Vulnerabilities in Browsers: Trends in Internet Explorer and Firefox

Jinyoo Kim, Omar H. Alhazmi, Yashwant K. Malaiya
Colorado State University
jyk6457|omar|malaiya@CS.ColoState.EDU

Abstract

Since the browsers serve as the gateway to the web, vulnerabilities in browsers can have great impact. Recently there has been considerable debate about the vulnerabilities in the two major browsers Microsoft Internet Explorer and Mozilla Firefox which represent two opposite development paradigms. Here we present a quantitative perspective involving vulnerability detection rates, severity and patch development. The available data suggests that the popular perceptions can sometimes be inaccurate and a detailed quantitative analysis of the data is needed for a careful evaluation of the risk. Making projections for the near future requires an understanding of the longer term trends. The need for reconciling alternating conventions for enumerating the vulnerabilities is also identified.

1. Introduction

The browsers and the web servers are among the most important components of the internet. Since their introduction in 1991, they are now a critical part of the local and global commerce, involving banking, trading, and e-commerce involving both consumers and businesses. Microsoft's Internet Explorer (IE) has been dominating the leading web browser in the market for several years [1]. However, in recent years, IE has been plagued by discovery and exploitation of numerous vulnerabilities that have compromised its security. In 2004, some security experts recommended switching to open-source Mozilla Firefox [2], regarding it to be a more secure web browser. During 2004 and early 2005, the Firefox's share of the installed base rose dramatically (Table 1). The share of Firefox is continuing to grow in 2006, although at a significantly slower pace.

Along with the market share, the number of vulnerabilities discovered in Firefox have also started to grow. It can be reasonably assumed that the reward function for finding a vulnerability is higher for a product with a higher market share. The assumption has indeed been shown to be valid for major operating systems [3]. Some questions then arise – is Firefox inherently more vulnerability-free or IE's woes have been just a result of its popularity? Is it possible to quantitatively analyze the available data to evaluate the vulnerabilities in IE and Firefox to do a fair comparison? We consider below the data available and significant factors to evaluate.

Table 1. Market share of IE and Firefox

Browser	Nov 2004	Apr 2005	Jan 2006	Jul 2006
IE	88.9%	86.63%	85.82%	83.05%
Firefox	4.58%	8.69%	11.23%	12.93%

2. The Browser Vulnerability Data

Here we use the data mined from National Vulnerability Database (NVD) maintained by National institute of Standards and Technology [4]. This database adheres to the CVE standard for identifying vulnerabilities developed by MITRE Corporation. On the other side, Secunia [5] uses a different enumeration approach. These differences may produce different results [6].

For IE, we examine the data for current version 6.x, released in August 2001. The usage of the previous version IE 5.x is now very small. For Firefox we examine data for the current version 1.5, introduced in November 2005.

3. Vulnerability Discovery Trends

Figures 1 and 2 below plot the data for IE 6.x and Firefox v1.5. To illustrate the trends, the data for IE v5 and v4 are also given. We assume that the vulnerability discovery process [7] is described by the recently proposed Alhazmi-Malaiya model which has been fitted for several operating systems [3] and web-servers [8]. The model assumes that the cumulative number of vulnerabilities show nearly linear rising trend until saturation occurs. IE v4 vulnerabilities show saturation in early 2001. IE 5 vulnerabilities still show a linear trend because of the shared vulnerabilities in the code inherited by 6.x. The available data for the Firefox 1.5 is limited; the plot in Figure 2 suggests that it appears

to have entered the linear phase. The Alhazmi-Malaiya model fits both IE 6.x and Firefox 1.5 well as indicated by the P-value (Table 2), where A,B and C are the model's parameters.

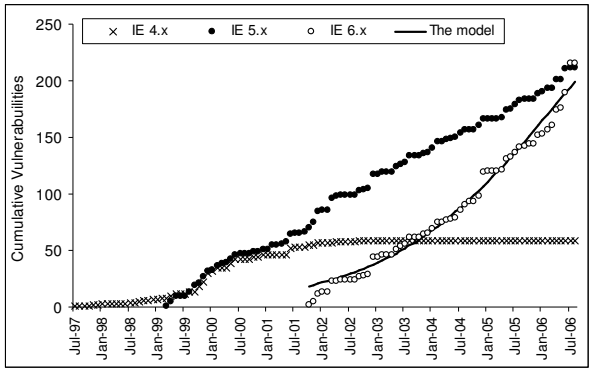

Figure 1. Fitting IE cumulative vulnerabilities

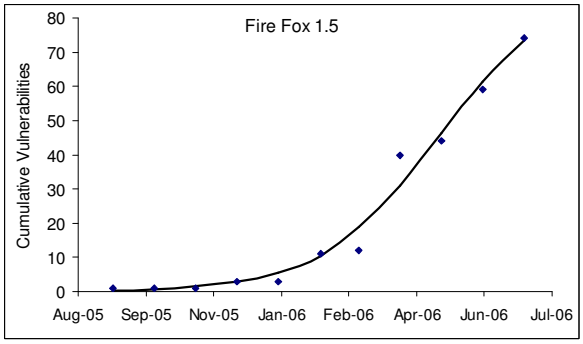

Figure 2. Fitting Firefox cumulative vulnerabilities

Table 2. Goodness of fit for IE 6.x and Firefox 1.5

	A	B	C	χ^2 P-value
IE 6.x	0.00015	359.946	0.0535	0.5504
Firefox 1.5	0.0074	92.245	5.014	0.6568

4. Analysis of Current Trends

To see the current trend, let us consider the year-to-date vulnerabilities. During 2006, 73 vulnerabilities were discovered in Firefox 1.5 compared to 60 in IE 6.x, as given in Table 3, which also classifies them according to severity (L:low, M:medium, H:high). The high-severity vulnerabilities are 33 for Firefox but only 15 for IE6.x. In addition we also note that the current slope of the model gives 12.4 vulnerabilities per month for Firefox, but only 3.5 for IE 6.x. This suggests we can expect a higher discovery rate for Firefox, with a larger fraction being of high severity

However the last two columns show that the Firefox patch rate is much better. The high severity patch rate is 72.5% for Firefox, but only 40% for IE6.x. Interestingly that leaves the same number of high severity vulnerabilities unpatched (9) at this time in the two browsers.

Table 3. Vulnerabilities of the first 7 months of 2006

Browser	Release Date	Total (L/M/H)	Mo. Rate	Patched (L/M/H)	Patch rate (%) (L/M/H)
IE 6.x	Aug 2001	60 (35/10/15)	3.5	10 (2/2/6)	5.7/20/40
Firefox 1.5	Nov 2005	73 (28/12/33)	12.4	35 (7/4/24)	25/33.3/72.5

5. Conclusions

Since 2004, there has been a perception that Firefox is much more secure compared with IE. However rising usage popularity of Firefox has also increased its popularity among hackers looking for vulnerabilities. The available data suggests a higher number of new vulnerability can be expected in Firefox 1.5 compared with IE 6.x in near future; they are also more likely to be of higher severity.

However that is only one component of the risk. Firefox developers are much better in developing patches with a significantly higher patch rate, thus significantly compensating for the higher vulnerability detection rate.

A product with a longer history and higher usage would have a higher number of past vulnerabilities, which does not necessarily imply that it has a higher number of inherent vulnerabilities. A better assessment is provided by the current discovery rate, the proportion with higher severity as well as the rate at which the vulnerabilities are currently patched. Other factors not considered here include the exploitation rates. Thus the evaluation of competing products should be repeated periodically using recent data to assess the current risk.

References

[1] One Stat, www.OneStat.com, (August 2006)

[2] R. Vamosi , *Why you should switch to Firefox now,* http://reviews.cnet.com/4520-3513_7-5515107-1.html, (Sep. 2004)

[3] O. H. Alhazmi and Y. K. Malaiya, Quantitative vulnerability assessment of system software. *Proc. Ann. Reliability and Maintainability Symp.* (Jan. 2005), 615–620.

[4] National Vulnerabilities Database, nvd.nist.gov, (Aug. 2006)

[5] Secunia, www.Secunia.com, (August 2006)

[6] R. McMillan, *After flap, Symantec adjusts browser bug count*, Computer World, (Aug, 2006). http://security.itworld.com/5043/060307browserbug/

[7] Andy Ozment. "Software Security Growth Modeling: Examining Vulnerabilities with Reliability Growth Models." Proc. Work. on Quality of Protection (QoP). Sept. 15, 2005.

[8] W. Sung-Whan, O. H. Alhazmi, and Y. K. Malaiya, *Assessing Vulnerabilities in Apache and IIS HTTP Servers*, *Proc. IEEE Int. Symp. on Dependable Autonomic and Secure Computing (DASC'06)*, (Sep.-Oct. 2006).