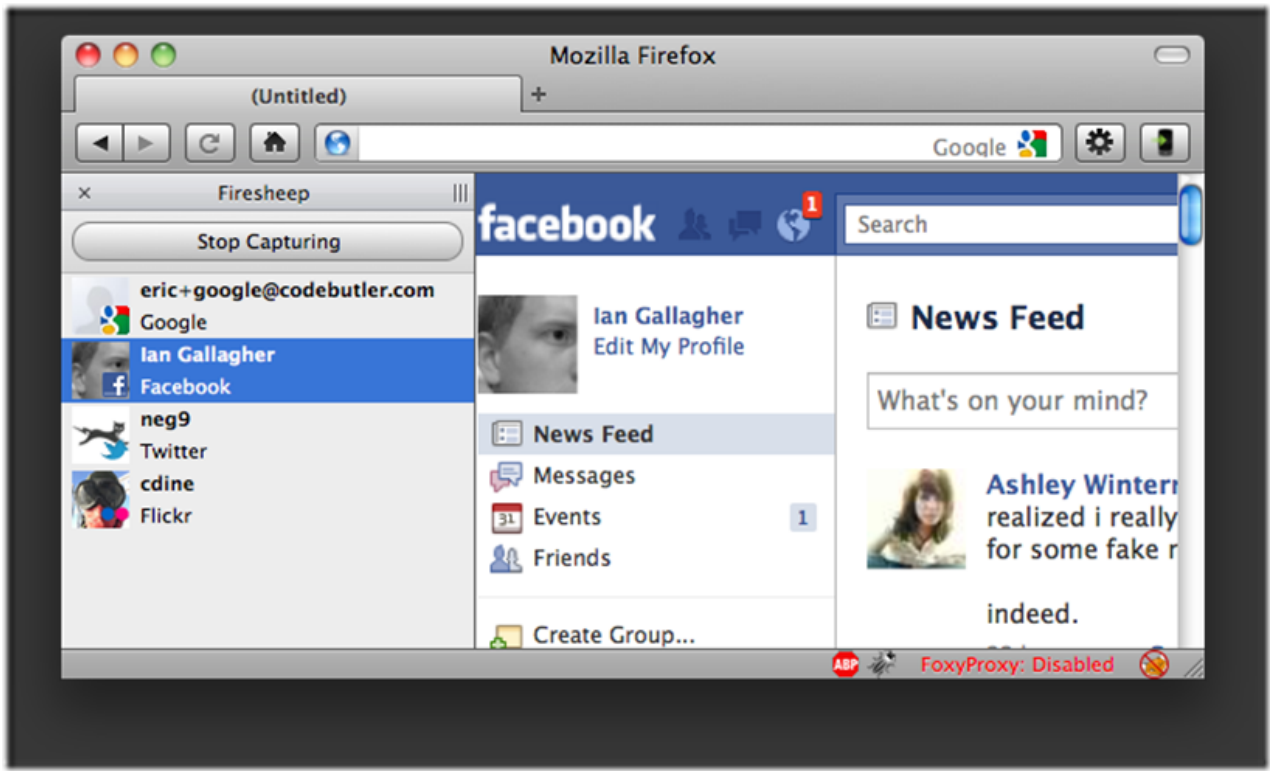
Baaa, Baaa, Firesheep

David Holmes, 2010-27-12

The most popular post on this blog is (by far) the short post "**Weaponizing Firefox.**" Since we posted it, there's been a new weaponizing tool, one that has gained much infamy in a short amount of time: **Firesheep**.

Put simply, **Firesheep** is a browser plug-in that lets you impersonate those around you by "stealing" their clear-text auth cookies. There's nothing really new about what it is doing, it's merely packaging the various techniques necessary into a click-able interface. Here's a screen shot from the **Firesheep** site.



The main attack comes from the fact that typically, a 'login-page' does all the heavy-lifting of authentication, but every request after that uses just a cookie to get back in. Mere ownership of a copy of the cookie counts as authentication after that first page. Firesheep collects those cookies and away you go.

Mitigation

So how do you foil Firesheep (and other **side-jacking** attacks)? I almost feel guilty for saying this, but the basic defense is to use SSL for everything; protect not just the login-page, but EVERY page. For many of F5's customers, that simply means buying more BIG-IPs, which they were probably going to do anyway. Google has an interesting post how they are not vulnerable to Firesheep because they've been **all-ssl** for a while now.

However, there have been reports that some of sites, like Google, are accidentally leaking the cookies when they send the HTTPS redirects. According to this blog, just firing up Chrome without going to any website will leak your GMail cookie. That seems hard to believe and yet totally believable at this stage in the game; eventually most of the leaks will get flushed out, right? Or maybe not.

There is an interesting proposal coming out called HSTS that mitigates the leak-on-redirect problem – I'll talk more about that in a future post.

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