Cracks emerge in the cloud

20 June 2014

A systematic analysis reveals that cloud storage services have security weaknesses that can inadvertently leak users' data.

As individual computer users increasingly access the Internet from different smartphones, tablets and laptops, many are choosing to use online cloud services to store and synchronize their digital content. Cloud storage allows consumers to retrieve their data from any location using any device and can provide critical backups in the case of hard disk failure. But while people are usually vigilant about enacting security measures on personal computers, they often neglect to consider how safe their files are in the cloud.

Now, findings from a team led by Jianying Zhou of the A*STAR Institute for Infocomm Research in Singapore promise to improve the security of popular online services and better protect users by revealing hidden flaws associated with an important cloud storage feature—the ability to share files with friends, co-workers or the public.

Sharing content is an attractive way to let far-flung colleagues view and collaborate on projects without using email attachments, which often have strict file size limitations. Data sharing can be: public, with no access controls; private, in which the cloud service provider authenticates sharing through login controls; or 'secret' uniform resource locator (URL) sharing where people without an account on the cloud service can access data by following a specific web link.

The A*STAR-led researchers analyzed the security of three well-known cloud service providers—Dropbox, Google Drive and Microsoft SkyDrive—and found that all three had vulnerabilities many users might encounter. They uncovered several risks related to the sharing of secret URLs. Because URLs are saved in various network-based servers, browser histories and Internet bookmarks, frequent opportunities exist for third parties to access private data. Furthermore, the URL recipient may send the link to others without the data owner's consent.

Another danger lies in the practice of URL shortening—reducing long web addresses to brief alphanumeric sequences for easier sharing on mobile devices. Although the original URL may point to a privately shared file, shortening changes this address into plain text unprotected by encryption. Zhou also notes that because short URLs have very limited lengths, they are susceptible to brute-force attacks that can dig out supposedly secret files.

Zhou explains that the root cause of cloud security problems lies in the need to balance usability with privacy protection. "Users should be careful when they share files in the cloud because no system is perfectly secure. The cloud industry, meanwhile, needs to constantly raise the bar against new attacks while keeping the service as functional as possible."

More information: Chu, C.-K., Zhu, W.-T., Han, J., Liu, J. K., Xu, J. & Zhou, J. "Security concerns in popular cloud storage services." *IEEE Pervasive Computing* 12, 50–57 (2013). DOI: 10.1109/MPRV.2013.72

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

APA citation: Cracks emerge in the cloud (2014, June 20) retrieved 4 March 2021 from https://phys.org/news/2014-06-emerge-cloud.html