Intrusion Detection and Prevention Systems (IDPS) and Security Issues

A. Ahmad Sharifi†, B. Akram Noorollahi††, and Farnoosh Farokhmanesh†††

†School Of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India
†† Department Of Management, Payam-e-Noor University Of Aliabad, Golestan, Iran
†††Department Of Information Technology and Services, Universitat Politècnica de Catalunya, Spain

Summary
Technical solutions, introduced by policies and implantations are essential requirements of an information security program. Advanced technologies such as intrusion detection and prevention system (IDPS) and analysis tools have become prominent in the network environment while they involve with organizations to enhance the security of their information assets. Scanning and analyzing tools to pinpoint vulnerabilities, holes in security components, unsecured aspects of the network and deploying of IDPS technology have highlighted.

Key words:
Intrusion, detection, prevention, vulnerability, security

1. Introduction

With computer systems increasingly under attack, information security are more serious in user views. Security protects computer and everything associated with it including networks, terminals, printers, cabling, disks and most important, it protects the available information in this environment. Today, users are the content[1], [2]. Driving the growth, and at the same time being driven by it, the explosion in computer networks is expanding the impact of the social web. The way that content is shared and accessed, is now the core of a new global culture, affecting and combining the spheres of personal and business life. The purpose is to protect against intruders who break into systems to catch sensitive data, steal passwords, or whatever misuse; they can do it. Confidentiality, integrity and availability are three distinct aspects in the security domain. Protection of information is ensured by confidentiality. Avoiding from corruption the information and permission to unauthorized access or malicious activity is achieved by integrity. Availability assures efficiency of working and ability for recovery in disaster situations. The security of the overall system is restricted by the safety of its weakest link. Any single weakness can affect the security of the system entirely. The threats include web site defacement, network penetrations cause corruption and loss of data, denial of service attacks, viruses, Trojans and endless series of new stories proves that the threats are real. In fact, network security involves with three realities: first, the defender has to defend against every possible attack, while the attacker only needs to find out one weakness. Second, the immense complexity of modern networks forms them impossible to secure properly. Third, professional attackers may encapsulate their attacks in programs, allowing ordinary people to use them. According studies vulnerability assessments and intrusion prevention or intrusion detection are just one aspect of IT security management. However, due to recent developments with the continuing spread of network connectivity IT security management, is faced with yet another challenge, requiring a structured approach for an adequate response.

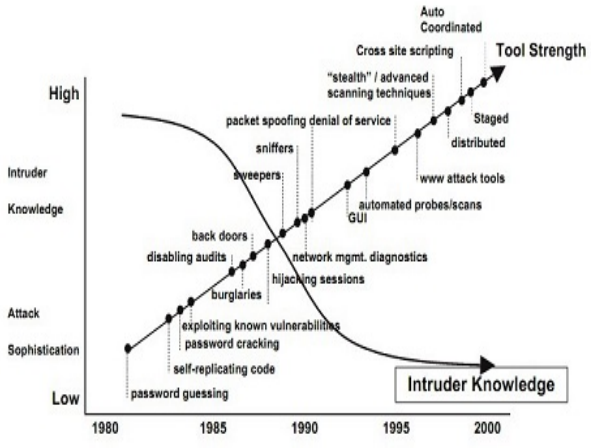

Figure. 1. Attack sophistication versus intruder technical knowledge (previous years)

In real world, security includes prevention, detection and response. Perfect prevention means no requirement for detection even though due to lack of pure prevention, this is not applicable, especially in computer networks.

Manuscript received November 5, 2014
Manuscript revised November 20, 2014

2. Threats, vulnerabilities and intrusions

Whereas, information is digital represented by zeroes and ones, they can be threatened by unauthorized accessibility. So proportional methods like environmental, personal, and administrative security must be get involved in this issue. The most obvious threat to an information resource is missing data, which almost caused by malicious behaviors internally or externally [3], [4]. Any authorized user who performs unauthorized actions that result in loss of control of computational assets, or actions resulting in unauthorized disclosure of information, is malicious insider one. In addition, these actions negatively impact the confidentiality, authenticity, and availability of information systems and information assets. The term vulnerability, describes a problem, i.e., a programming bug or common configuration error that allows a system or network to be attacked or broken into, mostly caused by complexity of networks. More precisely, vulnerability is a security hole, i.e., hardware, software or network weakness which allows an attacker to reduce an information assurance. Indeed, finding vulnerabilities is a main part of the hacker to attack. Security holes can be seen as open doors where they are thought to be closed. Poor passwords, bugs of software, a computer virus or a script code injection and weak links may result in vulnerabilities. According to the report, the number of vulnerabilities discovered in September 2011 is still on the rise with an increase of more than 70% over the past two years. Intruder and virus are named as two more popular threats in security and commonly addressed to as a hacker or cracker. Intruders can be classified in three classes:

Masquerader: An individual who pretends themself as legitimate accessibility to exploit legitimate user account.

Misfeasor: A legitimate user who access to unauthorized data, programs, or resources or who is authorized for such access but misuse his or her privileges.

Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls to surpass audit collection.

The masquerader is likely to be an outsider; the misfeasor commonly is an insider, and the clandestine user can be either an outsider or an insider. Password guessing attack to capture passwords, modifying to log information, spoofing data and other new daily produced mechanisms using malware; spywares, Trojans, will tend to hand the data to the attacker more reliable than previous methods familiarized by a security guard of environments. According to report of security companies, traditional email spam, still remains a significant problem especially in business. Users still need to keep their inboxes clear of junk and advanced mail filtering systems are a requirement in any business hoping to use email efficiently. All kinds of tricks are visible in social engineering to lure its victims. A good first step to combat the unknown threat is user education, but even informed efforts occasionally are hindered by unwise activities from legitimate parties. These kinds of threats are serious challenge facing businesses.

3. Intrusion detection and prevention system Experimental Consideration

3.1 Definition

Attempts to breach information security are raising every day, along with the availability of the vulnerability assessment tools that are openly available on the Internet freely, as well as for commercial use [5]. An intrusion occurs while an attacker attempts to get into an information system or cause disruption; in fact, its behavior intends to do harm. Intrusion detection and prevention systems help information system prepare for, and deal with attacks. They accomplish this by collection information from a diversity of systems, monitoring and then analyzing for possible security problems. Indeed, an intrusion detection system (IDS) after detection of a violation raises an audible or visual alarm, or it can be silent like an e-mail message or pager alert. Another extension of this technology is the intrusion prevention system (IPS), which can detect an intrusion and in addition prevent that intrusion to be successful by an active response. Whereas the two systems often coexist, the combined term intrusion detection and prevention system (IDPS) is commonly used to describe current anti-intrusion technologies. As IDPS terminology point of view, some standard terms list as below:

Alert: Raising an alert in the form of audible signals, e-mail messages, page notifications or pop-up windows.

Evasion: Changing format by an attacker to avoid from detecting by IDPS.

False negative: Failure of detecting a real attack by IDPS. Whereas, the main function of IDPS is detect and respond to attacks.

False attack stimulus: Triggering of alert by an event in the absence of an actual attack.

False positive: Raising alert by IDPS in the absence of an actual attack. They tend to pervasive users to be insensitive to alerts so, they reduce their activity to real intrusion events.

Noise: Alarm events that are accurate but do not pose significant threats to information security. Unsuccessful attacks are the most popular source of IDPS noise.

Site policy: Configuration and policy prepared by organization for implementation of IDPS.

Site policy awareness: So-called smart IDPS means the ability of IDPS to dynamical modify its configuration in response to environment activity.
True attack stimulus: Alarm triggering by an event and causes an IDPS to react as if a real attack is in progress.
Tuning: The process of adjusting an IDPS to maximize its efficiency in order to detecting true positives while minimizing both false positive and false negatives.
Confidence value: Measurement of correct detections by IDPS and identify certain types of attacks.
Alarm filtering: Classification of IDPS alerts so that they are manageable more efficiently. They are similar to packet filters whereas they can filter items by source and destination while they can filter by operating systems, confidence values and alert types.
Alarm clustering and compaction: Categorization of similar behavioral alerts on time into a single higher-level alarm. This clustering maybe based on combination of frequency, attack signature or target similarity that lead to reducing the number of alert generated.

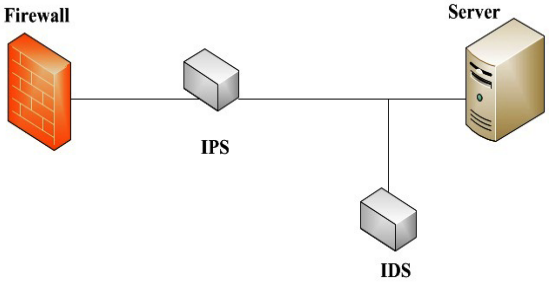

Figure. 2. IDS and IPS systems application

Preventing from bad behaviors caused by misused information and detection of attacks and security violations not prevent by other measures is main duty of IDPS. Furthermore, [6] it involves with documentation of existing threats and being a controller for security design. With providing of information about intrusions, advanced diagnosis, recovery, and various investigations allowable to perform for ongoing events including stopping the attack, terminating the network connection or user session, blocking the target accessibility, changing security.

3.2 Types of IDPS and operations

Two kinds of operations, including network-based and host-based systems are famous working domains which numerous of ongoing interesting patterns, are monitored by them. Based on functionality, anomaly based and signature based, sign to address [7], [8], [9]. Anomaly based one require making a decision, if the behavior of the system is the statistically significant departure from normal like; validity, the ratio of TCP connection, payload, number of accesses to specific files and login frequency. Signature based one works through recognizing specific patterns of events or behavior that portend or go along with an attack. A host based IDPS (HIDPS) is typically implemented in software and resides on top of the operating system. On the other hand, they rely on the events collected by the hosts they monitor. The duty is monitoring of internal behavior of the host such as the sequence of system calls made, file accessed and other methods using system or application logs and operating system audit trails to identify relevant events to an intrusion. Network based intrusion detection prevention systems (NIDPSs) gather input data by monitoring network traffic i.e., packets captured by network interfaces in promiscuous mode. While a situation occurs that the NIDPS designing for recognizing as an attack, it responds by sending notifications to administrators. Looking for attack patterns within network traffic, i.e., large collections of related items could indicate a Denial-Of-Service (DOS) attack or exchanging of a series of related packets in a certain pattern, indicating a port scan progress, is the main operation here as task. NIDPSs are installed at a specific place in the network, i.e., on the inside of an edge router from where it is possible to look for the traffic going into and out of a particular network part. They deploy to inspect a special category of host computers on a particular network part, or its installation for monitoring the network traffic entirely. In wireless environment, IDPS monitors and analyzes wireless network traffic, finding potential problems with the wireless protocols. Furthermore, wireless access point may contain IDPS capability in order to monitor. Wireless local area networks (WLANs) have exposed many different security flaws, aligning from misconfiguration of wireless access points (WAPs) to unreliable cryptographic algorithms. Mobile ad hoc networks are notably vulnerable because of their openness, varying topology, and lack of centralized management. The major important difference indicate today's NIDPSs rely on real-time traffic analyses upon a fixed infrastructure and so cannot function well in the mobile computing environment. NIDPSs are inclined to a salient ratio of false positive alerts. They are able to catch many but not all intrusions; alternatively, they are intrinsic to the nature of detecting intrusions in a network. In addition, their effectiveness depends limitedly on the specific design of the network infrastructure. Automatic response mechanisms, can be circumvented and exploited against the NIDPS owner to provoke denial of service conditions. Numerous methods exist that are able to evade detection. Hence, these systems must not consider in isolated manner. NIDPSs are a valuable cover of security protection within a defense-in-depth planning, however their flaws will have to be mitigate by further security layers and technologies. Whereas, many attacks occur so quickly, automated mechanisms designed to thwart them may not be able to stop from initially succeeding. In these

situations, intrusion prevention mechanisms often attempt to prevent the attack from spreading any further. Speed and accuracy are desirable features for an IDPS. High sensitivity implies a low false negative rate, whereas high selectivity implies a low false positive rate. The strategy for deploying an IDPS must be taken into account of factors, knowing how the IDPS will be managed and where position it need to be placed. The factors include number of administrator needed to install, configure and monitor as well as the number of management workstations, the size of the storage needed for retention of the data generated by the systems, and the ability of the organization to detect and respond to remote threats. IDPS control strategies include centralized control strategy, fully distributed control strategy and partially distributed control strategy are different methods to deploy. In all circumstances, designers have to select a deployment strategy based on a careful analysis for IT infrastructure requirements. Test facility has an significant capacity in this issue whereas, training scenarios can be developed collaborating monitoring of operations allowing users to recognize and respond to common attack circumstances.

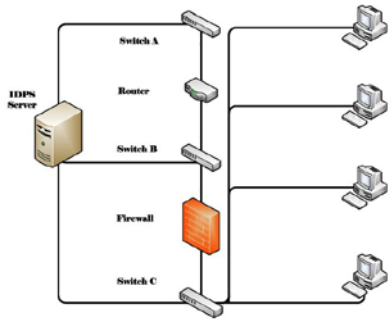

Figure. 3. NIDPS deployment in network environment [10], [11]

NIDPS products provide a broad diversity of security capacities. They normally carry out extensive logging of data connected to detected events. This data confirm the validity of alerts, to explore incidents, and to correlate events between the IDPS and other logging origins. Perfectly, network based IDPSs would be able to define all network actions like the runs of endpoints. Stateful protocol diagnosis techniques often attempt to prepare this by replicating the processing executed by collective types of clients and servers. This allows the IDPS to improve their detection accuracy slightly. Many attackers utilize client and server-specific processing attributes, like: handling character encoding, in their attacks as evasion techniques.

Table. 1. Information gathering capabilities

Capability	Method	Result
Identifying hosts	Ability to create a list of hosts by IP address or MAC address.	Hosts profile
Identifying Operating System	Recognizing of analyzing techniques like tracking port	OS versions to identify host vulnerable
Identifying Application	Keeping track of ports and monitoring	Identify potential vulnerable application
Identifying network characteristic	Collect traffic information like number of hops in path	Awareness changing network configuration

While network-based IDPSs offer extensive detection capabilities, they have some significant restrictions including analyzing encrypted network traffic, handling high-traffic loads, and resisting attacks against the IDPSs themselves. Attacks through encrypted network traffic, virtual private network (VPN) connections, HTTP over SSL (HTTPS) and SSH session typically cannot be detectable by NIDPS. Environment or interference on attack content are some response techniques. One critical issue is how to detect unknown patterns of attacks without generating too many false remains.

3.3 Necessity of IDPS in organizations

A simple principle of network security is a defense in-depth, which is a layered solution to secure valuable information on the network from malicious attacks using IDPS. After selection appropriated IDPS, it must be properly and efficiently deploy throughout the organization [12]. This job is performed through design of IDPS strategy and issuing IDPS policy. Some factors like; the quantity of network traffic limitations, permit for configuration, installation requirements and frequencies of logs undergo for monitoring, make document policy. The planning requires to create the policy will strengthen the communication between company management and security officials. Meanwhile, this will authorize organizational units to identify and solve conflicts before they become obstacles to successful IDPS deployment.

Table. 2. Logging capabilities

Capability	Application
Timestamp	Date and time
Connection ID	Unique number assign to TCP or other session
Event or alarm type	Realizing of occurrence types
Rating	priority, severity, impact, confidence
Protocols	Network, transport, and application layer
Path	Source and destination IP address, TCP , UDP or ICMP
Transmission	Number of bytes transmitted over a connection
Decoding payload	Application requests and responses
State information	Like authenticated user
Prevention	Avoiding action performed , in required state

Organizations should assimilate this policy into their comprehensive security policy or corporation rules and orders. Usage of incident response guidelines, staffing, setting, training and update signatures must be considered to imply as plan and economical resources for an effective deployment. In large companies more endpoint machines, servers and network segments indicate a more complicated

setup and a longer installation time. Due to numerous computers and geographical diversity, planning play a dominant role in a large enterprise IDPS deployment. The other well-known issue facing big companies includes scalability and the agent ratio. Considering the number of monitoring employees the IDPS managers for output, the employee skill and comfort level, the number of intrusion alerts per minute, the IDPS software carried out, and various other elements, the ideal agent ratio can alter from 5:1 to 50:1. Utilizing a subsection for testing aim or doing research at firms with a similar size, network structure, and intrusion risk may ease to pinpoint the optimal agent ratio when scaling for big companies.

4. Conclusion

Information security has become a legitimate concern for both organizations and computer users due to the growing confidence on computers and electronic transactions. Different techniques are used to support the security of an organization against threats or attacks. On the other side, attackers are discovering new techniques and ways to break these security policies. Firewalls, antivirus and antispyware are limited to provide security to the system against threats. The only way to strike them is realizing about their techniques to use for attack. Therefore, security of organizations will have to adopt such a firmest model or mechanism, which provides strongest protection against threats to ensure that the system will remain secure. IDPS provides the facility to detect and prevent from attacks by inheriting multiple approaches. Active IDPS seeks to restrict the damage that attackers can penetrate by making the local network resistant to appropriate use.

Acknowledgment

The authors would like to express their cordial thanks to Mr. Jallaledin Sharifi, manager of Sharif Network Company (http://www.sharifisp.com) for his valuable advice.

References

[1] U. A. Sandhu, S. Haider, S. Naseer, O. U. Ateeb, “A Survey of Intrusion Detection & Prevention Techniques”, International Conference on Information Communication and Management IPCSIT: IACSIT Press, Singapore 2011.

[2] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology: NIST Special Publication, February 2007.

[3] B. Menezes, Network Security and Cryptography: CENGAGE Learning, Chapter 14, 18, 19, 21, 22, 24, 2010.

[4] J. R. Vacca, Computer and information security handbook: Morgan Kaufmann Series in Computer Security, First edition, May 4, 2009.

[5] A. Fuchsberger, “Intrusion Detection Systems and Intrusion Prevention Systems”, Published in Elsevier: Information Security Technical Report 10, pp. 134-139, 2005.

[6] P. Innella, http://www.symantec.com /connect/articles/ managing-intrusion-detection-systems-large-organizations-part-one.

[7] EC-Council, Ethical Hacking and Countermeasures Version 6 Module XVII Web Application Vulnerabilities: International Council of E-commerce Consultants.

[8] R. E. Overill, “ISMS insider intrusion prevention and detection”, Published in Elsevier, Information security technical report 13, pp. 216-219, 2008.

[9] N. Godbole, Information systems security: Security Management, Metrics, Frameworks and Best Practices: JOHN WIELY, All Chapters, 2009.

[10] N. F. Mir, Computer and Communication Networks: Prentice Hall, Chapter 5, 9, 10, 2006.

[11] B. Forouzan, Data Communications and Networking: McGraw Hill, Fourth Edition, Chapter 13, 14, 15, 31, 32, 2006.

[12] A. S. Ashoor and S. Gore, “Importance of Intrusion Detection system (IDS)”, International Journal of Scientific and Engineering Research, vol 2, issue 1, January 2011.

Ahmad Sharifi received M.Tech in Computer Networks and Information Security from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India. In addition, he has received his bachelor in Electronic engineering from industrial University of Shahroud, Iran. Ahmad has professional experiences on technical engineering on ISP and network designs for many years. In addition, he is involving with teaching in universities. He interests in Cryptography, WSN, ADHOC, MATLAB, OPNET and other related issues. His personal website is www.ahmadsharifi.com. Furthermore, he cooperates with RIPE NCC www.ripe.net via www.sharifisp.com that is Internet Service Provider.

Akram Noorollahi. She has received the Bachelor's degree from Payam-e-Noor University of Aliabad, Golestan, Iran. She is expert on Microsoft Project and IT management. In addition, she has worked with IT industry to manage projects, designing and marketing

Farnoosh Farokhmanesh received the Bachelor's degree from Rajaee Teacher Training University, Iran. She worked as a technical ADSL support at Shatel ISP in 2009-2010, Iran. She is studding master in computer architecture in Universidad Politécnica de Cataluñ, Spain. She is a researcher on wireless sensor network at UPC University.