New anti-censorship scheme could make it impossible to block individual sites

August 10 2011

A radical new approach to thwarting Internet censorship would essentially turn the whole web into a proxy server, making it virtually impossible for a censoring government to block individual sites.

The system is called Telex, and it is the brainchild of computer science researchers at the University of Michigan and the University of Waterloo in Canada. They will present it Aug. 12 at the USENIX Security Symposium in San Francisco.

"This has the potential to shift the arms race regarding censorship to be in favor of free and open communication," said J. Alex Halderman, assistant professor of computer science and engineering at U-M and one of Telex's developers.

"The Internet has the ability to catalyze change by empowering people through information and communication services. Repressive governments have responded by aggressively filtering it. If we can find ways to keep those channels open, we can give more people the ability to take part in free speech and access to information."

Today's typical anticensorship schemes get users around site blocks by routing them through an outside server called a proxy. But the censor can monitor the content of traffic on the whole network, and eventually finds and blocks the proxy, too.

"It creates a kind of cat and mouse game," said Halderman, who was at the blackboard explaining this to his computer and network security class when it hit him that there might be a different approach---a bigger way to think about the problem.

Here's how Telex would work:

Users install Telex software. Halderman envisions they could download it from an intermittently available website or borrow a copy from a friend.

Internet Service Providers (ISPs) outside the censoring nation deploy equipment called Telex stations.

When a user wants to visit a blacklisted site, he or she would establish a secure connection to an HTTPS website, which could be any password-protected site that isn't blocked. This is a decoy connection. The Telex software marks the connection as a Telex request by inserting a secret-coded tag into the page headers. The tag utilizes a cryptographic technique called "public-key steganography."

"Steganography is hiding the fact that you're sending a message at all," Halderman said. "We're able to hide it in the cryptographic protocol so that you can't even tell that the message is there."

The user's request passes through routers at various ISPs, some of which would be Telex stations. These stations would hold a private key that lets them recognize tagged connections from Telex clients. The stations would divert the connections so that the user could get to any site on the Internet.

Under this system, large segments of the Internet would need to be involved through participating ISPs.

"It would likely require support from nations that are friendly to the cause of a free and open Internet," Halderman said. "The problem with any one company doing this, for example, is they become a target. It's a collective action problem. You want to do it on a wide scale that makes connecting to the Internet almost an all or nothing proposition for the repressive state."

The researchers are at the proof-of-concept stage. They've developed software for researchers to experiment with. They've put up one Telex station on a mock ISP in their lab. They've been using it for their daily web browsing for the past four months and have tested it with a client in Beijing who was able to stream YouTube videos even though the site is blocked there.

More information: The paper to be presented at USENIX Security is called "Telex: Anticensorship in the Network Infrastructure." Full text is at telex.cc/paper.html

Provided by University of Michigan

Citation: New anti-censorship scheme could make it impossible to block individual sites (2011, August 10) retrieved 23 April 2024 from https://phys.org/news/2011-08-anti-censorship-scheme-impossible-block-individual.html