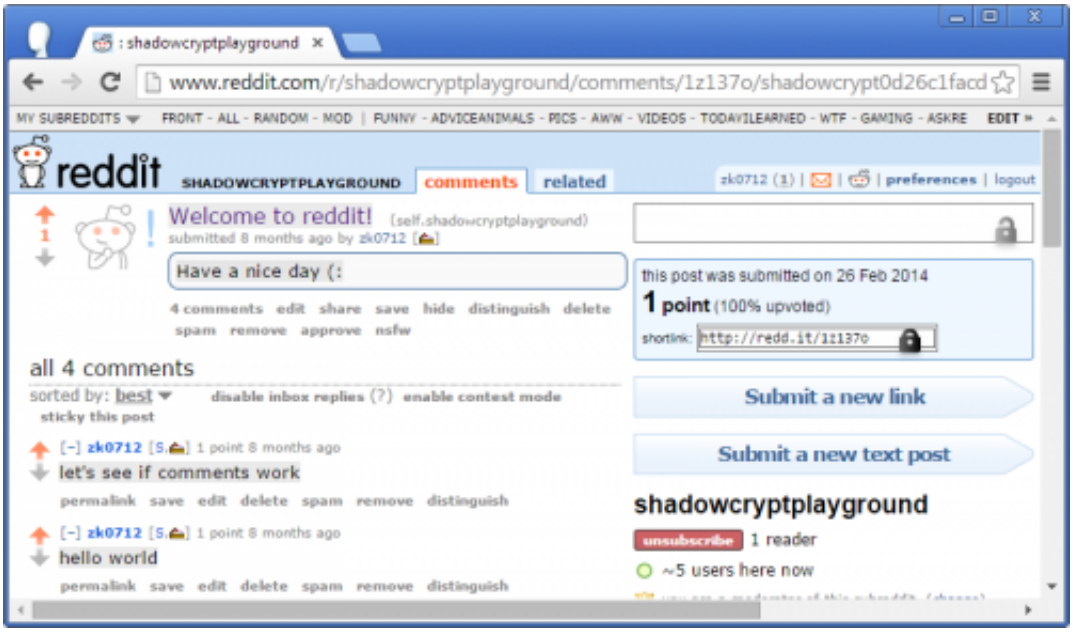
ShadowCrypt research project shows encryption approach

November 6 2014, by Nancy Owano



A team of researchers from UC Berkeley and University of Maryland believe they have come up with a previously unexplored design point, ShadowCrypt, that enables encrypted input/output without trusting any part of the web applications. That means they are suggesting a tool that can bring simple encrypted messaging to webmail and social networking sites. That means you could send and receive encrypted text on Facebook and Twitter. MIT Technology Review refers to it as a prototype browser extension, where the site operator or anyone

intercepting the posting sees only a garbled string of letters and numbers. The researchers, in their paper, "ShadowCrypt: Encrypted Web Applications for Everyone," prepared for presentation at the ACM Conference on Computer and Communications Security, discussed the chokepoint in their design.

"This chokepoint encrypts data before the application code (including the client-side code) can access it. The application can only view an encrypted version of the data. This requires isolating the input and output fields while still providing the application access to the encrypted data. Choosing this chokepoint means that no application code is in the TCB. This leads to a system secure against attackers at the client-side as well as the server-side. It also gives the user complete control over the data. In contrast, previous proposals required trusting application developers to handle data in a privacy-preserving manner."

They implemented ShadowCrypt as a Google Chrome browser extension. The extension is available on the Chrome Store for anyone to try out; ShadowCrypt also has its own web site.

When you install the extension, said the team, you have a few keys set up by default. These are to see if everything is working correctly. "Encryption is great for small group collaboration," said the site. "You can share your encryption key to allow your collaborators to see what you've written." ShadowCrypt is developed and maintained by the WebBlaze team, called WebBlaze, from UC Berkeley and collaborators from University of Maryland. They are Warren He, Devdatta Akhawe, and Sumeet Jain, and Dawn Song from Berkeley, and Elaine Shi from the University of Maryland. The source code is on their GitHub repository.

To put ShadowCrypt to work, explained Tom Simonite in MIT Technology Review, "you install the extension and then create

encryption keys for each website you wish to use it with. A small padlock icon at the corner of every text box is the only indication that ShadowCrypt is hiding the garbled encrypted version that will be submitted when you hit the 'send' or 'post' button."

Discussing future work in their paper, the team said "We are currently working on supporting additional schemes that can work transparently," such as Format Preserving Encryption and Attribute-based Encryption. In the longer run, they said their aim is to support encryption schemes that rely on modifications to existing web applications to work, such as Searchable Encryption or Fully Homomorphic Encryption.

More information: — www.technologyreview.com/news/ … ages-on-any-website/

— shadowcrypt-release.weebly.com/

— www.cs.umd.edu/~elaine/docs/shadowcrypt.pdf

Citation: ShadowCrypt research project shows encryption approach (2014, November 6) retrieved 10 April 2024 from https://techxplore.com/news/2014-11-shadowcrypt-encryption-approach.html