Feedback on block 2 (Metrics)

Feedback on: Group 10 - Phishing Websites
Provided by: Group 1 - Vulnerabilities

Summary of the paper

The major security issue identified in group 10's paper is phishing, which involves using webpages (i.e. with the help of hosting providers) to trick people into providing personal information. The perspective of the hosting providers is taken for the assignment.

An ideal list of incident metrics, control metrics and prevented losses metrics have been listed to help in estimating the security level. Metrics already exist in practice, such as website take-down time and the number of visitors who provided their personal information.

Metrics such as TLD analysis, using the ping command and timestamps are defined in the document, but the volume of the dataset plays a disadvantage, and it only lists only pairs of URL and timestamps. Hence the group concedes that most metrics cannot be calculated from the existing limited dataset, and extensive data enrichment would be necessary, which is argued to be infeasible.

Strengths

- The scope was well-defined in the introduction.
- The taken point-of-view of the hosting providers is an interesting perspective. They have a problem in the real world, of which easily computable metrics could have a major contribution of solving the issue.
- Ideal metrics are well-defined, concise and informative.
- Multiple actor viewpoints are identified in the report, after which a specific viewpoint was taken.
- Useful references are used to base the report in theory.

Major issues

- The security issue named is “one can argue that the hosting provider is therefore at least partially responsible for detecting and taking down such websites”, but this is not a security issue. The victims targeted and values at stake are not made explicit in the description of the security issue.
- Some of the listed ideal metrics are well motivated (or self-explanatory), but for some metrics it is unclear what would be the added value for the chosen perspective of hosting companies. For example: “Distribution of user responses to phishing attacks”.
- In the final paragraph of defined metrics, there are some useful ideas to get some useful information out of this (rather limited) dataset. However, these ideas are not fully translated into concrete metrics that could give an indication of the security level. E.g. the defined metrics of the ‘TLD’ is unclear. What can be derived from TLD information? This is not explained.
- The contents of dataset have not been evaluated, and there are no graphical representations of metrics.

Minor issues

- The document is not in the format of a scientific paper, i.e. the methodology (although there are some elements of methodology in the ‘Defined Metrics’ section) and conclusion sections are missing.
- It seems unlikely that *‘number of unique clicks on the phishing websites’* is a metric used in practise, given it is nearly impossible to measure. The same goes for *“the percentage of the visitors of the website who provided legitimate information”*.
- Phishing is defined as *‘the act of attracting or tricking people into visiting fraudulent websites’* but this is not true: phishing induces individuals to reveal personal information through any means such as email and websites.
- The actor organisations is defined as ‘*whose websites the fraudulent pages try to resemble*’, but below in Ideal Metrics, in the first bullet point, it is stated that fraudulent websites are hosted within the organisation. In the fourth bullet point again: *‘in the company’*.
- In addition to the well-described actors you have listed, other actors could be victims in terms of organizations (unlike individual persons), and government bodies.
- It is said that analysis would not be feasible because it would take 5+ days, but this claim of this limitation is not backed up in any way. This makes it hard to find a possible solution to the problem as the base information is missing.
- *‘The only metric that could perhaps be done for all entries is doing a ping to see if they are still up’*. This claim could use a remark stating that their could be false positives as websites which are seized by an agency or hosting providing could still respond to ping requests, but the actual website could no longer be active.