ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Attacks on Computer Network and Corresponding Security Measures

Gajanan D. Kurundkar*
Dept. of Computer Science, Shri Guru Budhiswami Mahavidyalya, Purna Dist. Parbhani(MS)
gaju_k_2001@yahoo.com

Quadri M.N
Dept. of Computer Science,
Yeshwant Mahavidyalaya, Nanded-(M.S.) India
mnq_1977@yahoo.com

Dr.Santosh D. Khamitkar
School of Computational Sciences, Swami Ramanand Teerth Marathwada University, Nanded (MS) (India)
s_khamitkar@yahoo.com

Abstract: Computer security means action of preventing and detecting unconstitutional use of your computer. Prevention measures help you to stop "intruders" from accessing any part of your computer system. With the free flow of routing data and the high availability of computer resources, possible threats to the networks can result in loss of privacy and in spiteful use of information or resources that can eventually lead to large financial losses. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done. *Intrusion detection* is the method of monitoring the events taking place in a computer system or network and analyzing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, standard security practices. Incidents have many causes, such as malware. Attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who mishandling their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not. Intrusion prevention systems repurpose-built hardware/software platforms that are designed to analyze, detect, and report on security related events. These are designed to inspect traffic and based on their configuration or security policy, they can drop malicious traffic. *Intrusions* encompass many undesirable activities, such as information theft and denial of service attacks.

Keywords : Intruder, cryptography, prevention, security, real time prevention, hash based protection, MD5 Algorithm

I. IS THE COMPUTER SECURITY IS IMPORTANT?

Computer security is the course of action of preventing and detecting unlawful use of your computer. Prevention measures help you to stop intruders from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done? We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs. Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending fictitious email from your computer, or examining personal information stored on your computer Intruders (also referred to as hackers, attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems. Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target. Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data. Unfortunately, intruders are always discovering new vulnerabilities to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems. Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure. Authentication occurs when any network ensures that only networking updates received from a trusted neighbor are used. This prevents a network from accepting and using unauthorized, malicious, or corrupted networking updates that may compromise the security or availability of the network

II. INTRUSION DETECTION

Intrusion detection is the art and science of sensing when a system or network is being used inappropriately or without Authorization. An intrusion detection system monitors systems network resources and activities using information gathered from these sources, notifies the authorities when it identifies a possible intrusion. Intrusion detection systems can also be categorized as knowledge or behavior-based. Most commercially available systems are knowledge based, matching signatures of known attacks against changes in systems or streams of packets on a network. Such systems are reliable and generate few false positives, but they can detect intruders using only attacks they already know about. They're often helpless against new attacks, so they must be continually updated with new knowledge about new attacks. Behavior- based intrusion detection instead looks at actions, attempting to identify attacks by monitoring system or network activity and flagging any activity that doesn't seem to fit in. Such activities may trigger an alarm - often a false alarm. Though false positives are common with a behavior-based on intrusion detection, so is the ability to detect a previously unreported attack. The intrusion detection notifies you of attempts to hack into, disrupt, or deny service to the system. It also monitors for potential extrusions, where your system might be used as the source of the attack. The term

intrusion detection is used two ways in i5/OS® documentation. In the first sense, intrusion detection refers to the prevention and detection of security exposures. For example, a hacker might be trying to break into the system using a user ID that is not valid, or an inexperienced user with too much authority might be altering important objects in system libraries. In the second sense, intrusion detection refers to the intrusion detection function that uses policies to monitor suspicious traffic on the system. Intrusion discovery involves gathering information about attacks coming over the TCP/IP network. The objective of an intrusion might be to get hold of information that a person is not authorized to have. The objective might be to cause business harm by rendering a network, system, or application unusable, or it might be to gain unauthorized use of a system as a means for further intrusions elsewhere. Most intrusions follow a pattern of information gathering, attempted access, and then destructive attacks. Some attacks can be detected and neutralized by the object system. Other attacks cannot be effectively neutralized by the target system. Most of the attacks also make use of *spoofed* packets, which are not easily traceable to their true origin. Many attacks make use of unwitting accomplices, which are machines or networks that are used without authorization to hide the identity of the attacker. For these reasons, a vital part of intrusion detection is gathering information, and detecting and preventing system attacks. Intrusion detection can be composed of several components: *Sensors* which generate security events, a Console to monitor events and alerts and control the sensors, and a central *Engine* that records events logged by the sensors in a database and use a system of rules to generate alerts from security events received. There are several ways to categorize intrusion detection depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple intrusion detection implementations all three components are combined in a single device or appliance.

III. THE TERMINOLOGY OF INTRUSION DETECTION IS AS FOLLOWS

A. ALERT/ALARM

A signal suggesting a system has been or is being attacked. True attack stimulus- An event that triggers an intrusion detection to produce an alarm and react as though a real attack were in progress False attack stimulus- The event signaling intrusion detection to produce an alarm when no attack has taken place False (False Positive) - An alert or alarm that is triggered when no actual attack has taken place False negative- A failure of intrusion detection to detect an actual attack Noise- Data or interference that can trigger a false positive Site policy- Guidelines within an organization that control the rules and configurations of intrusion detection Site policy awareness- The ability intrusion detection has to dynamically change its rules and configurations in response to changing environmental activity Confidence value-A value an organization places on intrusion detection based on past performance and analysis to help determine its ability to effectively identify an attack Alarm filtering- The process of categorizing attack alerts produced from an intrusion detection in order to distinguish false positives from actual attacks Dorothy E. Denning, assisted by Peter Neumann, published a model of an IDS in 1986 that formed the basis for many systems today.[2] Her model used statistics for anomaly detection, and resulted in an early IDS at SRI named the Intrusion detection expert system (IDES), which ran on Sun Workstations and could consider both user and network level data. A preliminary concept of an IDS began with James P. Anderson and reviews of audit trails. [3] An example of an audit trail would be a log of user access. Dorothy E. Denning, assisted by Peter Neumann, published a model of an IDS in 1986 that formed the basis for many systems today.[4] The Multics intrusion detection and alerting system (MIDAS), an expert system using P- BEST and LISP, was developed in 1988 based on the work of Denning and Neumann. [5] Haystack was also developed this year using statistics to reduce audit trails.[6] The current way of protecting network infrastructures relies on best practices, which include various basic techniques such as firewalls, intrusion detection systems, authentication Message Digest (MD5), etc[7].

B. Intrusion Prevention Policies

Intrusion Prevention is a new technology category that focuses on taking a proactive approach to IT security by *preventing* attacks on corporate IT resources, as opposed to similar technology that merely *detects* and reports on attacks that have already taken place. Intrusion Prevention is gaining visibility in corporate and government organizations due to the inherent limitations in existing security technologies, as witnessed by the significant financial loss experienced by organizations in 2001.Intrusion Prevention can be thought of as the logical follow-on to signature-based technologies such as Intrusion detection and antivirus, and to network-oriented protection solutions such as firewalls. system could be used as a stand alone for providing attack alerts to the administrator or it can be used as a base system for developing a network intrusion prevention system[8] Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are now considered a mainstream security technology. IDS and IPS are designed to identify security breaches. [9] Traditional security products have focused on the biggest threats that emerged as computer networking, email and web applications were adopted by corporations. As corporations adopted these technologies, they purchased products to solve the security issues inherent in these technologies, namely perimeter protection (firewalls), network protection (network-based intrusion detection), and file based security (anti- virus). IPSs yet another tool in the security infrastructure that could help prevent intrusions.IPS has developed out of IDS, but the two are really different security products that have different functionalities and strengths [10] These technologies do not address new attacks that ride over existing protocols to attack applications, or new content-based attacks that attack systems before vendors are able to release and distribute signatures and other countermeasures. Best Practices Any organization that intends to protect itself through the use of Intrusion Prevention technology should take a number of factors into consideration when evaluating products that address the organization's defined security requirements. Care should be taken that chosen solutions meet corporate security, manageability, and flexibility requirements, lest the solution be a partial one, or worse, introduce a significant management burde that overshadows the security benefits.

C. Host-Based Protection

As technologies such as high-speed networks, switching, and end-to-end encryption are more widely adopted, providing desired security at the network level becomes a major challenge. The best place to enforce security is at the desktops and servers, where the actual work is performed and the potential for damage is greatest. Host- based systems operate on the protected host, inspecting audit or log data to detect intrusive activity. A variety of log and audit functions can serve to drive ID algorithms. Host-based systems can

monitor specific applications in ways that would be difficult or impossible in a network- based system. [11] a combination of network and host-based approaches would have provided the best attack coverage. Also, novel attacks are difficult to detect because signatures do not generalize to new attacks and because network protocols or host audit logs were not analyzed sufficiently to extract attack evidence. [12]

D. Real-Time Prevention Decisions

To ensure the highest levels of security and minimize the ability to bypass the security policy on a host, application calls must be intercepted at the kernel level where the determination is made of their adherence to policy. Solutions that are implemented by replacing shared libraries or analyzing system audit logs can be bypassed relatively easily. Sharing the analysis work out among the former. In order to improve the efficiency and perform a real-time processing, the preprocessed data must be dynamically and optimally assigned. This assignment is performed taking into account both the capabilities of the machines where ANALYZER agents are located and the analysis demands.[13] An effective Intrusion Prevention strategy includes preventing violations in real-time, rather than noting attacks or system changes after the fact.

E. Defense in Depth – Protection from Attacks at Various Phases

In order to completely enforce a company's security policy, Intrusion Prevention must intercept all major points of communication between applications and the underlying system. Network control must limit client/server communications at the port and protocol level, as well as hosts for permitted communications; file system controls must allow/deny read and/or write access to folders and files on an individual and group basis; Attacks have multiple phases exploiting network and application-level weaknesses, replicating and distributing themselves, and making unauthorized changes to the system. A complete Intrusion Prevention strategy must protect systems from all of these phases, so that if a new class of attack is released, it will be thwarted at one or more of the stages.

IV. BEHAVIORAL APPROACH

The Intrusion Prevention approach must enforce appropriate system and application behavior to ensure that the security implemented is proactive, not reactive. Solutions that rely on signatures only provide security to the release of the most recent signature update. Detection of intruder usually identifies abnormal behavior by matching it against pre-defined descriptions of attacks. This is effective to detect known attacks but generally is very difficult for detecting new attacks.[14] Intrusions are based on observations of deviation from normal system usage pattern. They can be detected by observing significant deviation from the normal behavior.[15]

V. CENTRALIZED EVENT MANAGEMENT

All events generated by the agents must roll up into a centralized repository from which alerts and reports may be generated. Solutions that are considered must supportstan Dard alerting interfaces such as SNMP, paging, email, flat files, and allow for custom interfaces to the alerting system to easily integrate with corporate systems.

VI. CONCLUSION

This paper has described narration of the intrusion detection, reasons behind intruders in the systems and prevention mechanisms for the computer administrators should ensure that their Intrusion Prevention solutions meet the security, manageability, and flexibility requirements in order to avoid limited or unmanageable solutions.

VII. REFERENCES

[1] Whitman, Michael, and Herbert Mattord. 2009. Principles of Information Security. Canada: Thomson, pp 290 & 301
[2] Anderson, Ross. 2001. Security Engineering. New York: Wiley pp. 387-388
[3] Anderson, James P., 1980."Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co.
[4] Denning, Dorothy E., 1986. "An Intrusion detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy. Pp 119-131
[5] Lunt, Teresa F., 1990"IDES: An Intelligent System for Detecting Intruders, "Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22-23, pp 110-121.
[6] Lunt, Teresa F., 1993. "Detecting Intruders in Computer Systems," Conference on Auditing and Computer Technology, SRI International
[7] Khalid Abu Al-Saud, Hatim Mohd Tahir, Moutaz Saleh and Mohammed Saleh 2008. Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 and OSPF Journal of Computer Science 4 (9): 721-728,
[8] MeeraGandhi & S.K.Srivatsa Detecting and preventing attacks using network intrusion detection systems, Chennai
[9] Sourour Meharouech & Adel Bouhoula, A security policy and Network Cartography based Intrusion Detection and Prevention Systems, Tunisia
[10] Judy Weng & Glen Qin Network Intrusion Prevention Systems Polytechnic University.
[11] John McHugh, Alan Christie, and Julia Allen, the Role of Intrusion Detection Systems Software Engineering Institute, CERT Coordination Center.
[12] Peter Mell, Vincent Hu an Overview of Issues in Testing Intrusion Detection Systems1National Institute of Standards and Technology ITL,
[13] Álvaro Herrero1, María A. Pellicer1, and Ajith Abraham ,Hybrid Multi Agent-Neural NetworkIntrusion Detection with Mobile Visualization Department of Civil Engineering, University of Burgos C/ Francisco de Vitoria s/n, 09006 Burgos, Spain
[14] Wei Wanga Xiaohong Guana,b, Xiangliang Zhangc, Liwei Yanga, Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data A Center for Networked Systems and Information Security (CNSIS) and State Key Laboratory for Manufacturing Systems Engineering (SKLMSE), Xi'an Jiaotong University, Xi'an 710049,China
[15] Ajmal A. A.,Intrusion Detection System, Cochin University of Science and Technology Kochi.

