A CREDIBLE COST-SENSITIVE MODEL FOR INTRUSION RESPONSE SELECTION

Aderonke J., Ikuomola[1] and Adesina S., Sodiya[2]
[1,2]Department of Computer Science, University of Agriculture Abeokuta, Ogun State, Nigeria

1. INTRODUCTION

Due to the rapid expansion of computer networks during the past few years, the number of intrusions on computer networks has been on the increase. The constant increase of attacks against networks and their resources inspire a necessity to protect these valuable assets. Since intrusions take advantage of vulnerabilities in computer systems or use socially engineered penetration techniques, intrusion detection (ID) is often used as another way of protection. An intrusion detection system is used to monitor network traffic, check for suspicious activities and notifies the network administrator or the system [Khan et al., 2012]. Intrusion detection system does not perform any action to prevent intrusion; its main function is to alert the site security officer or system administrator that there is possible security violation [Sodiya et al., 2007]. In the process of detecting an attack, it is necessary to take corrective action to tackle the attack and ensure safety of the system. The process of counter-measuring these attacks is referred to as intrusion response [Strakhanova et al 2007]. Intrusion Response Systems (IRS), continuously monitor system health based on intrusion detection system alerts, so that malicious or unauthorized activities can be handled effectively by applying appropriate countermeasures to prevent problems from worsening and return the system to a healthy mode [Shameli-Sendi et al, 2012]. Despite the fact that the component of intrusion response system is integrated with the intrusion detection system, intrusion response (IR) has received less attention in the area of research.

In recent years, the trend toward modeling of cost-sensitive response system has become more important. The main goal of cost-sensitive response system is to strike a balance between damages made by the intrusion and the cost of response. However, defining an accurate measurement of these cost factors and ensuring consistent evaluation across various computing environments are common challenges in using a cost-sensitive approach. The objective of an intrusion response system is therefore to provide a counter-measure to intrusion. The problem of intrusion response system is that when the responses are deployed against a detected intrusion, they often alter the state of the system negatively, affecting resources and leading to damage. An intrusion response system needs to be cost-effective in that it should not cost more than the expected level of loss from intrusions. This requires that an intrusion system considers the trade-off among cost factors, which at the minimum level should include: the cost of damage caused by the intrusion, the cost of response to an intrusion and the operational cost; which measures time constraint (administrator time) and computing or system resources (storage, network bandwidth, processor time, among others). For example, intrusion which response cost is higher than the damage cost should not be acted upon beyond simple logging action.

2. PROTOTYPE

Prevalent cases of computer attacks have constant threats to the efficacy of homogeneous intrusion detection and response strategy. Hence, we propose a model that uses Cost-Sensitive Intrusion Response System in figure (1) below. The basic components include Intrusion Detection System and Intrusion Response Engine.

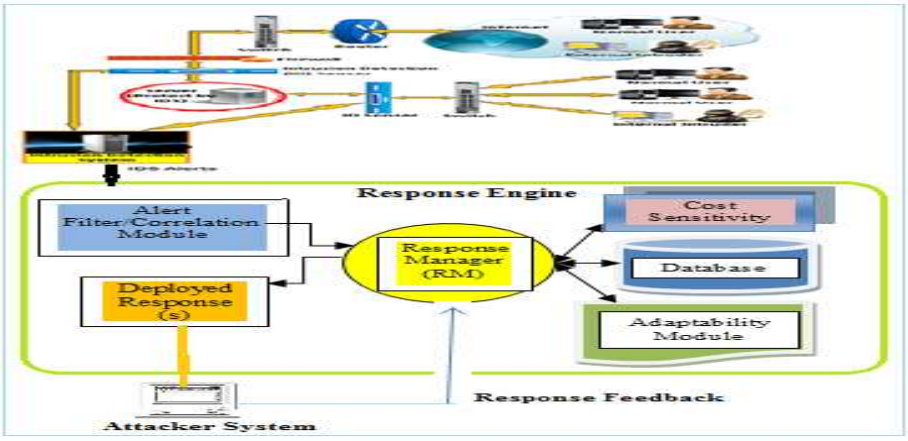

Figure 1: Prototype of a Cost-Sensitive Intrusion Response System (COSIRS)

A. Intrusion Detection System (IDS): The main task of intrusion detection system is to monitor the events occurring in the network and then analyze them for signs of intrusion. Once an intrusion has been detected, intrusion detection system raises alert and then passes the attack specific parameters to the Alert Filter and correlation module in the response engine.

B. Response Engine: Intrusion Response Systems (IRSs) take over after signs of intrusions are detected and then attempt to actively counter it. The response engine is made up of the following components: alert filter and correlation module, the response manager, adaptability module, cost-sensitivity evaluation module and database (consist of response action, profile and intrusion specification).

(i) Alert Filter and Correlation Module (AFCM): The filter gather alerts from the sensor in each managed network and then eliminate redundancies among those alert while these alert are correlated based on the similarities of selected features and the attack scenario.

The ACFM reduces the number of false alarms; it also informs the response manager of the intrusion Type, along with factors such as the target of the attack, speed, perceived perpetrator, etc

(ii) Response Manager (RM): This is the control or central module of the response engine. Information collected from the alert filter and correlation module are further process in this module. Decision on the response to be deployed is made based on the cost and the effectiveness of the response in the past.

(iii) Database (DB): The database contain information about the intrusion specification, profiles and response actions.

(iv) Cost Sensitivity Evaluation Module (CSEM): The evaluation of the response action effectiveness is based on the following factors which are: factors associated with the intrusion damage and factors describing the response cost.

(v) Adaptability Module (AM): The adaptability of the response is the ability of the system to dynamically adjust response selection to the changing environment during the attack time. The adaptability is based on the effectiveness of the response action in the past.

(vi) Response Deployment Module: It manages the responses that are available for a particular system and triggers a recommended response by the response manager.

3. METHOD

In order to build a Cost-Sensitive Intrusion Response model, the evaluation of the intrusion response cost is determined by three major cost factors: Operational Cost (OC), Damage Cost (DC) and Response Cost (RC).

$$DC_i = IS_i + OC_i \quad \text{(i)}$$

$$RC_r = IS_r + OC_r \quad \text{(ii)}$$

where IS_i = intrusion impact on the system

OC_i = cost of daily maintenance of various aspect of the detection system

IS_r = response impact on the system resources

OC_r = cost of daily maintenance of various aspect of the response system

4. TECHNIQUES TO VALIDATE COSIRS

The above design is proposed to be validated against static response system (traditional) and existing cost-sensitive response. Although, the implementation is in advanced stage, benchmarking will focus mainly on compatibilities of both models to handle true and false positives attacks, to give a feedback on the effectiveness of each response deployed and to deployed effective response with minimal cost.

5. CONCLUSION

In this work, we presented a model for the cost-sensitive intrusion response system. Currently the work is still under implementation and we proposed validating with static (traditional) and existing cost-sensitive models. The research aimed to review the cost associated with each of the response selection and the results obtained will be published upon completion to validate our claims. We also aimed at improving the current intrusion response system and measure its efficiency and performance. The premise is that cost-sensitive intrusion response laid emphasis on the balance between potential damage incurred by the intrusion and cost of the response.

6. REFERENCES

[1] Khan T. F, Farooqui Z. and Richhariya V., 2012. Identification of Intrusions in Network for Large Data Base using Soft Computing Approach. International Journal of Computer Sci ence And Technology, 3(1).

[2] Sodiya A.S, Adeniran O. and Ikuomola A.J., 2007. An Expert System-based Site Security Officer, Journal of Computing and Information Technology - CIT 15, 3, 227–235

[3] Stakhanova N., Basu S. and Wong J., 2007. "A taxonomy of intrusion response systems," *International Journal of Information and Computer Security*, 1, 169–184

[4] Shameli-Sendi A, Ezzati-jivan N, Jabbarifar M, and Dagenais M., 2012. Intrusion Response Systems: Survey and Taxonomy. *IJCSNS International Journal of Computer Science and Network Security, 12 (1)*