

Watching the watchers: Researchers Study National Efforts to Censor Traffic on the Internet

April 29 2010

(PhysOrg.com) -- Assistant Professor of Computer Science Jed Crandall and Ph.D. student Jong Chun Park are preparing to go to Genoa, Italy this summer to present their latest findings on Internet Censorship to the 30th International Conference on Distributed Computing Systems.

Their latest paper titled, “Empirical Study of a National-Scale Distributed Intrusion Detection System: Backbone-Level Filtering of HTML Responses in China,” outlines their investigation of the way the Chinese government has tried to censor information via the internet.

An increasing number of nations are trying to shield at least some elements of the internet from their citizens. In a Washington Post story Google’s chief legal office says more than 40 governments censor information today. The company reports on its blog that [Google](#) products are blocked at least partially in about 25 countries. Countries have a long list of reasons for censorship. Some try to block child pornography, some try to block hate speech. Some try to block sensitive political information. But Crandall says it’s very difficult for countries to completely block anything.

The paper that Crandall and Park will present details their monitoring of Chinese government efforts to filter HTML responses, a technique the Chinese censors abandoned between August 2008 and January 2009. Crandall and Park could see that it wasn’t working well, and guess that

Chinese censors arrived at the same conclusion. The paper details the technical problems of backbone level HTML response filtering and offers a look at the way the Chinese government tried to censor specific items of information.

Soon after the time that their study indicates the [Chinese government](#) gave up on HTML response filtering in the backbone, the censors made another attempt at content filtering called Green Dam. That project required software to be installed on individual computers, and faltered when computer manufacturers refused to install the software. Now the Chinese are looking at a technique they are calling Blue Shield.

Crandall says, “Blue Shield is more local network filtering. When they were trying to filter on the backbone they would just see packets fly by. They would try to reset connections whenever something happened but they were not really seeing the whole state of the connection.”

Blue Shield requires a major strategy change. Censors can no longer monitor information at the centralized backbone.

“Every little network has to implement Blue Shield,” Crandall says. “It’s not something they can just throw up in a few places on the backbone and monitor.” While the Chinese put Blue Shield into place, Crandall and Park will be looking at another kind of censorship. They are interested in what happens when the country decides to simply block a website.

Crandall compares that to traffic in Albuquerque, which has two interstate highways passing through it.

“You’ve got I-25 north and south, and I-40 east and west, and so if you wanted to block certain kinds of cars from entering Albuquerque you might block in those four places, but there’s still little back roads people

might use to get in and out of Albuquerque, and that's the question that interests us."

He and Park want to know whether complete blockage of web sites is always successful. "Do they try to block at the borders or do they block on the major pathways and how pervasive is the blocking?"

More information: Research paper:
www.cs.unm.edu/~crandall/icdcs2010.pdf

Provided by University of New Mexico

Citation: Watching the watchers: Researchers Study National Efforts to Censor Traffic on the Internet (2010, April 29) retrieved 27 April 2024 from <https://phys.org/news/2010-04-watchers-national-efforts-censor-traffic.html>

| |
|--|
| <p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p> |
|--|