Peer Review for Group 8

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

Summary

In the assignment, the group members assessed and created metrics with regard to Industrial Control Systems (ICSs). First, they explain the need for ICS security metrics. Then, they state their target security issue: disruptions of critical infrastructure (controlled by ICSs) and main actors: the owners of these ICSs. After these paragraphs, the four security aspects that ideal frameworks should target are explained. On top of that, they state the value of metrics that are understandable for all involved stakeholders (developer to CEO). Based on this, they state five ideal metrics. Then, six existing metrics and frameworks are discussed and an Applied Risk employee shares his practices regarding security metrics. Next, based on the dataset and the ideal and used metrics defined before, six metrics are designed and evaluated in detail. Finally, they conclude with the limitations and added value of their metrics to the users of ICSs and society as a whole.

Strengths

- All in all, the structure, thoroughness and clarity of the report is outstanding. Not only do the authors include all necessary parts, but they go a long way to find for example lots of *Existing metrics* and to squeeze every last bit of information out of their dataset during the metric evaluation. Well done!
- Nice to see that you actually involved an expert in this field (Applied Risk).
- Although not necessary, it is great to see ‘your’ definition of a metric before actually listing them.
- The evaluation of the metric *The number of firmware vulnerabilities*, is done very well. You limited yourselves to only examine the Siemens S7 devices, but as this was done thoroughly and was accompanied with a clear figure, it really showed the added value of this metric.

Major issues

- Claim in the introduction: *“The devices were not designed to be connected to the web in a safe manner”*. Why not? Reference?
- Although the metrics designed from the dataset were interesting and the evaluation of them based on the data of very good quality, a discussion of the extent to which the designed metrics impact the four security aspects (Controls, vulnerabilities, Incidents, (Prevented) losses), is missing. This should have been added to the conclusion (alongside with a visualisation like in the MOOC).
- In *Metrics that can be designed from the dataset*, your first metric *'Number of publicly accessible devices over time'* is not really clear. Does this mean devices that can be

bought on the market (meaning anyone can buy these devices)? Or do you mean active devices that can be accessed remotely (which is not supposed to be allowed)? If this becomes clear, then you can start explaining how this metric tells us something about the security level.

- Then, the next metric (forgive me for being a little bitchy *'update frequency'*), what do you mean with that? The frequency of which the manufacturer of the specific device releases updates? Or the frequency a device owner performs updates? If it is the case of the manufacturer, why does a lower update frequency mean that the device is more susceptible to exploits? Could it not just mean that there is no vulnerability for this specific device?

Minor issues

- An abbreviation should be written out fully the first time you use it and then in the rest of the document you can refer to the abbreviation. First sentence of the introduction change *ICS* to *Industrial Control Systems (ICS)* and refer to ICS in the rest of the document.
- Multiple times in the document you write *ICS system(s)/device(s)* which is double (Industrial Control Systems devices). Using just ICS or ICSs (plural) would have been better. Or explain when you are referring to a single device within an entire ICS.
- CORAS could use some more elaboration in the *Existing Metrics* section. Now you basically say CORAS uses UML, that’s it. How does this framework use it?
- The figure in the evaluation of the *Update frequency* metric is not clear. Above the figure, they state that the the figure shows the 10 most frequent version numbers of ICS software, but the labels on the x-axis sometimes are not even numbers or sensible characters. That is why the added value of this metric seems to be very limited in this case.