Assignment Block 2 Group 6

Reviewed by group 1 12-10-2015

Summary

Organizations need additional insight in the vulnerabilities that threaten information systems. They need to determine which vulnerabilities are a cause for concern and which require less attention. The problem owner to this issue/desire is the security department of a private organization. Other actors that influence the security issue are business stakeholder/enterprises, developers and attackers. It is shown how the vulnerability landscape of an organization and the probability that a type of vulnerability is exploited can be mapped. Furthermore, some real security and best-practice security strategies are given for the problem owner. Those strategies include among others: application whitelisting, personnel training and ISO/IEC standard. For the business stakeholders/enterprises, developers and attackers, strategies are also given. They include Risk Modelling Process for enterprises, different coding techniques and ways for an attacker to find vulnerabilities. Finally, a ROSI calculation is given based on one of the strategies of a developer within the Financial Services Industry.

Strengths of the assignment

- Clear structure of the paper.
- The data of the metrics is used for the ROSI calculations.
- Good section about the Relevant security differences revealed by the metrics (except some small issues).
- The figure of the loss distribution is a nice addition to the ROSI calculation.

Major issues

Section: Introduction

- Make sure you repeat the important points of the previous assignment. For example: we had to look back to your previous assignment to see that your issue is: it is impossible to make a system complete secure.

Section: Problem owner and strategies to mitigate the security issue

- No major issues.

Section: Relevant security differences revealed by the metrics

- You say the following in your paper: only 1.5% of the of the known XSS vulnerabilities were reported to be used in malware, while 12.6% of the SQL-injection vulnerabilities were reported to be used in malware. Where did you find those numbers? We cannot find those numbers in your previous assignment.

Section: Security strategy

- How do your strategies refer to the security issue and the problem owner?

Section: Other actors that influence the security issue

- Section 5.1: Where did you get this information, it seems like you just made it up. Make sure to use proper references.
    - For example: Enterprises have lots of complex, poorly designed, overly interdependent applications they've feared to fix. This may not be the issue for all enterprises.
- Section 5.2: Same as above.

    - For example: Business stakeholders usually don't give enough time and resources to developers for them to pay enough attention and testing effort to look up for SQL injection and XSS vulnerabilities.
- Section 5.3 Same as above.
    - For example you state this: SQL injection vulnerabilities are the most common flaws exploited in injection attacks.

Section: Security investment assessment with ROSI

- It is not clear how you calculate the annual rate of occurrence, for example:
    - Why do you multiply the percentages of the 'always vulnerable', 'regularly vulnerable' and 'occasionally vulnerable' categories in figure 2?
    - You multiply by the percentage from the metrics 1 and 2 of the previous assignment, what are the percentages?
    - Why do you not just assume that the company falls into one of those categories?

Minor issues

Section: Introduction

- No minor issues.

Section: Problem owner and strategies to mitigate the security issue

- No minor issues.

Section: Relevant security differences revealed by the metrics

- Instead of mentioning metric one and two, it may be better to repeat the metrics.

Section: Security strategy

- Most of the strategies you mention are not strategies, but more methodologies or solutions. It is not a roadmap of what the problem owner should do to mitigate/remove the risk.
- The strategies are described shortly, it could be more extensive. For example:
    - Application Whitelisting: does every company have to do this by themselves or will there be a cooperation between companies.
    - Personnel training: how do you know if the training was effective?

Section: Other actors that influence the security issue

- How do the strategies refer back to the security issue and problem owner?
- 5.1: do enterprises need to use all strategies or choose just one?
- We think that there is missing a heading at the end of 5.3.
- You only needed to define risk strategies for the actors that can help to tackle to problem, attackers are not a positive influence.
- There may be more positive actors: researchers, security experts (who work on for example ISO), etc.

Section: Security investment assessment with ROSI

- There are missing some €-signs.

General:

- Your paper is readable, however there are a lot of minor spelling errors.
- The links in your references do not always work when clicked on.