Using Machine Learning for Detection of Advanced Persistent Threats

ANOOP SINGHAL[1]; QINGTIAN ZOU[2]; XIAOYAN SUN[3]; PENG LIU[2]

[1]COMPUTER SECURITY DIVISION, NIST; [2]THE PENNSYLVANIA STATE UNIVERSITY; [3]CALIFORNIA STATE UNIVERSITY, SACRAMENTO

Introduction

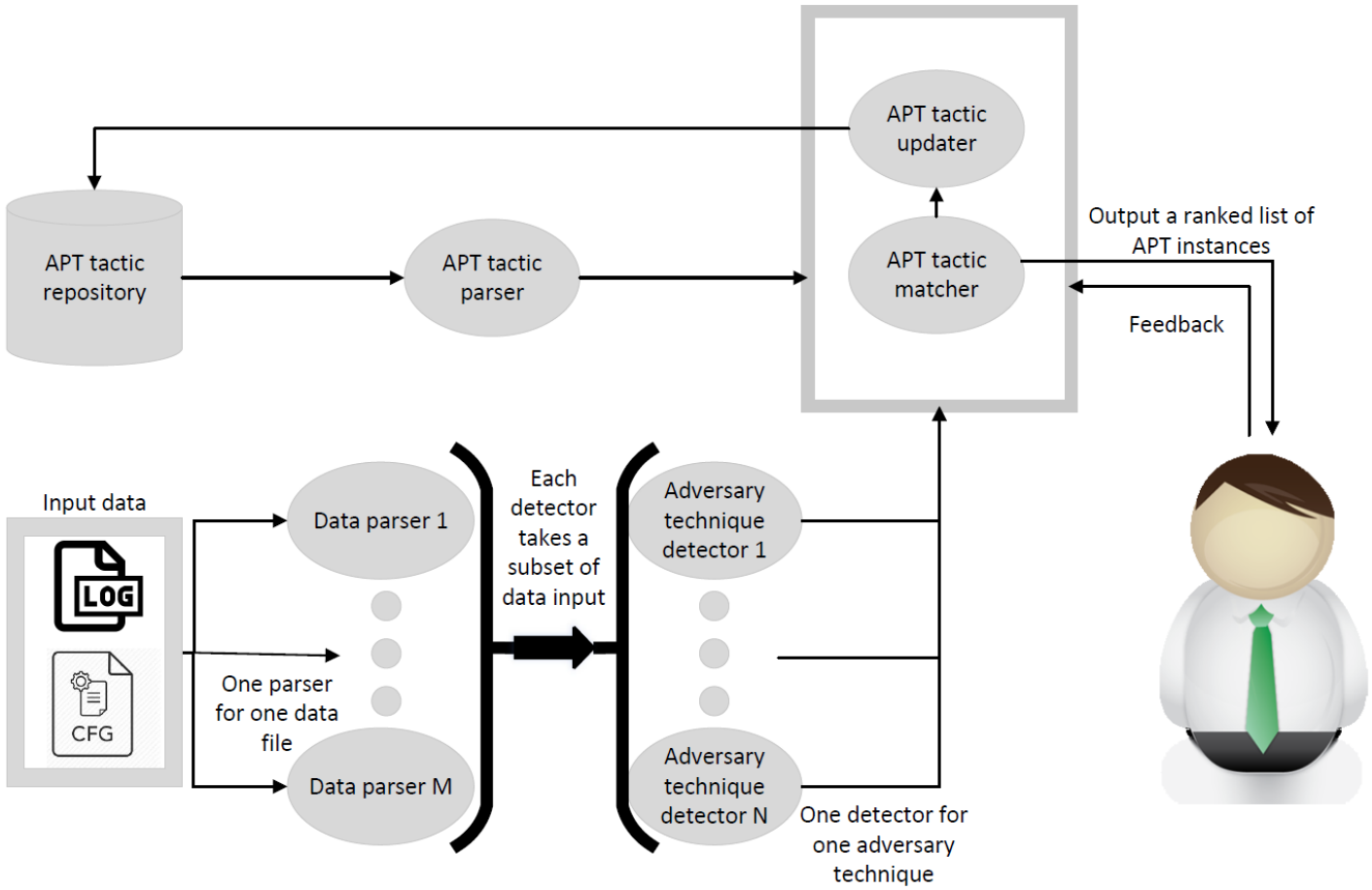
- Advanced Persistent Threat (APT) has become a big concern for enterprises, organizations and governments world-wide. Such attacks usually employ certain tactics, which may consist of different techniques in multiple attack steps. By recognizing the APT tactics the attacker is using, system administrators could deploy precise defense strategies and techniques accordingly.
- Many research works have been carried out to either detect an individual technique [1,2] or detect APT tactic as a whole [3, 4]. However, no existing framework or solution can simultaneously achieve accuracy and general applicability.
- We propose a framework that uses machine learning to automatically detect which APT tactics the attacker is following. The framework takes previously seen APT tactics, logs and system configuration files as input, and generates a ranked list of APT tactics based on how likely a tactic is followed by the attacker. The framework can also update the previously seen APT tactics in case the attacker changes his or her strategies.

Objectives

Develop a framework that is able to automatically:

- Detect individual APT techniques;
- Deduce how likely any known APT tactics are being used;
- Update known APT tactic repository if the attacker changes his/her attack strategies;
- And achieve accuracy and general applicability in detecting APT tactics.

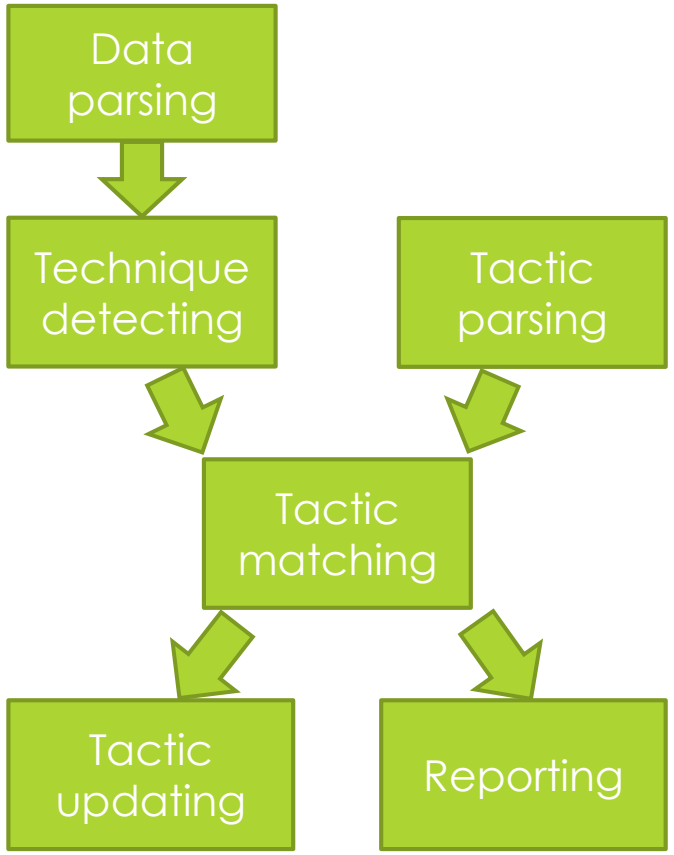
Proposed Framework



- **Inputs** includes (1) known APT tactics; (2) IT system information (e.g. logs and configuration files); (3) user feedback for online machine learning.
- **Data parsers** parse different types of system information.
- **Adversary technique detectors** detect different individual adversary techniques.
- **APT tactic parser** parses known APT tactics that are provided as files, such as DOT code files that can be visualized by Graphviz [5].
- **APT tactic matcher** matches the detected adversary techniques to one or more parsed candidate APT tactics.
- **APT tactic updater** adds newly found APT tactics to the APT tactic repository.
- **Outputs** include (1) a ranked list of APT tactics to the user; (2) newly found APT tactics to the repository.

Architecture

- **Data Parsing.** The collected data sources are first fed to the corresponding data parsers.
- **Technique Detecting.** Based on parsed data, the adversary technique detectors will determine whether certain adversary techniques are present or not.
- **Tactic Parsing.** The previous-seen APT tactics, which are stored in the APT tactic repository, are fed to the APT tactic parser.
- **Tactic Matching.** The APT tactic matcher will match the detected adversary techniques to one or more candidate APT tactics.
- **Tactic Updating.** When new variants of APT tactics are found, the frame- work will add newly found APT tactics to the APT tactic repository. In this way, the framework is consistently updating its tactic knowledge base.
- **Reporting.** At the end of tactic matching, the APT tactic matcher will report its results as a ranked list of "most likely" APT tactics (they are ranked based on likelihood).



Conclusions

We propose a framework for detecting APT tactics from logs and configuration files. The framework takes previously seen APT tactics, logs and system configuration files as input, and generates a ranked list of APT tactics based on how likely a tactic is followed by the attacker. The future work is to implement, validate and evaluate this framework.

References:

1. Milajerdi, S. M., Gjomemo, R., Eshete, B., Sekar, R., & Venkatakrishnan, V. N. (2019). HOLMES: Real-time APT Detection through Correlation of Suspicious Information Flows. *2019 IEEE Symposium on Security and Privacy (SP)*.
2. Oprea, A., Li, Z., Norris, R., & Bowers, K. (2018, December). MADE: Security Analytics for Enterprise Threat Detection. In *Proceedings of the 34th Annual Computer Security Applications Conference* (pp. 124-136). ACM.
3. Shen, Y., Mariconti, E., Vervier, P. A., & Stringhini, G. (2018, October). Tiresias: Predicting Security Events Through Deep Learning. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 592-605). ACM.
4. Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, *89*, 349-359.
5. Graphviz - Graph Visualization Software, https://www.graphviz.org/