New untraceable text-messaging system comes with statistical guarantees

December 7 2015, by Larry Hardesty

"Tor operates under the assumption that there's not a global adversary that's paying attention to every single link in the world," Nickolai Zeldovich says. "Maybe these days this is not as good of an assumption." Credit: MIT News

Anonymity networks, which sit on top of the public Internet, are

designed to conceal people's Web-browsing habits from prying eyes. The most popular of these, Tor, has been around for more than a decade and is used by millions of people every day.

Recent research, however, has shown that adversaries can infer a great deal about the sources of supposedly anonymous communications by monitoring data traffic though just a few well-chosen nodes in an anonymity network. At the Association for Computing Machinery Symposium on Operating Systems Principles in October, a team of MIT researchers presented a new, untraceable text-messaging system designed to thwart even the most powerful of adversaries.

The system provides a strong mathematical guarantee of user anonymity, while, according to experimental results, permitting the exchange of text messages once a minute or so.

"Tor operates under the assumption that there's not a global adversary that's paying attention to every single link in the world," says Nickolai Zeldovich, an associate professor of computer science and engineering, whose group developed the new system. "Maybe these days this is not as good of an assumption. Tor also assumes that no single bad guy controls a large number of nodes in their system. We're also now thinking, maybe there are people who can compromise half of your servers."

Because the system confuses adversaries by drowning telltale traffic patterns in spurious information, or "noise," its creators have dubbed it "Vuvuzela," after the noisemakers favored by soccer fans at the 2010 World Cup in South Africa.

Joining Zeldovich on the paper are joint first authors David Lazar, a PhD student in electrical engineering and computer science, and Jelle van den Hoof, who received his MIT PhD in the spring, and Matei Zaharia, an assistant professor of computer science and engineering and,

like Zeldovich, one of the co-leaders of the Parallel and Distributed Operating Systems group at MIT's Computer Science and Artificial Intelligence Laboratory.

Covering your tracks

Vuvuzela is a dead-drop system, in which one user leaves a message for another at a predefined location—in this case, a memory address on an Internet-connected server—and the other user retrieves it. But it adds several layers of obfuscation to cover the users' trails.

To illustrate how the system works, Lazar describes a simplified scenario in which it has only three users, named, by cryptographic convention, Alice, Bob, and Charlie. Alice and Bob wish to exchange text messages, but they don't want anyone to be able to infer that they've been in touch.

If Alice and Bob send messages to the dead-drop server, and Charlie doesn't, then an observer would conclude that Alice and Bob are communicating. So the system's first requirement is that all users send regular messages to the server, whether they contain any information or not.

If an adversary has infiltrated the server, however, he or she can see which users are accessing which memory addresses. If Charlie's message is routed to one address, but both Alice's and Bob's messages are routed to another, the adversary, again, knows who's been talking.

So instead of using a single server, Vuvuzela uses three. Corresponding to the three servers, every message sent through the system is wrapped in three layers of encryption. The first server peels off the first layer of encryption before passing messages on to the second server. But it also randomly permutes their order. So if, for example, Alice's message arrived at the first server before Bob's, and Bob's arrived before

Charlie's, the first server will pass them to the second in the order Bob, Alice, Charlie, or Charlie, Bob, Alice, or the like.

The second server peels off the second layer of encryption and permutes the message order yet again. Only the third server sees which messages are bound for which memory addresses. But even if it's been infiltrated, and even if the adversary observed the order in which the messages arrived at the first server, he or she can't tell whose message ended up where.

The adversary does, however, know that two users whose messages reached the first server within some window of time have been talking. And even that is more information than Vuvuzela's designers want to give away.

Here's where the noise comes in: When the first server passes on the messages it's received, it also manufactures a slew of dummy messages, with their own encrypted destinations. The second server does the same. So statistically, it's almost impossible for the adversary to determine even whether any of the messages arriving within the same time window ended up at the same destination.

Those statistical guarantees hold even if two of the three servers are infiltrated. As long as one of them remains uncompromised, the system works.

In recent years, one of the most interesting developments in cryptography has been the theory of differential privacy, which attempts to formalize intuitions about protecting the privacy of people whose data features in large, supposedly anonymized, data sets.

"The mechanism that [the MIT researchers] use for hiding communication patterns is a very insightful and interesting application of

differential privacy," says Michael Walfish, an associate professor of computer science at New York University. "Differential privacy is a very deep and sophisticated theory. The observation that you could use differential privacy to solve their problem, and the way they use it, is the coolest thing about the work. The result is a system that is not ready for deployment tomorrow but still, within this category of Tor-inspired academic systems, has the best results so far. It has major limitations, but it's exciting, and it opens the door to something potentially derived from it in the not-too-distant future."

More information: Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis. petsymposium.org/2015/papers/v … zela-hotpets2015.pdf

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology