A Methodology to Measure the Cost of CPS Attacks Not all CPS Networks are Created Equal

DECISION: Accept

AUTHORS: Martin Rosso, Emmanuele Zambon, Luca Allodi and Jerry Den Hartog

Summary of Reviews

- Review 1: -1 (3)
- Review 2: 1 (5)
- Review 3: 2 (3)

Reviews

Review 1

Total score: -1

Overall evaluation: -1

Reviewer's confidence: 3

This paper addresses the development of a basic framework using two metrics to evaluate attacker costs in CPS domains. While the overall aim of the research is somehow discernible, there are aspects of the methodology and motivation that require clarification. Moreover, some claims lack sufficient support, and the scoring system appears to be somewhat disconnected from the intended goal of the method. Below is a detailed list of areas for improvement.

# Introduction / Motivation

The current motivation for CPS-specific analysis is not fully clear. The intro states that operators cannot transfer knowledge/best practices from one domain to another. While I do agree that there are differences across domains, the paper could be clearer (e.g., using examples) what type of best practices are not applicable across domains. Naively, I would assume that the "cost" of an attack will be composed of the same dimensions independently of the context, but the assessment of those cost dimension would be different depending on the CPS context.

Similarly, the underlying assumption of the paper is that attackers suffer some costs from acquiring the necessary knowledge to launch a cyberattack. However, I am wondering how this fits together with all the literature around cybercrime as a service. For years now, the analysis of underground markets and forums has shown that these costs can be lowered by the commoditization of attack services. This allows attackers to acquire the necessary tools and support to launch an attack without any knowledge. While this might be left for future work or out of the scope of this paper, it would have been great to have an exploration of the financial cost (price) of these services as offered in underground forums.

In the paper, it's crucial to distinguish between "knowledge", "capabilities" and "skills" to ensure clarity. I would see “knowledge” as the understanding and awareness of information, facts, and concepts necessary to launch an attack, while skills involve the practical ability to apply that knowledge effectively to perform tasks or solve problems. By clearly separating these concepts and justifying whether the paper/sections center on knowledge, skills, or both, readers can better grasp what the authors are trying to research.

# Research questions

The phrasing of the RQs could be improved:

- RQ1: unclear what is the goal of that knowledge. I infer from the rest of the intro, that the paper is referring to knowledge from the attacker perspective. But the question could be misunderstood as of knowledge for defending these attacks. Again, I am not sure this RQ is only about knowledge or about skills.

- RQ2: This question does not seem to be CPS specific which somehow contradicts the storyline of the paper. Moreover, it is unclear if “characteristics” refer to the attacker, the attack, the CPS context,…

- RQ3: The phrasing of this question seems to lead to an obvious ‘yes’ answer without any research necessary. I would assume that the paper wants to specify differences in “attacks”, “costs”, “attacker skills”, … or something more specific that just answering that CPS domains are different in nature.

# Cap/Ctx definitions

Section 2 start by claiming that established cost metrics do not fit the CPS context without any support for this claim. Again, it would be great to exemplify which cost metrics are not suitable for this context. Naively, one would assume that (for example) financial costs would apply to most contexts.

Section 2.1. argues that current metrics fail to capture the overarching cost of an attack because they are focused on exploits. This argumentation is not fully clear as the difficulty to create an exploit is directly related to the knowledge about the system and vulnerability that is targeting. Why is this metric not capturing “knowledge” by proxy?

My other concern with the current conceptualization of attacker costs is that they seem to be reduces to capabilities and context. However, when looking at the Appendix A.3., the context metric scores seem to be defined for the *defender* rather than the *attacker*. For instance, when reading the definition of the “legislation and Regulation” this seem to neglect law enforcement actions that might deter or increase the cost of an attack. I was expecting here something about the cost of launching an attack from countries with nonexistent cybercrime penalties or tax heaven for operating with money mules. As it is now, the scoring of the different context factors does not seem to be related to the attacker cost but mostly to the defender costs.

# Methodology

Section 4.1 states “the following inclusion criteria ensure that *all* considered CPS incidents are in scope”, but then it limits the attacks to only those with physical impact. This seems contradictory, as just by applying any attack filter not all CPS incidents will be in scope.

Given the likelihood that severe CPS attacks may not be publicly disclosed, relying solely on public data could skew the results towards less impactful incidents. Have you considered the implications of this limitation on the validity of your findings? Exploring strategies to mitigate this bias, such as accessing non-public datasets or incorporating qualitative methods, could enhance the robustness of the paper. The paper does acknowledge this as a threat to the external validity, but it would be good to help the reader gauge the potential impact of this validity threat.

# Results

Figure 3 talks about attack “price.” I am not sure this is a typo or a new concept that is somehow related to attack cost. Moreover, I am also not sure about the choice of violin pots given the data size. Maybe traditional boxplot would be more helpful to show also outliers.

Review 2

Total score: 1

Overall evaluation: 1

Reviewer’s confidence: 5

This is a particularly interesting topic and interesting method for making progress on that topic. Overall this is makes a good contribution which could be strengthened by greater connection to prior work (ISO/IEC 18045:2022), drawing out qualitative insights from the small sample size or increasing the sample size to make quantitative insights better supported, and by improving reproducibility.

Did you consider ISO/IEC 18045:2022:

ISO/IEC 18045:2022(E): Information security, cybersecurity and privacy protection Evaluation criteria for IT security Methodology for IT security evaluation. Standard, International Organization for Standardization, Geneva, CH (Aug 2022) it seems very relevant to what you are doing.

2.2 is much harder to follow than other sections.

4.1. "Relatively recent" is too vague for reproducibility, what is the actual date you used? I am also less clear on the justification as to why they need to be relatively recent. Do you expect the importance of these factors to have changed over time?

At the end of 4.1 I don't really buy the reproducibility argument as you could make public the necessary additional information to enable reproducibility. It would be a lot more work though and is potentially unnecessary.

This is a very quantitative study, it might be enhanced by also drawing out qualitative insights from the 25 analysed incidents. The statistics are really on quite small numbers…

Figure 4 has a scale from -1 to 1 but only values from 0-1. Either scale should run from 0-1 or some explanation is required in the caption.

It would probably be helpful to include the raw rating numbers for the 25 incidents in the appendix. It wouldn't take up much space. Making the dataset of URLs of reports used to substantiate those 25 incidents available would also be very helpful. Particularly if you used something like perma.cc or archive.org to ensure that there are links available that will keep working in the future.

6.2 "Our results qualitatively confirm general intuitions and observations made in previous literature" I think you mean "quantitatively" not much qualitative going on here.

In A.4 I might mention that you think this work will benefit the industry and not cause any additional harm.

Minor comments

Footnote 1 should be a reference.

Why is only the "al" in "et al." italicised at least sometimes? Perhaps you need a macro.

Potentially relevant (particularly in 2.1, but not necessary): "When will my PLC support Mirai? The security economics of large-scale attacks against Internet-connected ICS devices" Dodson et al. https://ieeexplore.ieee.org/document/9493257

Structure in section 2 and 3 feels like it could be improved not sure about a separate 3.1 subsection with two paragraphs, one of which repeats content from 3.0. I feel that you probably need a bit more prior to 2 introducing your strategy across 2 and 3.

Something has gone wrong with your table captions so that they overlap your tables.

Table 1 item 4 something odd is happening in the way your references are being displayed with 27-35 used but displayed as 27-29,30-33,34,35.

Figures 3 and 4 are too small. Text in figures should match that of surrounding text so that if the surrounding text can be read then so can the text in the figures.

Figure 3 needs some more detail in the caption (half a sentence or so).

I am not completely sure of the validity of violin plots of when the number of samples is so small.

ISO standards referenced should have corresponding references in the reference list.

Review 3

Total score: 2

Overall evaluation: 2

Reviewer’s confidence: 3

I really enjoyed reading this paper, which contributes to the efforts of costing cybersecurity incidents affecting industrial control systems and commonplace smart systems that takes into account preparedness and environmental factors.

The formal acknowledgment of the differences between ICS and BAS is a welcome contribution and will hopefully contribute to inform policy/behaviour in the field.

At first, the research questions appear disconnected from the structure and make sense at the end of the piece. It is recommended to add a paragraph after the questions to explain how the sections address them.

Three considerations about the method are as follows:

1. There is some lack of clarity around CAP and att@ack tactics, particularly whether some Att@ck are intrinsically less sophisticated. If this is the case, authors should add a table in Annex II ranking steps in the low, medium and high categories.

2. The authors rightly talk about the limitations intrinsic in raters. It is recommended that they validate their method with multiple raters.

3. In the CTX, law and regulation is a crude category. The presence of sector-specific legislation creates incentives which however do not mandate for the procurement of secure CPS components. There is currently no jurisdiction that mandates the adoption of secure software and hardware. On this point, see Maria Grazia Porcedda, https://link.springer.com/chapter/10.1007/978-3-031-57978-3_2 . The EU’s Cyber Resilience Act will be the first instrument to address this gap.

At the end of 2.1, the authors refer to various pieces of literature but cite none. Citations need to be added there. Perhaps this could be a good point to engage with the work of T Moore on the economics of incidents and with R. Anderson on measuring the cost of cybercrime?

At 4.1, authors should correct ‘contradicting ‘ with ‘ contradictory’

In 6.1, Q3, the authors could highlight how BAS vulnerability could lead to diffuse data breaches with devastating consequences.

As an aside, while the choice to leave the details to the annex makes for a leaner paper, it sometimes complicates the reading for an interdisciplinary audience, such as WACCO’s. But otherwise, this is an enjoyable paper which provides a clear contribution.