UNIVERSITY OF MARYLAND

COLLEGE OF
COMPUTER, MATHEMATICAL,
& NATURAL SCIENCES

INFORMATION FOR...

SUPPORT CMNS

News & Events

SHARE

New Internet Routing Method Allows Users to Avoid Sending Data Through Undesired Geographic Regions

Censorship is one of the greatest threats to open communication on the Internet. Information may be censored by a user's country of residence or the information's desired destination. But recent studies show that censorship by countries through which the data travels along its route is also a danger.

Now, computer scientists at the University of Maryland have developed a method for providing concrete proof to Internet users that their information did not cross through certain geographic areas. The new system offers advantages over existing systems: it is immediately deployable and does not require knowledge of—or modifications to—the Internet's routing hardware or policies.

"With recent events, such as censorship of Internet traffic, suspicious 'boomerang routing' where data leaves a region only to come back again, and monitoring of users' data, we became increasingly interested in this notion of empowering users to have more control over what happens with their data," says project lead Dave Levin, an assistant research scientist in the University of Maryland Institute for Advanced Computer Studies (UMIACS).

This new system, called Alibi Routing, will be presented on August 20, 2015, at the Association for Computing Machinery Special Interest Group on Data Communication (ACM SIGCOMM) conference in London. Levin teamed with associate professor Neil Spring and professor Bobby Bhattacharjee, who have appointments in UMD's Department of Computer Science and UMIACS, on the paper.

Information transmitted over the Internet, such as website requests or email content, is broken into packets and sent through a series of routers on the way to its destination. However, users have very little control over what parts of the world these packets traverse.

Some parts of the world have been known to modify data returned to users, thus censoring content. In 2012, researchers demonstrated that Domain Name System (DNS) queries that merely pass through China's borders are subject to the same risk as if the requests came from one of the country's own residents.

To evaluate their Alibi Routing method, the researchers simulated a network with 20,000 participants and selected forbidden regions from the 2012 "Enemies of the Internet" report published by Reporters Without Borders—China, Syria, North Korea and Saudi Arabia—as well as the three other countries with the highest number of Internet users at the time of the study—the United States, China and Japan.

Alibi Routing works by searching a peer-to-peer network to locate "peers"—other users running the alibi routing software—that can relay a user's packets to its ultimate destination while avoiding specified forbidden regions. The peer is called an "alibi." The alibi provides proof—calculations that exploit the fact that information cannot travel faster than the speed of light—that at a particular time, a packet was at a specific geographic location sufficiently far enough away from the forbidden areas that the data could not have entered them.

If successful, users receive proof that their information reached its desired destination and that it did not traverse the forbidden regions. Alternatively, the response could indicate that the packets may have traversed forbidden areas.

Levin says the success rate for Alibi Routing depends on a few things, including how close the source and destination are to the forbidden region and how central the forbidden region is to Internet routing.

"There's also a safety parameter that we use. Basically, it's a way for users to select a desired level of confidence that the packet absolutely does not traverse the forbidden region," Levin says. "The larger the safety parameter, the harder it is to find an alibi. The smaller the safety parameter, the easier it is to find an alibi."

Based on simulated deployments, the system successfully found an alibi more than 85 percent of the time. With a small safety parameter, the success rate rose to 95 percent. The results suggest that users can typically avoid the part of the world they wish to route around, according to Levin.

Users do not always need an alibi, though. If two users are in the same room in Maryland and they want their information to avoid China, they don't need an alibi to help them; they can just send the data directly to one another and measure the time it takes to do so.

"For some of the countries we tested, we only needed an alibi about one-third of the time" says Levin.

The team plans to release a version of Alibi Routing—likely as an Internet browser plug-in—for users to test by the end of 2015.

"The more participants this type of peer-to-peer system has in different geographical locations, the more useful it will be," says Levin.

In addition to Levin, Spring and Bhattacharjee, additional authors on the paper include current computer science graduate student Youndo Lee and current electrical engineering graduate student Zhihao Li; and former students Luke Valenta (B.S. '14, computer science and mathematics), Victoria Lai (B.S. '14, computer science; B.A. '14, economics) and Cristian Lumezanu (M.S. '06, Ph.D. '09, computer science).

This research was supported by the National Science Foundation (Award No. IIS-0964541), the Office of Naval Research (Award No. N00173-13-1-G001) and an Amazon Web Services in Education grant. The content of this article does not necessarily reflect the views of these organizations.

The conference paper, "Alibi Routing," Dave Levin, Youndo Lee, Luke Valenta, Zhihao Li, Victoria Lai, Cristian Lumezanu, Neil Spring, Bobby Bhattacharjee, was presented August 20, 2015 at ACM SIGCOMM in London.

Media Relations Contact: Abby Robinson, 301-405-5845, abbyr@umd.edu; Melissa Brachfeld, 301-405-9711, melbrach@umiacs.umd.edu

Writer: Melissa Brachfeld

University of Maryland
College of Computer, Mathematical, and Natural Sciences
2300 Symons Hall
College Park, MD 20742
www.cmns.umd.edu
@UMDscience

About the College of Computer, Mathematical, and Natural Sciences
The College of Computer, Mathematical, and Natural Sciences at the University of Maryland educates more than 7,000 future scientific leaders in its undergraduate and graduate programs each year. The college's 10 departments and more than a dozen interdisciplinary research centers foster scientific discovery with annual sponsored research funding exceeding $150 million.

Date: Tuesday, August 18, 2015

Contact Us   Careers & Recruiting   Odyssey Magazine   CMNS Photo Library   UMD Home
UMD Directory   Web Accessibility

STAY CONNECTED:

The College of Computer,
Mathematical, and Natural Sciences
2300 Symons Hall, University of Maryland
College Park, MD 20742
p 301.405.2080 • f 301.314.9949