Peer Review for Group 2 on assignment Security Investments

By Group 13: Rob van Emous, Rien Heuver & Patrick van Looy

Summary

In this report we see an overview of data-analysis on Chinese android app platforms. Different stakeholders are identified and one problem owner is appointed of further analysis: the user of apps. Then two metrics are defined based on the dataset. One calculates a fraction of malicious apps on the platform, the other the probability of a user download a malicious app. Various strategies are then explained for the user to minimize the risk of having his phone infected by a malicious app.

The remaining stakeholders are then further elaborated on and their respective risk strategies are outlined. We also see a side by side comparison of some stakeholders that have contrasting strategies and a note on how currently defined strategies might become obsolete in the near future because of the quick developments in the digital revolution.

At last we have a laid out plan of the managerial consequences if a certain risk strategy were to be implemented for a certain stakeholder: the ROSI calculation. We see here what the assumed ROSI would be if the owners of Baidu were to implement a scanner that'd be looking for malicious app on their platform which could in turn be used to inform developers.

Strengths

- Both metrics are very meaningful. It is clear from the report that if these metrics are evaluated on elaborate data, the outcome is of true added value.
- Not only the problem owner is explained in good detail, all other stakeholders are also extensively mentioned and so are their respective strategies: a very extensive analysis.
- The section *contrasting strategies* gives a nice overview of some potential problems if all stakeholders were to act on their strategies.
- The ROSI calculation in the end was performed on information obtained from the actual dataset. This makes the ROSI much more relevant and meaningful to your report and gives a clear indication of the importance of well defined risk strategies.

Major issues

- Throughout the paper, many assumptions are made which sometimes seem unreasonable and/or lack explanation as to why the assumption is feasible. For

example, the distribution of app downloads being uniform and the assumptions at ROSI.

- The metrics are based on a malicious app being flagged as such if it hasn't been updated for 50 days or more, based on the distribution of last-updated values in your dataset. This number could have been based on the time it takes for attackers to find vulnerabilities in an app for example. If nothing as such would have been achievable (by doing paper research), then please explain so.
- In the explanation of metric 1, you mention that a small platform will have a higher maliciousness ranking if its apps are not getting updated. This is only true if for both platforms a comparable absolute number of apps is lacking updates. However, since this intuitively seems to be based on a percentage, not an absolute number, this comparison seems faulty.
- For metric 2: why is the impact for a platform with many apps and many users only half if all apps are malicious? It seems like for both example platforms A and B the impact will be 1 with your given scenario.
- Your ROSI is based on the platform owner while your appointed problem owner is the end-user. It would seem fitting if the ROSI were based on your problem owner.

Minor issues

- Typo: table 1 mentions "p360" while the app store is called just 360.
- Metric 2: you mention that the impact is 0 if there are no malicious apps on the platform or that no app at all is downloaded from the platform. The latter condition should however be that no malicious app is downloaded, other downloads can still take place with the impact still being equal to zero.
- *Risk Strategies by Problem Owner (User)*: you mention "from the slides" without giving a reference or mentioning what slides you are talking about.
- By the end of the next paragraph you mention that iPhone users have more access control than android users. First of all, a reference would have been nice here. Second of all, this seems hardly relevant since the dataset is on android platforms. Why mention iPhone at all?
- In the ROSI section just before *Benefits* we see an overview of actual costs: some of these are ongoing costs and they do mention a number. However, since these are ongoing costs, it would seem logical to have the time frame on which these costs are projected.
- In common calculations of ROI (and thus ROSI), the result is a fraction or percentage. Your outcome however is a certain amount of money per year. Giving the ROSI as a percentage provides more meaningful information to decision makers.