Hybrid Rule Threshold Adjustment System for Intrusion Detection

Mohamad Mehdi Moghimi
Research Staff
Sepehr Sadra Tehran Co. Ltd.
Tehran, Iran
moghimi@sepehrs.com

Mohamad Saraee
Assistant Professor, ECE Department
Isfahan University of Technology
Isfahan, Iran
saraee@cc.iut.ac.ir

101110100101001001010100100100010001110101100100111101010101011001001000111

8th International ISC Conference on
Information Security and Cryptology - ISCISC2011

101110100101001001010100100100010001110101100100111101010101011001001000111

This work has been supported by
ICT Security Research Center of Malek Ashtar University of Technology -Tehran Campus.

Outline of the Presentation

- Introduction
- Background
- Our Proposed Framework
- Testing and Evaluation
- Conclusions
- Questions from Audiences

Motivation

- Challenge:
  - Huge volume of Alerts Generated by Security Devices such as IDSs (It is hard to make sense out of a large pile of alerts!)

↓

we need alerts correlation

  - Computer Networks are changing over time. (Correlation rules become out of tune!)

↓

Rule-based Alert Management System should be adapted to this changing

- Solution:
  - Automatic Rule Adjustment

Alert Management System Adaption

- This Adaption can be achieved by adjusting the existing rules.
- Two types of automatic adjusting of the rules can be used:
  - Rule Structure Refinement.
  - Rule Threshold Adjustment.
- But, which one is more suitable solution?!!!

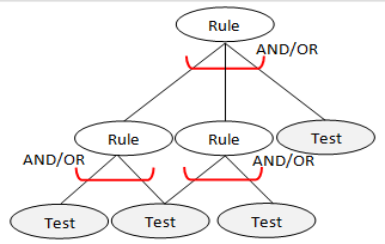
Rule Threshold Adjustment (cont..)

- Can be breakdown into
  - Online Threshold Adjustment.
  - Offline Threshold Adjustment.
- Aim: to develop a *Hybrid Rule Threshold Adjustment System* (HRTA) .

Background: Rule (Correlation Rule)

- Definition: a logical combination of conditions which if satisfied leads to triggering of actions specified by that rule.
- Every rule consists of two main parts:
  1. *Condition* part
  2. *Action* part
- The condition part of a rule consists of logical combination of tests and other rules.
  - Test Definition: a Boolean function defined on an input parameter
    - Numerical parameter such as IP, Port Number,…
    - Descriptive parameter such as attack type,…

Background: Rule ----(cont.)



Typical Rule Structure

Background: Existing Works on Rule Adjustment

- Rule Structure Refinement

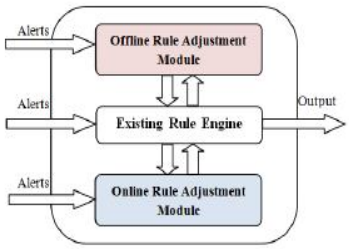
1. **SEEK and SEEK2**
   - Automatic knowledge-base refinement system
   - adding, deleting, or altering the rule-components in a knowledge base system.
2. **FOIL , GOLEM , and SILT**
   - based on the inductive logic
3. **TopGen**
   - Extension of KBANN

Background: Existing Works on Rule Adjustment (cont.)

- Are these solutions adequate?
  - rules are generated based on the expert knowledge and we can not modify their structure.
  - rules are very specific to catch certain attacks or network misconfiguration.
  - So, Unfortunately, **No**!!!!
- We need to design a new system which will be able to adjust the thresholds inside the rules based on the current environment of the network.
- To the best of our knowledge, no previous work on Rule Threshold Adjustment has been reported.

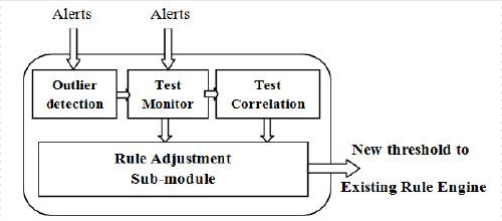
HRTA Framework

- Online adjustment:
  - more memory efficient and fast
  - prone to small error.
- offline adjustment
  - more memory and CPU intensive
  - more accurate.



Online Part

- Comprised of three steps:
  1. Monitor tests behavior to detect network changes.
  2. Determine whether the change is stable or not.
  3. Compute the new threshold.

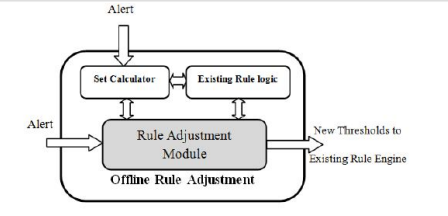


Online part

- For more details please see:
  - M.M.Moghimi, M Saraee, " A New Framework for Online Rule Threshold Adjustment in Intrusion Detection" IEEE CSI/ CSSE (2011).

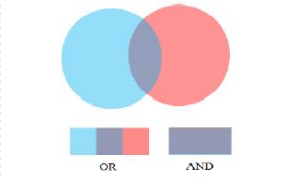
Offline part modules

- Set calculator: event set calculation for each of the rules and tests.
- Existing rule logic: holds the rules hierarchy that we are going to adjust.
- Rule adjustment: holds the offline adjustment algorithm



(Event) Set Calculator

- This calculation can be done by considering rule hierarchy!
- OR Condition: Union of the children sets
  - parent node inherits the number of events resulting from all children nodes
- AND Condition : Intersection of the children sets
  - the parent node gives at most the smallest event set of any of the children



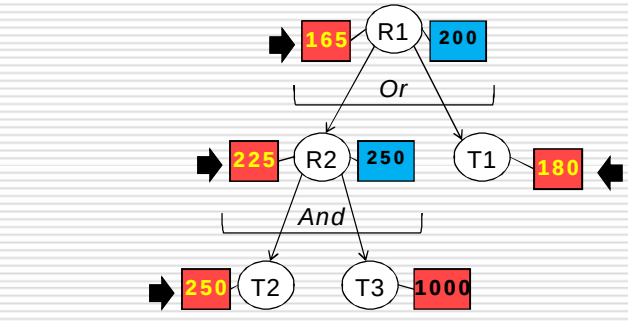
Adjustment algorithm for offline-part Adjustment(x)

```
1.  event_set= event_set_computation(x); // initial event set computation based on DFS

2. if (|event_set| > optimal_threshold(x))
    do{
       for(each branch of the node)
          if (a branch has OR condirion)
            node =select_L(x);//select child node of x with the largest set
          if (a branch has AND condition)
             node =select_S(x);// select child node of x with the smalles set
       if(node is a leaf) test_adjustmnet(node);
       else adjustment(node);
       new_event_set= event_set_computation(x);
    }until(|new_event_set|<= optimal_threshold(x))

3. add_to_rule_logic(x);  existing rule logic update with new thresholds
```

Example



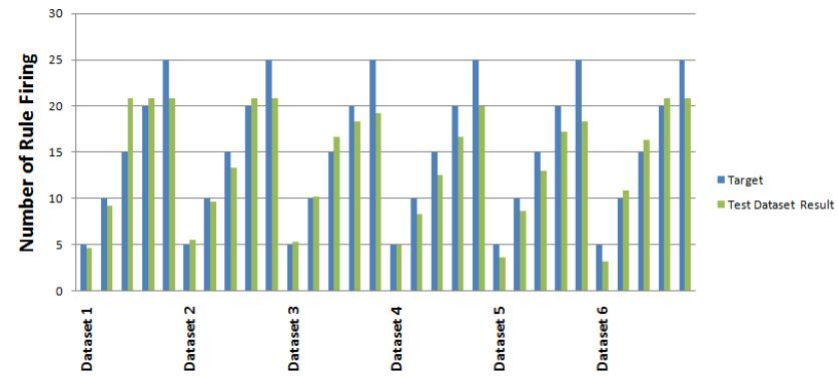
Cardinality of the event set for the node

Optimal Threshold for the node

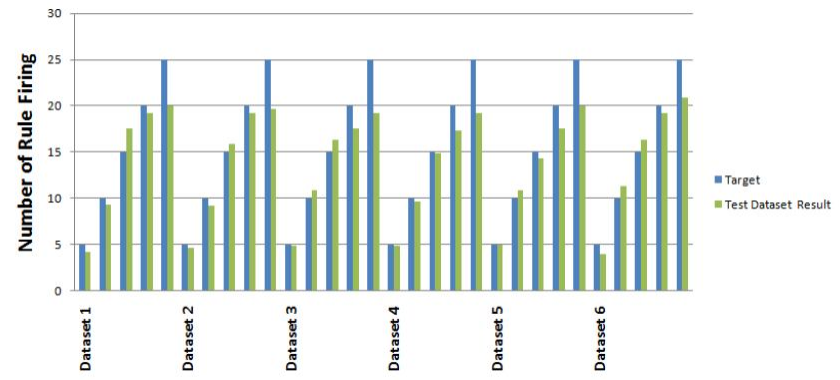
Case study: Testing and Evaluation

- Datasets:
  - We have prepared seven datasets.
    - real-world network events
    - collected from the internal university network.
  - Six of the datasets are 4hours long and one of them is 24 hours long.
- Testing Process:
  - We used two different rule-sets that we adjusted based on six different datasets with five different rule firing targets.
  - After finishing each run, we have checked the new set of thresholds and the final number of rule firings on the test dataset, which is twenty-four hours long.

Results for Rule-Set 1



Results for Rule-Set 2



Conclusions

1. Alert management systems needs to be adapted as a result of network gradually changes.
2. This Adaption handled by Rule Threshold Adjustment.
3. HRTA consist of:

- The online part
  - receives a stream of alerts, monitors them for detecting changes, and based on the them adjusts the thresholds inside the corresponding rules
  - more memory efficient and fast but prone to small error.
- The offline Part
  - the offline part module receives a set of alerts repeatedly, to adjust the thresholds of the rules and to reach an optimal number of rule firing.
  - more memory and CPU intensive but more accurate.

Thank you for your attention!

Any Questions Please,

Hybrid Rule Threshold Adjustment System for Intrusion Detection

Mohamad Mehdi Moghimi
Research Staff
Sepehr Sadra Tehran Co. Ltd.
Tehran, Iran
moghimi@sepehrs.com

Mohamad Saraee
Assistant Professor, ECE Department
Isfahan University of Technology
Isfahan, Iran
saraee@cc.iut.ac.ir

101110100101001001010100100100010001110101100100111101010101011001001000111

8th International ISC Conference on
Information Security and Cryptology - ISCISC2011

101110100101001001010100100100010001110101100100111101010101011001001000111

This work has been supported by
ICT Security Research Center of Malek Ashtar University of Technology -Tehran Campus.