

Re: Open source secure browser-based storage, with a \$1000 challenge

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-04/msg00431.html>

- *From:* iwhisper.info@xxxxxxxxxx
 - *Date:* 15 Apr 2006 13:55:55 -0700
-

I would not use such a service for storing highly critical data.

I see what you mean, I mispoke. I hadn't envisioned it for use for highly critical data. I actually developed it to store information I already use browsers for, like a growing collection of website passwords. I believe it could also be used for anonymous communications with reasonable security, but very low bandwidth.

But this is meant for ordinary people who need convenient, reasonable security and aren't willing to install and run complicated applications, and aren't capable of verifying that they personally have a valid copy of such applications.

If the remote server is the one supplying the Javascript code

Is this significantly different from downloading a "secure" application written in C++ or Java? A compiled program need only be downloaded once, but is more difficult to verify. With Javascript, the source code is the object code, and is clearly visible and verifiable.

And because the source code is distributed from a central server, no one need worry that they, alone, have a spiked copy of the software. Again, it seems to me that all downloaded applications are vulnerable to spoofing or spiking (I hope I used that term correctly), and Javascript is among the easiest platforms to protect against such an attack.

I would envision, if the open-source application or the website become widely used, recruiting people to run applications that automatically verify the Javascript. Something like a security related version of the SETI@home phenomenon (the social phenomenon, not the technical implementation). With a number of people monitoring the site, any change in the Javascript code could be detected quickly, and perhaps communicated through peer-to-peer reporting.

Re: Open source secure browser-based storage, with a \$1000 challenge

I believe this would protect users who chose not to run the application as well, if any breach were detected quickly.