3rd National Conference on Innovative Research Trends in Computer Science and Technology (NCIRCST 2018) ISSN: 2454-4248
Volume: 4 Issue: 3 31 – 36

Effective Analysis on Detection of the Security Attacks Based on the Doila Method in Mainframes

Thurkka S Banumathy D

Final year Student 2-Associate Professor

Department of Computer Science
Paavai Engineering College
Namakkal-637018

***ABSTRACT*:** The idea is to detect the misuse of authorizations by intruders based on the detection method. We present a modern approach of detecting the security attacks by using a detection method known as DOILA (Detection on Invalid Logon Attempts). In this paper, we will discuss on the development of the JCL coding to detect the security attacks and then we will test the coding in Mainframes environment to gauge its effectiveness. Since the virtual machines can be running different operating systems and applications, the attacker can generate attacks in a single vulnerability in any of the operating systems or applications. Our aim is to consider the design choices and develop an intrusion detection architecture that would enable efficient detection and prevention of different types of attacks in Mainframes environment.

***KEYWORDS*:** Job control language, intrusion, authorization, security attacks, invalid logon, personal communications, password threshold and access control.

*****

Introduction

Security Attack is defined as any action that compromises the security of information. Computer security is required because most organizations can be damaged by hostile software or intruders. There may be several forms of damage which are obviously interrelated. Computer security can be very complex and may be very confusing to many people. It can even be a controversial subject. Network administrators like to believe that their network is secure and those who break into networks may like to believe that they can break into any network. Improper installation, selecting wrong components, incomplete devices, lack of knowledge, unsecure or less secure network components can cause physical threat to the critical network resources. The purpose of information security is to preserve the three elements: confidentiality, integrity and availability.

Details

Confidentiality means allowing only authorized users or systems to access protected data. The most widespread form of confidentiality failure today occurs with identity theft. System integrity means that no unauthorized parties have intentionally or unintentionally altered the information (for example, billing records), and do not have the authority to alter it. Additionally, the proof that the data has not been modified by unauthorized persons is the accountability that bank auditors seek the most expressions), but little or no difference within classes (same person or expressions in various conditions). Availability is synonymous with uptime when discussing hardware. When considered in the larger picture, uptime is not just a function of hardware, but also of software stability and resilience to disaster or attack. Availability is about resilience, business continuity, and disaster recovery. It is essential to ensure backup information and systems are in place for recovery purposes.

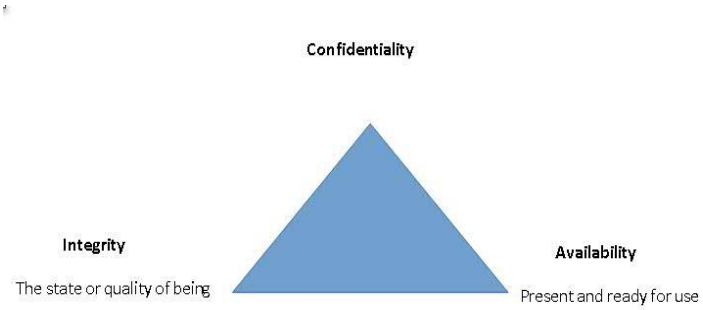

Fig 1: Security concept

Methods Of Authentication

Authentication is the process by which the computer system verifies who you are and also if a user enters the system, the user's identity must be verified through the use of some mechanism. Methods of authentication can be classified by one of three methods:

- Something that is known by the user (passphrase or password)
- Something that user owns (pass card, smartcard, digital certificates)
- Something that exists with user (fingerprint)

The security products authorize which resources the user may access and authorizes in what way the user may access them (read only, read and update). The security administrator is responsible for defining the system resources that need protecting (data, transactions, terminals, programs, and various other types of resources. the security product records these definitions in its database and then refers to this information to decide if a user should be permitted to access a system resource. Identification and authorization work together to implement the concepts of security.

INTRUSION DETECTION APPROCHES

Computers that are single or connected to networks are exposed to potentially damaging access by unauthorized

"hackers". To get rid of it, there must be an effective and proper intrusion detection system. An IDS generally detects unwanted manipulations of computer systems, mainly through the Internet. The manipulations may take the form of attacks by crackers. An intrusion detection system is used to detect several types of malicious behaviours that can compromise the security and trust of a computer system. Pattern matching based intrusion detection approaches are commonly used in the network based intrusion detection systems in which attack patterns are modelled, matched and identified based on the packet head, packet content or both. Attack patterns could also be established in host-based intrusion detection systems through concatenating the words representing the system calls in a system audit trail.

Rule-based expert system is one of the earliest techniques used for misuse detection. Expert systems encode intrusive scenarios as a set of rules, which are matched against audit or network traffic data. Any deviation in the rule matching process is reported as an intrusion. MIDAS was designed and developed to monitor intrusions for networked mainframe. It uses and analyzes audit log data by combining the expert system technology with statistical analysis.

Disadvantages Of Existing Detection Approaches

- Greatest visibility required
- Requires a high level of expertise and security awareness
- Resource limitations
- Larger amount of memory
- High burden on the practitioners to make sense of the data
- Fails to provide fine grained detail.

Doila Method And Benefits

System security must allow authorized users the access they need and prevent unauthorized access. Many company's critical data are now on computer and is easily stolen if not protected. RACF and the other available packages are add-on products which provide the basic security framework on a z/OS mainframe. The proposed method presents a modern approach of detecting the security attacks by using a detection method known as DOILA (Detection on Invalid Logon Attempts). This method can capture the knowledge of the number of successful and unsuccessful logon attempts and the number of excluded logons. The DOILA method can provide the number of invalid logon attempts throughout the day based on the terminal address and also isolate the malicious entities that are generating the attack traffic. The lists of the intruders who have exceeded the password threshold are determined by DOILA method which can be used to determine if any investigation is necessary based on these thresholds.
Some of the benefits of DOILA methods are no manual intervention required, self - explanatory on the report, no expertise required, reports generated on daily basis and the higher level of security.

System Architecture Of Proposed System

The submission of the detection jobs based on DOILA method scans the daily records of activity for 5 types of logon violations, invalid passwords, invalid new passwords, undefined user, auto revoke and revoked user. There is an ability to exclude specific user ids / terminals from the report if they are consistent. A note should be sent to the service provider to verify the errors are false positives and have them approve the exclusion of the user id/terminal. Every effort should be taken to eliminate these false positives, however, if all efforts fail to resolve the issue, then the exclusion list can be updated to include the user id /terminal.

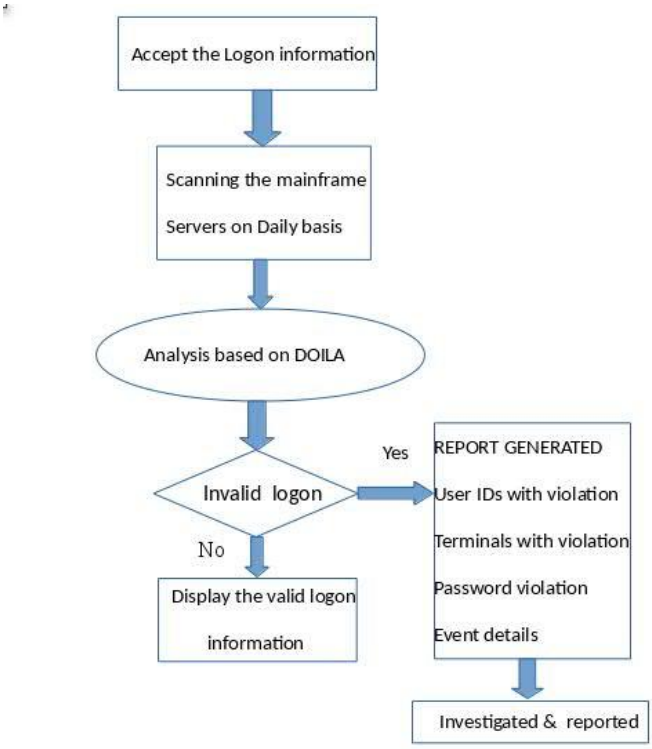

Fig 2: Architecture of DOILA method

The generated output is broken down into the following separate reports: VIOLATION SUMMARY - Reflects a summary of violations by type, from invalid logon attempts for valid user ids, to invalid logons to undefined user ids to revocation of user ids due to exceeding the system password limits. JOBINIT SUMMARY - This is self-explanatory, reflects the number of successful and unsuccessful logon attempts and the number of excluded user id/terminals. USER IDS WITH VIOLATIONS - lists the users which have exceeded the total violation count set. TERMINALS WITH VIOLATIONS - lists the users which have exceeded the total violation count set for a specific terminal. Use this report to determine if any investigation into terminal activities is necessary. PASSWORD VIOLATION DETAILS - Outlines in detail each invalid logon attempt by non-excluded user id/terminals. VIOLATIONS BY TIME THRESHOLD – This outlines violations by terminal within a specific time period of 1800 seconds. The report provides an event summary followed by the details for each event.

COMPARISION WITH PREVIOUS WORK

Several information security techniques are available today to protect information systems against unauthorized use. Initial research on Host based intrusion detection by Sandip K (2011)

[1] was based on the hypothesis that security violations can be detected by monitoring the system's audit data. This approach used 'user profiles' to represent the behavior of the users and used statistical methods to detect anomalies. Dorothy Denning [2] introduces a prototype that would analyze audit trails from government systems and track user activity. He named this system as Intrusion Detection Expert System (IDES), and it was the foundational research into IDS technology in 1985. This paper presents the first intrusion detection model, which has six main components: subjects, objects, audit records, profiles, anomaly records, and activity rules. Subjects refer to the initiators of activity in an information system; they are usually normal users. Objects are the resources managed by the information system, such as files, commands and devices. Audit records are those generated by the information system in response to actions performed or attempted by subjects on objects. IDS system called Network System Monitor (NSM) was introduced by Todd. Heberlein [3] in 1989 NSM was different from IDES and DIDS (Distributed Intrusion Detection System) in that it would analyze network traffic rather than system logs. NSM, along with the now commercially available Stalker IDS, helped to create new awareness and interest in IDS research for the commercial and public sectors.

The use of a time-based inductive machine (TIM) to capture a user's behavior pattern. As a general-purpose tool, TIM discovers temporal sequential patterns in a sequence of events was introduced by Teng, Chen, LU [4]. The sequential patterns represent highly repetitive activities and are expected to provide predication. The temporal patterns, which are represented in the form of rules, are generated and modified from the input data using a logical inference called inductive generalization. When applied to intrusion detection, the rules describe the behavior patterns of either a user or a group of users based on past audit history. The survey of several host-based and network- based IDSs, and identified the characteristics of the corresponding systems are identified. The host-based and systems employ the host operating system's audit trails as the main source of input to detect intrusive activity, while most of the network-based IDSs build their detection mechanism by monitoring network traffic, and some employ host audit trails was submitted by Mukherjee B, Heberlein L and Levitt K[5]. An outline of a statistical anomaly detection algorithm employed while most of the network-based IDSs build their detection mechanism by monitoring network traffic, and some employ host audit trails as well. An outline of a statistical anomaly detection algorithm employed in a typical IDS. The combination of the taxonomy was introduced by Kevin S, Roy A [6], the notion of activity scope provides us with a flexible and practical instrument to describe intrusion detection system. This taxonomy has been developed to describe the functional aspects i.e., the capabilities of intrusion detection system such that one can in a next step evaluate intrusion detection system for their potential to detect attacks, generate false positives etc. Phillip Brooke [7], presents a new IDS framework for mobile adhoc network (MANET) environments based upon the concept of a friend in a small world phenomenon. The two-tier IDS framework has been designed to overcome longer detection mechanisms and detection suffering from the potential for blackmail attackers and false accusations with the help of friend nodes. It is hypothesized that with the introduction of friend nodes, the impacts of the IDS problems can be minimized. It is noted that the proposed framework would not be able to work on a diverse MANET environments.

Sequeira and Zaki [8] designed and implemented a temporal sequence clustering- based intrusion detection which is user-profile dependent. This was done by collecting and processing UNIX shell command data. Though analyzing a user activity is a natural approach to detect intrusions, experience shows that it is far from accurate. It is because of the fact that user behavior typically lacks strict patterns. Dynamic usage by user gave a greater reflection of the features that define host behavior. In their work, user activity involves using programs. Programs obtain the required services by executing the specific system calls that provided the needed function. An unsupervised host-based intrusion detection system based on system call arguments and sequences was proposed by Maggi et al [9]. They defined a set of anomaly detection models for the individual parameters of the call and then describe a clustering process that helps to better fit models to system call arguments and creates interrelations among different arguments of a system call. Haystack [10] introduced a combined anomaly detection/misuse detection IDS that models individual users as well as groups of users. It assigns initial profile to new users, and updates the profiles once a pattern of actual behavior is recognized.

Coding Scheme

In our coding scheme, we create the code, JCL by analyzing the control instructions. Control instructions are able to affect the user execution environment, and they should only be available to the operating system. A hardware indicator can be set that indicates that a specific executing program has the privilege or not to use control instructions. Control instructions deal with many aspects of the user execution environment, such as: Memory allocation and access control, Data transfer between the system memory and external devices and User program execution and resumption. The z/Architecture also provides a set of general instructions that can be executed by any program; that is, both by user programs and operating systems. These general instructions are intended to be the building blocks of the user's problem-solving process.
Entering commands from TSO is one way to accomplish tasks in z/OS, but many other ways exist. One of the most popular and powerful ways is to create files that contain lists of things to do. These lists are called batch jobs and are written in z/OS Job Control Language (JCL), which fulfills roughly the same role as shell scripting languages in UNIX. JCL is a language with its own unique vocabulary and syntax. We use JCL to create batch jobs. A batch job is a request that z/OS will execute later. z/OS will choose when to execute the job and how much z/OS resources the job can have based upon the policies that the system administrator has set up.

JCL structure

```
//PSWDCNTL DD   *
 SORT FIELDS=(10,8,CH,A)
 INCLUDE COND=(11,4,CH,EQ,C'INVALID')
*      1: DATE      7:TIME     16:USERID      24:TERMINAL
31:ERROR1         *
```

```
 OUTREC
FIELDS=(1:52,5,7:1,8,16:40,7,24:63,6,31:11,24,26X)
 OPTION  VLSHRT
//*
//LOCKCNTL DD   *
 SORT FIELDS=(10,8,CH,A)
 INCLUDE COND=(11,5,CH,EQ,C'INVLD')
*     1:  DATE     7:TIME    16:USERID     24:TERMINAL
31:ERROR1 53:BY.. *
 OUTREC
FIELDS=(1:41,5,7:1,8,16:33,7,24:52,6,31:11,22,53:59,9,19X)
 OPTION  VLSHRT
//*
```

This is a key feature of z/OS: z/OS can manage multiple diverse workloads (jobs) based upon the service level that the installation wants. For example, online financial applications will be given higher priority and, therefore, more z/OS resources, and noncritical work will be given a lower priority and, therefore, fewer z/OS resources. z/OS constantly monitors the resources that are available and how they are consumed, reallocating them to meet the installation goals.

Connection with cisco any connect

The Cisco Any connect Secure Mobility client is a web-based VPN client that does not require user configuration. VPN, also called IP tunneling, is a secure method of accessing computing resources. Install the most recent version of the Java Runtime Environment before installing the Any connect program and add VPN to the list of trusted sites. This will allow the browser to easily and securely communicate with VPN. The user name and password are the user name and password which is used to connect to services. Choose the appropriate VPN Group Authentication Profile. Click the Start Any connect link on the upper-left side of the browser window to begin installing the Any Connect Secure Mobility client. Once the installation is complete, the connection will be automatically established to VPN.

Fig 3: Cisco Any Connect

Personal Communications provides communications device drivers for some legacy adapters. For Windows XP and later Windows operating systems, the device driver package requires a separate installation and removal process. In addition, some communication adapters may not be supported for Windows XP and later Windows operating systems. Installation of Personal Communications to a drive other than the Windows volume (the drive containing the Windows folder) may still require as much as 180 MBs of available free space on the Windows volume. This is due to the installation of files to the Windows and system folders, as well as the caching of the Installer database by the Windows Installer service, and the use of temporary disk space by the Windows Installer service during the installation.

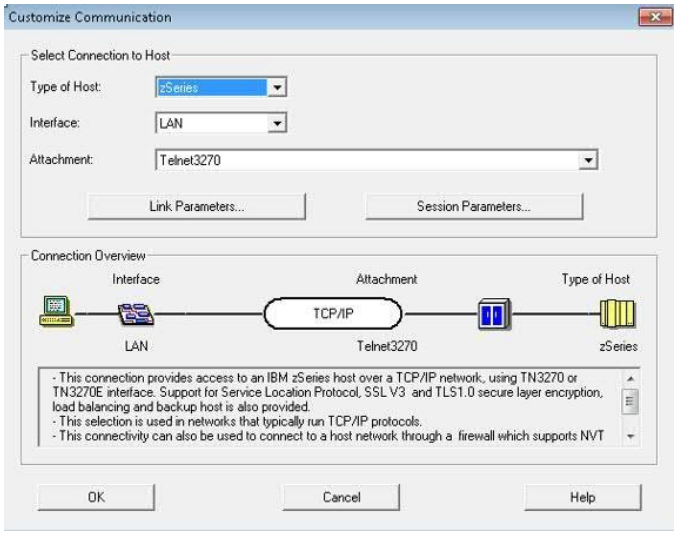

Fig 4: Connection on PCOMM

Encrypting TCP/IP data is a common way to secure these communications. Actually, the data is not only encrypted for the sake of confidentiality by the sender, but also it contains cryptographic check sums that assure the recipient of their integrity and the trustworthiness of the sender. The z/OS TCP/IP stack can be enabled to create or accept IPSec VPNs communications, and it automatically checks for hardware cryptographic coprocessors being in operation in the system. If this is the case, then the z/OS TCP/IP stack offloads the cryptographic computations to the coprocessors.

Doila Method In Z-Servers Using Racf

Making data secure on z/OS platforms involves not only protection of data from unauthorized access, but equally important—it protects from inadvertent destruction of data sets or files. Data sets can be protected by controlling who has access to them, and what access the individuals or groups have. The z/OS operating system contains a fully integrated UNIX component named z/OS UNIX. The addition of UNIX has allowed the z/OS operating system to add open standard technologies to its already impressive online and batch processing capabilities. z/OS UNIX workload may execute as either online or batch workloads, depending on the nature of the workload. A user is the term used to describe an individual person in a computer system. A group is the term used to describe a list of users that are somehow associated or "grouped" together.

02/09/18 USER IDS WITH 5 OR MORE VIOLATIONS - DEV

USERID	INVPSWD	INVNPWD	UNDFUSER	REVKAUTO	REVKUSER	TOTAL
AC52441	0	0	7	0	0	7
A202922	0	0	7	0	0	7

02/09/18 PASSWORD VIOLATION DETAILS - DEV

DATE	TIME	SYSID	REASON	TERMINAL	USERID
02/08/18	19:26:19	P83A	UNDFUSER		AC08725
02/08/18	19:26:19	P83A	UNDFUSER	SPS74551	AC08725
02/08/18	19:26:19	P83A	UNDFUSER		AC08725
02/08/18	19:26:19	P83A	UNDFUSER	SPS74551	AC08725
02/08/18	13:03:42	P83A	UNDFUSER		AC52441
02/08/18	13:03:42	P83A	UNDFUSER	SPS74554	AC52441
02/08/18	13:03:42	P83A	UNDFUSER	SPS72484	AC52441
02/08/18	13:03:42	P83A	UNDFUSER		AC52441
02/08/18	13:03:42	P83A	UNDFUSER	SPS74554	AC52441
02/08/18	13:03:43	P83A	UNDFUSER		AC52441
02/08/18	13:03:43	P83A	UNDFUSER	SPS74554	AC52441

Fig 5: Result Analysis

In any UNIX system, including z/OS, a unique numeric identifier is used to identify each user (UID) or group (GID) in UNIX systems. When adding a user or group to the system, the system administrator provides an alphanumeric name to represent the user or group and the system assigns an available numeric identifier to each user or group added. These numeric UIDs and GIDs, along with other information related to the user or group, have been traditionally stored in files named /etc/passwd and /etc/group, respectively. Because these files contain identifying information about the users and groups of users defined on the system, they are often a valuable source of information for hackers, so their contents should be protected from unauthorized access.

Recent Trends in Intrusion Detection Reporting

SMFID:S0W1	INTRUSION DETECTION HISTORY AND TRENDS						
DATES	07/01	06/29	--/--	--/--	--/--	--/--	--/--
TIMES	18:39	18:38	--:--	--:--	--:--	--:--	--:--
TOTAL	002	003	000	000	000	000	000
policy_elements							
SCAN Detection	--C	--C	---	---	---	---	---
Malformed Packets	---	---	---	---	---	---	---
Restrict Outbound	---	---	---	---	---	---	---
Restrict Protocol	---	---	---	---	---	---	---
Restrict IP Option	---	---	---	---	---	---	---
Restrict Redirect	---	---	---	---	---	---	---
Restrict Fragment	---	---	---	---	---	---	---
UDP Perpetual Echo	---	---	---	---	---	---	---
Floods	--C	---	---	---	---	---	---
Data Hiding	---	--C	---	---	---	---	---
TCP Queue Size	---	---	---	---	---	---	---
Global TCP Stall	---	---	---	---	---	---	---
EE LDLC Check	---	---	---	---	---	---	---
EE Malformed Packet	---	---	---	---	---	---	---
EE Port Check	---	---	---	---	---	---	---
EE XID Flood	---	---	---	---	---	---	---

Fig 6: IDS Baseline

It is becoming increasingly important to not only protect systems from attacks, but also detect patterns of usage that might indicate impending attacks. Many attacks follow a sequence of information gathering, unauthorized access to resources, and denial of service. It can be difficult to determine the originator of denial of service attacks. Correlating information gathering activities with access violation may help identify intruders before they succeed. An attack can be a single packet designed to crash or hang a system. An attack can also consist of multiple packets designed to consume a limited resource, thus causing a network, system or application to be unavailable to its intended users (that is, denial of service). DOILA method allows to turn on attack detection for one or more categories of attacks independently of each other. In general, the types of actions that can be specified for an attack policy are event logging, statistics gathering, packet tracing and discarding of the attack packets.

Resource Access Control Facility

RACF (part of f Security Server) and the other available Packages are add-on products which provide the basic security framework on a z/OS mainframe. It identifies and authenticate users, authorize users to access protected resources, control means of access to resources.

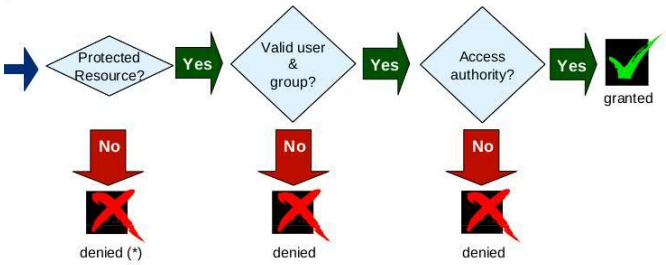

Fig 7: Access control structure

RACF works on a hierarchical structure:

- ALLOC allows data set creation and destruction
- CONTROL allows VSAM repro
- WRITE allows update of data
- READ allows read of data
- NONE no access

Some of the system tasks that also need to be protected on the z/OS environment are started tasks. Started tasks are system jobs that are brought up at system initialization time. Started tasks can also be kicked off at any time by an operator (or anyone with the authority to do so). Daemons such as LDAP, FTPD, and the HTTP Server are started tasks on z/OS. When a job is submitted on the system, it requires a user ID to validate that the user is authorized to submit jobs. The best balance of security practices needs to be planned and implemented.

Conclusion

To develop an intrusion detection architecture that would enable efficient detection and prevention of attacks in Mainframes environment. The survey on intrusion detection gives the overview of existing methods, advantages and disadvantages of the tools that are used to detect and prevent the intrusions. The proposed framework is expected to give us a faster and more reliable detection results than what has been offered by previous efforts. Detecting the actual penetration would be impossible without monitoring all the attempts made by the intruders. The detection method for identifying the invalid logon attempts is an extra layer of protection that enhances the overall security of the target system.

An open problem is the attempt by an intruder or attacker to go farther than the machine's connection to the network when the attacker tries to penetrate the files and programs residing on the machine, or even penetrate other networks that the machine is connected to. The level of security controls for your mainframe must be sufficient for the criticality of the data and business processes hosted on it. While the Mainframe is extremely

secure, there is still a variety of attack vectors that can result in a breach. Historically, risk may seem low but the recent increase in mainframe connectivity means mainframes need the same attention to security as any other device on the network because, 65% of the world's data resides on the mainframe. It is said that no computer system is 100% secure, but an effective level of security can be achieved. Effective security is not achieved, however, simply through the use of settings and tools, but rather through careful planning in advance by means of a well thought-out and integrated security detection methods. Security exposures could diminish the value of all work done to secure the underlying hardware and operating systems.

References

[1] D. E. Denning and P. G. Neumann, "Requirements and model for IDES-A real-time intrusion detection system," Comput. Sci. Lab, SRI International, Menlo Park, CA, Tech. Rep., 1985.
[2] S. Forrest, S. Hofmeyr, A. SoMayaji, and T.Longstaff,(1996), A Sense of Self for Unix Processes,Proc. IEEE Symp. Security and Privacy, pp.120-128.
[3] K. Ganesh, M. Sekar, and V. Vaidehi(2011), Semantic intrusion detection system using pattern matching and state transition analysis," Recent Trends in Information Technology (ICRTIT), 2011 International Conference ,pp. 607-612.
[4] T. F. Lunt. "Automated audit trail analysis a n d intrusion detection: A survey," Proc.. 1 lth National Computer Security Conf., Baltimore. MD. Oct. 1988.
[5] H. S. Vaccaro and G. E. Liepins, "Detection of anomalous computer session activity." Proc.. 1989 Symposium on Research in Security and Privacy. Oakland. CA, pp. 280.289. May 1989.
[6] J. Hochberg et al., "NADIR: a n automated system for detecting network intrusion and misuse." Computers and Security. Vol. 12, no. 3, pp. 235-248. May 1993.
[7] L. T. Heberlein et al.. "A network security monitor."Proc.. 1990 Symposium on Research in Security and Privacy. Oakland, CA, pp. 296-304, May 1990.
[8] S. M. Bellovin, "There Be Dragons," Proc., Third UNIX Security Symposium. Baltimore,MD. Sept. 1992.
[9] T. Bartoletti, "SPIWNIX: Security Profile Inspector for UNM computer systems," Proc.. 3rd Workshop on Computer Security Incident Handling, Hemdon. VA. Aug. 1991.
[10] G. Creech and J. Hu(2014), A semantic approach to host-based intrusion detection systems , Computers, IEEE Transactions, vol. 63, no. 4, pp. 807-819.
[11] F. Bin Hamid Ali and Y. Y. Len(2011), Development of host based intrusion detection system for log files, Business, Engineering and Industrial Applications (ISBEIA), 2011 IEEE Symposium , pp. 281-285.
[12] E.Kesavulu Reddy, V.Naveen Reddy, P.Govinda Rajulu(2011), A Study of Intrusion Detection in Data Mining, Proceedings of the World Congress on Engineering WCE 2011, vol. 3.
[13] Shruthi.K.R, Shweta Hiremath, Tejaswini V Nalwade, Mangala C N(2014), A Host Based Intrusion Detection System Using Semantic Approach To System Call Patterns, IEEE Sponsored International Conference On Empowering Emerging Trends In Computer, Information Technology & Bioinformatics International Journal of Computer, Information Technology & Bioinformatics (IJCITB), Volume-2, Issue-2 .
[14] Debar H. and Dacier Marc and Wespi Andreas(1999), Towards a taxonomy of intrusion-detection systems, Computer Networks, vol 31,number 8, pages 805-822.
[15] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S.Choi. A taxonomy of computer program security flaws, with examples. ACM Computing Surveys, 26(3):211–254, September 1994.