User behavior Pattern -Signature based Intrusion Detection

Zakiyabanu S. Malek,
Faculty of Computer Technology,
GLS University,
Ahmedabad, Gujarat, India,
zakiya.malek@glsuniversity.ac.in

Bhushan Trivedi
Faculty of Computer Technology,
GLS University,
Ahmedabad, Gujarat, India,
bhushan.trivedi@glsuniversity.ac.in

Axita Shah
Rollwala Computer Centre,
Gujarat University,
Ahmedabad, Gujarat, India
axitashah@gmail.com

***Abstract*-Technology advancement also increases the risk of a computer's security. As we can have various mechanisms to ensure safety but still there have flaws. The main concerned area is user authentication. For authentication, various biometric applications are used but once authentication is done in the begging there was no guarantee that the computer system is used by the authentic user or not. The intrusion detection system (IDS) is a particular procedure that is used to identify intruders by analyzing user behavior in the system after the user logged in. Host-based IDS monitors user behavior in the computer and identify user suspicious behavior as an intrusion or normal behavior. This paper discusses how an expert system detects intrusions using a set of rules as a pattern recognized engine. We propose a PIDE (Pattern Based Intrusion Detection) model, which is verified previously implemented SBID (Statistical Based Intrusion Detection) model. Experiment results indicate that integration of SBID and PBID approach provides an extensive system to detect intrusion**

Keywords-Intrusion Detection, Pattern Based Intrusion Detection, Intrusion Detection using Statistics

1. INTRODUCTION

Intrusion Detection (ID) is one of the security mechanisms to identify authorized or unauthorized user behavior in the system or network. An unauthorized user is known as an intruder and it might be insider or outsider [7]. Models of Intrusion Detection System (IDS) are of two types: Anomaly adjunct and misuse-signature adjunct. Out of these two, Misuse Detection detects known attack and anomaly adjunct identifies attack by behavior deviation.

An intrusion detection system is developed on the conception of user's unauthorized behavior based on observer authorized behavior [9]. The deviation of user behavior considers as an intrusion. To identify intrusive behavior, user activity log and user's current activity are inputted to an intrusion detection system. New techniques developed by researchers can observe and detect the present position of the user if there is a difference between the user's current state with stored profile an alert will be generated [10].

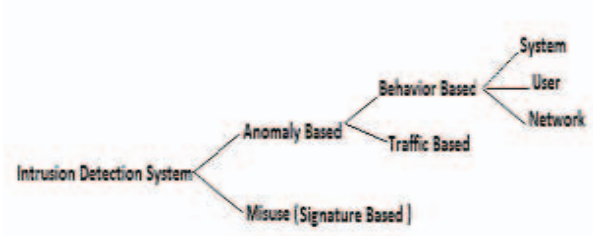

Fig.1 Types of IDS

Signature-based IDS gives high true positive rates for known patterns. It is lightweight and easy to implement. The detected pattern also knows as a signature. The signature-based IDS store pattern in the database and compare user current activity with a stored pattern to detect authorized user or an unauthorized user hence it simply detects the known pattern. We have proposed signature based intrusion detection based on user behavior using pattern matching technique.

In this paper section 2 provide a literature review, section 3 discussed the concept of Intrusion Detection - pattern adjuncts, user behavior adjuncts and signature specific behavior. Given Proposed System uses authorized user's rules to detect intrusion, section 4 talks about our proposed model with implementation using jess and section 5 concludes the proposed research with leading research enhancement in future.

2. LITERATURE REVIEW

Pattern or Signature detection for intrusion detection systems is rule-based techniques. Such systems are

978-1-7281-6823-4/20/$31.00 ©2020 IEEE

built on numerous conditional if-then rules for their detection. System matches current contextual information with the given list of rules. System allows to continue access if rules are matched otherwise any violation in rule matching leads to an ID. Rules are developed or coined by analyzing all possible intrusions or any malicious activities by experts and then transferring them into conditional rules which are later used by inference modules of IDSs to compare against logs (monitoring data) to identify any type of intrusion. Researchers in [10] have implemented a solution to identify an unauthorized user based on user activity through Time series and Markov chains statistical techniques. Haystack [11] evolved an outlined framework to identify spiteful use, leakage, pretence attacks, denial of the service, attempt to unauthorized user's break-ins, and access control of ID for detecting Intrusion. Forrest [12] identifies an attack by deviating the sequence from the normal profile which is analyzed based on the call orders.

Rule based Systems in [1][2] are extremely useful for pre-defined signatures to discover well-known attacks. Following are the examples of Rule based systems - NIDES (Next-generation Intrusion Detection Expert System) [5], IDES (Intrusion Detection Expert System) [4], and MIDAS (Multics Intrusion Detection and Alerting System) [3].

The rule provides a mechanism to identify it is authorized or unauthorized. Rules are comparably easy to create and understand. Generally designed by expert or system generated. Rules are applied to user behavior log to identify that user ongoing activity is intrusive or not. For that a huge set of rules required which covers every aspect of authorized and unauthorized user activity. Signature-based IDS are looking for known patterns for malicious activity and given rule set is their strength [6].

Rules are designed in two ways, either by expert or system generated automatically and applied repeatedly to collected facts [2]. Whenever the rule is fired, it generates either an alert for system administrator or takes some actions automatically like blocking user or termination of the session, etc. and this will be executed until all rules are fired.[7] An alert for terminating the session, blocking user account generated whenever the rule is triggered. Initially, the research is based on statistical analysis [13] but not suitable for large datasets. Hence, many issues are been lay down in the existing system. To solve the existing issues, a new system needed which enhances the results of the signature adjunct IDS using a combined hybrid approach.

3. RULE/PATTERN BASED INTRUSION DETECTION USING USER BEHAVIOR

There are several techniques used for to identify intrusions. But still, a few challenges are to be overworked upon. The existing systems fail to distinguish between authorized and unauthorized behavior accurately. Sometimes the system generates a false alarm when the system interprets normal user as intruder. The intrusion detection system performance can be improved reducing false alarm with clearly making a distinction from the user's normal and abnormal activity by observing the user's activity log.

To distinguish between the normal and abnormal user behavior we identify user parameters and construct the user's initial behavioral normal/usual profile. This profile is not constant and may vary as per the usage of the system (Change in user behavior). In rule based study it involves rules and the rules are either designed by the system or given by an expert. These rules are applied to the gathered user behavior details. The rules are stored in a rule engine. User behavior details consist of user behavior log while rules comprise as an if-then statement which is easy for human beings to understand by applying these rules on user behavior details it can easily identify where it is intrusive or not. If the rule is triggered, then the system reports to block an account of the user or may erect an alarm to notify. The below figure 2 shows the rule based scenario.

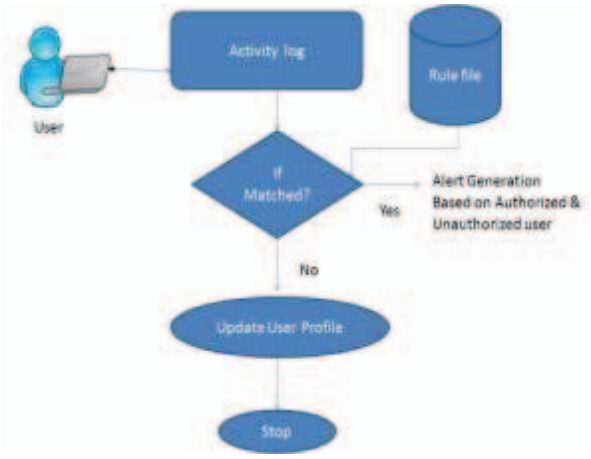

Fig. 2. Rule based scenario

4. PROPOSED MODEL

a. Generate dataset
b. Generate rule using Jess
c. Evaluate model and result

d. Alert generation based on Authorized and Unauthorized user

A. Pattern based Intrusion Detection Engine [PIDE]

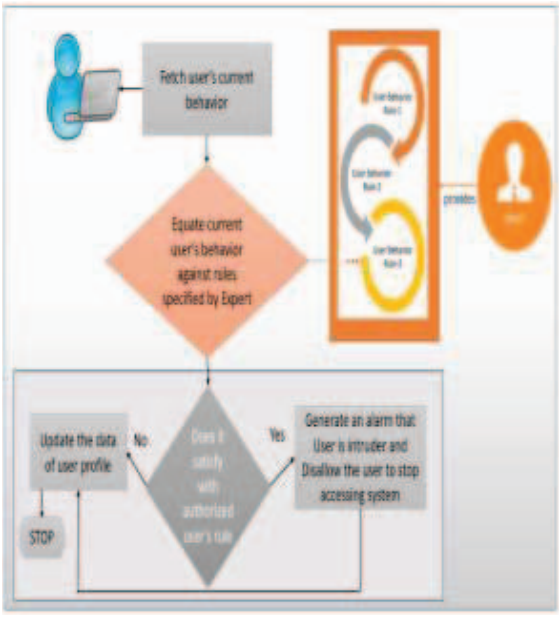

Fig. 3. Pattern-based Intrusion Detection Engine [PIDE] Model

Figure- 3 specifies the flow of the PIDE Model. The expert provides authorized and unauthorized user's rules. Our engine matches the user's current behavior with rules specified by the expert. If the current activity satisfies with authorized user's rule then the system generates an alarm that users are an intruder and block the user else it will update the user's profiles.

B. Experiment & Result

We have used the user profile dataset of Zakiya[14] which contains parameters different of a keyboard, Mouse, applications running, processor usage, etc Zakiya[14] had developed a statistical engine which apply logistic regression and Statistical mean on different user's dataset and test cases with different features. To continue with the work we assign an expert. Now, experts knowing normal user behavior hence, the expert provides rules in Pattern based Intrusion Detection Engine PIDE. Here, we have used JESS to provide rules. The following Figure:4 shows the JESS rule file. The rule based detection collects various data for possible attacks to identify authorized and unauthorized activities. Rules are to be defined in such a way that only doubtful activities are noticed without disturbing authorized users.

```
;Authorized user
(defrule authorized-user
  (username {UserName == "sneh"} )
   =>
  (printout t "valid" crlf))
 ;Unauthorized user
(defrule unauthorized-user
  (username {UserName != "sneh"}  )
   =>
  (printout t "invalid" crlf))
;Unauthorized Website Counter
(defrule unauthorized-websitecounter
  (websitecounter {Websitecouter > 40} )
 =>
  (printout t "unauthorized" crlf))
;Unauthorized File Counter
(defrule unauthorized-filecounter
  (filecounter { Filecounter > 230} )
   =>
  (printout t "unauthorized" crlf)
)
```

Fig. 4. Jess Rule file

After implementing the jess rule we generated results of test cases and compare them with Zakiya[14] test result shown in Table 1. As Zakiya [14] said for an unauthorized user using statistical mean is good and the Authorized user logistic regression is good. The below table result it shows that PIDE provides 75% accuracy.

TABLE 1: THE STATISTICAL ENGINE, PATTERN JESS RULE OUTCOME COMPARED WITH THE ACTUAL RESULT BASED ON USER LOG

	Actual Result	Statistical Mean	Logistics Regression	Pattern Jess Rules
case1	Authorized	[redacted]	Authorized	Authorized
case2	[redacted]	[redacted]	Authorized	[redacted]
case3	Authorized	Authorized	Authorized	[redacted]
case4	[redacted]	[redacted]	Authorized	[redacted]
case5	[redacted]	[redacted]	Authorized	[redacted]
case6	Authorized	[redacted]	Authorized	Authorized
case7	[redacted]	[redacted]	Authorized	[redacted]
case8	Authorized	[redacted]	Authorized	Authorized
case9	Authorized	[redacted]	Authorized	Authorized
case10	[redacted]	[redacted]	Authorized	[redacted]
case11	[redacted]	[redacted]	Authorized	[redacted]
case12	Authorized	[redacted]	Authorized	[redacted]
case13	Authorized	[redacted]	Authorized	[redacted]
case14	Authorized	[redacted]	Authorized	Authorized
case15	Authorized	[redacted]	Authorized	[redacted]
case16	[redacted]	[redacted]	Authorized	[redacted]

Here, in the below Table 2, Compared to previous result of [14], Proposed Pattern based technique shows 100% accuracy in Unauthorized user identification and 5:4 ratio in authorized user shown in the Confusion matrix.

TABLE 2: CONFUSION MATRIX

	Authorized	Unauthorized
Authorized	5	4
Unauthorized	0	7

5. CONCLUSION AND FUTURE ENHANCEMENT

Rule based detection involves the use of a specific set of rules for identifying known patterns hence, there are so many benefits of pattern rule based system but still isn't give 100% result as unavailability of a systematic approach to build an accurate rule based system. Our proposed pattern based technique works well in identifying unauthorized user.

Generally, rule based systems are designed based on previous experience, expert opinion, instinct and sometimes doing different experiments. It is also possible that one rule can be interrelated with the other rule because of the existence of a logical connection between a large set of rules specified in the repository. It is also very difficult to observe how individual rule works with the overall system. Hence, this will lead to wrong results. The other thing is that if the patterns are clearly defined then it is easy to use and has a low false alarm but it requires specific knowledge of intrusion pattern and it cannot detect unknown/new patterns.

To overcome the above mentioned issue we analyze that only signature based intrusion detection could not achieve an effective result. Hence, we have to apply the concept of anomaly based intrusion detection with existence once. As a part of future research we will try to use machine learning approaches to achieve low false alarm by combining anomaly adjunct Intrusion detection with the signature adjunct intrusion detection.

REFERENCES

1. Maithili Arjunwadakr, R.V. Kulkarni"The rule-based Intrusion Detection and Prevention Model for Biometric System", Journal of Emerging Trends in Computing And Information Sciences, OCT-2010
2. Todd Vollmer, Jim Alves-Foss, Milos Manic, "Autonomous rule creation for intrusion detection" 2011 IEEE Symposium on Computational Intelligence in Cyber Security
3. M. Sebring, E. Shellhouse, M. Hanna, and R. Whitehurst, "Expert systems in intrusion detection: A case study", Proceedings of the 11th National Computer Security Conference, 1988, pp. 74–81
4. T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Eclwards, P. Neumann, H. Javitz, and A. Valdes, "IDES: The Enhanced Prototype. A Real-Time Intrusion Detection System", Tech. report, Technical Report SRI Project 4 185-010, SRI-CSL-88, 1988
5. D. Anderson, T. Lunt, H. Javitz, A. Tamaru and A. Valdes, "Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES)", Computer Science Laboratory, SRI International, Menlo Park, CA Technical Report SRI-CSL-95-06.
6. V. K. Kankanala, "Web-based Network Intrusion Detection System," Texas A&M University, Corpus Christis, Graduate Project Technical Report, 2006.
7. Zakiya Malek, Bhushan Trivedi," The Rule Based Intrusion Detection Model for User Behavior", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015
8. Z. Malek and B. Trivedi, "GUI-based user behavior intrusion detection," *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, 2017, pp. 2050-2055.doi: 10.1109/ICPCSI.2017.8392076
9. Tomas D. Gravey, Teresa F. Lunt, "Model based intrusion detection", 14th National Computer security conference , Washington Dc. October 1991.
10. Denning, D. E.. An intrusion detection model, IEEE Transactions on Software Engineering, CA,. IEEE Computer Society Press;1987.
11. Patcha, A. and Park, J. M. An overview of anomaly detection techniques: Existing solutions and latest technological trends.Computer Networks, 51(12);2007; 3448–3470
12. Forrest, S., Hofmeyr, S. A. , Somayaji, A. and Longstaff, T. A. A Sense of Self for Unix Processes, IEEE Symposium on Research in Security and Privacy, Oakland, CA, USA, 1996;120--128.
13. 13.Manikopoulos, C.and Papavassiliou, S. Network intrusion and fault detection: A statistical anomaly approach. IEEE Communications Magazine, 40(10);2002 76–82.
14. S. Malek, Zakiyabanu & Trivedi, Bhushan & Shah, Axita. (2019). User Behavior-Based Intrusion Detection Using Statistical Techniques: Second International Conference, ICAICR 2018, Shimla, India, July 14–15, 2018, Revised Selected Papers, Part II. 10.1007/978-981-13-3143-5_39.