iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

User Behaviour based Intrusion Detection System Overview

Zakiyabanu S. Malek[1], Bhushan Trivedi[2]
[1]*Ph.D Scholar, Pacific University, Udaipur*
[2]*Ph.D Supervisor, Pacific University, Udaipur*

Abstract: ***An intrusion detection is a techniques used to identify attack on the computer, hence the need of effective intrusion detection system is must. It is impossible to develop completely secure system because highly secure systems have security flaws and they are vulnerable to misuse by legitimate users. Most of the existing intrusion detection research is on network and system based behaviour. Now analysis of user activity is a natural approach to detect anomalies, but researchers experience shows that it is far from accuracy. This is because user behaviour is quite dynamic compare to network and system as users are not stick on certain patterns. Hence, user behaviour based anomaly detection is challenging field to increase accuracy of anomaly detection. The main objective of this paper is to provide information about the current research and development on user behaviour based intrusion detection system. It also describe what is intrusion detection system? , classify types of intrusion detection system and summary of advantages and disadvantages, Behaviour based intrusion detection system and research requirements.***
Keywords: IDS, BIDS

I. INTRODUCTION

The attacks on the systems have been increasing considerably nowadays and so the need to protect the system against such attacks. Many systems have been developed to protect against various attacks, but the perfect system is far from being invented. Intrusion Detection Systems are one of the special purpose systems that are designed to protect computer systems against harmful attacks. It is the security management systems for computers and networks. It gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

As, intrusion detection is used to identify intrusions and intruder. Intruder may be insider or outsider. An intruder is an unauthorized user who pretend to be an authorized user and carry out malicious activity. Intruders behaviour different from expected users behaviour. The analysis on behaviour difference is used to detect intrusion. In order to know expected user behaviour, audit record of the users must be maintained as input to an Intrusion Detection System.

An intrusion can be defined as an attempt to gain unauthorized access to network resources[49]. An unauthorized user can read unprivileged data, perform unauthorized modification to data and disturb system settings etc.

II. ABOUT INTRUSION DETECTION SYSTEM

Intrusion Detection system is classified into two categories: signature-based misuse detection and anomaly detection[42,45]. Signature based misuse detection technique is limited to the only known unauthorized users only. How to identify new unauthorized users is one of biggest challenges faced by signature or misuse detection[46]. To overcome this limitation of signature-based misuse detection, the concept of anomaly detection was introduced[16]. In reality, most anomaly detection techniques attempts to set up normal activity profiles by computing various metrics and an intrusion are detected when the actual system behaviour deviates from the authorized user profile[55].

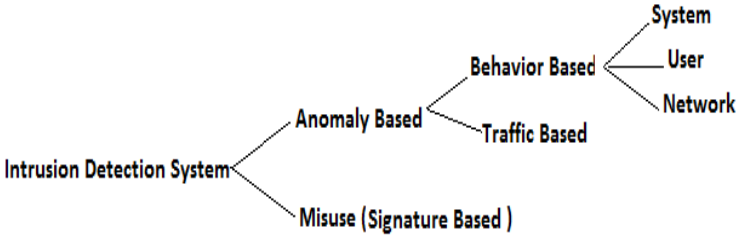


Fig 1. Types of IDS

A. Misuse (Signature based/Knowledge based) Detection

The misuse (signature-based) detection is used pattern matching technique and detect known attacks. Here IDS compare all incoming or outgoing activity against all known threats in its knowledge base and raise an alarm if any activity matches information in the knowledge base. The information stored in this knowledge base is usually known as signatures [37]. The process for actually comparing a signature with an attack include simple string matching – which involves looking for unique key words in network traffic to identify attacks – to more complex approaches such as rule-based matching which defines the behaviour of an attack as a signature [37]. Various string-matching (or pattern-matching) algorithms are used to inspect the content of packets and identify the attacks signature in IDS. There are mainly two kinds of algorithms, viz. i) Single-keyword pattern matching algorithms viz., Brute force algorithm, Knuth-Morris-Pratt Algorithm [56], and Boyer-Moore algorithm [38]; and (ii) Multiple-keyword pattern matching algorithms viz., Aho-Corasick [34], Wu-Manber Algorithm [54], Horspool Algorithm [43], Quick search algorithm [53], Piranha [36], and E2xb [35].

1) Advantages of Misuse detection[56].

a) Signatures are very easy to develop and understand, if we know what pattern should appear (user/system/network behaviour) we are trying to identify.

b) It has lower false alarm rates than behaviour-based IDS. This high precision is caused by the fact that a Signature based IDS is explicitly programmed to detect certain known kinds of attacks

c) Alarms are more standardized and more easily understood than behaviour-based IDS.

2) Disadvantages of Misuse detection[56].

a) The detection rate of attacks is relatively low

b) Signature database must be continually updated and maintained as more different signatures require additional work for the IDS, which reduces performance [56].

c) New, unique, or original attacks may not be detected because is not yet stored in database.

The difference in the speed of creation of the new signatures between the developers and the attackers determine the efficiency of the system. Since this technique could only identify known attacks alternatives had to be thought for identifying novel attacks, and so anomaly based detection system came into picture.

B. Anomaly (Behaviour based) Detection

Since the signature based detection system could only identify attacks whose signatures were known, anomaly based detection was a solution to the constraint of the signature based detection technique. The anomaly based system works by analyzing the authorized system/user/network behaviour that resides in the profile of the system/user/network and then looks for any deviations from the stored behaviour to the current behaviour[40]. Thus any change in behaviour from the authorized/normal behaviour could be considered as a potential intrusion.

Anomaly-based IDS attempt to characterize normal operation, and try to detect any deviation from normal behaviour [52]. The main challenge in anomaly detection technique is in learning what is considered ―normal behaviour. The work by Axelsson [37] describes the two main approaches which are used to achieve this goal: self-learning or programmed anomaly detection.

In the self-learning approach, the anomaly detection system will begin to automatically monitor events, such as live network traffic, on the environment it has been implemented on and attempt to build information on what is considered authorized normal behaviour [37]. This is otherwise known as online learning [48].

In the programmed approach, the anomaly-based IDS must manually learn what is considered normal behaviour by having a user or some form of function ―teaching the system through input of information [37]. This is otherwise known as offline learning, and may involve feeding the system a network traffic data set which contains normal network traffic [48].

1) Advantages of Anomaly detection[52].:

a) Dynamically adapt to new, unique, or original attacks.

b) Because of profile based- Are less dependent on identifying specific operating system vulnerabilities

2) Disadvantages of Anomaly detection[52].:

a) Higher false alarm rates which means a lower precision

b) It also needs periodic online retraining of the behaviour profile as usage pattern is not static.

c) It tends to be computationally expensive because several metrics are often maintained that need to be updated against every system activity and, due to insufficient data, they may gradually be trained incorrectly to recognize an intrusive behaviour as normal due to insufficient data [56].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

C. IDS Architecture

An intrusion detection system can be categorized as host based intrusion detection and network based intrusion detection [32] shown in figure 2. As name suggest host based IDS execute on standalone machine while network based are implemented on network to observe network data transfer to and fro[31]. The following figure describe pros and cons of both intrusion detection system.

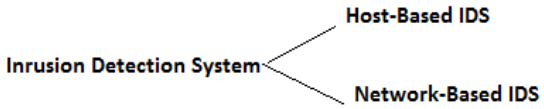


Fig 2 IDS Architecture

D. IDS Detection/Alerts

IDS detect an intrusion and raised an alarm. Now depending on the type of alarm the following types of detection alerts or results are possible.

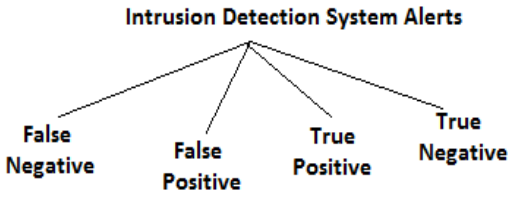


Fig 3 IDS Alerts

TABLE 1
IDS ALERTS

IDS Alert	Description
False negative (FN)	Represents the number of intrusions seen by the IDS as normal.
False positive (FP)	Represents the number of normal activities seen by the IDS as intrusions.
True positive (TP)	represents the number of intrusions seen by the IDS as true intrusions.
True negative (TN)	Represents the number of normal activities seen by the IDS as normal.

From the TABLE 1 we can says that True positive occur when actually attack occur and IDS raised an alarm where in True Negative there is no attack still IDS raised the alarm. False positive has a very serious drawback in IDS because it consider legitimate activity as an attack and lastly when IDS missed to find attack False Negative occur. For example if unauthorized user enter into system and change the system privilege files and if IDS do not detect it then that situation is false negative on the other side sometimes it is required that authorized user modify system privileges after getting permission from higher authority in this scenario IDS detect it as attack then it is false positive. Hence if false positive occur then it will take more effort to identify system accuracy while false negative makes the situation terrible because it fails to identify attacks.

E. IDS Attacks

People can harm the system by knowingly and unknowingly, in both the case different types of attacks are carried out. The following figure 4 describe some of the well known attacks.[32]

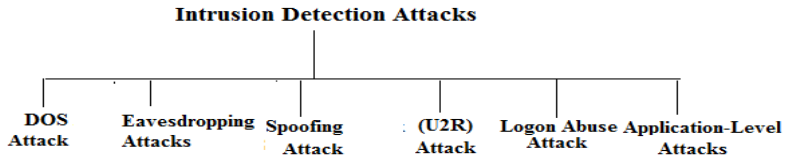


Fig 4 IDS Attacks

TABLE 2
CATEGORY WISE ATTACK TYPE

Attack	Attack Category
Password file modified	Misuse
Four failed login attempt	Anomaly/Misuse
Failed connection attempts on 60 sequential ports	Anomaly/Misuse
User who usually logs in around 11pm from India dorm logs in at 5:00am from a USA IP address	Anomaly
UDP packet to port 1434	Misuse

F. IDS TOOLS

There are many open source and licensed intrusion detection tools are available in market. The following TABLE 3 describe about tools, their category, support for different operating systems, human computer interface etc..

TABLE 3
IDS TOOLS

Features / Tools	HIDS	NIDS	ATTACKS DETECTED / CONDUCTED	HUMAN-COMPUTER INTERFACE	LICENCE	PLATFORM SUPPORTED
SNORT	No	Yes	DOS and CGI Attacks, Intrusion attacks, Port Scans, SMB probes Layer 3 and above attacks.	GUI/ Command Line	Open Source	Linux, Windows, Free BSD, MAC OS
OSSEC HIDS	Yes	No	Attempts to access non-Existent files Secure Shell Attacks, FTP Scans, SQL Injections, File system attacks	GUI	Open Source	Linux, Windows, Free BSD, MAC OS
FRAGROUTE	NO	Yes	Insertion, Evasion, and Denial of Service	Command Line	Open Source	Linux, Free BSD
METASPLOIT	No	Yes	Vulnerability Exploitation	Command Line	Open Source	Linux, Windows, Free BSD, MAC OS
TRIPWIRE	Yes	No	Root Kit Detection, File Integrity Checks	Command Line	Open Source	Linux, Windows, Free BSD, MAC OS

III.USER BEHAVIOUR BASED IDS

Anomaly of user behaviour is identify by observing user activity.For that, it is necessary to get user behaviour and build a user profile. This profile is used to identify or detect user's normal/authorized or abnormal/unauthorized behaviour. Normal and abnormal behaviour means for example one user might always start his bank transaction after looking his account balance and reading new offers. This action would be normal. But if his/her account accessing pattern is different such as start transfer money transaction first, then this new behaviour might be clue that unauthorized user was acting under the authorized user identity.

To detect anomaly at the initial stage, it is very important to create a strong & correct user profile because all the final result completely depends on the user profile. When the concept of behaviour-based intrusion detection arise in the 1970s that time there were no GUI so all the experiments were done on command line of data users typically on Unix operating system. From 2000

onwards people starts are working on GUI based system but in case of GUI based system, its selection of the parameter such as mouse movement , keyboad movement, application running, CPU & Memory usage, Login-logaout session activity etc. for profile generation is a very challenging task.

IV. BIDS BACKGROUND

Initially when the concept of user behaviour arises system only concentrate on command line data but gradually technology enhances keyboard and mouse usage play major roles to identify anomaly [3].

Therefore different parameters such as typing speed; usage (if any) of the numeric keypad; usage of function, cursor, and control keys and speed of mouse movement [9, 11, 51] are consider to identify user anomaly.[9] said that there is no need of special hardware for collection of keyboard biometrics but the major concern is privacy and there is no data set available for further research. [6,7,8] they collected data of 15 user having same age group used from one and the same computer with mouse and mouse pad lead to improve error rate up to 20%.

A framework was proposed for collecting user behaviour based on mouse activity, typing speed as well as background processes [40]. The authors used binary classification problem for user identification and intrusion detection, and used support vector machine for learning and classifying user profile parameter sets.

The technique was claimed to have a high detection rate with few false positives. However, the dataset was not made available to public due to copyright issues. For user verification [17] author consider all human behaviour for profiling it includes shopping style , web browser accessing style etc also consider combination of two or more than two biometrics together. [8,23,33] said that only mouse pattern is not enough to identify user anomalous behaviour and users those who not using mouse it is very difficult to identify anomaly in this scenario. [25,39] study user browser visit history, such as number of website viewed, and audit data. [30,47], talks about other parameters like processor utilization , login logout etc.[30] uses a machine-learning approach for monitors user and system behaviour on GUI based system by storing number of bytes transferred over the last 10 seconds and achieve low false alarm without cycle stealing. [44] uses One-class SVM on Linux based GUI system to identify masquerade attack.

The paper [12] presented a new approach of generating user behaviour profiles in the form of datasets. The generated datasets will not only include the traditional user command data but will also contain the behaviour characteristics of users such as mouse movements while a system is being used and keyboard characteristics such as typing speed. The user behaviour characteristics are used to generate templates, which can be further customized.

The framework is called USim which can achieve rapid generation of user behaviour data based on these templates for GUI based systems. The templates created by USim framework are highly tunable and require minor changes in the parameters to provide similar datasets for covering a range of user behaviours.

USim Data Structure more emphsize on[12]

A. User

1) Mouse movement

2) Keyboard movemnt

3) Commands

*a)*Typed command

*b)*Keystroke combination

*c)*mouse click based

B. System

1) Background Process: The paper[41] identify masquerade by comparing user current activity (such as keyboard pattern, application usage, CPU memory usage) with stored profile . [50] identify anomaly from user current activity and previous activity. They store user behaviour in five different cluster and by applying cluster rule minimize false alarm.

The following TABLE 4 describe the summary of work done in User behaviour based in intrusion detection .

TABLE 4

User Behavior based IDS			
Base	**Parameters**	**Result**	**Citation**
Unix	Command line	Do not support GUI systems	[1],[5]
Unix	Command line	Deviation from the behavior model is attack	[2]
Linux	Mouse Movement & Keystroke	Only command line data alone cannot efficient detect intrusion attack	[3]
Windows	Event logging tool developed	Tool captured user data for windows and analyze effectiveness using HMM based IDS on collected data	[4]
GUI based	mouse actions	Only mouse movement is not enough to identify intrusion	[6 7 8]
GUI based	Revisit of webpage	High false alarm	
GUI based	Keyboard Biometrics	Data set is not available for testing need to consider other parameters as well	[9]
GUI based	Algorithm based on Typing pattern	Only typing patterns are not sufficient to identify intrusion	[11]
GUI based	User behavior based on mouse activity, typing speed as well as background processes, user expertise. .	High detection with low false alarm.	[10][12]
Mainframe based	Study of mainframe users	It talks about mainframe only.	[13]
Command line based	User behavior	Also contains details about resource usage.	[14] [15] [16]
	User profile based on behavioral biometrics	Attacks from unauthorized user are reduced	[17]
Keystroke	Keyboard pattern	Other parameters are required for better result.	[18 19 20 21 22]
Mouse Dynamics	Mouse usage pattern	Fail if user not use mouse.	[8, 23]
Application specific characteristics	Websites viewed in a browser	Identify user website access pattern	[24 25 26]
Unix	Behavioral IDSs focus on Unix command line usage		[27 28]
Frequency of commands, and audit data	Consider resource utilization like CPU & memory as well login logout period	Very high detection rate but not applicable to GUI	[29 30]

V. ISSUES AND CHALLENGES

From the previous research approaches we can say that : The research emphasize on the user behaviour based intrusion detection by considering various parameters of user. Some researcher used only command line data, training and testing time is very high, only few parameters were captured in GUI based systems, Low detection rate with high false positive. Hence, it require that user behaviour based intrusion detection systems include combination of different parameters together to reduce false alarm which is user's keyboard pattern, mouse usage pattern, resource (I/O, memory, Processor, Files) usage etc.

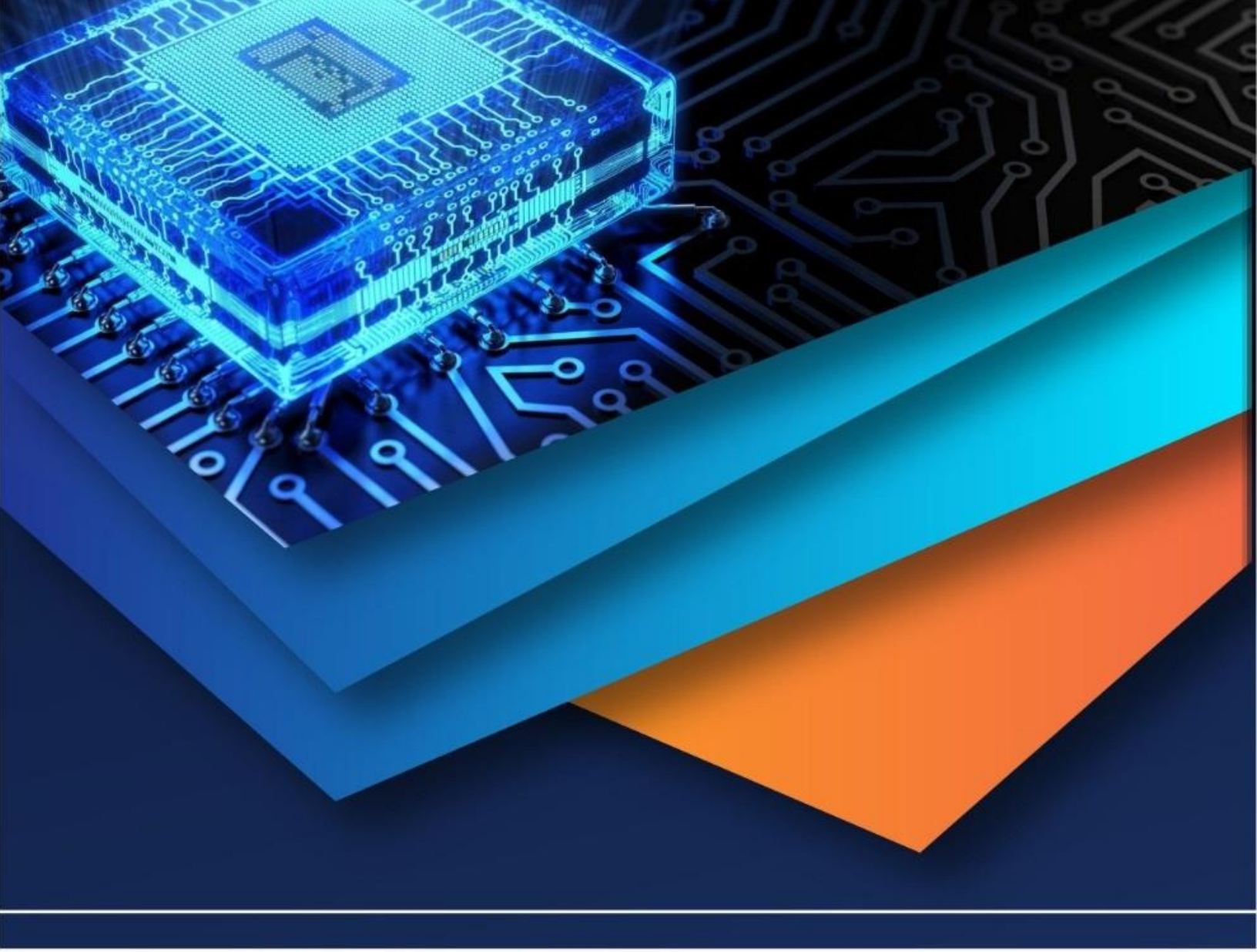
VI. CONCLUSION AND FUTURE SCOPE

In this paper, we discussed about the Intrusion detection System(IDS), Types of (IDS) and Behaviour based IDS (BIDS). The paper also gave basic knowledge and understanding of User Behaviour Characteristics. From the survey of different user Behaviour based Intrusion detection system it is conclude that due to the dynamic behaviour of user, the more number of false positive occur hence there is still lots of scope to reduce false positive by combining different User behaviour Characteristics. In next paper we will cover BIDS using Statistical based, Rule based and Machine learning based methods.

REFERENCES

[1] Erbracher, R.F., Prakash, S., Claar, C.L. and Couraud, J.; Intrusion detection: Detecting masquerade attacks using UNIX command lines; usu.edu
[2] Huang, L., and Stamp, M. (2011); Masquerade detection using pro_le hidden markov models; Computers and Security; 30(8), 732{747
[3] Bhukya, W.S., Kommuru, S.K., and Negi, A. (2007); Masquerade detection based upon GUI user pro_ling in linux systems; Advances In Computer Science, ASIAN 2007
[4] Arshi Agrawal, User Profiling in GUI based Windows Systems for Intrusion Detection Master's Project San Jose State University SJSU ScholarWorks Master's Theses and Graduate Research
[5] Schonlau, M. (1998); Masquerading user data;
[6] Goecks, J., and Shavlik
[7] , J. (1999); Automatically labeling web pages based on normal user actions; IJCAI Workshop on Machine Learning for Information Fil-tering
[8] Hashia, S., Pollett, C., and Stamp, M. (2004); On using mouse movements as a biometric; San Jose State University;http://www.cs.sjsu.edu/faculty/pollett/masters/Semesters/Spring04/Shivani/shivanipaper.pdf
[9] Pusara, M., and Brodley, C.E. (2004); User re-authentication via mouse move-ments; http://www.csis.pace.edu/~ctappert/it691-11fall/projects/mouse-pusara.pdf
[10] Peacock, A., Ke, X., and Wilkerson, M. (2004); Typing patterns: A key to user identification; IEEE Security & Privacy
[11] Shavlik, J., Shavlik, M., and Fahland, M. (2001); Evaluating software sensors for actively profiling Windows 2000 computer users; Fourth International Sym-posium on Recent Advances in Intrusion Detection
[12] Monrose, F. & Rubin, A. 1997, 'Authentication via keystroke dynamics,' in Proceedings of the 4th ACM conference on Computer and communications security, ACM, Zurich, Switzerland, pp. 48-56.
[13] Garg, A., Rahalkar, R., Upadhyaya, S., and Kwiat, K. (2006); Profiling users in GUI based systems for masquerade detection; Information Assurance Workshop
[14] Boies, S. J. 1974, 'User Behaviour on an Interactive Computer System,' IBM Systems Journal, vol. 13, no. 1, pp. 2-18.
[15] Anderson, J. P. 1980, 'Computer Security Threat Monitoring and Surveillance,' James P. Anderson Company.
[16] Eugene, S. 2008, 'James P. Anderson: An Information Security Pioneer,' IEEE Security & Privacy, vol. 6, no. 1, pp. 9.
[17] D. E. Denning, "An Intrusion Detection Model", IEEE Transactions on software engineering, vol. 13, no. 2, pp. 222-232, Feb. 1987.
[18] Yampolskiy, R. V. & Govindaraju, V. 2008, 'Behavioural biometrics: a survey and classification,' Int. J. Biometrics, vol.1, no. 1, pp. 81-113.
[19] Umphress, D. & Williams, G. 1985, 'Identity verification through keyboard characteristics,' International Journal of Man Machine Studies, vol. 23, no. 3, pp. 263-273.
[20] Monrose, F. & Rubin, A. 1997, 'Authentication via keystroke dynamics,' in Proceedings of the 4th ACM conference on Computer and communications security, ACM, Zurich, Switzerland, pp. 48-56.
[21] Bergadano, F., Gunetti, D. & Picardi, C. 2003, 'Identity verification through dynamic keystroke analysis,' Intelligent Data Analysis, vol. 7, no. 5, pp. 469-496.
[22] Leggett, J., Williams, G., Usnick, M. & Longnecker, M. 1991, 'Dynamic identity verification via keystroke characteristics,' International Journal of Man-Machine Studies, vol. 35, no. 6, pp. 859-870.
[23] Revett, K. 2009, 'A bioinformatics based approach to user authentication via keystroke dynamics,' International Journal of Control, Automation and Systems, vol. 7, no. 1, pp. 7-15.
[24] Revett, K., Jahankhani, H., Magalhães, S. T. & Santos, H. M. D. 2008, 'A Survey of User Authentication Based on Mouse Dynamics,' in Global E-Security, 4th International Conference, ICGeS 2008, Springer, London, UK, pp. 210-219.
[25] Tauscher, L. & Greenberg, S. 1997, 'How people revisit web pages: emprical findings and implications for the design of history systems,' International Journal of Human Computer Studies, vol. 47, no. 1, pp. 97-138.
[26] Cockburn, A. & McKenzie, B. 2001, 'What do web users do? An empirical analysis of web use,' International Journal of Human-Computer Studies, vol. 54, no. 6, pp. 903-922.
[27] Cheung, D. W., Kao, B. & Lee, J. 1998, 'Discovering user access patterns on the World Wide Web,' Knowledge-Based Systems, vol. 10, no. 7, pp. 463-470.
[28] Lane, T. & Brodley, C. E. 1997, 'An Application of Machine Learning to Anomaly Detection,' in Proceedings of the 20th National Information Systems Security Conference, pp. 366-380.
[29] Balajinath, B. & Raghavan, S. V. 2001, 'Intrusion detection through learning behaviour model,' Computer Communications, vol. 24, no. 12, pp. 1202-1212.
[30] Li, L., Sui, S. & Manikopoulos, C. N. 2006, 'Windows NT User Profiling for Masquerader Detection,' in Networking, Sensing and Control, 2006. ICNSC '06. Proceedings of the 2006 IEEE International Conference on, pp. 386-391
[31] Bukhtoyarovf V. and Semenkin E., "Neural Networks Ensemble Approach for Detecting Attacks in computer Networks," WCCI 2012 IEEE World Congress on Computational Intelligence, June, 10-15, 2012 - Brisbane, Australia
[32] Chang R., Lai L.,Su W., Wang J., Kouh J., "Intrusion Detection by Backpropagation Neural with Sample-Query and Attribute-Query", International Journal of Computational Intelligence Research, ISSN 0973-1873 Vol.3, No. 1 (2007), pp. 6-10
[33] Ahmed, A. A. E. & Traore, I. 2005, "Anomaly intrusion detection based on biometrics", in Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, pp. 452-453
[34] Aho, A and Corasick, M. (1975). —"Efficient String Matching: An Aid to Bibliographic Search", Communications of the ACM, 18, 1975, pp. 333-40.
[35] Anagnostakis, K. G., Markatos, E. P., Antonatos, S. and Polychronakis, M. (2003). "E2xB: A domain-specific string matching algorithm for intrusion detection", In Proceedings of the 18th IFIP International Information Security Conference (SEC2003), May 2003
[36] Antonatos, S., Polychronakis, M., Akritidis, P., Anagnostakis, K.G., and Markatos, E.P. (2005). "Piranha: Fast and Memory-Efficient Pattern Matching for Intrusion Detection", ;in Proc. SEC, 2005, pp.393-408.
[37] Axelsson, S. (2000) "Intrusion-detection systems: A taxonomy and survey" Tech. Rep. 99-15, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 2000.
[38] Boyer, R. and Moore, S. (1977). "A Fast String Searching Algorithm." ,CACM, 20, 1977, 762-72

[39] Cheung, D. W., Kao, B. & Lee, J. 1998, "Discovering user access patterns on the World Wide Web,' Knowledge-Based Systems", vol. 10, no. 7, pp. 463-470.
[40] Gong, F. (2003). "Deciphering Detection Techniques: Part II Anomaly Based Intrusion Detection [White Paper]", McAfee Security, McAfee Security White Paper, 2003, Retrieved October 10, 2012, from https://secure.mcafee.com/japan/products/pdf/Deciphering_Detection_Techniques-Anomaly-
[41] Grant Pannell and Helen Ashman " Anomaly Detection over User Profiles for Intrusion Detection", Proceedings of the 8th Australian Information Security Management Conference, University of South Australia
[42] H. Debar, M. Dacier and A. Wespi, “To-wards Taxonomy of Intrusion Detection systems”, Computer Networks: The International Journal of Computer and Telecommunications, vol. 31, no. 9, pp. 805-822, April 1999.
[43] Horspool, R. N. (1980). "Practical fast searching in strings. Software Practice and Experience", 10(6):501–506, 1980.
[44] Imsand, E. S. & Hamilton, J. A. 2007, "GUI Usage Analysis for Masquerade Detection", in Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC, pp. 270-276.
[45] K. Jackson, "Intrusion Detection Systems (IDS): Product Survey", Los Alamos National Labora-tory, 1999.
[46] L. Wei, M. Tavallaee and A. A. Ghorbani, “Detecting Network Anomalies Using Different Wavelet Basis Functions”, IEEE Conference on Communication Networks and Services Research, CNSR 2008, pp. 149-156, Aug. 2008.
[47] Li, L., Sui, S. & Manikopoulos, C. N. 2006, "Windows NT User Profiling for Masquerader Detection," in Networking, Sensing and Control, 2006. ICNSC '06. Proceedings of the 2006 IEEE International Conference on, pp. 386-391.
[48] Pfleeger, C. and Pfleeger, S. (2003). "Security in computing". Prentice Hall, 2002.
[49] R. Heady, G. Luger, A. Maccabe, M. Servilla, "The architecture of a network level intrusion detection system", Technical report, Computer Science Department, University of New Mexico, Aug. 1990
[50] Sandip K Pal., Manish Anand "User Behaviour based Anomaly Detection for Cyber Network Security " ,Jan 2014, HAPPIEST MINDS TECHNOLOGIES ,By Happiest Minds, Analytics Practice
[51] Shavlik, J. & Shavlik, M. 2004, "Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage," in Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, Seattle, WA, USA, pp. 276-285
[52] Stillerman, M., Morceau, C., and Stillman, M. (1999)., " Intrusion Detection for Distributed Applications", Communications of the ACM, 42(7), July, 1999, 62-69.
[53] Sunday, D. M. (1990), "A very fast substring search algorithm", Communications of the Association for Computing Machinery, 1990, pp. 132-142.
[54] Wu, S., and Manber, U. (1992). "Fast Text Searching With Errors." Technical Report TR-91-11, Department of Computer Science, University of Arizona., 1991. To appear in Proceedings of USENIX Winter 1992 Conference, San Francisco, January, 1992.
[55] Y. Yasami, M. Farahmand and V. Zargari, “An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks”, IEEE International Conference on Systems and Networks Communications (ICSNC 2007), pp. 69-69, Aug. 2007
[56] Knuth, D. E., Morris, J. H., and Pratt, V. R. (1977),"Fast pattern matching in strings". SIAM Journal on Computing, 6(2), June 1977, pp. 323–350



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY