Chapter 8

PROTECTING YOUR WEB BROWSER

INTRODUCTION

There has been much debate lately between two different browsers, namely Microsoft's Internet Explorer and the Mozilla Project's Firefox web browser. Security is in the center of this debate, accompanied by features and usability. This chapter focuses on the security aspects, particularly the risks involved with running any web browser and how to overcome some of these security shortcomings. Internet Explorer and Firefox will be used as examples, as these are the most commonly used, and therefore the most commonly exploited [1].

The browser debate going on today will probably continue throughout the well into 2007 and beyond. There may even be a full-blown Browser War status in the near future. Regardless of the outcome, and regardless of who wins, the bottom line is that you will need to secure your web browser. This may not always translate into actual browser or operating system configuration, but may mean being aware of your web browsing behavior. There are certainly some good tips to securing your web browser that you can configure. This chapter covers some in them briefly. However, you will find less malware (spyware, adware, and viruses) on your computer by changing your browsing habits and being more aware of your clicking. Almost all the browser exploits require that you click on something. Now, lets come back to reality and realize that people are going to click stuff, children especially, that could trigger malicious software to run on your computer. So your strategy is two fold: maintain a secure environment and be an educated user. The goal of this chapter is to help you in both of these areas. First, the chapter shows examples of the more common threats, and then moves on to the defensive measures. The weaknesses shown here are not the most critical, but they will help you to understand the basics of how web browser exploits work and how they are used in attacks [1].

BROWSER WEAKNESSES

As previously stated, this chapter focuses on the risks involved with running Internet Explorer and Firefox. These browsers are the most commonly exploited; because they are the most commonly used [1].

Internet Explorer

Internet Explorer has had its share of problems. In 2005 alone, Microsoft released numerous updates that fixed various security problems. These are the vulnerabilities that have been recognized by Microsoft. Vulnerabilities that have not yet been fixed by Microsoft also exist and pose an even greater threat, because there is no patch for them, yet [1].

The example chosen here is of a unpatched Internet Explorer vulnerability that will be explained in detail. The vulnerability deals with the status bar, which is the space in Internet Explorer (and all other browsers) in the lower left hand corner that displays, among other things, the destination of the hyperlink that you currently have your cursor positioned over. Due to a bug in Internet Explorer it is possible to construct a link that will display one web site link in the status bar, but really take you to a different web site [1].

This vulnerability poses a threat because you may think that you are being taken to your bank's web site, but in reality you are going to a web site created by an attacker attempting to gather your personal information through a phishing attack. It is important to note that this vulnerability also exists in MS Outlook Express [1].

Mozilla Firefox

Firefox has gained popularity as a web browser very quickly. It is a trimmed down version of the Mozilla web browser. It does have some security advantages, however it does not include support for technologies such as MS ActiveX, which coincidentally has posed many security issues for Internet Explorer. Not all web sites/applications will work in Firefox, but most agree it works well for general web browsing. Of course, just as any software, Firefox has its share of security problems too. It contains a similar bug that was previously explained with Internet Explorer, using a slightly different exploit. It too will allow a malicious user to "spoof" the real destination of a link in a web site. This time it only works when hovering over the link, right clicking, and choosing "Save Link As…" [1].

This exploit only works with Firefox version 1.0.1 and appears to have been fixed in later versions. If you ry it with 1.0.3 and 1.0.4, you can see the "hidden" link to "http://www.google.com" if you clicked and held the mouse button down on the link or right clicked and chose "Save Link As…". For fun, go to http://www.google.com – using Internet Explorer and notice that it spoofs the status bar successfully [1].

It's interesting to see that a vulnerability originally released for Firefox seems to work better in Internet Explorer. Even so, there still is not an exploit that works well with both [1].