Investigating the Impact of Merging Sink States on Alert-Driven Attack Graphs

The effects of merging sink states with other sink states and the core of the S-PDFA

Authors

Jegor Zelenjak
contact: J.Zelenjak@student.tudelft.nl

Supervisor: Azqa Nadeem
Responsible professor: Sicco Verwer

Affiliations

Delft University of Technology

Security analysts have to manually analyse thousands or even millions of intrusion alerts daily. Attack graphs (AGs) can help visualise attacker paths. However, knowledge about existing vulnerabilities and network topology is required. [1]

1. Background

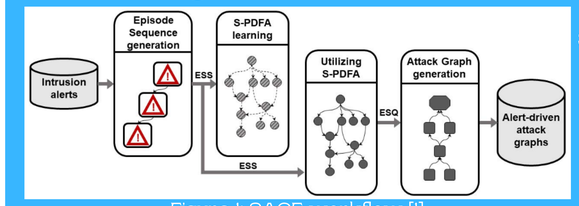

Figure 1: SAGE workflow [1].

SAGE: create AGs from alerts [1].

- Severe alerts are infrequent
- Same alert ≠ same behaviour
- Interpretable + explainable
- No expert knowledge needed!

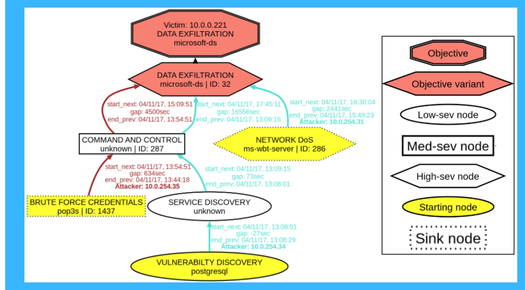

Figure 2: Attack graph.

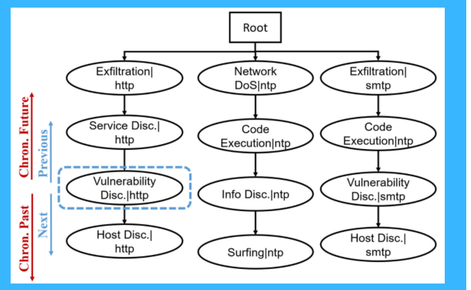

Figure 3: Suffix-based probabilistic DFA [1].

2. Problem

- No ground truth? ⇒ Try different modelling assumptions ⇒ Pick the best
- Infrequent data? ⇒ Sink states (not touched in the S-PDFA) ⇒ Larger AGs

Try merging sinks with other sinks and the S-PDFA core (after the main merging process)

3. Methodology

Figure 4: Experimental workflow.

- Collegiate Penetration Testing Competition dataset (2017 and 2018)
- Original SAGE vs modified SAGE

Chosen metrics

- **Size** (hypothesis: decreases)
- **Complexity** (hypothesis: decreases)
- **Interpretability** (hypothesis: decreases)
- **Completeness** (hypothesis: decreases)

4. Results

- **Size** (result: slightly decreases)
- **Complexity** (result: about the same)
- **Interpretability** (result: decreases)
- **Completeness** (result: the same)

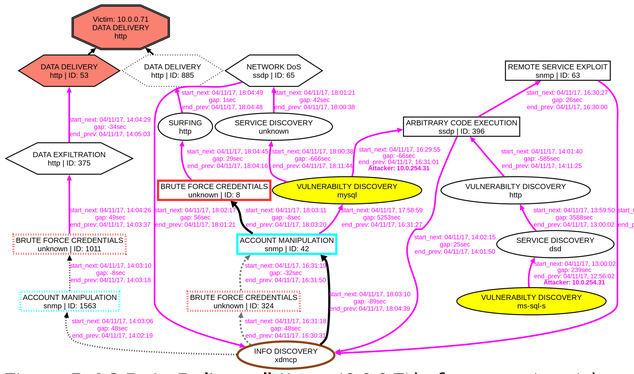

Figure 5: AG **Data Delivery|http** on 10.0.0.71 before merging sinks with other sinks and the core of the S-PDFA.

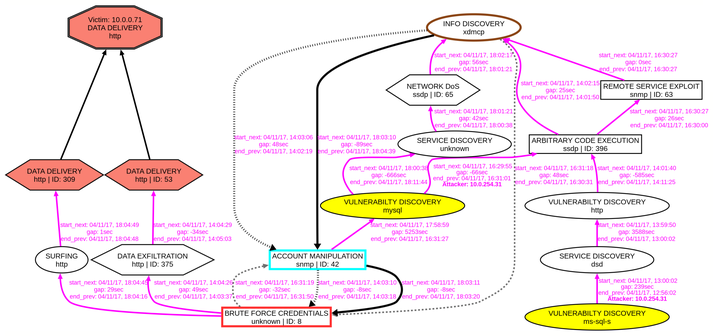

Figure 6: AG **Data Delivery|http** on 10.0.0.71 after merging sinks with other sinks and the core of the S-PDFA: an example of a loss of context (see Figure 7 for the merge in the S-PDFA).

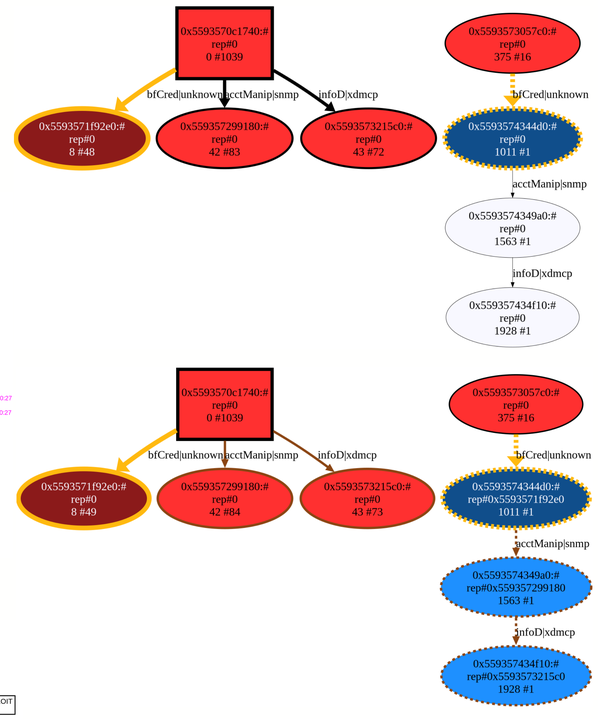

Figure 7: the corresponding merge of state 1011 with state 8 in the S-PDFA (yellow); further merges of state 1563 with state 42 and state 1928 with state 43 (brown). This merge results in the loss of context in the attack graph in Figure 6.

5. Conclusion

- Smaller attack graphs cannot compensate the worsened interpretability
- Merging sinks with the core and other sinks does not seem promising
- A new tool to investigate S-PDFA merges: get-merges.sh
- Other modelling assumptions regarding merging sinks could be tested

References

[1] Azqa Nadeem, Sicco Verwer, Stephen Moskal, and Shanchieh Jay Yang. Alert-driven Attack Graph Generation using S-PDFA. IEEE Transactions on Dependable and Secure Computing (TDSC), 2021.

TU Delft