Richie Steigerwald

On October 24, 2010, Eric Butler, a web developer from Seattle, announced a new Firefox extension that he created. The extension, which he calls Firesheep *, is an extremely simple tool that makes it easy to log in to social media sites–as the stranger sitting next to you. As soon as the tool was released it became a sensation; people who downloaded it were granted the ability to log in to the Facebook, Twitter, and Google profiles of strangers without guessing any passwords, writing any code, or even using any complicated hacking techniques. All they had to do was click a button. The only requirement was that someone nearby be connected to one of these social media sites.

The blog post that Butler wrote to announce Firesheep describes exactly how easy it is to log in as someone else on a website like Facebook: "After installing the extension you'll see a new sidebar. Connect to any busy open wifi network and click the big "Start Capturing" button. Then wait. As soon as anyone on the network visits an insecure website known to Firesheep, their name and photo will be displayed. Double-click on someone, and you're instantly logged in as them. That's it." Firesheep is a simple interface for a not-so-complicated hacking technique. The problem with these websites that Firesheep exploits is very simple.

When you log in to a website, Facebook for example, they send you back a temporary and unique identifying message called a cookie. Every time you ask Facebook for a page or a picture, you give them back a cookie. If you give them back the same cookie that they give to you, then they know that it is you so they send you all of the information that you want and have permission to look at. If you give them a different cookie, then they assume that you are someone else–they assume that you are the person that they gave the other cookie to.

You can see now that if you can figure out what someone else's cookie is, then you can see all of the information that they have permission to look at. You, as far as Facebook knows, are that person. What is most troubling about this is just how easy it is to get someone else's cookie.

Due to the way wifi works, making a web request over an open wifi connection is the computer equivalent of shouting out loud. When the computer shouts, it announces to the world what your cookie is. Firesheep listens to the computers who are shouting, then saves the cookies they broadcast so you can log in using their cookie.

This type of hacking is called session hijacking. It enables hackers to steal the online identities of anybody on the same network. This security issue has been around long before Firesheep, but Firesheep exposed the problem to many more people. Firesheep easily exploits session hijacking vulnerabilities on several websites, particularly Facebook.

It is important to note that this vulnerability is not a bug with Facebook. Session hijacking occurs between the user and the website. In order for this to happen, a hacker has to be tapping the connection between you and Facebook and listening in. To prevent people from stealing your cookie, you must agree with Facebook to have your connection encrypted. The technology used for encrypting the connection is called Secure Socket Layer or SSL. When it comes to online security, SSL is generally regarded as the most practical solution to this problem; it is the technology that banks require their customers to use when making online transactions.

Facebook offers SSL to protect users from session hijacking. In order for users to protect themselves, they can enable HTTPS which encrypts their entire session. This is done in Facebook by going to the "Account Settings" page, navigating to the "Security" tab, opening the "Secure Browsing" accordion fold, checking the box to enable secure browsing, and clicking the "Save Changes" button.

According to a 2009 AP-MTV poll, over 12% of teens and adults surveyed said that someone impersonated them or spied on them by logging into their email account or Facebook, MySpace, Twitter, or other Internet account without their permission. As of May 2011, 9.6 million users out of Facebook's 800 million active users, or 1.2%, have enabled HTTPS protection.

According to a Facebook security blog post, "Encrypted pages take longer to load... Facebook is slower using HTTPS.". It is Facebook's goal to provide a medium for its users to communicate effectively. If their software is slow then their software is less effective. If Facebook implemented site-wide HTTPS by default then every user would be slowed down. This would make using Facebook a less satisfying experience for users and could potentially reduce the number of users.