Math student detects OAuth, OpenID security vulnerability

3 May 2014, by Nancy Owano

(Phys.org) —To get right to the point, a doctoral candidate in math has discovered two holes in OAuth and OpenID that could leak data and redirect victims to unsafe sites. Friday's tech sites accordingly were buzzing with news of the discovery about a vulnerability in OAuth and OpenID protocols. Be cautious, said the reports, of links that ask you to log in through well known sites such as Facebook and Google. The OAuth 2.0 and OpenID login tools are "used by many websites and tech titans" including Google, Facebook, and Microsoft, among others," said Aloysius Low, writer at CNET Asia and Seth Rosenblatt, who covers Google and security for CNET News.

Chris Brook noted in *Threatpost*, the Kaspersky Lab Security News Service, that openID and OAuth are commonly used authorization protocols, separate but complementary. (Both are open specification in the realm of authentication and access control.) "OAuth issues access tokens to clients by a server, similarly OpenID acts as a decentralized method to allows users to use the same digital identity across the Internet. They are perhaps best known as the easiest way for users to log-in to sites using passwords from providers like Google or Twitter without having to worry about the main site's credentials from being used."

The person who made the discovery is Wang Jing, a PhD student in mathematics at the Nanyang Technological University in Singapore. He announced that OAuth 2.0 and OpenID have a "serious Covert Redirect vulnerability. It could lead to Open Redirect Attacks to both clients and providers of OAuth 2.0 or OpenID. For OAuth 2.0, these attacks might jeopardize 'the token' of the site users, which could be used to access user information."

As for OpenID, Wang said that "the attackers may get user's information directly. Compounded by the large number of companies involved, this vulnerability could lead to huge consequences if left unresolved." Wang said he reported the vulnerability to related companies.

(Jill Scharr, writing in *Tom's Guide*, pointed out that "Normal phishing attempts can be easy to spot, because the malicious page's URL will usually be off by a couple of letters from that of the real site. The difference with Covert Redirect is that an attacker could use the real website instead by corrupting the site with a malicious login popup dialogue box.")

Addressing this issue, James Barrese, CTO, PayPal, said on Friday that customers were not impacted. "We have carefully investigated this situation and can tell you that this vulnerability has no impact on PayPal and your PayPal accounts remain secure."

He said when hearing that "security researchers recently discovered a flaw in open source login tools OAuth 2.0 and OpenID (which are widely used by many websites and web services, including some offered by PayPal) we moved quickly to determine the impact to our customers." Barrese noted that "When PayPal implemented OAuth2.0/OpenID, we engineered additional security measures to protect our merchants and customers."

CNET advised that "Users who wish to avoid any potential loss of data should be careful about clicking links that immediately ask you to log in to Facebook or Google. Closing the tab immediately should prevent any redirection attacks."

APA citation: Math student detects OAuth, OpenID security vulnerability (2014, May 3) retrieved 1 July 2022 from https://techxplore.com/news/2014-05-math-student-oauth-openid-vulnerability.html