Hardening the Browser

Protecting Patron Privacy on the Internet

Eric Phetteplace, Guest Columnist

Correspondence concerning this column should be addressed to: ***M. Kathleen Kern****, Associate Reference Librarian and Associate Professor of Library Administration, University of Illinois at Urbana-Champaign, 300 Library, 1408 West Gregory Drive, Urbana, IL 61801; e-mail: katkern@uiuc.edu.*

Eric Phetteplace *is Emerging Technologies Librarian at Chesapeake College, Wye Mills, Maryland.*

When Eric Phetteplace asked me if browser privacy would be an appropriate topic for the Accidental Technologist column, I asked how soon he could write it. Even though he graduated in May 2011 and moved to start a new job, he presented me with the column this fall. In "Hardening the Browser," Eric poses some questions for consideration about how involved libraries should be in training our patrons on Internet privacy. He also provides a lot of practical how-to information that will be useful for your library and for your personal web browsing.—*Editor*

Article 3 of the current Code of Ethics of the American Library Association states that "[ALA members] protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted." This noble maxim has led many librarians to be advocates for the right to privacy, even to the point of resisting federal legislation such as the USA PATRIOT Act. However, merely protecting a patron's circulation records has become but a small hillock of the privacy terrain in our modern information environment. As more and more time is spent accessing and producing content online, libraries need to position themselves to offer Internet privacy to patrons as well.

The much-publicized "Firesheep" add-on for Mozilla Firefox highlights the need for education surrounding privacy on the Internet.[1] While traffic sent over HTTP on a public wireless network has always been vulnerable, Firesheep makes stealing others' log-in credentials a trivial procedure. Simply open Firefox, click a button to start capturing log-in credentials from others on the same public network, and soon you can post to their social media accounts, such as Facebook. While Firesheep runs only on Firefox, it can exploit unprotected users in any other browser. The add-on is not in Mozilla's official directory of enhancements for Firefox and it was created as a proof of concept, meant to highlight vulnerabilities that already exist and not to create further ones. However, there also is nothing to stop malicious users from employing Firesheep to their own ends.

While discussions around Firesheep typically note that public Wi-Fi hot spots occur in coffee shops or airports, many libraries also provide wireless networks. As of 2010, 85.7 percent of public libraries offered wireless Internet access, and another 5.9 percent planned to make wireless connections available within a year.[2] As such, it is the responsibility of librarians to educate users of the risks and insulate them against potential attackers. While not all librarians are able to secure their institution's networks or even choose the software

settings on their public computers, simply spreading awareness of online privacy problems and potential solutions is a major step forward in an increasingly important area of information literacy. This column will detail three layers where protections can be implemented: in the choice of an Internet browser, the user settings within the software, and, finally, add-ons that extend the browser's functionality, providing additional security beyond the default architecture.

CHOOSING THE RIGHT BROWSER

The easiest defense is at the level of the Internet browser itself. Selecting software that has historically proven to be secure, such as Mozilla Firefox or Google Chrome, immediately places your users in a safer arena. On the other hand, Internet Explorer is a notoriously insecure piece of software, and Apple's Safari browser has proven to be similarly vulnerable. Both browsers were hacked on the first day of the 2011 "Pwn2Own" event at the CanSecWest computer security conference, while no participants even attempted to hack Firefox and Chrome.[3] It should not have to be mentioned, but Internet Explorer 6 still holds a modicum of marketshare in the United States and is regarded by some as the most insecure piece of software ever developed.[4] Part of the reason for this is the ActiveX Controls that interactive websites can use in Internet Explorer. These controls run with the same level privileges as the user running the program, which gives malware opportunities to interact with many elements of the Windows operating system, including downloading files and executing programs. If your library or any of your users are still using Internet Explorer 6, migration to a newer version is absolutely essential. It speaks volumes that Microsoft itself has an Internet Explorer 6 Countdown site that advises "friends don't let friends use Internet Explorer 6," yet that same site shows 1.4 percent market share in the United States as of September 30, 2011.[5]

On the other hand, Google Chrome has developed a few innovative approaches to security.[6] First of all, plug-ins such as Shockwave Flash are often a source of security vulnerabilities, which is further exacerbated by users failing to update to the latest versions when they become available. To address this issue, Chrome packages plug-ins along with its own automatic updates that run seamlessly in the background, never providing the user an opportunity to opt-out of valuable security patches. Especially for large, public computing labs not running virtualized software, automatic updates save IT staff time and reduce user confusion. Second, Chrome "sandboxes" plug-ins so that even when vulnerabilities are exploited, they cannot break into the larger operating system environment. Thus problems analogous to malicious ActiveX Controls with too great of privileges are circumvented. Finally, Chrome also works to inform users of site security, from highlighting the "https" prefix in green font beside a safety lock to warning when users are about to visit a malicious website.

It is worth noting that Google's branded version of the Chromium open-source project automatically reports certain information back to the Mountain View-based company, including crash reports, mistyped URLs, the location where Chrome was downloaded, and anything typed into the address bar (or "omnibar" in Chromium-speak). These tracking activities could be circumvented by using SRWare Iron, a fork of the Chromium project that is more or less identical to Chrome but with the Google reporting stripped out and a few additional privacy measures added in. However, Iron does not yet include Chromium's automatic updating mechanism and thus may pose ulterior problems beyond Google's monitoring.

Before Chrome was released to the public in December 2008, Mozilla had long been pioneering safety on the Internet. The Firefox browser comes with a robust private browsing mode and is less susceptible to attacks than Internet Explorer. The fact that both Firefox and Chromium are open-source also enhances their security, since it is easier for savvy users to discover, report, and fix problems. However, perhaps the chief advantage of Firefox is the large number of powerful add-ons that can provide additional security measures to users. Specific add-ons will be recommended below.

Finally, newer and more secure Internet browsing platforms are being designed with security in mind from the start. While security concerns clearly dictated aspects of Chromium's architecture, additional efforts are underway to make even more secure software. Opus Palladianum (by researchers at the University of Illinois) and Microsoft's Gazelle project both promise to bring a higher level of security to the browser, but neither is available for public trial yet.

CHOOSING THE RIGHT SETTINGS

Once a library has deliberately chosen a browser, an appropriate configuration can provide a base layer of protection. Selecting a targeted set of user preferences helps users to avoid exposing their data, either to others using the same computer or malicious users who have gained access to their files. The goal is to make the browser as amnesiac as possible while still maintaining usability. Browsing history, download history, form autofill information, and most especially passwords should all be erased each time the browser is exited. Figure 1 shows an example of effective settings in Firefox 4's Security menu. Both Chrome and Firefox offer private browsing settings that enforce a certain level of privacy: for the most part, closing and reopening a private browsing window will clear all saved information such as logins and history. This is called "Incognito mode" in Chrome and "Private Browsing mode" in Firefox.

On public computers, appropriate browser settings are vital. Someone should never be able to open a browser only to return to the previous users' session in a password-protected service or view their navigation history. While it is simple to choose a good configuration in a browser, maintaining those settings over time may be difficult as users have access to the

software's menus. However, Firefox allows administrators to create a permanent set of preferences to which the browser returns each time it restarts. By locking down settings, users can alter preferences during their browsing session, but their changes will be lost when the browser is closed. Chrome has an extension that password-protects the preferences menu.

Finally, below the browser itself and its settings, one can also encourage use of HTTPS sites instead of their insecure alternatives, a one-by-one version of the HTTPS Everywhere add-on mentioned in the next section. No one should be signed into Twitter or Facebook with an HTTP at the beginning of the URL; both services offer an "HTTPS-only" box—Facebook's is unchecked by default—buried in their user preferences. Twitter's checkbox is under Settings > Account > HTTPS Only (the very last option listed) while Facebook's corresponding setting is more obscured given the immensity of their Account menu, under Account Settings > Security > Secure Browsing. Because of the sensitive information available on social networking sites, as well as the possibility of impersonation or identity theft, these settings are increasingly important. Many libraries teach social networking classes; spending a moment to point out the importance of HTTPS-only can be a valuable addition to lesson plans.

Figure 1. Strong Security Setting in Firefox 4. Note that "Remember passwords for sites" is unchecked.

While there was some publicity when those social media titans introduced secure sites, many more sites provide HTTPS alternatives. Perhaps the best example is the underutilized Google SSL (https://encrypted.google.com), which sends one's Google search terms over a secure transfer protocol. While search terms may seem innocuous, there are certainly numerous situations wherein a user may prefer to keep them private, such as researching medical or legal issues. Chrome users can set Encrypted Google as the omnibar's

Table 1. Extensions for Google Chrome and Mozilla Firefox

Google Chrome

KB SSL Enforcer
The Chrome version of HTTPS-Everywhere, this extension forces traffic onto HTTPS sites if available. It is less refined than the Firefox add-on, sometimes redirecting the browser to broken or empty HTTPS sites, and also slightly more vulnerable to packet sniffing due to a weakness in Chrome's APIs.

WOT
Web of Trust relies on crowdsourced feedback on sites, evaluating them on factors such as trustworthiness, vendor reliability, privacy, and child safety. A small circle appears next to links in major search engines and web interfaces, colored green for safe sites and orange-to-red for more questionable ones. The breadth of Web of Trust ensures ratings for almost all major sites.

NotScripts
An emulation of the Firefox NoScript extension, this add-on attempts to overcome weaknesses in Chrome's extensions APIs via HTML5 storage caching. However, it is not quite as polished as NoScript with more frequent bugs and a requisite password that hinders its usability.

AdBlock Plus for Google ChromeTM (Beta)
The (unrelated) AdBlock extension is also very good at removing ads and preventing pop-ups. Both extensions are among the most popular ones for Chrome, with millions of installations.

Mozilla Firefox

HTTPS-Everywhere
Arguably the most important item in this table, HTTPS-Everywhere detects what domain a user is on and, if possible, sends their traffic over encrypted HTTPS rather than insecure HTTP. The add-on works seamlessly and is perhaps the best response to Firesheep-style attacks available for any platform. A download link is present on the Electronic Frontier Foundation's website (www.eff.org).

Web of Trust
Web of Trust is available for Firefox under its full name as opposed to the acronym WOT.

NoScript
Easily the most powerful security add-on, NoScript requires user approval to run any script, making almost all potential attacks opt-in. While a potent tool for power users, if installed on public computers NoScript will probably disorient the majority of patrons while blocking harmless scripts on legitimate websites.

AdBlock+
While this extension is designed to eliminate obnoxious ads, it has the added bonus of blocking malware and preventing some sites (such as the music service Pandora) from stealing Facebook login credentials.*

* Whitson Gordon, "Block Sites from Using Your Facebook Login with AdBlock Plus," Lifehacker, May 18, 2010, http://lifehacker.com/5542041/block-sites-from-using-your-facebook-login-with-adblock-plus (accessed May 28, 2011).

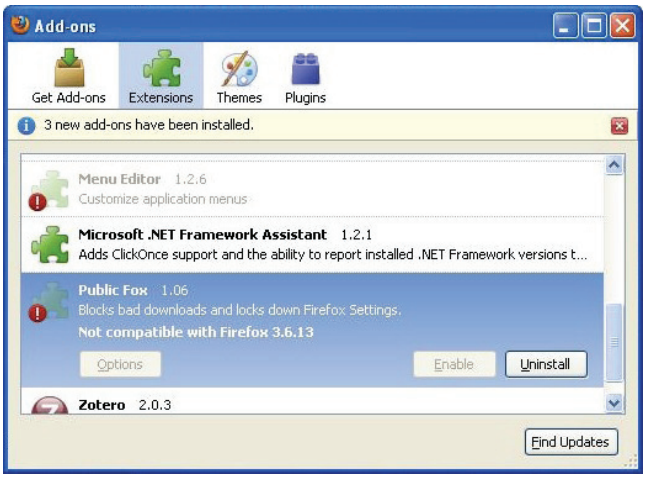

Figure 2. A Pop-up on a public workstation shows that some extensions were broken by an update and interrrupts the user's browsing experience.

default search engine by selecting "Manage Search Engines" in the "Basics" Preferences menu. DuckDuckGo (https://duckduckgo.com) is another search engine that offers an HTTPS version that can be set as the default. DuckDuckGo promises not to track its users' activities as an added benefit. HTTPS for e-mail services is even more important; Gmail has HTTPS on by default (see the "Always use https" radio button under Mail Settings > General > Browser Connection) while Yahoo! Mail, for instance, does not provide an analogous option.

ENHANCING THE BROWSER

Besides employing appropriate settings, there are browser extensions or add-ons that can augment functionality beyond what is typically available. Extensions can range from the somewhat trivial—changing the color or "theme" of the browser—to completely transformational, very nearly converting one browser into another. See Table 1 for a sample of useful extensions for Chrome and Firefox, both of which have impressive options available. All the add-ons outlined here are free downloads from the respective Chrome Web Store (https://chrome.google.com/webstore?category=ext) and Firefox Add-ons (https://addons.mozilla.org) listings. Analogous options can be discovered for most browsers, as both Internet Explorer (http://www.iegallery.com) and Safari (http://extensions.apple.com) have their own add-on galleries.

Extensions are typically developed by third parties, not browser developers, and have varying degrees of longevity. While extensions in the official directories listed above are vetted to some degree, there have been instances of malicious code exposing users to further harm rather than protecting them. It is always worth researching an extension before using it in the field, especially when the stakes are as high as they can be in matters of privacy. Reading reviews, including the brief ones in Mozilla's Add-ons or the Chrome Web Store, can alert you to potential issues that other users have encountered. Noting the number of downloads and currency of updates is an indicator of how likely the extension is to be maintained into the future. Lastly, testing the extension in a safe environment can help verify that it indeed does what it asserts to do. For instance, one can install HTTPS-Everywhere on a test workstation, then visit several high-profile websites where a user would want their traffic to be encrypted, e.g., Amazon, Gmail, Google Search, Facebook, and Yahoo! Mail. Does the URL begin with "https"? If not, then the extension is not living up to its claims.

Since extensions can significantly alter the browsing experience, it is worth contemplating how users will react and even performing usability tests before employing too many on public workstations. Updates also can break extensions and disorient the user upon opening the browser, as in figure 2. Some of the best extensions will be nearly seamless, such as AdBlock, where it is often not evident that content is being hidden, but others will be extremely disruptive, as when NoScript breaks the shopping cart application of an online vendor. Even Web of Trust may confuse patrons who do not know what the green circles signify. Then there are also extensions which work, but only to a limited degree. BlackSheep (https://www.zscaler.com/blacksheep.html), for instance, is meant to detect whether anyone on the same connection is using FireSheep. However, mere detection is not preventive and thus there are far more appealing alternatives.

CONCLUSION

No amount of secure software design and customization can entirely eliminate the threats that exist online. Phishing forms can cause users to turn over valuable information regardless of the security of their browsing platform. Hidden HTTPS-only options are very much left to the user's discretion; a user signed into Facebook will be on an HTTPS site only if they have selected the option for themselves. The best extensions can be circumvented, whether by innovative attackers or users who do not understand their options. Even with the stellar NoScript and HTTPS-Everywhere add-ons, a user can opt-in to malicious scripts and manually override HTTPS protection for particular domains. Thus educating users and library staff is the best way to enhance online privacy. Teaching workshops on the subject, or marketing particular solutions to known problems, is inherently valuable because it spreads awareness of an increasingly important issue.

Librarians must encourage users to develop approaches to Internet privacy that best suit their particular modes of browsing. All of the options listed in this article come with their own benefits and drawbacks; there is no panacea. If someone is uncomfortable moving beyond their outdated version of Internet Explorer, then pushing a new user interface with complicated privacy options on them solves little, but librarians can at least be informed about the risks present. Some users may prefer the ultimate defense of a dozen

extensions in a locked-down settings environment, while others will be content simply using a state-of-the-art browser. Though protecting privacy is enshrined in the American Library Association's Code of Ethics as a fundamental tenet of the librarian profession, librarians can strive to inform our patrons about online security far more than we currently do. If we install Firefox or Chrome with every available security extension on our public computers, it will still be for naught when our users go into a coffee shop with a public Wi-Fi connection, open up Internet Explorer on their laptop, and log in to Facebook using unencrypted HTTP. Publicizing security services that your library provides as well as universally available ones can help make our users safer no matter where they are.

ACKNOWLEDGEMENT

Many thanks to Brian Duggan, Tech Projects Developer at the Urbana-Champaign Independent Media Center, for his insights into network and browser security.

References

1. Kate Murphy, "New Hacking Tools Pose Bigger Threats to Wi-Fi Users," *New York Times*, Feb. 16, 2011, www.nytimes.com/2011/02/17/technology/personaltech/17basics.html (accessed June 1, 2011).
2. U.S. Census Bureau, *Statistical Abstract of the United States: 2012* (Washington, D.C.: Government Printing Office, 2011): 723, www.census.gov/compendia/statab/2012/tables/12s1154.pdf (accessed Oct. 10, 2011).
3. Wikipedia, The Free Encyclopedia, "Pwn2Own," http://en.wikipedia.org/wiki/Pwn2Own#Contest_2011 (accessed May 25, 2011).
4. Dan Tynan, "The 25 Worst Tech Products of All Time," *PC World* (May 26, 2006). www.pcworld.com/article/125772–3/the_25_worst_tech_products_of_all_time.html (accessed June 3, 2011).
5. Microsoft, "The Internet Explorer 6 Countdown," www.theie6countdown.com (accessed Oct. 10, 2011).
6. Charles Reis, Adam Barth, and Carlos Pizano, "Browser Security: Lessons from Google Chrome," *Communications of the ACM* 52, no. 8 (2009): 45–49, http://cacm.acm.org/magazines/2009/8/34494-browser-security/fulltext (accessed June 3, 2011).