Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Overview of Current Intrusion Detection Techniques

Sri .Ozair Ahmad [*1], Sri. O.S.Khanna[2], Sri. T.Vinod Kumar[3], Sri. M.Purushotham Reddy[4], Sri. S.Satish Kumar[5]
[1]MACET,Patna, [2]NITTTR, Chandigarh, [3,4]VBIT, Proddatur, [5]CBIT, Proddatur

Abstract: Intrusion detection is a significant focus of research in the security of computer systems and networks. The intrusion detection system basically detects attack signs and then alerts. This paper presents the technologies which are discussed are designed to detect instances of the access of computer systems by unauthorized individuals and the misuse of system resources by authorized system users. A review of the foundations of intrusion detection systems and the methodologies which are the focus of current development efforts are discussed.

Keywords: Intrusion detection, anomaly detection, misuse detection, computer security.

I. INTRODUCTION

This paper discusses the current research and development efforts to detect internal and external penetrations of computer systems and networks. The area of intrusion detection is central to the concept of computer security. While a number of methods can be employed to protect the data stored within a computer system, the ability to identify instances of an attack on the computer is paramount if an effective security mechanism is to be developed.

Halme and Bauer ([3]) have identified intrusion detection as one of six components in their taxonomy of anti-intrusion techniques. The first three components which they identified; prevention, preemption, and deterrence, are primarily based on passive measures which decrease the likelihood of a successful attack on a system. These components address the policy related issues of information security and those elements which can be incorporated into a system with minimal effort. Examples of these include the establishment of organizational security guidelines, security education and training, and the posting of warning notices on the initial screens of a system.

The need for effective intrusion detection mechanisms as part of a security mechanism for computer systems was recommended by Denning and Neumann ([7]). They identified four reasons for utilizing intrusion detection within a secure computing framework:

1. Many existing systems have security flaws which make them vulnerable, but which are very difficult to identify and eliminate because of technical and economic reasons.
2. Existing system with security flaws cannot be easily replaced by more secure systems because of application and economic considerations.
3. The development of completely secure systems is probably impossible.
4. Even highly secure systems are vulnerable to misuse by legitimate users.

II. FUNDAMENTALS OF INTRUSION DETECTION

2.1 Evolution of Intrusion Detection Mechanisms

The first major work in the area of intrusion detection was discussed by J.P Anderson in [2]. Anderson introduced the concept that certain types of threats to the security of computer systems could be identified through a review of information contained in the system's audit trail.

1. External Penetrations - Unauthorized users of the system
2. Internal Penetrations - Authorized system users who utilize the system in an unauthorized manner.
3. Misfeasors - Authorized user who mislead their access privileges.

Anderson indicated that a particular class of external attackers, known as clandestine users, were particularly dangerous to the system resources. Clandestine users are those who evade both system access controls and auditing mechanisms through the manipulation of system privileges or by operating at a level that is lower than what is regularly monitored by the audit trail. Anderson suggested that clandestine users could be detected by lowering the level which is monitored by the audit trail, monitoring the functions that turn off the audit systems, or through a comparison of defined "normal" usage patterns of system resource usage with those levels which are currently observed.

2.2 INTRUSION DETECTION APPROACHES

All current intrusion detection systems make four assumptions about the systems that they are designed to protect:

1. Activities taken by system users, either authorized or unauthorized, can be monitored.
2. It is possible to identify those actions which are indications of an attack on a system
3. Information obtained from the intrusion detection system can be utilized to enhance the overall security of the network.

4. A fourth element which is desirable from any intrusion detection mechanism is the ability of the system to make an analysis of an attack in real-time.

There are currently a variety of approaches being utilized to accomplish the desirable elements of an intrusion detection system. Two of these, anomaly detection and misuse detection, form the core of several intrusion detection techniques which currently exist. Other approaches, such as pattern recognition, are attempting to identify new methods of identifying information system attacks.

ANOMALY DETECTION

Anomaly detection is the general category of intrusion detection which works by identifying activities which vary from established patterns for users, or groups of users. Since masquerading as a legitimate user is a very powerful method for an attacker to gain access to system resources, this type of approach looks for the variations in behavior which might indicate a masquerade. Anomaly detection typically involves the creation of knowledge bases which contain the profiles of the monitored activities.

Several types of profiles are generally used in anomaly detection. User profiles contain the parameters of a user's typical session. While these profiles are potentially the most useful in identifying indications of anomalous behavior, they are also the most difficult to create and to maintain. A balance must be struck between establishing short -term profiles, which establish patterns of recent activity and long-term profiles, which establish a historical overview of a user's activities. Unless they are updated frequently, user profiles can lead to a large number of false alarms as the user's activities change over time.

To avoid, or at least modify, the adverse effects of the system's legitimate users, some anomaly detection systems include the use of user group profiles. In this method the user is placed in a work group which may or may not represent the actual assigned duties of the user. More frequently the group characterizes individuals with similar computer usage patterns. While group profiling assists in the maintenance of the detection mechanism, these profiles are often defined so broadly that unauthorized users can slip through the screen by behaving roughly similar to the typical user in the group.

Other profiles which are frequently used in anomaly detection include resource profiling, (monitoring the system-wide use of accounts, applications, communication ports, etc.), and executable profiling, (monitoring the use of printers, files, and other resources which cannot easily be attributed to a single user). This user-independent form of profiling is useful in detecting the presence of viruses and Trojan horses.

Anomaly detection mechanisms are usually dependent on input from an operating system's audit record. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must is utilized by the anomaly detector. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

MISUSE DETECTION

This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse detection also utilizes a knowledge base of information. The misuse knowledge bases include specific metrics on the various techniques employed by attackers when the knowledge base was created.

When applied to misuse detection, the rules become scenarios for network attacks. The intrusion detection mechanism identifies a potential attack if a user's activities are found to be consistent with the established rules. The use of comprehensive rules is critical in the application of expert systems for intrusion detection.

Like anomaly detection techniques, misuse detection systems suffer from the potential performance degradation which results from a dependency on audit trails for input. This disadvantage can be mitigated by improved system performance and reduced audit record sets.

COMBINED ANOMALY/MISUSE DETECTION

Research has also been conducted into intrusion detection methodologies which combine the anomaly detection approach and the misuse detection approach ([5]). These techniques seek to incorporate the benefits of both of the standard approaches to intrusion detection. The combined approach permits a single intrusion detection system to monitor for indications of external and internal attacks.

PATTERN RECOGNITION

In this approach, a series of penetration scenarios are coded into the system.

Pattern recognition possesses a distinct advantage over anomaly and misuse detection methods in that it is capable of identifying attacks which may occur over an extended period of time, a series of user sessions, or by multiple attackers working in concert. This approach is effective in reducing the need to review a potentially large amount of audit data.

The key disadvantage of pattern -recognition techniques is the reliance of the system on predefined intrusion scenarios.

NETWORK MONITORING

A final method of detecting system intrusions which is currently in use is the use of various network monitoring techniques. [6] These methodologies passively monitor network activity for indications of attacks.

Network monitoring offers several advantages over traditional audit -based intrusion detection systems. Because many intrusions occur over network at some point, and because networks are increasingly becoming the targets of attack, these

techniques are an excellent method of detecting many attacks which may be missed by audit -based intrusion detection mechanisms.

The greatest advantage of network monitoring mechanisms is their independence from reliance on audit data. Because these methods do not require input from any operating system's audit trail they can use standard network protocols to monitor heterogeneous sets of operating systems and hosts.

III. CURRENT INTRUSION DETECTION TECHNIQUES

The following is a review of the significant developments in intrusion detection research which have been made in the past several years.

3.1 NIDES

SRI International began research into an intrusion detection expert system in 1985. [5] The result of the research, the Intrusion Detection Expert System (IDES) has become a standard in intrusion detection systems. Several current systems are based in part on IDES prototype technology, ([8, 9, 10]).

The Next -Generation Intrusion Detection Expert System (NIDES) is the comprehensive enhancement to IDES. [1] NIDES is a real-time intrusion detection application which integrates a statistical analysis -based anomaly detector and a rule -based misuse detection system. This combination gives NIDES the ability to detect penetrations from internal and external attacks.

3.2 DIDS

The Distributed Intrusion Detection System (DIDS) is an intrusion detection mechanism which was developed jointly by the University of California at Davis, Lawrence Livermore Laboratory, Haystack Laboratory and the U.S. Air Force. DIDS combines attributes of a network monitoring system with the system-level capabilities of an audit record -based combined anomaly/misuse detector. DIDS incorporates a monitor on each host, a monitor on the local area network (LAN), and a DIDS director.

Each host monitor consists of a host event generator and a host agent. The host event generator reviews the audit data from the host for indications of events which may be part of an attack. The DIDS host event generators also utilize user and group profiles to identify anomalous behaviors in the audit record. The information identified by the host event generator is reported to the DIDS director by the host agent.

The LAN monitor is the network equivalent of the host monitor. It includes the LAN event generator and the LAN agent. However, unlike the host event generator, the LAN event generator does not review audit data. The LAN event generator utilizes the network monitoring approach to review all network traffic, including host-to-host connections and resources used. The information obtained by the LAN event generator is reported to the DIDS director by the LAN agent.

The DIDS director forms the heart of the intrusion detection mechanism. It is composed of three components, the communications manager, an expert system and a user interface. The communications manager is receives input from each of the host monitors and from the LAN monitor and forwards the information to the expert system for analysis. The communications manager is also capable of forwarding requests for additional information from the expert system to the host monitors and the LAN monitor. The DIDS expert system is a rule-based system which is responsible to analyzing the information received from the monitors and reporting it to the security official. The final component of the DIDS system, the user interface, allows a security official to interactively review the status of the system, receive reports from the expert system, and request additional security-related information from the system.

3.3 STAT/USTAT

The State Transition Analysis Tool (STAT) and USTAT, the variation of STAT which was designed specifically for the UNIX operating system environment, are rule -based penetration detection approaches which characterize the process of an attack on a computer system as a series of transitions from an initial state to a compromised state. The technique defines specific events, called signature actions, which occur between each of the intermediate transitions. The omission of any of the signature actions results in a failed attack on the system.

3.4 TRIPWIRE

In November 1992, the COAST laboratory at Purdue University introduced Tripwire. Tripwire is an integrity checking program which permits a system administrator to monitor system files for addition, deletion, or modification. The program is estimated to have been installed on several thousand systems worldwide.

While it is not an intrusion detection mechanism, Tripwire does provide valuable information for the process of detecting attacks on a system. Tripwire is designed for the UNIX operating system environment. the program has proven to be scaleable, portable, and manageable.

Tripwire utilizes input from a configuration file and a database to identify areas of interest. The configuration file consists of a description of the file systems which are to be monitored. The database contains the signatures of files which match the configuration. The signatures of the files are calculated based on a the contents of the system files. The signature computation is easy to derive but impossible to reverse.

3.5 GRIDS

Researchers in the COAST laboratory have recently proposed a novel approach to intrusion detection based on the analysis of activity graphs. The Graph-Based Intrusion Detection System (GrIDS) is designed to analyze network

activity in large networks for the presence of attacks. [4]

GrIDS aggregates the actions of a networks users into the activity graphs. Based on a review of the structure of these graphs the system can identify patterns which indicate intrusive behavior. In addition to diagramming the basic network activity, GrIDS incorporates supplementary information in the form of attributes to the tree-like structure of the diagram. Information received from other intrusion detection devices and network monitors can be included in the attributes of the activity graphs.

Individual types of graphs will be maintained in graph spaces with the GrIDS system. Because there are a number of possible attacks on the network, multiple graph spaces must be maintained. Each graph space is dependent on a specific rule set which modifies the graphs within it's graph space based on inputs to the system.

3.6 THUMBPRINTING

Thumbprinting is a method of tracking intruders through a sequence of logins, referred to by the authors as a connection chain. While it is not intended to be an independent intrusion detection system, it could prove to be a valuable addition to other technologies.

Thumbprinting was developed by researchers at the University of California at Davis in response to a weakness in DIDS. Because DIDS is unable to correlate to parts of a connection chain when a user has exited and then reentered outside of the DIDS domain, thumbprinting was devised to compare the content of the connections in the chain. Since commands issued by a user should remain the same as they pass through the various hosts in the connection chain, summaries of the content of connection at two points could be compared to determined if they were links in the same chain. The summaries would be generated by passively monitoring the network traffic at each host.

3.7 COOPERATING SECURITY MANAGERS

While DIDS takes a centralized security approach to network intrusion detection, Cooperating Security Managers (CSM) decentralizes the process. A separate CSM is run on each computer which is connected to the network. [11]

Each CSM consists of six elements. The heart of the CSM is the Security Manager (SECMGR). The SECMGR receives input from the various CSM components and coordinates with CSM's on other hosts as users pass through the network. The command monitor (CMNDMON) intercepts the commands from the user and forwards them to the host intrusion detection system (IDS). While CSM requires the presence of an intrusion detection system on each host, the actual mechanism is separate from the CSM and can therefore be any intrusion detection tool. Any intrusions detected by the IDS are reported to the SECMGR. The CSM Intrusion Handler (IH) is one of the distinguishing characteristics of CSM. Instead of simply reporting intrusive activity to a security administrator, the IH can also be configured to take more active measures against an intruder. These include terminating the user's current session, disabling the account being utilized by the alleged intruder, or backing up files which may be modified or deleted by an attacker. The SECMGR uses TCP to communicate with other CSM's through the communication handler (TCPCOM).

CSM only communicates with the CSM immediately before it in the connection chain, not all hosts on the network. Each CSM is responsible for relaying the message through the network.

In addition to addressing the need for detecting intrusive activity in a networked environment, CSM is also scaleable and portable because it is not specifically designed for any particular network-wide operating system. Each CSM is unaware of the operating environment on the other CSM's hosts. As long as a CSM has been developed for the operating system which is used on a host, it can be attached to a CSM - monitored network.

IV. CONCLUSION

We have presented an overview of the technologies which are being utilized for the detection of attacks against computer systems. We have also reviewed of some of the significant techniques which hold the promise of effectively protecting computer systems.

The security of information in computer-based systems and networks continues to be a major concern to researchers. The work in intrusion detection techniques and methodologies which has been a major focus of information security-related research in the past two decades is certain to continue. The area of intrusion detection is continuing to evolve. While a number of methodologies and tools have been designed to assist in the identification of intruders, no definable standard has been developed which could serve as the basis for a deployable intrusion detection tool. However, as the processing capabilities of computer systems improve and the innovative approaches to intrusion detection continue to be developed, the creation of an effective intrusion detection standard is inevitable.

REFERENCES

[1] Anderson, D., Frivold, T. & Valdes, A. (May, 1995). Next -generation Intrusion Detection Expert System (NIDES): A Summary. SRI International Technical Report SRI-CSL-95-07.

[2] Anderson, J.P. (April, 1980). Computer Security Threat Monitoring and Surveillance. Technical Report, J.P. Anderson Company, Fort Washington, Pennsylvania.

[3] Halme, L.R. & Bauer, R.K. (1995). AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques. Proceedings of the 18th National Information Systems Security Conference. Baltimore, MD.

[4] Levitt, K. (March 4, 1996). GrIDS-A Graph-Based Intrusion Detection System for Large Networks. Technical Report. University of California Davis.

[5] Lunt, T.F. (1989). Real-Time Intrusion Detection. Proceedings from IEEE COMPCON.

[6] Mukherjee, B., Heberlein, L.T. & Levitt, K.N. (May/June, 1994). Network Intrusion Detection. IEEE Network. pp. 26-41.

[7] Neumann, P.G. (1985). Audit Trail Analysis and Usage Collection and Processing. Technical Report Project 5910, SRI International.

[8] Smaha, S.E. (1988). Haystack: An Intrusion Detection System. Proceedings of the 4th Aerospace Computer Security Applications Conference.

[9] Sebring, M., Shellhouse, E., Hanna, M. & Whitehurst, R. (1988). Expert Systems in Intrusion Detection: A Case Study. Proceedings of the 11th National Computer Security Conference.

[10] Vaccaro, H.S. & Liepins, G.E. (1989). Detection of Anomalous Computer Session Activity. Proceedings of the IEEE Symposium on Security and Privacy.

[11] White, G.B., Fisch, E.A. & Pooch, U.W. (January/February, 1996). Cooperating Security Managers: A Peer-Based Intrusion Detection System. IEEE Network.

BIBLIOGRAPHY

Ozair Ahmad pursuing his M.E (Electronics&Communication Engineering) from NITTTR,Chandigarh. Presently he is working as Assistant Professor in Electronics&Communication Engineering, **MOULANA AZAD COLLEGE OF ENGINEERING AND TECHNOLOGY**, Neoraganj,Neora,Patna-Bihar,India.

Sri.O.S.Khanna., working as Associate Professor , National Institute of Technical Teachers' Training and Research Chandīgarh, India since 1984. Research field: Electrical and Electronic Engineering - Wireless and Mobile Communication,Wireless Sensor Networks.Worked as R&D Engineer at **Electronics Consortium Pvt Ltd.** Delhi, India during Nov 1979 - Jan 1981.Worked as Design and Development Engineeer at **Unitron Limited** Farīdābad, India Oct 1978 - Nov 1979 Worked as Junior Scientific Officer at **Defence Research & DevelopmentOrganization,India** Hyderabad, India during Jan 1976 - Oct 1978

Vinodkumar Tummalur pursuing his M.E (Electronics&Communication Engineering) from NITTTR,Chandigarh. Presently he is working as Assistant Professor in Electronics&Communication Engineering, **VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY**, Proddatur,Kadapa dist , A.P,India.

M.Purushotham Reddy received his M.Tech (Computer Science & Engineering) from Jawaharlal Nehru Technology University, Anantapuramu and Pursuing Ph.D(Computer Science & Engineering) from Jawaharlal Nehru Technology University, Anantapuramu . Presently he is working as Associate Professor in Computer Science & Engineering , **VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY**, Proddatur,Kadapa dist,A.P,India.

S.Satish Kumar received his M.Tech (Elcetronics Instrumentation & Communication Systems) from Sri Venkateswara University,Tirupati. Presently he is working as Assistant Professor in Electronics & Commnication Engineering, **CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY**, Proddatur,Kadapa dist, A.P,India.

