New smartphone vulnerability could allow hackers to track user location

July 28 2023

Hackers may use machine learning to exploit a text-messaging vulnerability, according to new research led by Northeastern Ph.D. student Evangelos Bitsikas. Credit: Alyssa Stone/Northeastern University

A newly discovered vulnerability in text messaging may enable attackers to trace your location, according to Northeastern Ph.D. student

Evangelos Bitsikas.

His research group exposed the flaw by applying a sophisticated machine-learning program to data gleaned from the relatively primitive SMS system that has driven texting in mobile phones since the early 1990s. His work can found on the pre-print server *arXiv*.

"Just by knowing the phone number of the user victim, and having normal network access, you can locate that victim," says Bitsikas, who will formally present his research at the 32nd USENIX Security Symposium in Anaheim, California. "Eventually this leads to tracking the user to different locations worldwide."

SMS security has improved marginally since its initial creation for 2g systems three decades ago, Bitsikas says. When a text is sent to you, your phone responds automatically with a notification to the sender—essentially a receipt of delivery.

Using Bitsikas' method, a hacker would send multiple text messages to your cellphone. The timing of your automated delivery replies would enable the hacker to triangulate your location—regardless of whether your communications are encrypted.

The timing of each automated delivery notification sent by your phone leaves a fingerprint of your location. Those fingerprints weren't a problem until Bitsikas' group used machine learning to develop an algorithm capable of detecting them.

"Once the machine-learning model is established, then the attacker is ready to send a few SMS messages," says Bitsikas, who is pursuing his Ph.D. in cybersecurity. "The results are fed into the machine-learning model, which will respond with the predicted location."

Bitsikas has found no evidence that the vulnerability—which so far has been leveraging Android operating systems—is currently being exploited.

"This does not mean that [hackers] aren't going to make use of it later on," Bitsikas says. "The procedure might be difficult to scale. The attacker will need to have Android devices in multiple locations sending messages every hour and calculating the responses. The collection itself can take days or weeks depending on how many fingerprints the attacker wants to collect.

"Not only are the collection and the analysis difficult, but then you have also the problem of sufficiently and appropriately configuring the machine-learning model, which is related to deep learning."

The concern, says Bitsikas, is that a deep-pocketed organization could exploit the flaw to locate government leaders, activists, CEOs and others who desire to keep their whereabouts private.

"We are researchers with limited resources and we are not experts in data science," Bitsikas says of his group. "What I'm afraid of is that advanced attackers—hacker groups, state-sponsored agencies, police, who of course have more resources—can achieve greater impact with this kind of attack."

Before publishing the research, Bitsikas shared it with GSMA, a global organization of more than 15,000 member experts that oversees the health and welfare of the mobile ecosystem.

"Our results and findings have been verified by GSMA," Bitsikas says. "They have acknowledged the results, saying that this is a difficult problem to solve considering also the cost and effort for deploying complete countermeasures."

Closing the vulnerability would require an overhaul of the global SMS system, Bitsikas says. He has been told that GSMA plans to add countermeasures that will make the hack more difficult to achieve—but won't close the window entirely.

"It's different from Microsoft or Apple creating a software patch to solve a security vulnerability," Bitsikas says. "These networks cannot be changed instantly everywhere."

Bitsikas is planning additional research that may build upon this breakthrough.

More information: Evangelos Bitsikas et al, Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings, *arXiv* (2023). DOI: 10.48550/arxiv.2306.07695

Provided by Northeastern University