Investigating Episode Prioritisation in Alert-Driven Attack Graphs

Analysing PICA: A Novel Approach to Episode Prioritisation

Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology

1. Background

Alert Fatigue

Figure 1: Intrusion alerts leading to alert fatigue.

SAGE Compresses alerts into attack graphs (AGs) [1]

Large quantity/size of AGs → need interactive dashboard [2]

Figure 2: From alerts to AG interactive exploration.

Prioritising Attack Stages

Issue: current metric not granular and ignores paths

Proposed Solution: PICA (Paths, Integrity, Confidentiality, Availability)

Figure 3: The CIA triad.

2. Problem Definition

Baseline

$$Urgency(AS) = Prevalence(AS) \cdot Severity(AS)$$

PICA

Node urgency is the normalised in-degree × weighted CIA average
AS urgency is the average of the top X% urgent nodes

3. Methodology

1. How does PICA affect the **(number of) urgent attack stages**?
2. How are PICA's **urgent nodes position**ed in the attack graphs?
3. What are the **effects** of **changing** the **weights** in PICA?

4. Results

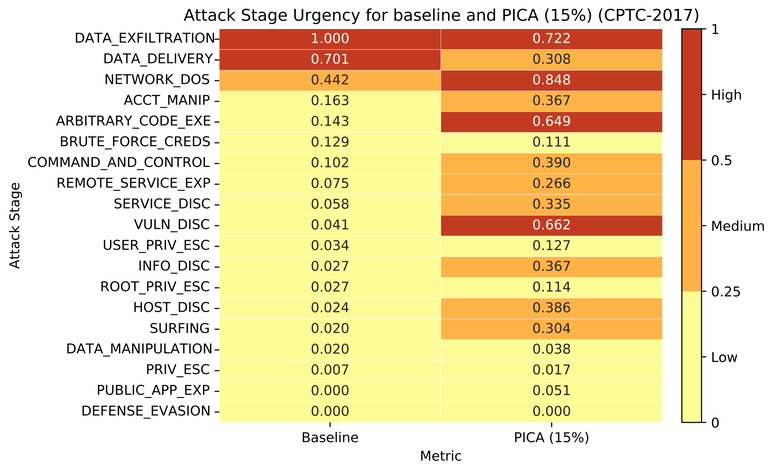

Figure 4: Urgency scores for baseline and PICA (15%) on CPTC-2017.

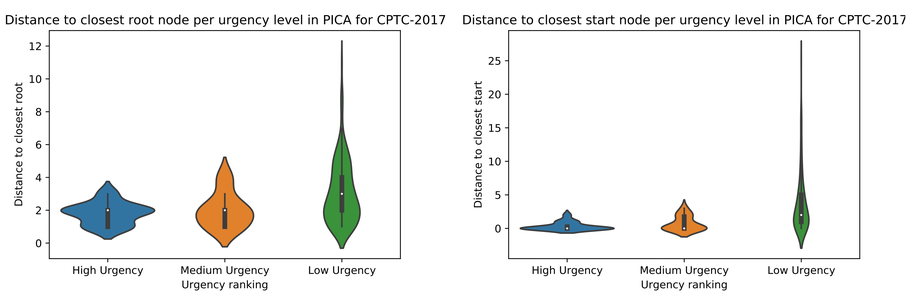

Figure 5: Distance to root node (left) and starting node (right) for nodes in different urgency levels in PICA (15%) for CPTC-2017.

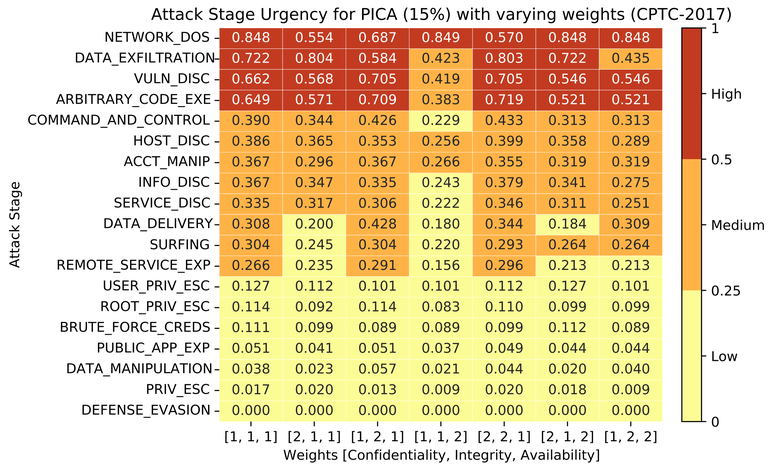

Figure 6: Urgency scores PICA (15%) with varying weights for the CIA triad on CPTC-2017.

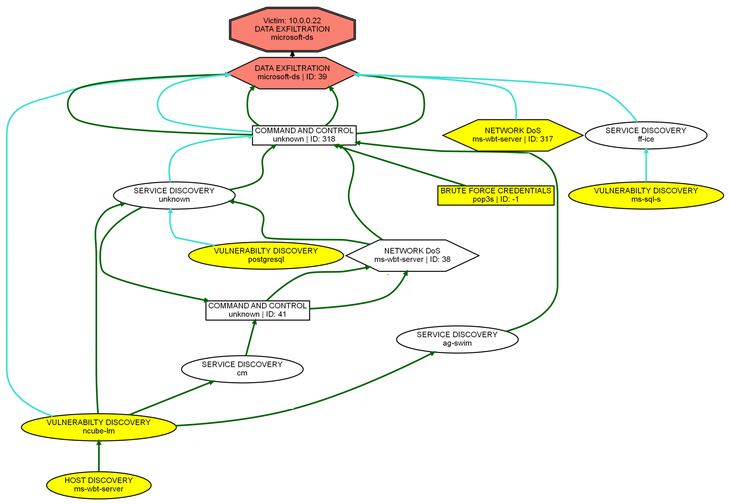

Figure 7: Example attack graph

5. Limitations

- Detection of many low-in-degree nodes
- Treats nodes as sequential
- Merging of low-severity nodes with (possibly) different context

6. Future Work

- Weighted node count, e.g. paths, objective distance
- Not merging low-severity nodes with (possibly) different contexts
- Different normalisation techniques
- Information loss in sub-graphs objectives

7. Conclusion

- PICA with 15% average a good balance between few urgent discovery attacks and retaining highly-urgent attacks
- PICA is more evenly balanced over the urgency levels, while baseline is more skewed
- Discovery attacks increase in urgency
- Objectives are often starting nodes
- Weights only have the desired impact on (close to) high-urgency attack stages

Contact

Student
Senne Van den Broeck
S.M.Z.VandenBroeck@student.tudelft.nl

Responsible Professor: Sicco Verwer
Supervisor: Azqa Nadeem

References

[1] Azqa Nadeem, Sicco Verwer, and Shanchieh Jay Yang. "SAGE: Intrusion Alert-driven Attack Graph Extractor". In: *Symposium on Visualization for Cyber Security (Vizec)*. IEEE, 2021.

[2] Azqa Nadeem, Sonia Leal Diaz, and Sicco Verwer. "Critical Path Exploration Dashboard for Alert-driven Attack Graphs". In: *https://vizsec.org/files/2022/vizsec_p4_abstract.pdf* (2022).