Is the Mozilla FireFox 3 SSL policy bad for the web?

Lori MacVittie, 2008-05-08

Slashdot is discussing a recent rant regarding Mozilla FireFox 3's SSL policy regarding self-signed certificates. The rant claims that the policy is "bad for the web."

> Nat Tuck Thu on Mozilla SSL policy bad for the Web
>
> Mozilla Firefox 3 limits usable encrypted (SSL) web sites to those who are willing to pay money to one of their approved digital certificate vendors. This policy is bad for the web. Not only does it make users less secure overall by reducing the number of encrypted connections, it damages the basic principle of equality among web participants.
>
> The problem is this: When a Firefox 3 user visits an encrypted web site with a self-signed certificate or a certificate signed by an unapproved (new or non-profit) provider, Firefox doesn't show the page. Instead, it shows a scary "you are being hacked"-style warning that requires 4 clicks and an "add an exception" dialog box to bypass.

The author states that SSL is good for two things: authenticating web sites and encrypting communications. And I can't argue with that at all.

Self-signed certificates obviously aren't good for authenticating a web site. It's like me printing out a certificate declaring me to be me on my printer and signing it. That's why certificate authorities exist, and in the real world why notaries and other officials exist - to provide an objective third party that verifies identity and authenticates with their signature and seal the veracity of the identity claim.

Nat agrees, but argues that the second use of SSL, encrypting communications, is just as important, particularly when a wireless connection is in use. And it is the impairment of this functionality that appears to be at issue.

The problem is that there are other means of encrypting wireless (and wired) network traffic, and in fact SSL on a web site doesn't provide secure communications for many other protocols, the security of which I would be much more concerned with. Now, securing web site traffic - particularly when I'm going to be transmitting my credit card info - is important. It needs to be encrypted, certainly. But anyone with whom I'm going to do business had better be responsible and financially stable enough to afford a signed, valid SSL certificate.

But Nat also argues that many sites can't afford SSL but wish to provide encryption, so self-signed certificates are a valid means of achieving this goal. The question then becomes, as he points out, what kind of an interface users should see upon encountering a self-signed certificate.

Nat claims: *Obviously it shouldn't show a green address bar like the new (extra high price, major corporation only) EV certificates. But there is absolutely no excuse for it to be significantly less inviting to a normal user than an unencrypted site.*

I disagree. The average user needs to be very aware when the SSL certificate being used is not validating anything and is only being used to encrypt communications. It needs to be made very clear to circumvent the use of self-signed certificates on sites that may be phishing for data, when using SSL would increase the chances of a user trusting the site.

Treating self-signed sites with suspicion is necessary in order to preserve the validity of valid certificates and the trust users put into them. Not making it clear to users could easily engender a false sense of security and that often leads to Not Good Things happening. If that means a significantly less inviting user interface upon encountering a self-signed certificate is required, then I'm all for it.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113