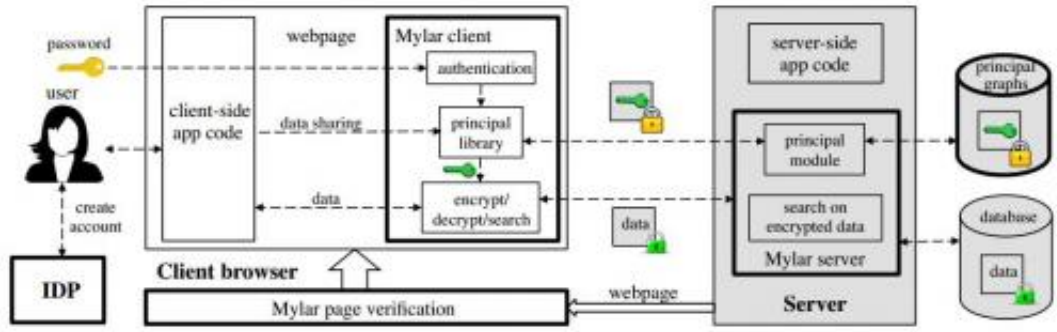
MIT researchers develop Mylar – a platform for building secure web applications

March 26 2014, by Bob Yirka



System overview. Shaded components have access only to encrypted data. Thick borders indicate components introduced by Mylar. Credit: Raluca Ada Popa, et al.

(Phys.org) —A team of researchers at MIT, led by Raluca Ada Popa has developed a platform for building secure web applications that is based on ensuring data on servers is always encrypted—they call it Mylar. In announcing the new platform, the developers noted that Mylar can protect user data from snooping even if a hacker obtains full access to a server.

The traditional approach to securing user data on servers, is to accept data from a user (generally from a web browser), then encrypt it before saving to a hard drive on a server. When the user requests the data, the server opens the file, decrypts it and then sends what has been requested.

The weakness of this approach, Popa notes, is that if a hacker gains control over a server, they can decrypt everything on it. A better approach she says, is to have encryption and decryption occur on the user end—that's the essence of Mylar.

With the Mylar platform, encrypting and decrypting are performed via code in a user's browser, thus users never see it happening—it's seamless. The advantages of such an approach are obvious, hackers can't read data files, and notably, neither could government snooping programs such as PRISM.

Popa says Mylar would allow users to send passwords to others using public encryption keys, so that data could be shared with other intended users. Also there are extensions that prevent someone with server access from stealing encryption keys and also for searching for information in stored files.

Of course there are reasons companies that run servers haven't already adopted a similar platform. One of the big ones is that if a user forgets their password, they are never going to get their data. Another is that many companies that host data make money from ads which rely on knowledge about the content of data files. Also there is the problem of the need for a standard shared by users across the Internet.

Undaunted by naysayers, the team at MIT reports that they have already lined up several users ready to try the new platform and expect more to follow. They also note that there is a precedent, CryptDB, also developed at MIT, to encrypt database information in a similar fashion, is now in use by Google, SAP and other companies. The team will be presenting a paper describing Mylar at USENIX next month.

More information: — Building Web Applications on Top of Encrypted Data Using Mylar, www.usenix.org/conference/nsdi …

ns/presentation/popa , (PDF)

— Mylar, css.csail.mit.edu/mylar/

via TechnologyReview