Protection for whistleblowers: Computer science professor working on system that would allow for secret data transfer

June 20 2013

Volker Roth, a professor of computer science at Freie Universität Berlin, is working in a project called AdLeaks to create a system that would make it possible for an individual to submit data over the Internet while remaining unobserved.

The AdLeaks system is currently being checked and tested as part of the EU CONFINE project. A first version of the source code is available as download for interested persons. Unobserved data transfer is relevant, for example, for so-called whistleblowers, persons with inside information who inform the public about corporate or official corruption. Examples of whistleblowers are Mark Klein, and more recently Edward Snowden, who revealed the extent to which the U.S. National Security Agency (NSA) monitors the Internet.

The current discussion focuses heavily on the PRISM program that, as recently became publicly known, allows the NSA to access user data stored by Google, Apple, Microsoft, and other companies. What is often forgotten is that the NSA also accesses data directly from the glass fiber connections over which a great deal of the communication in the Internet takes place. This includes the contents of the affected communication, as well as the call data showing who communicated with whom and when.

"You have to admire the civil courage of Edward Snowden, who sacrifices his future for his democratic convictions, when he reports

abuse," says Professor Volker Roth. Not all whistleblowers dare to step out in public, which is often associated with stigma, loss of employment, or [criminal prosecution]... "Even whistleblowers who wish to remain anonymous, take risks when they pass information through the Internet because the information collected by the NSA allows the organization to trace connection data calls made once or [Internet connections] far into the past." Encryption would not change anything in that regard. It is better to use anonymizing services such as Tor that route the connections through several computers and disguise their origin.. The New Yorker magazine advises potential whistleblowers to do just that and report anonymous information to its own strongbox service.

Whether this step is sufficient for an organization such as the NSA remains unclear. "Just using Tor might make one appear suspicious," says Volker Roth. The Tor network also tries to establish a low latency of connections, which may enable a traffic analysis, whereby a wiretap measures when users send data and when data reach their goal. Sufficient commonality makes it possible to assign connections to individuals. "If both user and server are based in the U.S., the NSA might be able to perform such traffic analysis," according to Roth.

It was this risk via traffic analysis that led him, along with a group of students, to seek another solution. In cooperation with [computer science] professor Sven Dietrich from the Stevens Institute of Technology in New Jersey, they are developing a system that, even with full surveillance of the Internet, permits data transmission that cannot be easily traced.

The so-called AdLeaks system robs the connection data of their significance.. It utilizes small programs, with which most websites are designed to be dynamic and interactive. Embedded in popular websites, this type of program automatically encrypts and transmits empty messages to the AdLeaks server, whenever such a website is viewed.

Whistleblowers can use a modified browser that encrypts confidential messages instead of empty messages. An observer monitoring the Internet cannot distinguish between the two. He/she cannot draw any meaning from the connection data because all Internet users transmit the same type of data, and no intention can be presumed. The necessary software is distributed in a similar manner to all users, without having to be downloaded.

Provided by Freie Universitaet Berlin