Security versus Integration

Lori MacVittie, 2008-28-04

History says integration wins, will that trend continue?

Andrew Storms has a nice writeup on PayPal's recent decision to limit the supported browsers used with its service (i.e. this is a one browser site, buddy) in an effort to "protect customers".

This isn't just a case choosing IE over Firefox, or vice-versa, this move is about requiring a certain set of security functions to be available and active in a browser, and will not necessarily block out the major browser vendors - just older versions of those browsers. Apparently one of those features required will be EV SSL (Extended Validation Secure Sockets Layer).

> *In a white paper that outlines a five-pronged action plan aimed at slowing the phishing epidemic, Barrett [PayPal Chief Information Security Officer] said there's a "significant set of [PayPal customers] who use very old and vulnerable browsers" and made it clear that any browser that falls into the "unsafe" category will be banned.*

This isn't as ominous as it first sounds, it's just a case of requiring that consumers of PayPal's service be upgraded to the most secure version of the browser possible. These types of requirements have been put in place before, it's really not a big deal despite all the brou-ha-ha that surrounded this news.

I don't agree with Andrew's assessment that decisions like this could lead in a one-browser one-site web. The fight between 40-bit and 128-bit encryption and sites requiring the latter - to the exclusion of those with the former - did not drive the world to a single-browser. It merely forced those who were running inferior versions of browsers to update. What this type of decision ***might*** do, however, is to get rid of the "optional" update of browsers and force a "mandatory" update instead. It's too easy to forget, or turn off updates, or just not understand the risks associated with not updating - especially when there's a critical security patch included.

But let's assume that Andrew is right and we're headed (necessarily) toward a one-browser one-site (i.e. true client-server) model and that there's nothing we can do about it. We can even assume that it's a Good Thing. This would certainly make phishing attempts nearly impossible to pull off and it's true that Apple's iTunes hasn't (thus far) suffered from this software model.

That leaves only one (fairly substantial) problem that Apple hasn't had to face because it isn't core to their business model: **integration**. PayPal makes its money and bases its business model on easy integration with merchant sites. If it were to move out of the general browser and into an iTunes model it would require a lot more work to integrate with merchant sites. That's ignoring the fact that building a custom application (let alone supporting it across multiple platforms) is expensive and time-consuming.

Andrew theorizes:

> *The next disruptive technology to hit consumers and enterprises will be the single site browser. This will be web browser-like client software that can do nothing but be used for a single website. Think of this as traditional client/server application. If you need to use your financial system, you launch browser X; then if you need to use the ERP system, the user launches browser Y. At the outside of the spectrum, this feels like a 10-year step backwards in user productivity and IT operations management.* ***In all likelihood though, what we will probably see is still a single browser, but one that is intelligent enough to lock all network traffic to single known and trusted site. In this scenario, the user would need to logoff and switch context between system X and system Y; all the while the browser ensures no errant information gets transmitted to any other system.*** [emphasis added]

That's disruptive, all right. In more ways than one. Anything that interrupts a business process between two entities - and this would do that - is going to pose a major obstacle in consumers- and merchants - adopting that service. It's like filling up your shopping cart and then requiring that you print out your order and mail it in. It's certainly more secure and absolutely protects consumers from phishing attempts, but it's *too* disruptive both to the consumer and merchants, and that's not something a provider like PayPal can afford to do.

Imbibing: Coffee

Technorati tags: MacVittie, F5, security, browsers, client-server computing, integration

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