Researchers mount successful attacks against Tor network—and show how to prevent them

July 29 2015, by Larry Hardesty

Credit: AI-generated image (disclaimer)

With 2.5 million daily users, the Tor network is the world's most popular system for protecting Internet users' anonymity. For more than a decade, people living under repressive regimes have used Tor to conceal their Web-browsing habits from electronic surveillance, and websites hosting content that's been deemed subversive have used it to hide the locations

of their servers.

Researchers at MIT and the Qatar Computing Research Institute (QCRI) have now demonstrated a vulnerability in Tor's design. At the Usenix Security Symposium this summer, they show that an adversary could infer a hidden server's location, or the source of the information reaching a given Tor user, by analyzing the traffic patterns of encrypted data passing through a single computer in the all-volunteer Tor network.

Fortunately, the same paper also proposes defenses, which representatives of the Tor project say they are evaluating for possible inclusion in future versions of the Tor software.

"Anonymity is considered a big part of freedom of speech now," says Albert Kwon, an MIT graduate student in electrical engineering and computer science and one of the paper's first authors. "The Internet Engineering Task Force is trying to develop a human-rights standard for the Internet, and as part of their definition of freedom of expression, they include anonymity. If you're fully anonymous, you can say what you want about an authoritarian government without facing persecution."

Layer upon layer

Sitting atop the ordinary Internet, the Tor network consists of Internet-connected computers on which users have installed the Tor software. If a Tor user wants to, say, anonymously view the front page of The New York Times, his or her computer will wrap a Web request in several layers of encryption and send it to another Tor-enabled computer, which is selected at random. That computer—known as the guard—will peel off the first layer of encryption and forward the request to another randomly selected computer in the network. That computer peels off the next layer of encryption, and so on.

The last computer in the chain, called the exit, peels off the final layer of encryption, exposing the request's true destination: the Times. The guard knows the Internet address of the sender, and the exit knows the Internet address of the destination site, but no computer in the chain knows both. This routing scheme, with its successive layers of encryption, is known as onion routing, and it gives the network its name: "Tor" is an acronym for "the onion router."

In addition to anonymous Internet browsing, however, Tor also offers what it calls hidden services. A hidden service protects the anonymity of not just the browser, but the destination site, too. Say, for instance, that someone in Iran wishes to host a site archiving news reports from Western media but doesn't want it on the public Internet. Using the Tor software, the host's computer identifies Tor routers that it will use as "introduction points" for anyone wishing to access its content. It broadcasts the addresses of those introduction points to the network, without revealing its own location.

If another Tor user wants to browse the hidden site, both his or her computer and the host's computer build Tor-secured links to the introduction point, creating what the Tor project calls a "circuit." Using the circuit, the browser and host identify yet another router in the Tor network, known as a rendezvous point, and build a second circuit through it. The location of the rendezvous point, unlike that of the introduction point, is kept private.

Traffic fingerprinting

Kwon devised an attack on this system with joint first author Mashael AlSabah, an assistant professor of computer science at Qatar University, a researcher at QCRI, and, this year, a visiting scientist at MIT; Srini Devadas, the Edwin Sibley Webster Professor in MIT's Department of Electrical Engineering and Computer Science; David Lazar, another

graduate student in electrical engineering and computer science; and QCRI's Marc Dacier.

The researchers' attack requires that the adversary's computer serve as the guard on a Tor circuit. Since guards are selected at random, if an adversary connects enough computers to the Tor network, the odds are high that, at least on some occasions, one or another of them would be well-positioned to snoop.

During the establishment of a circuit, computers on the Tor network have to pass a lot of data back and forth. The researchers showed that simply by looking for patterns in the number of packets passing in each direction through a guard, machine-learning algorithms could, with 99 percent accuracy, determine whether the circuit was an ordinary Web-browsing circuit, an introduction-point circuit, or a rendezvous-point circuit. Breaking Tor's encryption wasn't necessary.

Furthermore, by using a Tor-enabled computer to connect to a range of different hidden services, they showed that a similar analysis of traffic patterns could identify those services with 88 percent accuracy. That means that an adversary who lucked into the position of guard for a computer hosting a hidden service, could, with 88 percent certainty, identify it as the service's host.

Similarly, a spy who lucked into the position of guard for a user could, with 88 percent accuracy, tell which sites the user was accessing.

To defend against this type of attack, "We recommend that they mask the sequences so that all the sequences look the same," AlSabah says. "You send dummy packets to make all five types of circuits look similar."

"For a while, we've been aware that circuit fingerprinting is a big issue

for hidden services," says David Goulet, a developer with the Tor project. "This paper showed that it's possible to do it passively—but it still requires an attacker to have a foot in the network and to gather data for a certain period of time."

"We are considering their countermeasures as a potential improvement to the hidden service," he adds. "But I think we need more concrete proof that it definitely fixes the issue."

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