IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. V (Nov – Dec. 2014), PP 14-15
www.iosrjournals.org

Efficient Techniques for Unauthorized Attacks with Time-Stamp

R.Swathi

Abstract: *In many applications it is very useful to identify the unexpected activities on data with respect to time. Cyber security is one of the application area in which we are using intrusion detection system to monitor the network traffic for unauthorized activities and it generates alerts for different types of attacks. For this we propose Efficient algorithm named as Top-k PUS which identifies unexplained sequences and for alerts generation we are using GM Approach which consists of probabilistic methods. Finally experimental results Show that those are efficient with detection accuracy and time*

I. Introduction:

Intrusion Detection System:

Intrusion detection system is to monitor network traffic for unauthorized attacks and it generates alerts. Alert correlation methods join these alerts into multistep attacks

Intrusion detection Techniques:

Intrusion Detection techniques consists of 2 methods. Namely, signature-based and profile based or anomaly-base methods. A signature based method contain intrusion activities which is a set of conditions with respect to packet headers and payload content. Normally signature-based methods are widely used to sense nasty activities. In profile-based methods, anomalous is occured, which is a deviation from the norm for example, a set A of known activities and observation sequence cannot shown by either.so,we need to represent Zero-day attacks, that never expect before by previous activities.

Correlation techniques :

The correlation is a relationship between alerts. From these alerts we can identify attacks. The correlation provides exact way for occurring the actual attacks. Intrusion Detection system and correlation techniques depending on models, in which they identify very easily of activities and cannot correctly for events.

A network intrusion consists of more number of attacks. The network can be protected from these number of intrusions is important. It is usually impossible for intrusions which corresponds to the individual attacks. usually intrusion detection system packed with false alerts that may be either in normal traffic or failed attacks. To protect from more number of intrusions we will combine individual alerts into attack scenarios. Alerts are depending upon same number of attributes and knowledge about alert types. Apart from different knowledge, we are using nested loop. In this each latest alert searches for all old alerts. for example, computer forensics nested loops will give good performance which are having constant number of alerts.

Correlation of IDS alerts using Grammar based approach:

Intrusion detection system is used to find out intrusions. especially this is used for security purpose. Protecting from more number of intrusions is a challenging task. Attribute Context Free is used for representing multiple attacks.ACF includes data about attack and knowledge about consequences to enhance the correlation results. For generating parse trees, modified LR parsers depending upon ACF grammars. The IDS become a part of network security.

IDS detects the attacks and will produce more number of alerts regrettably, it provides impossible number of alerts. these number of alerts are false positive alerts are up to 99%.The reasons for occurring these false positive alerts are having limitations at runtime, specifying detection signatures and if environment is dependent. The main objective is to reducing the number of alerts.so,we have to construct more number of attacks from raw alerts. For this using modified LR parser algorithm.

Intrusion Detection in Anomaly based network:

The new type of attacks are continuously occurring, for this we will provide security. It is more challenging. Intrusion detection techniques in Anomaly based network are used to care for target systems and network activities. Commonly used intrusion detection techniques in Anomaly based network are

Event boxes: This box is used for monitoring the network system by sensor elements.
Database boxes: This is used for storing data from event box for subsequent process by analysis box.
Analysis box: This is used for processing and analyzing events behavior. if necessary alarm will be produced.

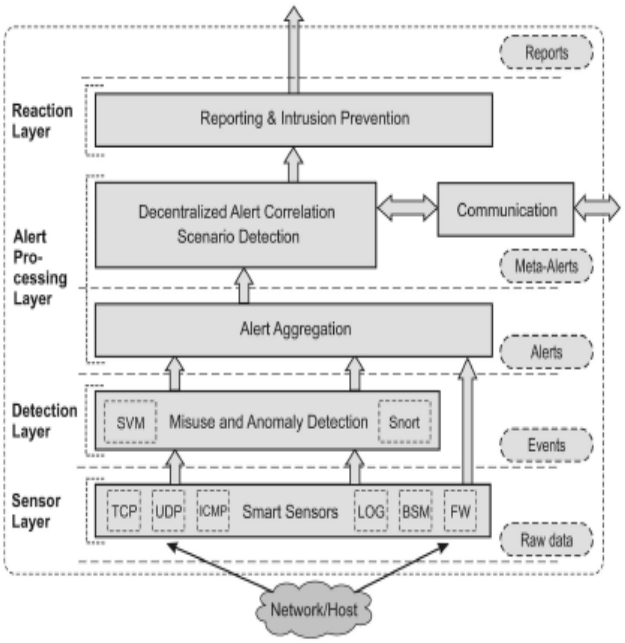

Fig. 1. Architecture of an intrusion detection agent.

II. Techniques used:

GM Approach:

- The system is divided into independent layers that will improve efficiency and performance.
- The number of alerts will be reduced.
- In some experiments, the number of missing attacks are low or even zero.
- The user will be logged in, if there is no intrusion.
- The intrusions will be detected in user level, packet level & process level.

Whenever an input is given the IDS will recognize the type of attack and pass it to all the subsequent layers.

Top-k pus:

- It considers only relevant sequences individually.
- The length of the sequence must be at least having probability that of unauthorized sequences greater than lowest.
- Then the sequence is maximum by adding object identifier on right.
- The object identifier is extended at a time until probability decreases.
- Then a binary search is performed until we will find maximum length of unexpected sequence.
- If the unexpected sequence have the probability greater than lowest then the maximum sequence is aborted.
- Here the object identifier savings the time.

III. Conclusion:

- This paper addresses finding subsequences that are not explained by the activities. For this We propose a Top-k PUS and GM Approach with probabilistic model for alert generation.