ReasONets: A Fuzzy-based approach for Reasoning on Network Incidents

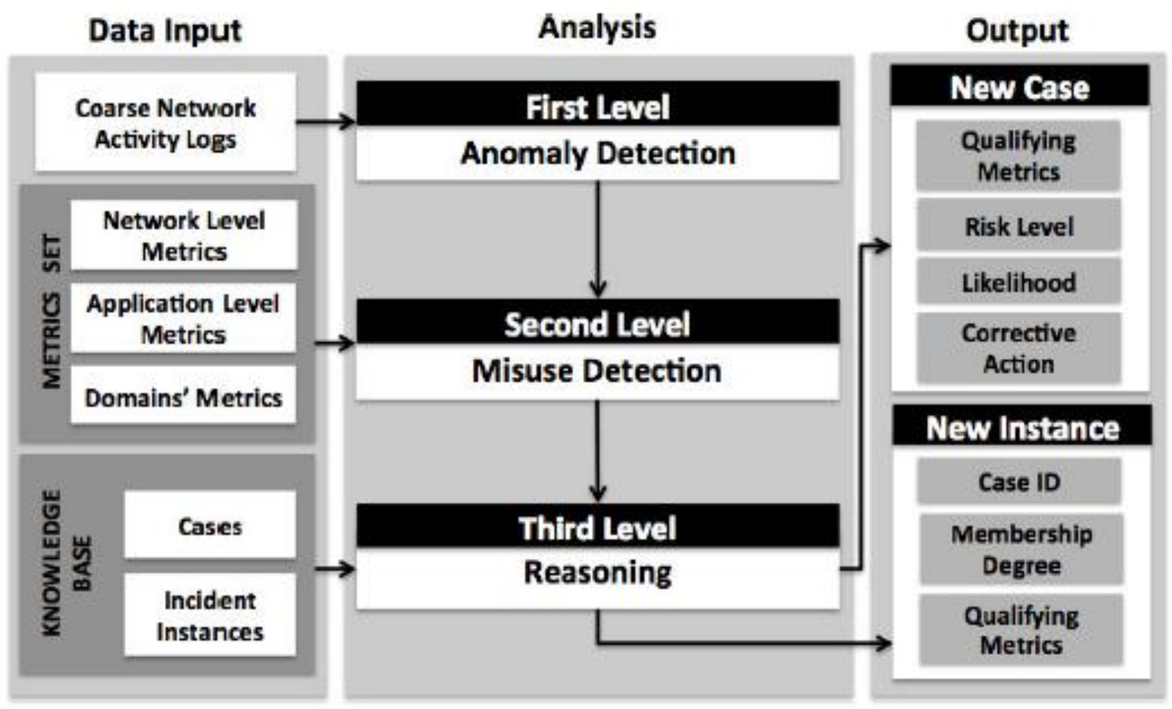
Giuseppe Petracca, Anna Squicciarini, William Horne and Marco Casassa Mont.

Project Objective

- Provide an approach for deeper and real-time understanding of ongoing events in a monitored network.
- Accurately detect anomalies in the behavior of machines and inappropriate use of the network.
- Identifying the nature and severity of the observed security incidents, by efficiently limiting the quantity of needed information.

Our Approach

- First system combining detections and classification of network events with real-time reasoning.
- Use of Fuzzy Ranking for disambiguating incidents, in case a clear mapping to known cases cannot be determined.
- Inference on completely unknown domains, plus early identification of malicious domains, and inference on their relationship with well-known malicious domains.



Case Retrieval and Analysis – Key Steps

1. **Rank candidate cases** by producing **Membership Degrees** for the incident.
2. **Verify presence of a dominant case**. Select first k Nearest Neighbor cases from the set of ordered cases. Check cohesion of the k-NN. Search a dominant case. If a dominant case is found, we model the incident as an instance of it.
3. **Apply fuzzy ranking**. We compute an additional ranking for each case in the previous k-NN set. Fuzzification and Defuzzification functions employed with the purpose of values normalization.
4. **Create a new case**. If not possible to find a dominant case, classify the incident as new case by starting the case profiling process. Store it in the KB.
5. **Merge cases**. Model periodically optimized: if several incidents with same features are mapped on the same subset of cases merge them in a single case.

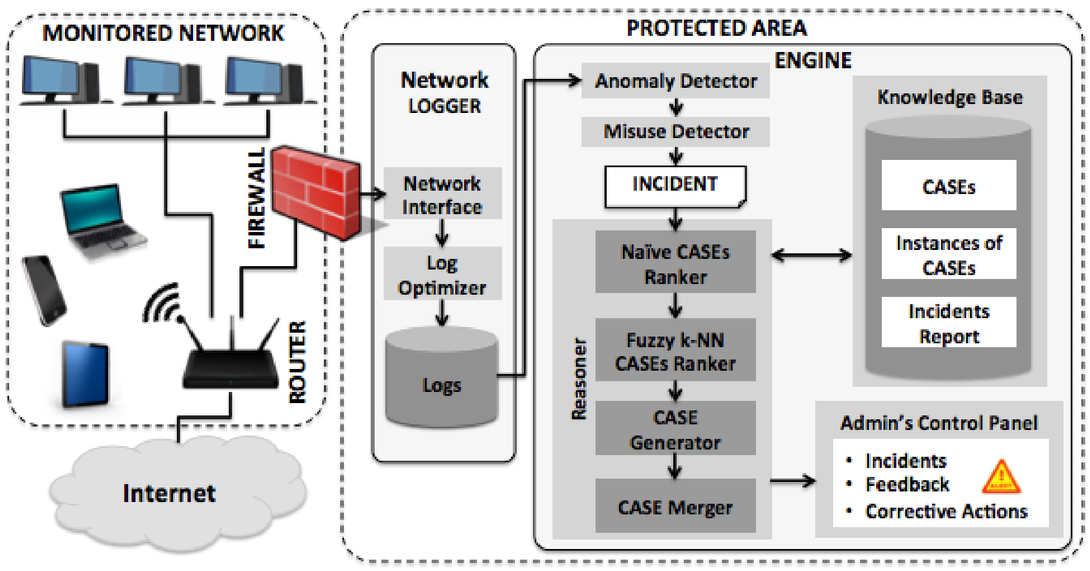
Membership Degree

$$m_{inc}(c) = \frac{\sum^{inst \in c}\left[m_{inst}(c) \times \sum^{|f|}\left(\beta - \left\|\frac{inc(f)}{\left(\frac{\alpha(f)}{\beta}\right)} - \frac{inst(f)}{\left(\frac{\alpha(f)}{\beta}\right)}\right\|\right)\right]}{\sum^{|f|}\left(\beta - \left\|\frac{inc(f)}{\left(\frac{\alpha(f)}{\beta}\right)} - \frac{inst(f)}{\left(\frac{\alpha(f)}{\beta}\right)}\right\|\right)}$$

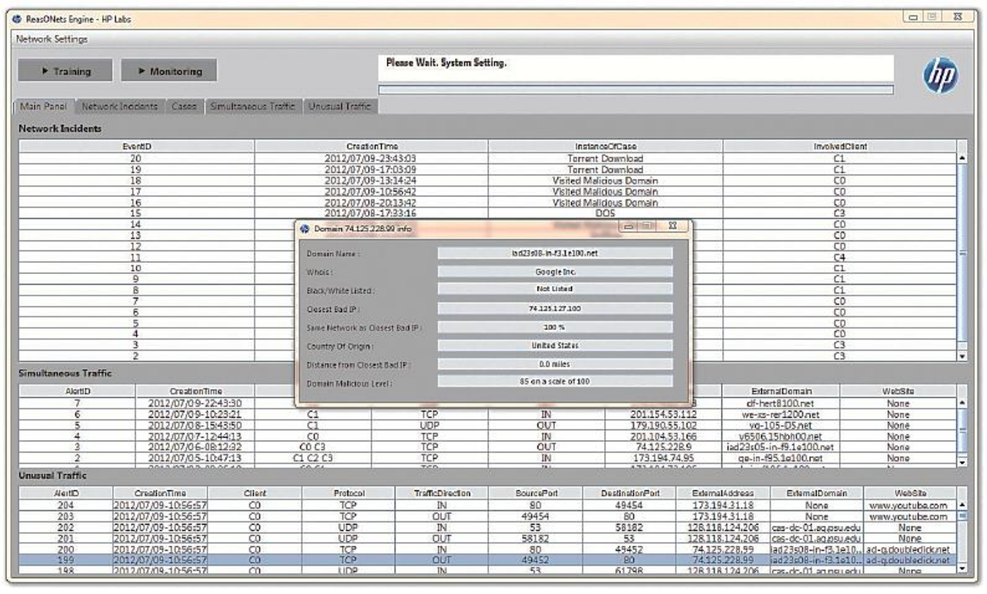
Fuzzy Ranking

$$r_c \times p_c \times \left(\sum^{|f|} w_c(f) \times Defuzzy\left[\beta - ||Fuzzy\left(inc(f)\right) - Fuzzy\left(c(f)\right)||\right]\right)$$

The ReasONets Architecture



Graphic User Interface



A research project sponsored by **Hewlett-Packard Labs** in collaboration with the College of Information Sciences and Technology**, Penn State University.**

Contact: gxp18@psu.edu