Determining the distribution of severe vulnerabilities among different browsers: An empirical research

Economics of Cyber Security Final Assignment

Maria Baltoglou [4412842]

November 2015

Abstract

This paper presents a statistical analysis approach in order to explain the distribution of severe-level vulnerabilities in the three most popular web browsers, namely Internet Explorer, Google Chrome and Mozilla Firefox. This research is based on the hypotheses that the count of severe vulnerabilities is proportional to the popularity of the particular browser and to the time between patches that vendors release. The objective of this empirical study is two-fold; firstly, to provide insights in the mistakes that vendors make when developing products and secondly to relate the findings to the overall security and reliability of the browsers. The paper pinpoints that the browser with the largest number of severe vulnerabilities is Internet Explorer, followed by Chrome and then by Firefox. The reason for this finding is that Microsoft in the first versions neglected security over an effort to overtake Netscape's dominance, thus attackers now more actively seek vulnerabilities for Internet explorer. Other vulnerable features inherent to the browser and its operating system are also indicators. Finally, the research highlights that the count of severe vulnerabilities per se is not an indicator of browser's overall safety.

1. Introduction

The rapid advancement of technology the last decades brought about the need for cyber security, i.e. the protection of information technology systems against fraud and theft (Moore, 2010). The number of incidents including data breaches, malware, scams and targeted attacks are of great importance since such incidents are often translated to economic loses. Researches have shown that those economic loses are crucial not only at organizational, but also at national level as the annual cost of cybercrime for the UK was estimated to be £27 billion in 2011, with firms incurring £21 billion, government £3 billion and citizens the remaining £3 billion (Anderson, et al., 2012).

Nevertheless, attacking a system practically means that the system is vulnerable. Specifically, as regards web threats which are quite common, having the chance to attack a browser or a website means that there are certain flaws in it. A daunting question that remains to be solved, discussed in Anderson and Moore (2006), is why there are so many vulnerabilities in web-based products. Logic dictates that if companies wish to prevent systems from being compromised then secure software would dominate in the marketplace and products would have been designed without flaws. Although this would save a lot of money as well as frustration, it is not always the case; vendors are mainly interested in winning the "tipping point" with their products, being first to market or dominant in existing markets. These motivations make them overlook the security of the products since most of the times this is a time-consuming activity (Anderson & Moore, 2006).

This paper focuses on analyzing the distribution of vulnerabilities found in web browsers, and especially the ones characterized as "severe". As regards the latter point, the severity of vulnerabilities can be measured by the Common Vulnerability Scoring System (CVSS) which estimates how much concern a vulnerability entails. A score of 7-10 is assessed as "high". Analyzing this security issue can provide insights in the kind of "mistakes" that vendors make as well as on whether browsers with more severe vulnerabilities are less secure than others with lower level vulnerabilities. This is an interesting study and analysis to perform since during 2015 there has been an increase of 42% in the number of vulnerabilities that are found in the most popular browsers (Secunia, 2015). Browser-based exploits can lead to permanent loss of data, personal detail theft, financial losses and increased man hours spent to fix the issue.

As browsers become more complex, the number of risks inherent in them rises. A lot of information is usually stored within a browser, making it attractive to potential attackers to try to exploit them in order to benefit from this information. The factors that can have an impact on the browser's security are several, with the main ones being buffer overflows, scripting and platform vulnerabilities (Oriyano & Shimonski, 2012). Regarding browser vulnerabilities, it is evident that the last years the security updates for different categories of browsers have increased (Seltzer, 2014). This pinpoints to the fact that more attention is paid to browser vulnerabilities and therefore further studies concerning the underlying reasons for the existence of vulnerabilities and their impacts could be of help.

2. Literature Review

In order to conduct a research about the distribution of severe vulnerabilities in web browsers it is essential to firstly perform a literature review on the existing research done for the issue under investigation.

On the one hand, many institutes such as Symantec, Kaspersky and Secunia issue reports that discuss trends in threats and vulnerabilities, including those found in web browsers. These reports usually compare annually the vulnerabilities detected and how they evolve with time. For instance, Symantec's *Internet Security Threat Report* (Symantec, 2015) compares the number of web threats between the reference year and the previous one, while it also reports the total number of vulnerabilities found in browsers the last four years. Similarly, *Secunia Vulnerability Review* (Secunia, 2015) presents some key figures and facts on vulnerabilities for the years 2008-2015. Reviewing the aforementioned reports can provide important insights on whether vulnerabilities follow an increasing trajectory as well as on the undertaken countermeasures to mitigate them. Studying the trends helps in seeing the issue from a holistic perspective by getting information about global security aspects. The aforementioned reports are treated as one basic category of research for the literature review.

On the other hand, there are several journal articles available that can offer explanations about the variables involved in this security issue. Firstly, Accuvant Labs issued a report in 2011 which compares three different browsers (Internet Explorer, Google Chrome and Mozilla Firefox) in terms of overall security. This report is used as a guideline throughout this paper and as a measure of comparison between browser trends in 2011 and 2014. The report is quite extensive, taking into account metrics such as count of vulnerabilities, timeline data, severity, browser architecture and URL blacklist services. Next, it analyzes browser add-ons as well as anti-exploitation techniques. The study concludes that as the complexity of browsers increases and as the data available are inconsistent, it is really hard to derive unbiased comparisons.

Secondly, Holm & Afridi (2015) have written an interesting paper regarding the CVSS system and whether its scores are accurate or not. In order to assess the severity of vulnerabilities, CVSS is most commonly used by the majority of people however it is not explored if the scores reflect reality. The study concludes that the accuracy highly depends on the type of vulnerability; some of them, like XSS and information exposure are given too low base scores while others, such as SQL injection or improper input validation have too high scores. The findings of this paper should be kept in mind while trying to estimate the level of severity of the vulnerabilities.

Thirdly, Acer & Jackson (2010) discuss browser security from a new perspective. Specifically, they challenge three conventional paradigms: (1) that browsers that receive infrequent patches are safer than those that receive frequent patches, (2) that browsers with less number of bugs are safer and (3) that the only way that a browser vendor can improve security is through the reduction of vulnerabilities. Their research concludes that what matters most is not patch frequency but rather patch deployment and bug count does not

reflect the vulnerability's severity and the vendor reporting methodologies. Also, the authors conclude that the most crucial security features in browsers are ignored due to negative news articles which equal patch releases to poor security of the particular browser.

Fourthly, the book "Client-Side Attacks and Defense" (Oriyano & Shimonski, 2012), offers a detailed description of browsers, their characteristics and the security issues that are related to them.

Finally, the paper "The Economics of Information Security" (Anderson & Moore, 2006) offers interpretations on the reasons that systems are vulnerable, which can be helpful in providing explanations about the behavior of vendors and the mistakes they make in association to vulnerable browsers. The authors conclude that market failures shape people's incentives regarding security, however prevention is always preferable than trying to police mistakes afterward.

The five preceding research literature sources can shed light into the security issue being analyzed in this paper. Furthermore, they all are indicative of the large significance of browser vulnerabilities and the need for their mitigation.

3. Research Question, Objective and Hypothesis

As already mentioned in the introduction, this paper focuses on vulnerabilities found in web browsers and relates the severity level with the overall security and the common mistakes that vendors make. Thus the research question to be answered is formulated as follows:

"How can the distribution of severe-level vulnerabilities found in browser categories be explained?"

The browsers chosen to be studied are the ones characterized as "most popular", namely Internet Explorer, Google Chrome and Mozilla Firefox (Leather, 2014; Secunia, 205). Browser exploits usually take the form of malicious codes that take advantage of ActiveX, HTML, Java, Javascipt or other web-related technologies and cause the browser to run arbitrary code, altering the user's browser settings without their knowledge.

The underlying hypothesis of the issue under investigation is that the browsers that are classified as the most popular will contain more vulnerabilities characterized as "severe" than other less vulnerable browsers. Additionally, it is assumed that the higher the number of severe vulnerabilities in a browser, the less the time the vendor should take to release a patch as severe flaws create the urgency to fix them. The first assumption derives from the annual reports of Secunia and Symantec indicating that the majority of vulnerabilities discovered in the most popular browsers are rated as "Highly Critical". The second assumption is based on the literature which emphasizes on the conventional paradigms such as the time between patches being an indicator of safety (Acer & Jackson, 2010; Wang, 2014).

The research question can be explored quantitatively by using various metrics. Some of them can be directly derived from the previous assignments of the course Economics of Cyber Security; these are the CVSS score as well as popularity and market share as indicators of security. Other metrics such as the number of reported vulnerabilities per browser and the time between security patches will also be used.

The objective of the research is to find how the critical vulnerabilities are distributed across the different categories browsers and relate this to vendors' errors and browser's overall reliability.

4. Methodology

Based on the research question *"How can the distribution of severe-level vulnerabilities found in browser categories be explained?"* formulated under Section 3, the methodology to be followed is descriptive in nature, i.e. it is meant to describe the characteristics of the browsers under study as well as the factors that influence the distribution. The description will include statistical calculations such as averages and frequencies in order to determine the distribution of vulnerabilities. For answering the hypotheses regarding the relation between severity level of vulnerabilities and popularity of the browser on the one hand, as well as time between patches on the other hand, Pearson's correlation test is considered the most appropriate approach. Regression analysis, although can provide insights in how the variation in the severity of vulnerabilities can be explained by other variables, cannot be used since the sample size is too small and thus the results will be subject to inaccuracy. The correlation test will indicate whether the above variables are related as well as how. Thus, the research will be both qualitative and quantitative, aiming to provide a complete answer to the questions posed above.

4.1 Detailed methodology for testing the hypotheses

The first hypothesis that "there is a positive relation between the number of severe vulnerabilities found in a browser and the popularity of this browser" is tested with the Pearson's correlation coefficient. This correlation test is judged as appropriate since both variables are numeric, nevertheless it should be kept in mind that the sample size is small; almost the total market share is divided among five categories of browsers as can be seen in Table 1 below (Leather, 2014).

Browser	Market Share
Internet Explorer	58,01%
Google Chrome	20,37%
Mozilla Firefox	15,08%
Safari	5,16%
Opera	0,99%
Other	0,40%

Table 1: Browser categories and their respective market share in 2014.

The data were entered into IBM SPSS software and the Pearson test was used in order to get the correlation coefficient with the number of severe vulnerabilities on the browsers (see next section) and the scatter plot.

The same methodology was followed in order to determine the negative relation between the number of critical vulnerabilities and the time between patches released by vendors. As already mentioned it is assumed that the frequency of patch releases indicates that vendors are interested in securing their browsers by removing the bugs as soon as possible; in that sense, the more frequent patches for a browser mean that the number of severe vulnerabilities are reduced. The days between security updates for each browser can be seen in Table 2 (Wang, 2014):

Browser	Days between patches
Internet Explorer	30
Google Chrome	15
Mozilla Firefox	28
Safari	54
Opera	48

Table 2: Browser categories and the amount of time between security patches released by their vendors.

4.2 Detailed methodology for research question

In order to find the distribution graphs the NVD database was used to get the data. The research was based on the following products, according to popularity:

1. Internet Explorer (Vendor: Microsoft): This browser is part of Microsoft Windows Operating Systems and accounts for 58,01% of market share. Trends show that Internet Explorer is considered the most vulnerable browser with many vulnerabilities discovered in it each year (Symantec, 2015).

2. Google Chrome (Vendor: Google): It is a freeware web browser and since its first release in 2008 it is becoming increasingly popular. Its market share in 2014 was 20,37%, being second after Internet Explorer. However, as Chrome's popularity increases so are expected to do the vulnerabilities found in it.

3. Mozilla Firefox (Vendor: Mozilla): It is a free and open-source browser that was released in 2004 and has been highly successful with a respective market share of 15,08%. Similarly in this browser the vulnerabilities appear to be proportional to its popularity.

For each of the above-said browsers, the total number of vulnerabilities was obtained from NVD database for the year 2014. Next, the number of those vulnerabilities with a CVSS score of 7-10 (i.e. high severity) was found through the database. The percentage of lower level vulnerabilities was also looked upon to better determine the distribution. The raw data were converted to graphs with the use of Excel. Finally, literature research was used in order to determine the parameters and factors that can shed light to vendors' mistakes.

5. Results

This section offers an analytical explanation of the results obtained by applying the methodology described under Section 4.

5.1 Hypotheses results

Regarding the testing of the first hypothesis it was found that there is indeed a positive correlation between the popularity of the browser and the number of severe-level vulnerabilities detected in it. Table 3 shows that the correlation between the two variables is 0,52 indicating a moderate positive relationship.

Correlations

		SV	Market_Share
SV	Pearson Correlation	1	,520
	Sig. (2-tailed)		,369
	N	5	5
Market_Share	Pearson Correlation	,520	1
	Sig. (2-tailed)	,369	
	N	5	5

Table 3: Pearson's correlation between the number of the severe vulnerabilities and the popularity of the browser.

Although the sample is really small (n=5), Figure 1 can be interpreted as a linear relation between the variables:

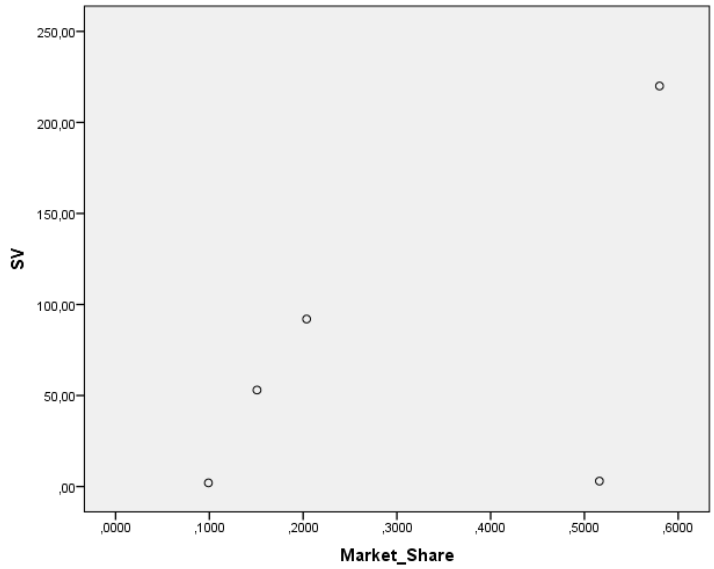

Figure 1: Scatter plot of number of severe vulnerabilities and market share of the browser.

The positive relation between the market share of the browser and the number of severe vulnerabilities is somehow an expected finding; it is a lot interesting creating high-threat vulnerabilities that can reach a large percentage of the population since the benefits of exploitation would be higher compared to less popular alternatives. Nevertheless this

relationship should not be extrapolated to the general statement that "browsers with less count of vulnerabilities are safer" (Wang, 2014); after all, simple bug count does not reflect severity and moreover disregards the fact that some of the vulnerabilities may not be published at all (Acer & Jackson, 2010). The only way to relate severity with the overall security of the browser is to look at numbers regarding the total attacks made on each of the web browsers. However, these are considered sensitive data and cannot easily be found from open sources.

The testing of the second hypothesis gave a Pearson coefficient of -0,56 (see Table 4) revealing that the number of severe vulnerabilities is related to the time between patches that the vendors release, but this time negatively.

Correlations

		SV	Patch_time
SV	Pearson Correlation	1	-,567
	Sig. (2-tailed)		,319
	N	5	5
Patch_time	Pearson Correlation	-,567	1
	Sig. (2-tailed)	,319	
	N	5	5

Table 4: Pearson's correlation between the number of severe vulnerabilities and the time between patches.

However, the scatterplot cannot be interpreted as showing a linear relationship since the dots are randomly dispersed in Figure 2. Thus, a linear relationship between these two variables cannot be confirmed.

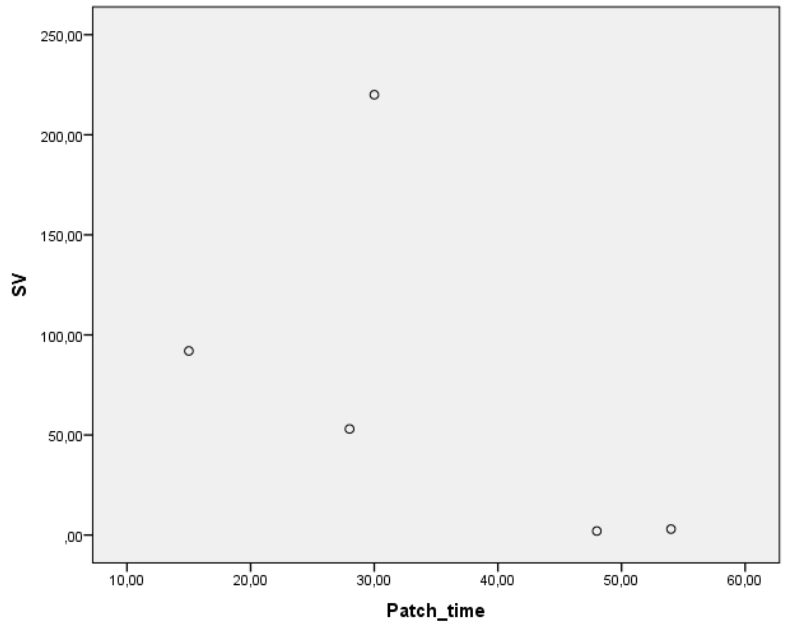

Figure 2: Scatter plot between number of severe vulnerabilities and time between patches.

This finding contradicts the literature which claims that vendors who respond immediately in order to fix the issue are the ones with the safer browsers (Wang, 2014). Hence, the

statement that browsers using faster updates benefit users since they will have vulnerabilities for a shorter period of time (Acer & Jackson, 2010) depends also on other factors; time between patches does not represent itself an indicator of less severe-level vulnerabilities in browsers. This can be reflected in the fact that vendors sometimes may address the vulnerabilities that are easy to fix quickly and neglect the more severe vulnerabilities (Accuvant Labs, 2011). Therefore, this metric cannot be related to the number of severe vulnerabilities in the browsers.

5.2 Research question results

The results derived from the NVD database for the distribution of severe-level vulnerabilities among the different categories of browsers can be visualized in the following graphs.

The first figure shows the total number of vulnerabilities that was found respectively in Internet Explorer, Google Chrome and Mozilla Firefox. As expected, the number of vulnerabilities is proportional to the popularity of the browser. As already explained, this is a reasonable finding since the more people use a browser, the more are the incentives to cause harm in the particular browser and affect this large percentage of users. Again, it should be noted that the data represented in the figure do not mean that Internet Explorer in the least secure browser and Firefox is the most secure; it could mean for example that Internet Explorer has the most vulnerabilities because it is easier for researchers to exploit the vulnerabilities and therefore pay more attention to Internet Explorer. Similarly, Chrome may be the second because it is a bounty program so again researchers pay substantial attention to it. Lastly, Firefox might have the fewer vulnerabilities because it requires more quality assurance before creating a patch. In short, the total count of vulnerabilities cannot stand as a succor in determining the safety of the browser.

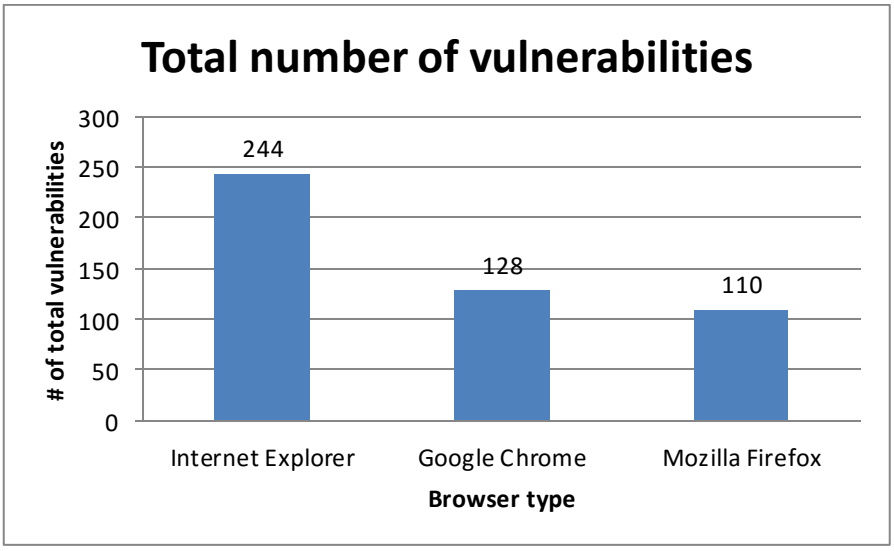

Figure 3: Total number of vulnerabilities for each browser in 2014.

One step further, Figure 4 shows how these vulnerabilities are distributed according to their CVSS scores. One might have expected that vulnerabilities of low criticality should be more

common in most browsers, however the data obtained for the year 2014 show the opposite; in almost all the three browsers the category "high severity" is significantly larger than the other two categories. The only exception seems to be Mozilla Firefox which has roughly an equal number in high and medium severity vulnerabilities. This confirms the statements of security institutions (Secunia, 2015; Symantec, 2015) that the majority of the vulnerabilities nowadays are mostly "critical". However, specific attention should be given to how exactly "critical" is defined. For the purposes of this research, a critical vulnerability is one that scores 7-10 in CVSS, as provided by NVD. CVSS is the most common standard used to classify vulnerabilities nevertheless its validity has recently been challenged (Holm & Afridi, 2015). More specifically, it was found that cyber security experts judged differently specific vulnerabilities presented to them than did the CVSS; the final conclusion was that experts believe that some vulnerabilities are scored higher than they should whereas others are scored lower. For this reason, it should be taken into account that the real numbers indicating severity might differ in reality.

Despite the fact that it might be reasonable to assume that a browser with more severe vulnerabilities is less secure in general, it should be taken into account that severity creates the urgency to issue a patch in order to fix it as soon as possible. For this reason it is naïve to draw the conclusion that Internet Explorer is the least secure, followed by Chrome and Firefox being the most secure based on Figure 4. The only conclusion that can be based on the distribution below is that Microsoft applies a higher risk rating to convey their message while Mozilla rates the vulnerabilities with a lower severity (Accuvant Labs, 2011).

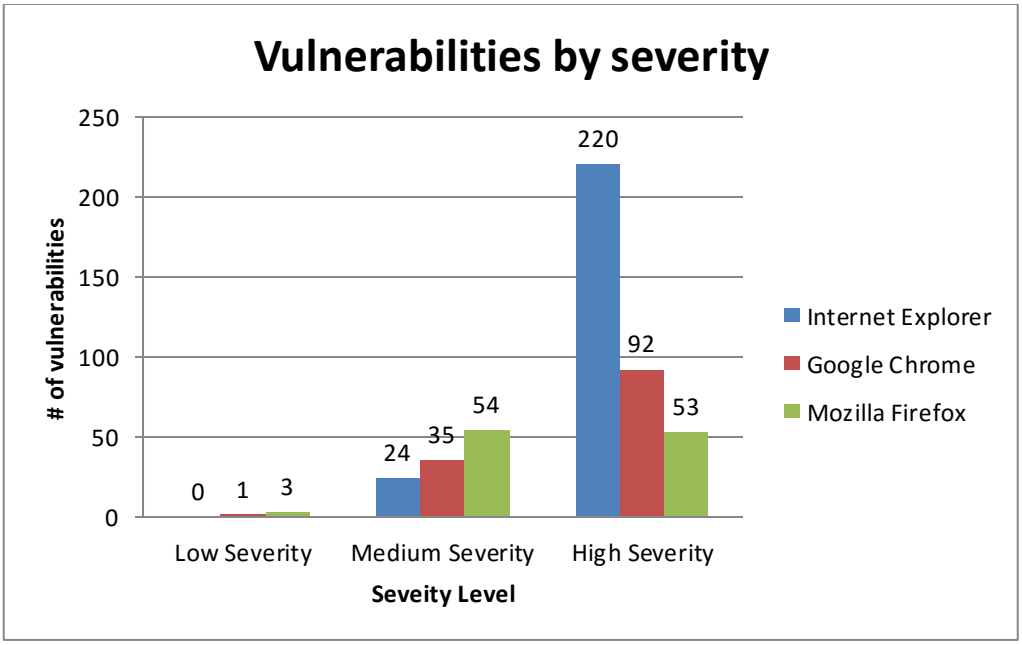

Figure 4: Number of vulnerabilities by severity for each browser.

According to these data, Figure 5 depicts the distribution of vulnerabilities for each browser separately. It can be distinguished a more triangular shape for Internet Explorer and for

Google Chrome, while for Firefox the shape is trapezoidal. A better comparison between the three web browsers can be obtained by studying Figure 6.

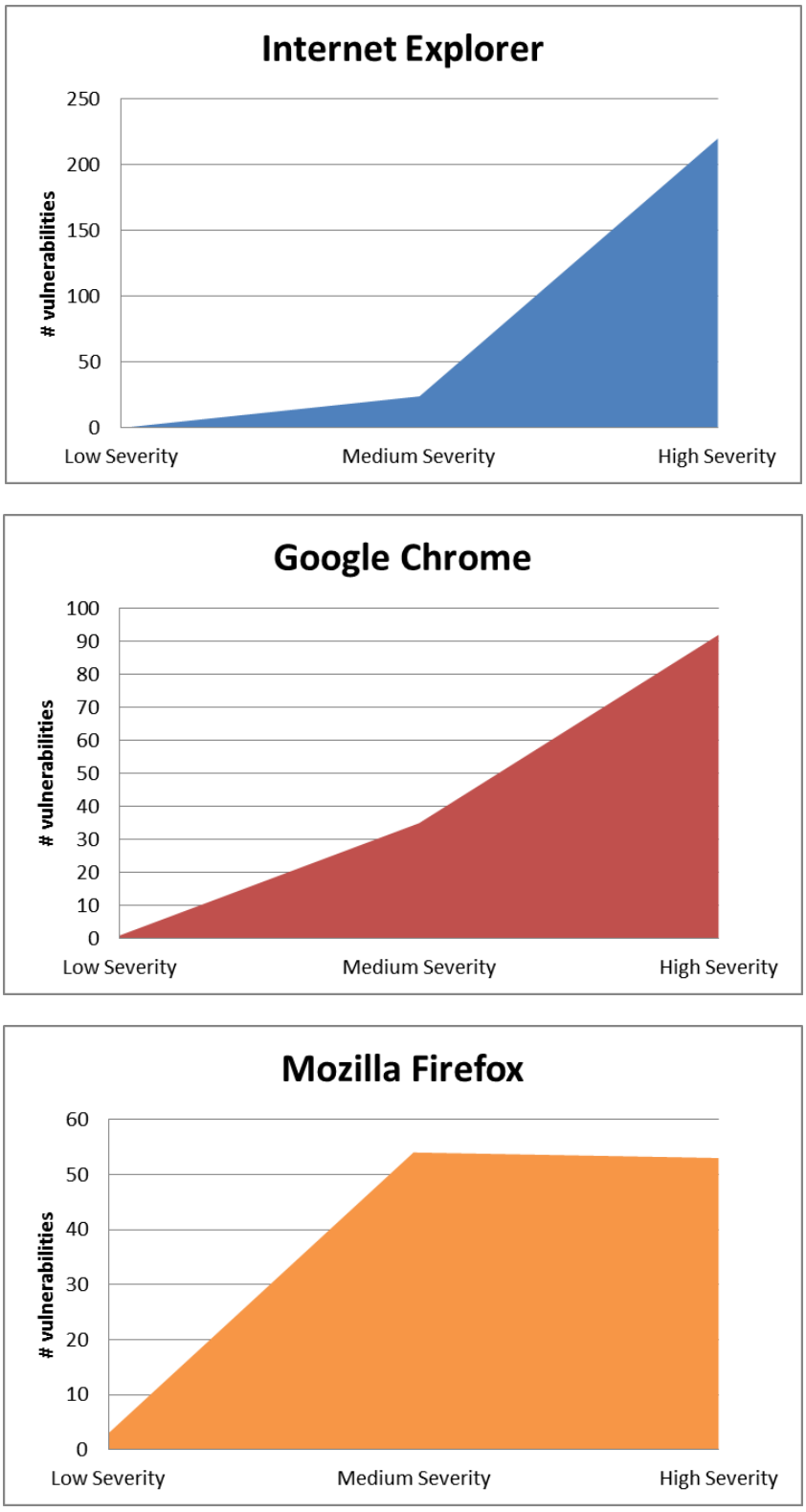

Figure 5: Distribution of vulnerabilities according to severity for each browser.

Since Internet Explorer and Google Chrome appear to have more "high severity" vulnerabilities, it would be interesting to investigate the kind of mistakes made by Microsoft and Google. Generally, literature identifies some of the incentives that vendors make vulnerable software being the "tipping point", lock-in effects, externalities and information asymmetries (Anderson & Moore, 2006). On the one hand, vendors are highly interested in winning the "tipping point", i.e. having the largest percentage of consumers using their product. For this reason it is essential that they release their products as soon as possible in order to dominate in an emerging market. On the other hand, vendors are much interested in creating lock-in effects; a lock-in situation refers to making it difficult for customers to abandon their programs. Additionally, the role of externalities is also a crucial factor determining the mistakes that vendors make. Knowing that the "costs" of vulnerable products will mostly be allocated to end-users, vendors have little incentives investing in making the browsers secure. Apart from that, information asymmetries can play a role in vendor's negligence; information asymmetry in software industry means that vendors might make claims about the security of their products however end users eventually might not trust them since there is no actual way to check the product's reliability. The aforementioned characteristics affect all three vendors discussed in this paper. Below, several reasons that can explain the distribution of Figure 5 and 6 and relate it to literature are being elaborated.

An argument for the large number of critical vulnerabilities in Internet Explorer could be that developers neglect safe coding since they are more interested in reaching the tipping point. As it is known Microsoft modified Internet Explorer, especially its first versions, in an effort to overtake Netscape's dominance (Oriyano & Shimonski, 2012). This urgency of releasing products quickly usually results in overlooking the safe coding techniques thus making the browser vulnerable. This resulted in Internet Explorer being stigmatized as a browser highly associated with security problems; this can raise the awareness of attackers who more actively search and find vulnerabilities in it, since it is historically proved that this browser can be relatively easily exploited. Hence, knowing that Internet Explorer suffers from security problems, makes the attackers to focus their attempts on finding and exploiting these problems. Apart from that, a third reason that explains the high number of critical vulnerabilities in Internet Explorer is that it uses Dynamic-Link libraries (DLLs) that interact with the browser's processes and add specific functionalities. However, DLLs can be a gateway for exploitations, making the users target for client-side attacks (Oriyano & Shimonski, 2012). Hence, the underlying operating system appears to be connected with the severe vulnerabilities found in Internet Explorer. It should also be taken into account that Internet Explorer by default saves information by up to 30 days in its browser history, while Google Chrome and Firefox both give the option to adjust the number of days. This wealth of information makes Internet Explorer an attractive target for the hackers. Therefore, these four facts can offer an explanation for the high percentage of severe vulnerabilities discovered in Internet Explorer.

Furthermore, an example that well illustrates the lock-in effect is Google's aim to make Google Chrome a lightweight product that offers higher security, speed and stability compared to other browsers. However, in its effort to design Chrome to not lack advantages

that other browsers have but also to be lightweight, Google made available many add-ons and extensions (Oriyano & Shimonski, 2012). Although these add-ons provide additional features to the users, they are highly vulnerable due to their similarity with web applications thus rendering the overall security of the browser lower (Shahriar, Weldemariam, Zulkernine, & Lutellier, 2014). Another explanation that Chrome has also a significant percentage of critical vulnerabilities is because of its openness which allows developers to directly work with the source code. Regarding both Chrome and Internet Explorer it should be noted that both browsers do not give the option to users to customize the list of phishing websites nor malware websites; this might be an additional explanation on why these browsers have a higher number of severe vulnerabilities. However, Google Chrome appears to have less severe vulnerabilities than Explorer due to the fact that its architecture is simpler and a no-frills browser equals to greater security because there are fewer paths that are interconnected.

Lastly, Firefox appears to have less severe vulnerabilities since it is used by a smaller percentage of people compared to the other two browsers. Another fact that can partially explain that Firefox has less severe-level vulnerabilities than the other two browsers is that users can configure many options through the security settings and keep their browsing safer. In addition, as discussed in Oriyano & Shimonski (2012), Firefox is based in many robust standards (such as HTML, XML) while it offers many security techniques like sandboxing and encryption for communications. The most important feature that has an impact on the vulnerabilities found is the "bug bounty", a program where developers and researchers can report flaws for a reward. This method encourages researches to actively report bugs preventing in this way attackers from exploiting these bugs.

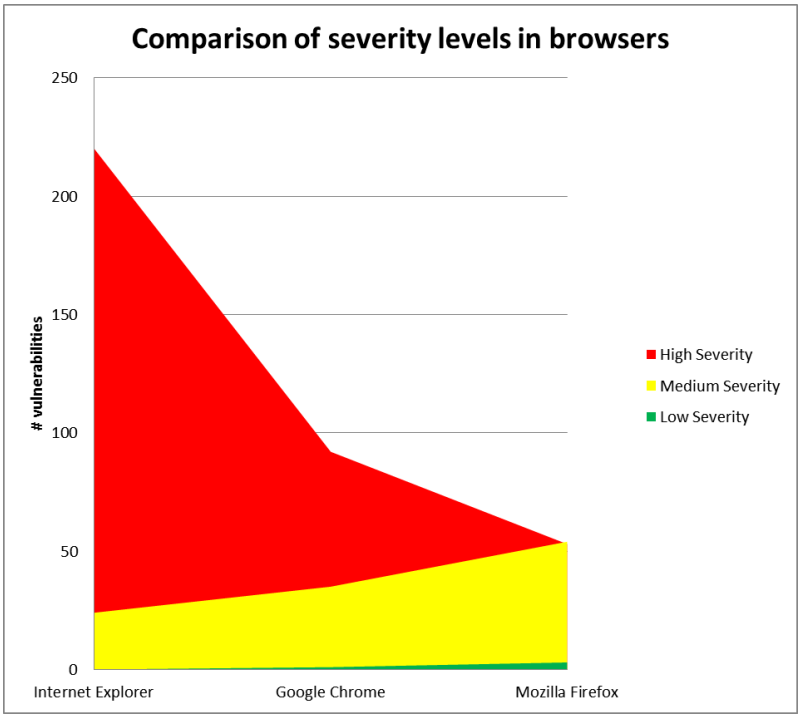

Figure 6: Level of severity of total vulnerabilities, compared for the three browsers.

As can be seen from the comparison graph in Figure 6, Internet Explorer has the largest percentage of severe vulnerabilities, followed by Chrome and then by Firefox. The pattern is exactly the opposite when it comes to medium and low severity, with Firefox possessing the largest percentage, followed by Chrome and finally by Internet Explorer. However, taking into consideration the whole discussion regarding the above results in this Section , it derives that the comparison of the percentages representing severe vulnerabilities in each browser cannot be a reliable estimator per se for the overall security of the browser; seeking an answer to this question requires obtaining from the companies the real data of attacks performed on their products and looking at more complex metrics that have to do with the architecture of the browser. The comparison, however, can shed light in the mistakes that vendors make while developing their products.

6. Limitations

This research, aiming to estimate the distribution of severe-level vulnerabilities among different browsers and relate them to the overall security of the browser, was subject to a number of limitations.

Firstly, there are several data available for the metrics however it is difficult to determine whether they are biased or not. For example, Secunia (2015) mentions that the number of vulnerabilities in 2014 were 504 for Google Chrome, 289 for Internet Explorer and 171 for Mozilla Firefox whereas the NVD database gives 128, 244 and 110 total vulnerabilities respectively. The same holds for the popularity of browsers; different sources mention different market shares for each browser. Moreover, several details regarding vulnerabilities such as the actual number of exploits per year per browser, are considered sensitive and thus there are no information available. This inconsistency makes it difficult to obtain a more complete view regarding the issue of overall browser security.

Secondly, the CVSS standard used to measure the severity of vulnerabilities is proven to be a subjective metric (Holm & Afridi, 2015) thus not capturing the real scores of certain vulnerabilities. Additionally, vendors can choose their own rankings for their advisories. Thus, it becomes even more complex to make cross-browser comparisons when the degree of subjectivity is so large.

Finally, the study did not take into account that a vulnerability's severity in isolation may be very different than when this vulnerability is combined with others; nevertheless, this cannot be determined since each vendor follows different ranking techniques. Hence, the conclusions to be drawn from the research are highly dependent on the availability of certain information, regardless whether it is accurate or biased.

For the purposes of this study, metrics that were related to previous assignments written for this course were used; these metrics were assumed representative for getting insights into aspects like security and vendors' behavior nevertheless it should be noted that there is a plethora of other metrics that can also shed light to these aspects.

A recommendation for further research on the topic would be to focus on more complex metrics, such as complexity of the browser, coupling and cohesion (Chowdhury & Zulkernine, 2010). Furthermore, the severity levels should be derived, if possible, from opinions of cyber security experts rather than based on standards such as CVSS. Generally, it should be well considered the fact that trying to make comparisons between browsers as well as analyzing the techniques that vendors use or the mistakes they make will remain a daunting task since most data are undisclosed mainly for marketing reasons.

7. Conclusions

This paper represents an empirical study with the aim to provide an answer to the research question *"How can the distribution of severe-level vulnerabilities found in browser categories be explained?".* The research was performed on the three browsers that hold the highest market share on desktop platforms, namely Internet Explorer, Google Chrome and Mozilla Firefox. The data collected referred to year 2014.

The methodology followed was a statistical analysis, based on data gathered from the NVD database as well as other sources of literature. The Pearson's correlation test performed to test the hypotheses that the number of severe vulnerabilities is one the one hand related to the popularity of a particular browser and on the other hand to the time between available patches, proved that the first hypothesis is indeed true while the second is not. More specifically, the number of severe vulnerabilities found in a browser is positively related to the market share that the browser possesses, whereas there is no correlation between this number and the time that vendors need to release a patch. The latter point does not support some other researches that use the time between patches as an indicator of browsers' security (Acer & Jackson, 2010; Wang, 2014).

Furthermore, the data collected from the NVD database at first place indicated that Internet Explorer is the browser containing the most severe-level vulnerabilities, followed by Google Chrome and then by Mozilla Firefox. It was found that the reason for obtaining such a distribution lies on several factors. Firstly, as regards Internet Explorer the large number of severe vulnerabilities can be explained by the notoriety of the browser's security that makes attackers to more actively seek for flaws. Microsoft's emphasis on having a large market share leads to neglecting safe coding techniques and this can also contribute to increased number of vulnerabilities. Apart from that, Explorer supports the use of DDLs which are linked up and usually open paths to the user's system making it more vulnerable. Concerning Google Chrome, the significant number of severe vulnerabilities can be attributes to both its open source code as well as to the several plug-ins that are offered to users and are highly vulnerable. What makes Chrome having less critical vulnerabilities than Explorer is its simpler architecture, since it includes lesser features than the other browsers in order to be faster and more secure. Finally, the reasons that Firefox appears to have the smallest percentage of severe vulnerabilities of all the three browsers is due to its robust standards, the several options of security techniques it offers and the "bug bounty" program, which gives high incentives to researchers to report vulnerabilities.

It should be noted at this point that although the distribution of severe vulnerabilities shed light on the mistakes that each vendor makes, it was not indicative of the overall security of the browser. This means that it is at least naïve to state based on the distribution that Mozilla Firefox is the safest browser. The level of severity creates the urgency to issue a patch in order to fix the vulnerability as soon as possible, thus the decision of users regarding "which browser is the safest to use" should be based on more complex metrics. A reason for not determining the overall reliability of the browser based on the count of critical vulnerabilities is associated with the limitations of this paper; On the one hand CVSS score that is used to rank the vulnerabilities is a subjective metric (Holm & Afridi, 2015) and

thus the distribution in reality might be skewed. On the other hand, the majority of the data regarding browsers, vulnerabilities and attacks are not a perfect reflection of reality since marketing plays a crucial role in modern societies. Therefore, a general conclusion is that economics can greatly influence the way people think; vendors might develop vulnerable products due to financial reasons and attackers seek to exploit vulnerabilities certainly for economic gains. Overall, the research conducted in this paper supports most of the existing literature (Accuvant Labs, 2011; Anderson & Moore; Holm & Afridi, 2015; Oriyano & Shimonski, 2012), while it pinpoints that achieving security in information systems is not only a matter of implementing technical measures, but also understanding people's incentives with the use of economics.

Bibliography

Accuvant Labs. (2011). *Browser Security Comparison: A quantitative Approach.* Accuvant Labs.

Acer, M., & Jackson, C. (2010). *Critical Vulnerability in Browser Security Metrics.* Carnegie Melon University.

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., και συν. (2012). Measuring the Cost of Cybercrime. *WEIS*.

Chowdhury, I., & Zulkernine, M. (2010). Using complexity, coupling, and cohesion metrics as early indicators. *Journal of Systems Architecture*, 294-313.

Holm, H., & Afridi, K. K. (2015). An expert-based investigation of the Common. *Computers & Security*, 18-30.

Leather, A. (2014, August 4). *Google Chrome Browser Market Share Tops 20%: Leaves Firefox In Its Dust.* Ανάκτηση October 30, 2015, από Forbes: http://www.forbes.com/sites/antonyleather/2014/08/04/google-chrome-browser-market-share-tops-20-leaves-firefox-in-its-dust/

Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, 103-117.

Oriyano, S.-P., & Shimonski, R. (2012). Security Issues with Web Browsers. Στο S.-P. Oriyano, & R. Shimonski, *Client-Side Attacks and Defense* (σσ. 91-105). Waltham: Elsevier Inc.

Secunia. (2015). *Secunia Vulnerability Review 2015: Key figures and facts on vulnerabilities from.* Copenhagen: Secunia.

Seltzer, L. (2014, November 11). *Why are there more browser vulnerabilities these days?* Ανάκτηση October 29, 2015, από ZD Net: http://www.zdnet.com/article/why-are-there-more-browser-vulnerabilities-these-days/

Shahriar, H., Weldemariam, K., Zulkernine, M., & Lutellier, T. (2014). Effective detection of vulnerable and. *Computers & Security*, 66-84.

Symantec. (2015). *Internet Security Threat Report.* Mountain View: Symantec Corporation.

Wang, A. (2014, August 2). *Are You Using The Most Secure Web Browser?* Ανάκτηση October 30, 2015, από SecurityWatch: http://securitywatch.pcmag.com/web-browsers/325447-are-you-using-the-most-secure-web-browser

Secunia.com,. (2015). *Resources Vulnerability Review 2015 Browser Security Secunia*. Retrieved 28 October 2015, from http://secunia.com/resources/vulnerability-review/browser-security/