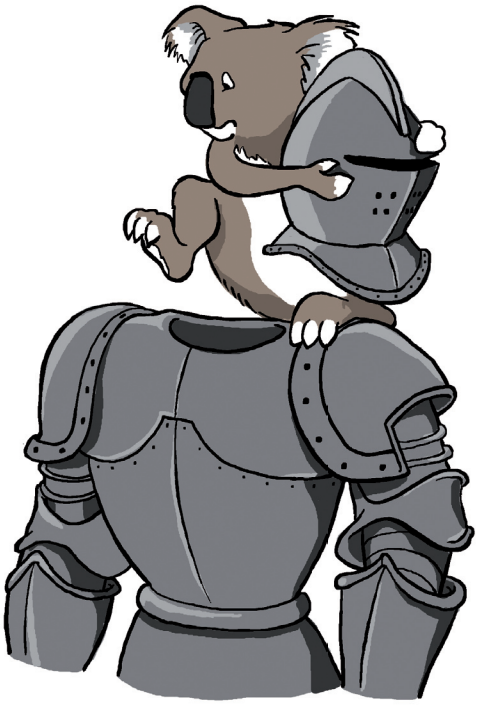
Secure Browsing



With a little bit of common sense and some handy tools, you can browse the web securely – mostly. BY JAMES STANGER

When I was asked to write about ways users could secure their home-based Ubuntu installations, the first phrase that came to mind was "web browser." I was a bit surprised by this, because it didn't seem to be the most scintillating or even natural topic. After all, most people with a technical background would immediately think of securing daemon-based services such as Virtual Network Computing (VNC) [1], Secure Shell (SSH) [2], or even DNS [3], each of which has fallen victim over the years to repeated, successful attacks (even in Ubuntu).

Yet, if you think about it, the browser is the primary way to access today's online world from an Ubuntu system. Are you interested in social networking sites such as Facebook, LinkedIn, and Twitter? You're going to use a browser, naturally, even though Twitter uses SMS. Are you a cloud computing type? The browser is your best friend there, too – really, maybe your only friend right now. Are you just interested in visiting CNN or Boing Boing to grab some news about current events? Yep – the browser is – and has to be – your tool of choice.

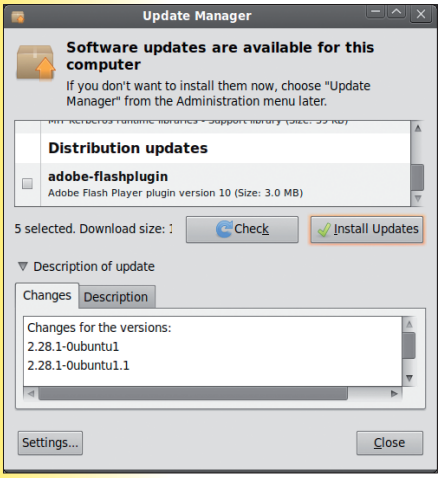


Figure 1: Update manager showing an update to the Adobe plugin.

Keeping Services Safe

So, we don't need to worry about securing daemons? Not so fast. The most commonly hacked daemons (also called "services") in end-user and even server-based Ubuntu systems remain VNC and SSH. The short answer is keeping services such as these deactivated if you're not using them. If you are using these services, then make sure you update them fastidiously. Also, make sure that you password-protect them and also activate any and all alerts and reasonable log entries associated with them. If someone logs on to your system, you'll want to know about it and be able to track their access. Look for future column entries from me to learn more about securing various services on your Ubuntu box.

The browser is also the primary means for getting your system into trouble. In fact, my initial instinct to discuss web browser security for your Ubuntu system seems to be justified in light of recent events. On Tuesday, January 14, 2010, just a couple of weeks after I was asked to write this column, a team of hackers used a botnet and other software to attack Google, Adobe, and others, primarily by exploiting bad code written into Internet Explorer.

Careful analysis has shown that the attack code explicitly goes after Internet Explorer and allows hackers to install and run software on the victim's hard disk. This type of exploit is known as a "zero-day" attack because Microsoft hadn't been able to release a patch for this particular problem, which is very difficult to guard against. This attack has worried many adherents to Internet Explorer, because their formerly innocuous little browser has become a platform for attack.

Yeah, I'm aware that Internet Explorer doesn't run natively in Ubuntu. Known that for years. But let's not get too smug and (yet again) bash our Windows friends for using a lame browser. Sure, it's fun to do that, but there is more to this event than gratuitous Microsoft bashing. The lesson isn't simply, "Let's use another browser."

Others have taken a second lesson from this attack, I've noticed: These people worry that attackers of various types, from individuals to governments, increasingly feel empowered – or worse, entitled – to attack others for ideo-

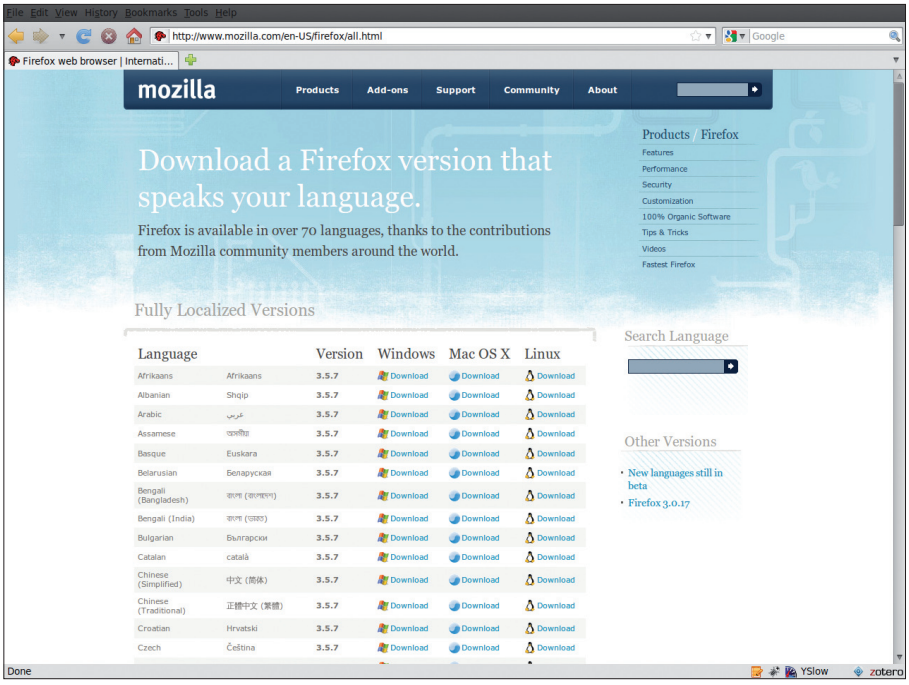


Figure 2: The Firefox download page.

logical reasons. That isn't the primary lesson we can derive from this attack either. The most important lesson is that the web browser, regardless of vendor, is the primary target that hackers will use to exploit you. Yes, even more than your email client.

So, if you're going to compute securely on your Ubuntu system, I want to talk first about securing the software you use to access the world. Don't think for a second that your version of Firefox or Opera running on Ubuntu will keep you eternally safe. Safer? Maybe. But it's up to you to make sure that your system is as safe as possible. So, I'll talk about some ways to take control of your surfing experience..

Here are some tools and tricks for securing your web browser and system. To begin, I'll take a look at ways to secure Firefox. These include:

1. Update regularly.
2. Tame macro-based content, including Flash.
3. Manage cookies.
4. Verify the sites you're browsing.

Updating Regularly

The primary way to secure Firefox is to make sure that you update regularly. Ubuntu's developers are constantly obtaining updates from partner projects, including Firefox and other browser developers. Although it's tempting just to dismiss system updates, you should take the time to keep your system current. You'll find that these updates will regularly update your browser, and not just because Ubuntu wants to make sure you have the latest, cool features. Many of these updates are designed to resolve problems that have been detected in the browser's code.

If you think you might have missed an update and want to conduct a manual update just in case, launch the Update Manager by going to *System | Administration | Update Manager*. You will see the Update Manager, as shown in Figure 1. Interestingly enough, it just so happens that while writing this article, an update became available for the Adobe plugin for the Firefox web browser.

To install the updates Ubuntu recommends, simply click on the *Install Updates* button and enter your "root" or "superuser" password.

Installing from a Tarball

One thing I've noticed is that Canonical, the owners of Ubuntu, can sometimes take a while to provide the most recent version of Firefox. This can be annoying from an "uber-geek" perspective, because it's always nice to have the latest and greatest software.

But sometimes, the problem is more serious because not having the latest browser version can open up a security breach on your system. To solve this problem, consider bypassing Ubuntu's Synaptic package manager and installing the package manually with the use of a binary distribution package.

To obtain the binary software, go to the Firefox download page [4], as shown in Figure 2.

Choose the correct language for your installation and then download the "tarball" (which is a compressed software package) to your desktop. Simply use Archive Manager to open and install the package. Or, if you're "old school" like me, you can download the file and then manually unpack the tarball and install it:

```
$ tar -jxvf firefox-3.5.7.tar.bz2
```

To run Firefox, just change into the directory and run the *firefox* command:

```
$ cd firefox/
$ firefox &
```

Browser Plugin Updates

If you're using Ubuntu's installation of Firefox, it's best to use Synaptic package manager to install the updates. Also, you can use the *Tools | Add-ons* window from within Firefox, or go directly to the add-ons page [5]. Although I am fairly conservative about the add-ons that I use, I do find them useful. Before I download an add-on, however, I make sure to do a bit of research about the quality of the download. I always use either Synaptic or the official Mozilla Add-on pages. Although neither is fool-proof, I've grown to trust that they won't allow poor-quality software to be posted. Let's take a look at a few add-ons.

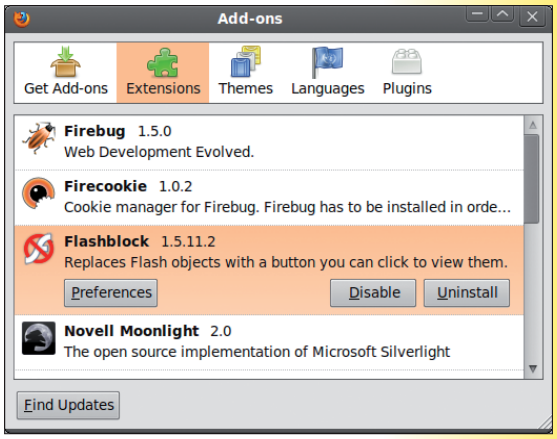


Figure 3: Flashblock installed in Firefox 3.5.

Macro-Based Content: Flash and Silverlight

Flashblock is useful because it allows you to determine exactly when you want to run Flash in your browser. Installing this plugin, like any other, is a breeze: Simply click on the link, download the add-on, and then restart your browser. Once installed, you can go to *Tools | Add-ons* to configure Flashblock's preferences, as shown in Figure 3.

Preferences that you can adjust include exempting sites; for example, I use several sites regularly as I give presentations concerning my

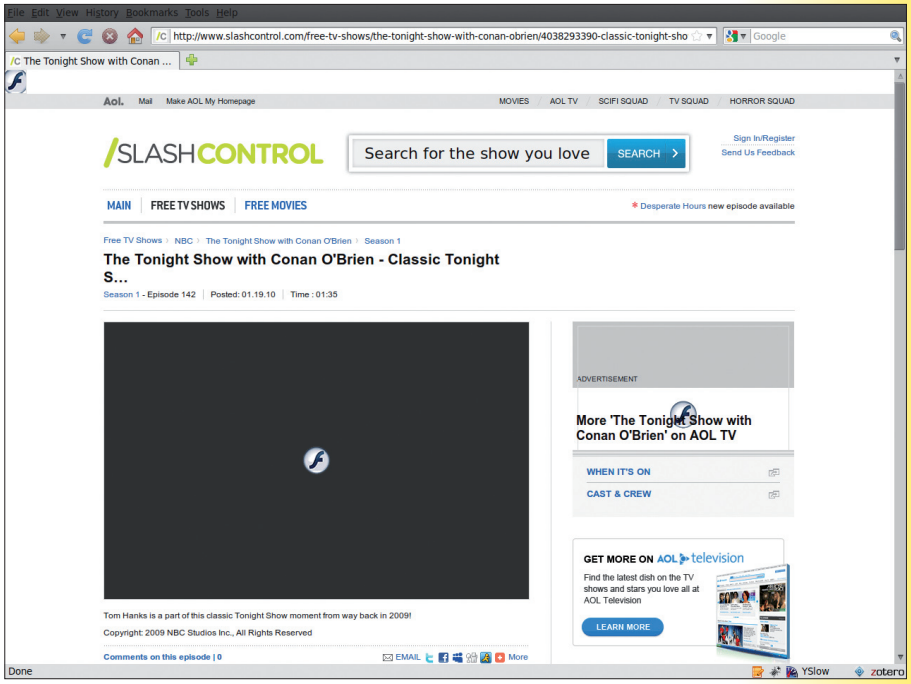


Figure 4: Using Flashblock.

Which Version of Ubuntu?

For this particular article, I'm using Ubuntu 9.10, the latest version for standard notebook computers. Most of the software and steps I've outlined here apply to earlier versions, as well.

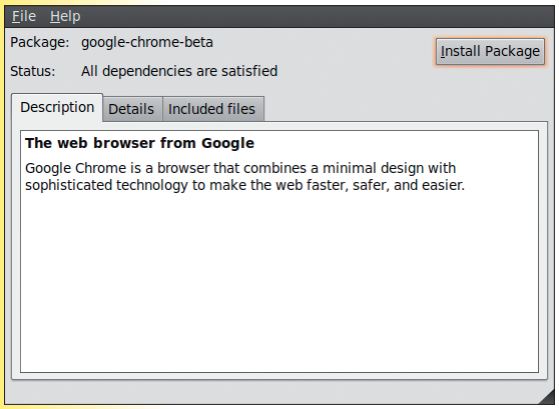


Figure 6: Using Gdebi to install Google Chrome.

company's web training product, CIW. For these sites, I always want the Flash to run automatically. Note that in order for this plugin to run, you will need to configure Firefox to run JavaScript.

Figure 4 shows how Flashblock doesn't let Flash run automatically. Instead, you see a blue icon in a gray screen. It's kind of ugly, but this icon is designed to let you choose what you want to see.

All you have to do is click on the blue *f* in the screen, and the image will play.

Managing Cookies

Cookies are values stored in your browser's memory, often in simple text files. Cookies are ubiquitous and useful. They store your preferences for websites and also aid with authentication. Back in the late 1990s, a lot of people thought that cookies were somehow inherently evil.

Well, they aren't. However, websites often use cookies to help track your web-based activities. Therefore, you need a good way to manage them. Good add-ons for managing cookies include:

- Firecookie
- Viewcookies
- BetterPrivacy
- CookieKiller

I especially like BetterPrivacy because it allows you to manage various types of cookies, including long-term and non-expiring cookies that many people feel are intrusions to their privacy.

Each of the add-ons mentioned above is available from the Mozilla site. The Flash Player can also deposit cookies, and both BetterPrivacy and CookieKiller allow you manage these types of cookies, as well.

Verifying Sites

When I browse the web, I often want to know more about the sites I'm browsing. Add-ons such as ShowIP, IP detection/Resolver, and WOT Safe Browsing Tool make it possible for me to learn more about a specific site. To begin, I learn the IP address of the website I'm visiting because it helps me determine the site's country of origin.

The WOT (Web of Trust) Safe Browsing tool [6] is especially useful because it allows you to conduct quick searches about websites to verify that the site is legitimate. The add-on works by using social networking; you and thousands of others help rate sites and report problems. By participating in the Web of Trust, you are helping the community – and yourself – browse more safely. In Table 1, I describe a number of other types of add-ons that would be useful additions.

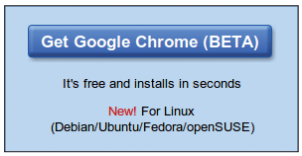


Figure 5: Downloading Google Chrome.

Opera

You've probably noticed that I've focused on Firefox so far in this column. That's because it's the most popular browser in most parts of the world. However, Opera is also a fine browser [7]. I consult for a social networking company known as Jeeva, and I've found that Opera is especially useful in my current gig, because the social networking software that this client uses just plain doesn't like Firefox's upload interface.

Opera has a solid reputation for security, and I highly recommend it. To download Opera, open up Synaptic package manager by going to *System* | *Administration* | *Synaptic Package Manager*, and then search for Opera. I've found that typing *Opera browser* in the standard search window narrows down the results quite a bit.

Chrome Browser

Google's Chrome browser [8] is increasingly interesting to me, because it is based on the Gekko engine, the same one that Apple uses for its Safari browser. If you have an iPod touch or an iPhone (or a Mac), you already know that Safari is a fine browser.

To download Chrome, go to the website, where you will see an image similar to that shown in Figure 5.

Click on the appropriate button to download the installation binary to your desktop. Then, use the Gdebi Package Installer, shown in Figure 6, to complete installation.

When you have installed the Google Chrome package, simply type *chrome* in a terminal or go to *Applications* | *Internet* | *Google Chrome* to run the application. Figure 7 shows Google Chrome visiting the *Linux Pro Magazine* website.

Google Chrome is attractive from a security standpoint because the code has been reviewed and pared down; when code is more simple, it is often more secure. Even though Chrome may have fewer features, I've found that it has a good history in terms of stability and security.

The "Mostly" Part

So far in this column, I've focused mostly on software. Updates, add-ons, and alternative browsers are all important, but they can't protect against "wetware" errors. Wetware is a word that security professionals use to refer to human beings and the mistakes that they can make. Consider the practice of "phishing," for example, wherein hackers use subtle tricks, known as "social engineering" to dupe individuals into revealing sensitive information, such as credit card numbers.

End Users and Power Users

Ubuntu's main contribution is that it allows everyone to become a power user just by being an interested, careful citizen of the Internet. Sure, you can start your journey to becoming a power user by merely launching Firefox and becoming a passive user of the web. But if you want, you can do more. You can take charge of your browsing experience, as well as enjoy more security than the average user. Ubuntu helps you make your browsing experience more secure and enjoyable in many practical ways, as I show you in this article.

Ubuntu's combination of the Debian operating system with a pragmatic, user-based approach is unprecedented in the industry. It provides more than a secure platform that has been reviewed and vetted by hundreds of experts with various perspectives. Ubuntu also empowers you as a user. From printing to web browsing, it is an operating system that is uniquely suited for today's computing environment.

Interested in the nascent cloud computing model everyone is talking about? Then you're going to use a web browser to access it. Even if you want to ignore the cloud and stick to the standard installed software platform we've been using for the past two decades, the web browser is still your primary means of accessing the world.

Sure, Ubuntu just works, but the beauty of this particular flavor of Linux is that you can also find out exactly how it works and make it work better for your particular needs. That's the beauty of Canonical's model, as well as the larger open source model that Canonical has adopted.

Figure 7: Using Google Chrome.

Phishing is effective only after a user has somehow lowered his or her guard, either out of naiveté or some form of desperation (e.g., "I've just got to have that piece of software").

As you browse the web, make sure you control your own behavior. In the same way that the best car can't protect a reckless driver, the most up-to-date, cutting-edge browser can't protect someone who throws caution to the wind. To help yourself surf more securely using Ubuntu, consider the following practices:

1. Use common sense: Your brain is the best anti-hacker tool available.
2. Update your software regularly (yes, I know I've already said this, but it bears repeating).
3. Conduct backups: I mentioned previously that "zero-day" attacks are very difficult to guard against. If you lose your data to such an attack, the only way you'll get it back is to restore from a current backup.
4. Avoid downloads and websites you don't fully understand.

Conclusion

Lately, I've noticed that the following cliché has become relevant in my professional life: "Sometimes your friends can cause you more problems than your enemies." Imagine going to a party with a friend, only to have him make you look bad. Or, even worse, suppose that this friend drives to you to party, gets drunk without your knowing it, and then starts driving you home. Suddenly, this friend is more than an embarrassment – he now poses a threat to your well-being.

What does this have to do with browsing the web? Everything, actually. Remember that when your browser takes you to a web site, you're bringing a bunch of powerful programming with you. Hackers, phishers, and various lowlifes have effectively one goal: to use the lines of code found in that browser software against you. Ubuntu and Firefox help you solve this problem because, unlike many other companies, they believe in creating open code that anyone can review and improve. Instead of relying on "security through obscurity," Ubuntu and Firefox creators rely on the open source ethos. The open source ethos is less an "anti-corporate" mentality than it is the belief that multiple experts should be able to review the software code that you use. Let me extend that metaphor about the friend you bring to a party: If you're going to go to a party with a friend, or even go with a partner to visit important people and places to gather information vital to your personal life and career, don't you want to know exactly how that friend will behave when you make those visits? If software – in this case, your web browser – is your friend, you'll want to be confident that your friend won't embarrass or harm you. The ethos behind open source is transparency, coding smarts, and the belief that "given enough eyeballs, all bugs are shallow." That's a relatively famous saying from Linus Torvalds, known as "Linus's Law." In essence, you should be able to "look beneath the hood" of the vehicles, as it were, that you use to get onto the information superhighway.

So, enjoy your browsing experience in Ubuntu. Consider the software and the common sense steps I've outlined, and you'll be able to move forward with real confidence as you securely surf the web. ■

Table 1: Additional Add-ons

Type	Description
NoScript	Blocks malicious scripts by allowing JavaScript, Java, and other potentially dangerous content from trusted sites only.
Anonymizing add-ons	Anonymizers can help you more securely browse the web, because they don't allow your activity to be recorded on your Ubuntu system. A popular example is Stealther.
Password storage tools	Add-ons such as Roboform Toolbar are useful because they securely store passwords for easy retrieval.
User agent switchers	A user agent switcher allows you to avoid having to use a Windows-based system when accessing Internet Explorer-specific systems. That alone can protect you from various exploits that target Windows-based systems. In this way, your entire Ubuntu distribution, and not just your browser, becomes a security tool. Additionally, your very behavior is more secure, because now you're accessing the web (and the larger Internet) using a peer-reviewed, open platform.

Info

[1] VNC: *http://en.wikipedia.org/wiki/VNC*

[2] SSH: *http://en.wikipedia.org/wiki/Secure_Shell*

[3] DNS: *http://en.wikipedia.org/wiki/Domain_Name_System*

[4] Firefox: *http://www.mozilla.com/en-US/firefox/all.html*

[5] Firefox add-ons: *https://addons.mozilla.org*

[6] Web of Trust: *http://www.mywot.com* or *http://www.youtube.com/user/MyWOT*

[7] Opera: *http://www.opera.com/*

[8] Chrome: *http://www.google.com/chrome*