Researchers uncover privacy flaws that can reveal users' identities, locations and digital files

21 October 2011

A team of researchers, including Keith Ross (pictured), the Leonard J. Shustek Professor of Computer Science at NYU-Poly, has uncovered privacy risks connected to using Skype.

(PhysOrg.com) -- Researchers at Polytechnic Institute of New York University (NYU-Poly) and colleagues in France and Germany will soon notify Internet scholars of flaws in Skype and other Internet-based phone systems that could potentially disclose the identities, locations and even digital files of the hundreds of millions of users of these systems.

Their paper, "I Know Where You are and What You are Sharing," will be presented during the Internet Measurement Conference 2011 in Berlin on November 2, 2011. The authors are Chao Zhang and Keith Ross of NYU-Poly; Stevens Le Blond of the Max Planck Institute for Software Systems (MPI-SWS), Germany; and Arnaud Legout and Walid Dabbous of the French research institute I.N.R.I.A Sophia Antipolis.

Ross, the Leonard J. Shustek Professor of Computer Science at NYU-Poly, explained that the team uncovered several properties of Skype that can track not only users' locations over time but also their peer-to-peer (P2P) file-sharing activity.

Even when a user blocks callers or connects from behind a Network Address Translation (NAT) - a common type of firewall - it does not prevent the privacy risk, he said. The research also revealed that marketers can easily link to information such as name, age, address, profession and employer from social media sites such as Facebook and LinkedIn in order to inexpensively build profiles on a single tracked target or a database of hundreds of thousands.

"These findings have real security implications for the hundreds of millions of people around the world who use VoIP or P2P file-sharing services," said Ross. "A hacker anywhere in the world could easily track the whereabouts and file-sharing habits of a Skype user - from private citizens to celebrities and politicians - and use the information for purposes of stalking, blackmail or fraud." Ross explained that these privacy weaknesses are fairly easy to exploit, and that a sophisticated high school-age hacker would likely be capable of executing similar attacks.

The team first observed that with VoIP (Voice and Video over IP) systems, when Alice establishes a call with Bob, Bob reveals his IP address to Alice. Alice can then use commercial geo-IP mapping services to determine Bob's location and Internet Service Provider (ISP).

The team also found that Alice can initiate a Skype call, block some packets and quickly terminate the call to obtain Bob's IP address without alerting Bob with ringing or pop-up windows. Alice can make this attack even when Bob is not on her contact list or even when Bob explicitly configures Skype to block calls from non-contacts. By repeating the process on, say, an hourly basis, Alice can track the locations and movements of any Skype user over weeks or months, without the user having any idea that he is being tracked.

To demonstrate the potential severity of these security vulnerabilities, the researchers tracked the Skype accounts of about 20 volunteers as well as 10,000 random users over a two-week period, using techniques that neither harmed nor disrupted the service, utilized any requests for which the service was not designed nor interfered with users. All data were anonymized for user safety. Skype and Microsoft Corp. were informed of the researchers' findings.

The researchers used commercial geo-location mapping services and found that they could construct a detailed account of a user's daily activities even if the user had not turned on Skype for 72 hours. In one example, they accurately tracked one volunteer researcher from his visit at a New York university to a vacation in Chicago, a return to a New York university, lodging in Brooklyn, then to his home in France. "If we had followed the mobility of the Facebook friends of this user as well, we likely would have determined who he was visiting and when," the authors said.

They calculated it would cost a marketer who wanted to create a database only $500 per week to track 10,000 users - and perhaps less, since they did not delve deeply into optimization.

In another experiment, they queried the 50,000 most popular downloads on BitTorrent, a popular P2P file-sharing system. Because it enables sharing of large files, it is a favorite of digital pirates. When a common IP address was found on both Skype and BitTorrent, the researchers were able to determine the files that identified individuals downloaded or shared. They noted that the same information could be obtained from other P2P applications, such as eMule or Xunlei.

A fairly straightforward and inexpensive fix would prevent hackers from taking the critical first step in this security breach - that of obtaining users' IP addresses through inconspicuous calling. The researchers say that redesigning the Skype protocol so that a user's IP address is never revealed unless the call is accepted would offer substantially greater privacy.

Skype claims it has more than a half-billion registered users and a monthly average of 170 million active ones who use its application for phoning, texting, instant messaging and video conferencing. By one report, one in five overseas calls is made via Skype. One study found BitTorrent may account for a quarter to more than a half of all Internet traffic.

While Skype was the only service tested in this study, the researchers claim that some of the security issues are fundamental to all real-time P2P communication systems, and that the proposed defenses may offer guidelines for enhancing privacy of other popular applications.

Provided by New York University

APA citation: Researchers uncover privacy flaws that can reveal users' identities, locations and digital files (2011, October 21) retrieved 17 September 2021 from https://phys.org/news/2011-10-uncover-privacy-flaws-reveal-users.html

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.