LeastAuthority.com Announces A PRISM-Proof Storage Service

Wednesday, July 31, 2013

LeastAuthority.com today announced "Simple Secure Storage Service (S4)", a backup service that encrypts your files to protect them from the prying eyes of spies and criminals.

"People deserve privacy and security in the digital data that make up our daily lives." said the company's founder and CEO, Zooko Wilcox-O'Hearn. "As an individual or a business, you shouldn't have to give up control over your data in order to get the benefits of cloud storage."

verifiable end-to-end security

The Simple Secure Storage Service offers *verifiable* end-to-end security.

It offers "end-to-end security" because all of the customer's data is encrypted locally — on the customer's own personal computer — before it is uploaded to the cloud. During its stay in the cloud, it cannot be decrypted by LeastAuthority.com, nor by anyone else, without the decryption key which is held only by the customer.

S4 offers "*verifiable* end-to-end security" because all of the source code that makes up the Simple Secure Storage Service is published for everyone to see. Not only is the source code publicly visible, but it also comes with Free (Libre) and Open Source rights granted to the public allowing anyone to inspect the source code, experiment on it, alter it, and even to distribute their own version of it and to sell commercial services.

Wilcox-O'Hearn says "If you rely on closed-source, proprietary software, then you're just taking the vendor's word for it that it actually provides the end-to-end security that they claim. As the PRISM scandal shows, that claim is sometimes a lie."

The web site of LeastAuthority.com proudly states "We can never see your data, and you can always see our code.".

trusted by experts

The Simple Secure Storage Service is built on a technology named "Least-Authority File System (LAFS)". LAFS has been studied and used by computer scientists, hackers, Free and Open Source software developers, activists, the U.S. Defense Advanced Research Projects Agency, and the U.S. National Security Agency.

The design has been published in a peer-reviewed scientific workshop: *Wilcox-O'Hearn, Zooko, and Brian Warner. "Tahoe: the least-authority filesystem." Proceedings of the 4th ACM international workshop on Storage security and survivability. ACM, 2008.* http://eprint.iacr.org/2012/524.pdf

It has been cited in more than 50 scientific research papers, and has received plaudits from the U.S. Comprehensive National Cybersecurity Initiative, which stated: "Systems like Least-Authority File System are making these methods immediately usable for securely and availably storing files at rest; we propose that the methods be further reviewed, written up, and strongly evangelized as best practices in both government and industry."

Dr. Richard Stallman, President of the Free Software Foundation (https://fsf.org/) said "Free/Libre software is software that the users control. If you use only free/libre software, you control your local computing — but using the Internet raises other issues of freedom and privacy, which many network services don't respect. The Simple Secure Storage Service (S4) is an example of a network service that does respect your freedom and privacy."

Jacob Appelbaum, Tor project developer (https://www.torproject.org/) and WikiLeaks volunteer (http://wikileaks.org/), said "LAFS's design acknowledges the importance of verifiable end-to-end security through cryptography, Free/Libre release of software and transparent peer-reviewed system design."

The LAFS software is already packaged in several widely-used operating systems such as Debian GNU/Linux and Ubuntu.

https://LeastAuthority.com