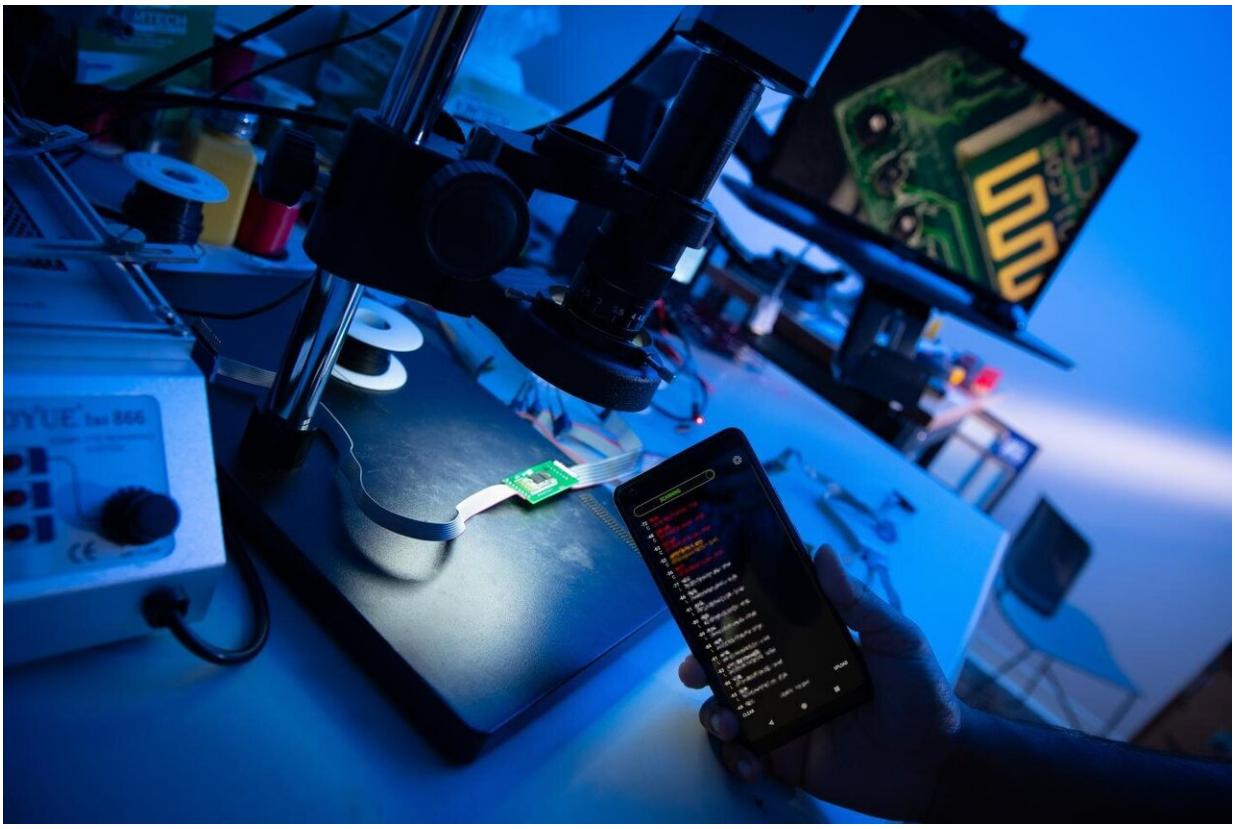
In one year of operation, Bluetana has led to the discovery of 42 Bluetooth-based skimmers across three U.S. states, all of which were recovered by law enforcement agents. "We were surprised that there were so many skimmers in the field that had not been discovered by other detection methods such as regular manual inspections," said Aaron Schulman, a UC San Diego assistant professor in computer science. "We even found two skimmers that were installed in gas pumps and had evaded detection for six months."

Researchers will present their work on Bluetana at the USENIX Security 2019 conference Aug. 14, 2019 in the San Francisco Bay Area.

What do skimmers do and how much are they worth

to criminals?

Skimmers have a high return on investment for criminals: skimmed debit card numbers can be used to withdraw cash and skimmed credit card numbers to make expensive purchases. A skimming device costs $20 or less to manufacture and can bring in more than $4,000 per day, depending on how many people use the gas pump and how the criminal converts the stolen numbers to cash.



A researcher holds up a phone equipped with the Bluetana app with a skimmer in the background. The red characters on the screen are Bluetooth signatures from skimmers. The identifiers are blurred so that criminals would not be able to read them. Credit: David Baillot/University of California San Diego

Criminals break into the pumps, many of which can be opened using a universal master key, to install the skimmers. Skimmers are connected to both the keypad and the magnetic stripe reader inside the gas pump. This allows the devices to collect not only customers' card numbers, but also their billing ZIP code and PIN, in the case of a debit card transaction.

It takes Bluetana, on average, three seconds to detect a skimmer. By contrast, law enforcement officials can take 30 minutes on average to find skimmers during manual inspections.

"UC San Diego is an important and active partner on our Southern California Electronic Crimes Task Force, and has been able to provide technological solutions to current investigative needs," said Special Agent in Charge James Anderson of the Secret Service. "Our office looks forward to presenting them with other investigative challenges."

Next steps

As more gas stations adopt payment systems exclusively for credit and debit cards with chips, criminals will use technologies to capture information from these types of cards. Researchers will have to follow suit. Visa and MasterCard are mandating that all gas stations in the United States use the chip-based systems by October 2020.

"Bluetana is not the last word," Levchenko said. "As criminals evolve, our techniques will need to evolve also."

Provided by University of California - San Diego