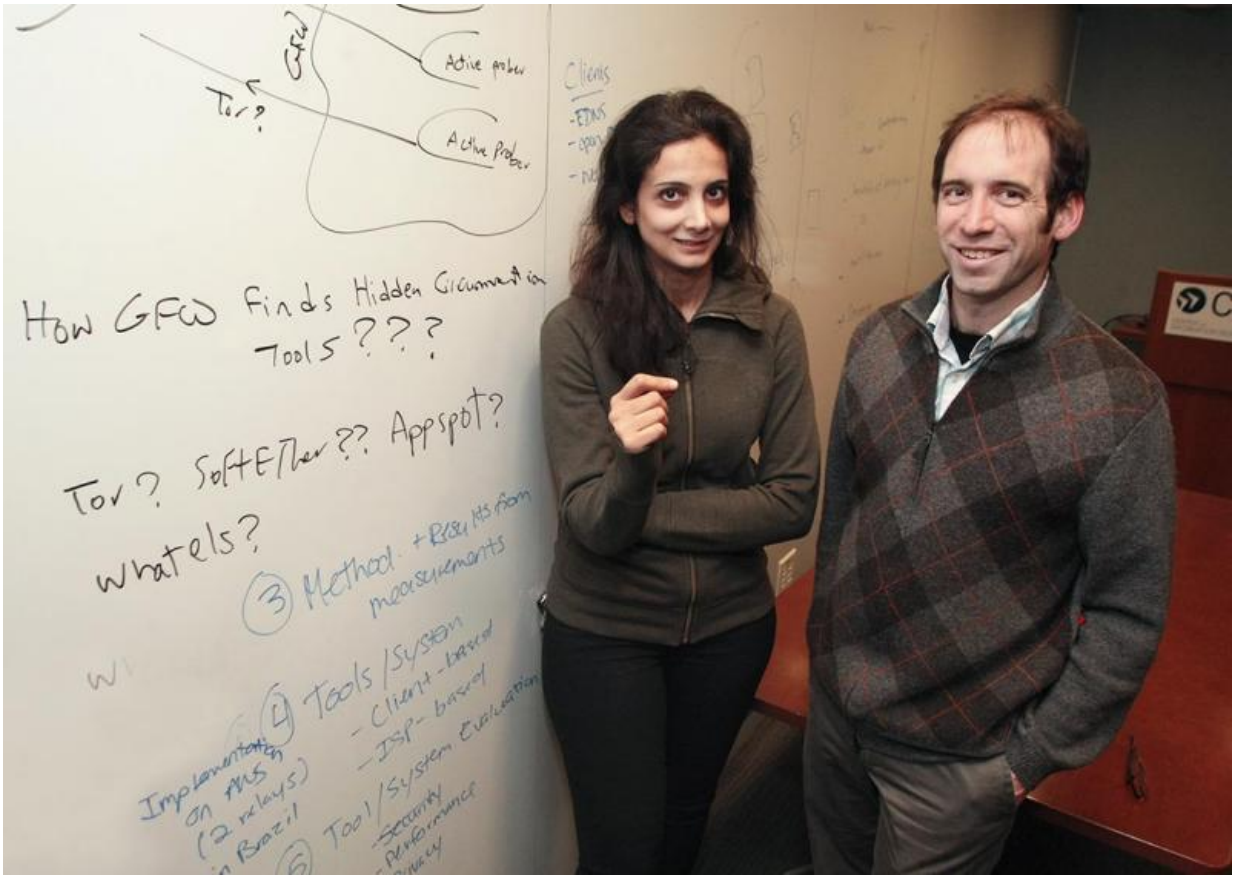
Researchers discover new steps in the escalating cat-and-mouse game of internet censorship

April 19 2016, by John Sullivan



From left, Princeton researchers Roya Ensafi, a postdoctoral researcher in computer science, and Nick Feamster, a professor of computer science, are investigating methods that the Chinese government uses to control computer communications entering China from the rest of the world. Credit: Office of Engineering Communications

Researchers have found that the "Great Firewall" technology that controls internet traffic entering and leaving China is not merely an apparatus that statically blocks traffic. It also actively sends probes to other machines that are connected to the internet, preemptively searching for internet infrastructure and services that seek to circumvent its defenses.

"The Great Firewall is actively trying to find these sites so it can block them," said Nick Feamster, a professor of computer science at Princeton and the acting director of the University's Center for Information and Technology Policy. "Active reconnaissance is the next step in the arms race."

In contrast to the decentralized management that characterizes much of the internet, China's internet is tightly controlled: traffic entering and leaving the country passes through infrastructure in just a few physical locations.

"It allows the Chinese government to see most traffic between China and the rest of the world," said Roya Ensafi, a postdoctoral researcher in computer science at Princeton who worked on the project.

In a paper presented at the Association for Computing Machinery's SIGCOMM Internet Measurement Conference in Tokyo on Oct. 30, the researchers demonstrated how the Great Firewall identifies and blocks traffic. As a first step, Ensafi said, the system searches for keywords and terms in a message: something like "Falun Gong" might cause the Great Firewall to block subsequent communication, for example.

To circumvent these controls, citizens often use software that obfuscates the communications, such as the Tor network. This system sends traffic

through a sequence of network nodes called relays in between the sender and receiver. At each relay, traffic is re-encrypted, ensuring that no node in the network can link the sender to the receiver. The encryption itself also provides a level of confidentiality.

The Great Firewall can typically determine that certain traffic is being sent with Tor, even if it cannot determine the content of the communications. "Tor traffic is encrypted as it crosses the Great Firewall," Ensafi said. "The government can't read the traffic, but they can fingerprint it."

Network operators in China do not want to block all internet connections, but they do want to prevent users from accessing any service that helps them circumvent the Great Firewall, the researchers said. When the firewall determines that traffic might involve Tor usage, they typically need to take extra steps to confirm that the traffic pertains to Tor before blocking the communication.

"Incorrectly blocking traffic that appears to be Tor traffic but is not can cause collateral damage, and they [network operators] cannot afford to block everything," Ensafi said. "To increase the confidence in what they are blocking, they began actively probing machines that appear to be running Tor infrastructure."

Ensafi said that the Great Firewall infrastructure checks machines that it deems might be entry nodes in the Tor network. Because Tor has a distinct "handshake" when clients attempt to connect to an entry node, the Great Firewall can discover entry nodes to the Tor network simply by probing suspected entry nodes and determining that they conform to the expected handshake.

"If they guess it is Tor, they try to make a connection to establish whether it is using the Tor protocol," Ensafi said. "If it is, they block

traffic coming from that connection."

Keith Winstein, an assistant professor of computer science at Stanford University who was not involved in the research, said the paper carefully measured the probing techniques used by the Great Firewall.

"It really shows a level of sophistication of the Chinese system that I don't think was publicly appreciated before," said Winstein, who also has an appointment at the Stanford Law School. "It is hard to think of a more important topic for security research than the cat-and-mouse game between the authors of communications tools and governments who want to monitor and police communications on the internet."

The researchers said it is not possible for systems like Tor to completely prevent the Great Firewall from probing the Tor network because the firewall continually changes the locations from which it sends its active probes.

One way to avoid blocking is to deploy circumvention systems like Tor across a set of machines distributed across the Internet, known as a Content Delivery Network (CDN). These delivery networks tend to host content for a large number of internet websites and services. Therefore, firewall administrators would not be able to simply block access to the network locations hosting the Tor entry nodes without also blocking access to other content, thus inflicting significant "collateral damage."

The researchers said Tor has begun to take this approach and is also trying to make its communications more difficult to detect in general.

"In response to the Great Firewall's active probing, Tor developers are developing new techniques to obfuscate the handshakes between the client and Tor entry nodes," Ensafi said. "These obfuscation techniques work by encapsulating the initial handshake inside other 'innocuous'

protocols to make it more difficult to identify the initial handshake."

The ongoing efforts to obfuscate Tor traffic has led to a cat-and-mouse game, as Tor tries to disguise its traffic, and Chinese network operators continue to develop techniques to detect it.

"It is an ongoing battle," Ensafi said.

Provided by Princeton University

Citation: Researchers discover new steps in the escalating cat-and-mouse game of internet censorship (2016, April 19) retrieved 5 May 2024 from https://phys.org/news/2016-04-escalating-cat-and-mouse-game-internet-censorship.html