Security Metrics - Review of group 9

Reviewed by group 14

Summary(motivation, methods, results, clarity)

In this assignment, the students investigate the metrics regarding a malware domain list. They first identify the anti-virus companies as their main actor. Afterwards, they state that the costs and benefits of security are of major importance for anti-virus companies, as well as the security level. 7 questions are crafted as ideal metrics. They found several non-academic, one academic and one consultancy report explaining the metrics used in practise. Combining the ideal and practical metrics, they came up with two metrics designed by themselves: a location based metric & the VirusTotal score. Finally, they evaluated the choice and graphical representation of their own metrics.

Strengths

- Existing Metrics used in practice: It is good to see that you have found some interesting reports on existing metrics used in practice, especially as they come from different fields.
- The assignment was well structured and easy to read, making it a very clear report.
- Evaluation: The evaluation of figure 6 is strong, since this was also a remark we made before reading chapter 5. This shows that you performed some critical analysis on your own metrics.
- VirusTotalScore: This is a very interesting suggestion for a metric as it uses the tools of multiple anti-virus companies. Also the idea of keeping a score and a treshhold for accepting a URL as malicious is pretty strong. However we would like to suggest to have a look at giving weights to the result based on which company gives which advice about the URL. For example you might want to give a heavier weight to Bitdefender giving the mark Suspicious than you would give to Avira giving the mark Malware.

Major issues

- Ideal Metrics: The suggested metrics are good. However a motivation about why these questions are important is missing. We would like to know what is the underlying goal of these questions.
- Existing metrics used in practise: Although 5 reports have been found, we only see a view examples of which metrics are used in practice. We would like to see more metrics which are being used in practice.

- Existing metrics used in practise: The explanation about the metrics that are used are sometimes very limited. For example when talking about software complexity metrics you mention Mcabe's Cyclomatic Complexity. It is nice to see an example, however we still do not understand what this metric actually measures. We would like to see a bigger elaboration on this.
- Figures 3, 4 and 5: Combine these statistics into one bar chart if you want to compare the companies, or leave two figures out if that's not the goal because they're three examples of the same metric. However if you do believe all the three figures are interesting, it would be best to give a motivation about why you choose to include these figures. These figures are (probably) taken from the other papers and we expect that they will be introduced there with some motivation as well.

Minor issues

- Introduction: References to 'malicious URLs', it is not explained how a user could actually be infected by a malicious website.
- Introduction: The narrative is unclear. The paragraph goes from explaining malware to explaining that it is problem for users and how antivirus company can aid users in that respect, which is quite a good way to understand the problem, but the link with how the antivirus company becomes the the main actor is unclear. We think this is the case because little attention is paid to what dataset is used for this research.
- Figure 1: a pie chart is not the best visualization because they're weak for displaying exact numerical percentages[1], we suggest using a bar chart.
- Figure 1: 'Other' is not a top 10 country. This problem is also solved when using a bar chart.
- Figure 3: We assume that the y-axis is times 1000 because figure 4 and 5 are in order of millions.
- Figure 6: We would advise to use a logistic scale on the y-axe, as this gives a less high peak on the USA and makes it easier to read the values of the other countries.

[1] https://www.quora.com/How-and-why-are-pie-charts-considered-evil-by-data-visualization-experts