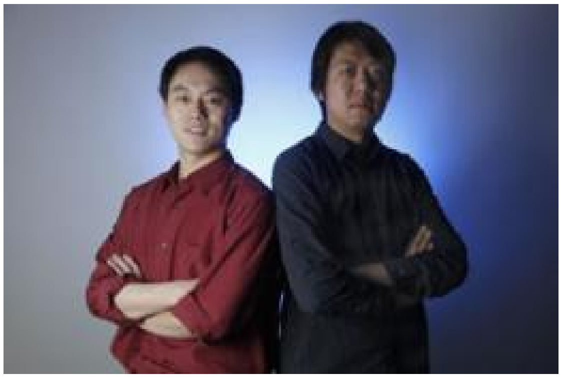
Informatics students discover, alert Facebook to threat allowing access to private data, bogus messaging

February 3 2011



IU Bloomington School of Informatics and Computing PhD students Rui Wang, left, and Zhou Li discovered and reported the privacy vulnerability to Facebook last month.

(PhysOrg.com) -- A Facebook security vulnerability discovered by a pair of doctoral students at Indiana University Bloomington's School of Informatics and Computing that allowed malicious websites to uncover a visitor's real name, access their private data and post bogus content on their behalf has been repaired, Facebook has confirmed.

The vulnerability discovered by Rui Wang and Zhou Li enabled malicious websites to impersonate legitimate websites, and then obtain the same data access permissions on Facebook that those legitimate websites had received.

Wang and Li said the vulnerability occurred when a user informed Facebook of his or her willingness to share information with popular websites like ESPN.com or YouTube. Whenever a website makes such a request to Facebook via the user's browser, Facebook passes a secret random string called an authentication token back to the requestor for identification. Whoever holds that authentication token can convince Facebook that they are, say, ESPN.com and then gain unfettered access to the shared data.

Facebook confirmed the discovery and in a statement said the problem was repaired and that the belief was that no sites had been compromised.

"Researchers at Indiana University reported a vulnerability in our Platform code to us, and we worked quickly with them to resolve it. It was fixed shortly after it was reported. We're not aware of any cases in which it was used maliciously," the statement said. "We thank the researchers at Indiana University for bringing this to our attention, and for demonstrating the value of responsible disclosure."

The researchers identified a flaw in the way the token was transmitted using two Flash objects: one inside Facebook's iframe passes the token to the second, which in this case would be embedded at ESPN.com. The transfer mode can be selected through "transport='flash'" with the security guarantee being that both flash objects are supposed to come from the same domain (i.e., Facebook) before they can talk.

The researchers found, however, that such a same-domain assumption is not always valid because Adobe Flash allows cross-domain communication with an unpredictable domain name that is prepended by an underscore symbol in the connection name. This allows an attacker website to steal an authentication token by choosing the transport='flash,' replacing the receiver flash with its own and then initiating a cross-domain communication with the flash inside the Facebook-controlled iframe to get the token and send it to the attacker's flash.

"This vulnerability has several implications," Wang said. "Basically, any user with a valid Facebook session loses anonymity and privacy to any website, even one with embarrassing or sensitive content."

Facebook allows some websites like bing.com to directly access a user's public data without explicit consent. This enables the malicious website impersonating that site to do the same. Moreover, if the user has ever granted any website, such as The New York Times, YouTube, Farmville or ESPN, the permission to connect to their Facebook account, further damage can be inflicted, including disclosure of private data that the user does not want to share with others, and impersonation of the user to post bogus news or comments on friends' walls. This form of propagation resembles the famous MySpace worm released in 2005, they said.

The researchers created a video demonstration of how the Facebook bug worked:

"Our attack utilized a feature of Adobe Flash called unpredictable communication, and an important distinction between an unpredictable communication and a normal communication is that the former is done through a connection where the name starts with an underscore symbol," Li said. "Therefore, Facebook could check for this symbol to determine if a potentially malicious website tries to do unpredictable communication."

And that is exactly what Facebook started to do once they were alerted to the problem by Wang and Li, who were working under the supervision of School of Informatics and Computing Associate Professor XiaoFeng Wang and Shuo Chen, a researcher in Microsoft

Research's Internet Services Research Center.

XiaoFeng Wang, the students' adviser, said Facebook relies on same-domain communications that allow websites to specify Adobe Flash as the communication mechanism.

"In a normal situation, two flash objects can only do same-domain communications, and, in fact, security of Facebook's authentication crucially depends on same-domain restrictions," he explained. "However, Facebook allowed the Adobe Flash communication mechanism but did not disallow the unpredictable domain names. This is how a malicious website could establish a channel to enable two flash objects in different domains to communicate."

To portray the seriousness of the vulnerability, the team made a video demo that can be viewed here.

Facebook officials noted that a contact form at both the Facebook Help Center and from the "Whitehats" tab on the Facebook Security Page are available in the rare instances in which vulnerabilities are found.

"We also recently rewrote our responsible disclosure policy to make it even easier for researchers to let us know when they find a vulnerability, so we can fix it quickly and before it's exploited. Our new policy was praised by the Electronic Frontier Foundation in a recent blog post here," the statement said.

Provided by Indiana University

Citation: Informatics students discover, alert Facebook to threat allowing access to private data, bogus messaging (2011, February 3) retrieved 9 April 2024 from
https://phys.org/news/2011-02-informatics-students-facebook-threat-access.html