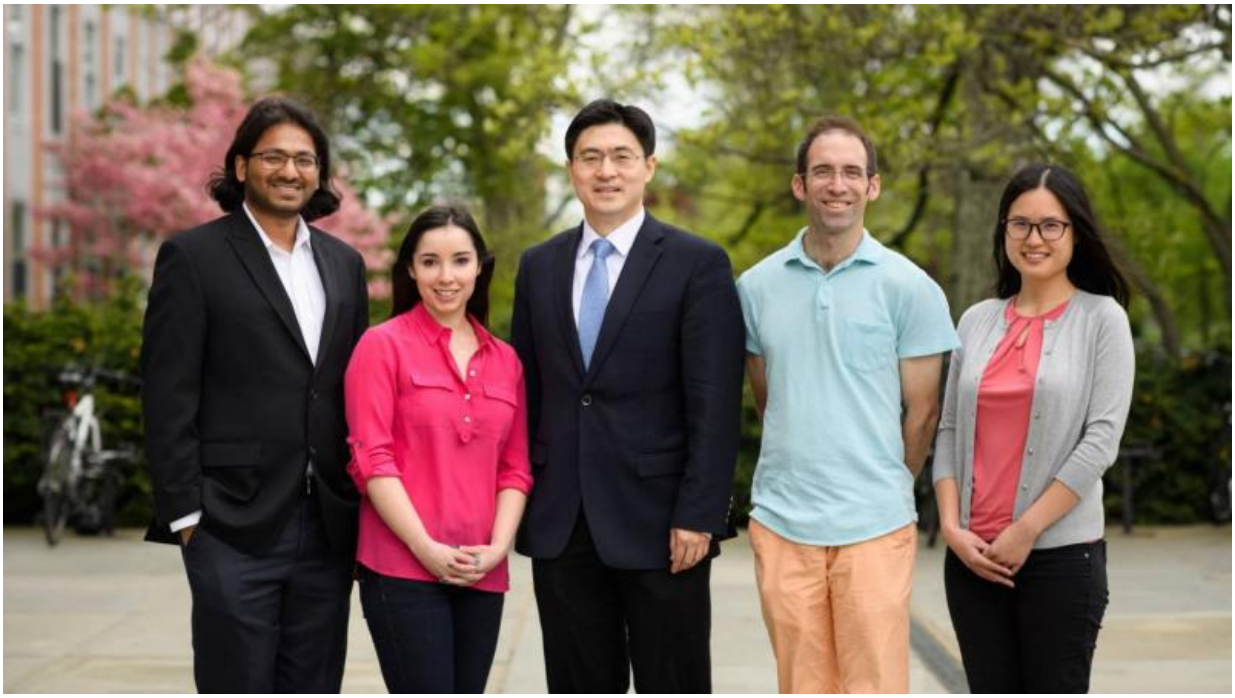
Research identifies methods to protect against online privacy attacks

June 2 2017, by Josephine Wolff



A team of Princeton researchers has developed a method to detect and defend against attacks on the Tor system, which provides anonymity to internet users. Team members include, from left, Prateek Mittal, an assistant professor of electrical engineering; Anne Edmundson, a graduate student in computer science; Mung Chiang, the Arthur LeGrand Doty Professor of Electrical Engineering; Nick Feamster, a professor of computer science and deputy director of the Center for Information Technology Policy; and Yixin Sun, a graduate student in computer science. Credit: Sameer A. Khan/Fotobuddy

When Congress voted in March to reverse rules intended to protect Internet users' privacy, many people began looking for ways to keep their online activity private. One of the most popular and effective is Tor, a software system millions of people use to protect their anonymity online.

But even Tor has weaknesses, and in a new paper, researchers at Princeton University recommend steps to combat certain types of Tor's vulnerabilities.

Tor was designed in the early 2000s to make it more difficult to trace what people are doing online by routing their traffic through a series of "proxy" servers before it reaches its final destination. This makes it difficult to track Tor users because their connections to a particular server first pass through intermediate Tor servers called relays. But while Tor can be a powerful tool to help protect users' privacy and anonymity online, it is not perfect.

In earlier work, a research group led by Prateek Mittal, an assistant professor of electrical engineering, identified different ways that the Tor network can be compromised, as well as ways to make Tor more resilient to those types of attacks. Many of their latest findings on how to mitigate Tor vulnerabilities are detailed in a paper titled "Counter-RAPTOR: Safeguarding Tor Against Active Routing Attacks," presented at the IEEE Symposium on Security and Privacy in San Jose, California, in May.

The paper is written by Mittal, Ph.D. students Yixin Sun and Anne Edmundson, and Nick Feamster, professor of computer science, and Mung Chiang, the Arthur LeGrand Doty Professor of Electrical Engineering. Support for the project was provided in part by the National Science Foundation, the Open Technology Fund and the U.S. Defense Department.

The research builds on earlier work done by some of the authors identifying a method of attacking Tor called "RAPTOR" (short for Routing Attacks on Privacy in TOR). In that work, Mittal and his collaborators demonstrated methods under which adversaries could use attacks at the network level to identify Tor users.

"As the internet gets bigger and more dynamic, more organizations have the ability to observe users' traffic,′ said Sun, a graduate student in computer science. "We wanted to understand possible ways that these organizations could identify users and to provide Tor with ways to defend itself against these attacks as a way to help preserve online privacy."

Mittal said the vulnerability emerges from the fact that there are big companies that control large parts of the internet and forward traffic through their systems. "The idea was, if there's a network like AT&T or Verizon that can see user traffic coming into and coming out of the Tor network, then they can do statistical analysis on whose traffic it is," Mittal explained. "We started to think about the potential threats that were posed by these entities and the new attacks—the RAPTOR attacks—that these entities could use to gain visibility into Tor."

Even though a Tor user's traffic is routed through proxy servers, every user's traffic patterns are distinctive, in terms of the size and sequence of data packets they're sending online. So if an internet service provider sees similar-looking traffic streams enter the Tor network and leaving the Tor network after being routed through proxy servers, the provider may be able to piece together the user's identity. And internet service providers are often able to manipulate how traffic on the internet is routed, so they can observe particular streams of traffic, making Tor more vulnerable to this kind of attack.

These types of attacks are important because there is a lot of interest in

being able to break the anonymity Tor provides. "There is a slide from an NSA (the U.S. National Security Agency) presentation that Edward Snowden leaked that outlines their attempts at breaking the privacy of the Tor network," Mittal pointed out. "The NSA wasn't successful, but it shows that they tried. And that was the starting point for this project because when we looked at those documents we thought, with these types of capabilities, surely they can do better."

In their latest paper, the researchers recommend steps that Tor can take to better protect its users from RAPTOR-type attacks. First, they provide a way to measure internet service providers' susceptibility to these attacks. (This depends on the structure of the providers' networks.) The researchers then use those measurements to develop an algorithm that selects how a Tor user's traffic will be routed through proxy servers depending on the servers' vulnerability to attack. Currently, Tor proxy servers are randomly selected, though some attention is given to making sure that no servers are overloaded with traffic. In their paper, the researchers propose a way to select Tor proxy servers that takes into consideration vulnerability to outside attack. When the researchers implemented this algorithm, they found that it reduced the risk of a successful network-level attack by 36 percent.

The researchers also built a network-monitoring system to check network traffic to uncover manipulation that could indicate attacks on Tor. When they simulated such attacks themselves, the researchers found that their system was able to identify the attacks with very low false positive rates.

Roger Dingledine, president and research director of the Tor Project, expressed interest in implementing the network monitoring approach for Tor. "We could use that right now," he said, adding that implementing the proposed changes to how proxy servers are selected might be more complicated.

"Research along these lines is extremely valuable for making sure Tor can keep real users safe," Dingledine said. "Our best chance at keeping Tor safe is for researchers and developers all around the world to team up and all work in the open to build on each other's progress."

Mittal and his collaborators also hope that their findings about potential vulnerabilities will ultimately serve to strengthen Tor's security.

"Tor is amongst the best tools for anonymous communications," Mittal said. "Making Tor more robust directly serves to strengthen individual liberty and freedom of expression in online communications."

More information: Counter-RAPTOR: Safeguarding Tor Against Active Routing Attacks: www.princeton.edu/~pmittal/pub … /counter-raptor-sp17

Provided by Princeton University