Introduction to Intrusion Detection System

Rajeev Singh

B.Tech (ECE), Guru Nanak Institute of Technology, Kolkata-700114, West Bengal, India

Abstract: **An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization IDPSes typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall), or changing the attack's content. In this paper, we examine the vulnerabilities of networks and say that we must include intrusion detection in the security architecture. We have showed such architecture and evaluated key mechanisms in this architecture such as applying intrusion detection, anomaly detection and misuse detection for both wired & wireless networks.**

Keywords: **IDS, Need for IDS, Types of IDS, Architecture**

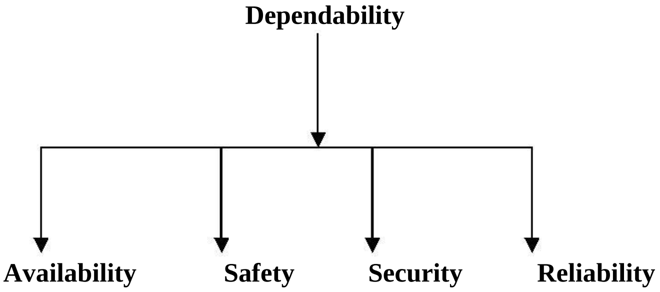
1. INTRODUCTION

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions. It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called **Intrusion Detection.**

1.1 Computer Security and its Role

One broad definition of a secure computer system is given by Garfinkel and Spafford as ***one that can be depended upon to behave as it is expected to***. It is always a point of benefit to integrate security with dependability and how to obtain a dependable computing system.

Dependability is the trustworthiness of a system and can be seen as the quality of the service a system offers. Integrating security and dependability can be done in various ways. One approach is to treat security as one characteristic of dependability on the same level as availability, reliability and safety as shown in the figure.



A narrower definition of security is the possibility for a system to protect objects with respect to confidentiality, authentication, integrity and non-repudiation.

Confidentiality: Transforming data such that only authorized parties can decode it.
Authentication: Proving or disproving someone's or something's claimed identity.
Integrity checking: Ensuring that data cannot be modified without such modification being detectable.
Non – repudiation: Proving that a source of some data did in fact send data that he might later deny sending

1.2 Threats of security

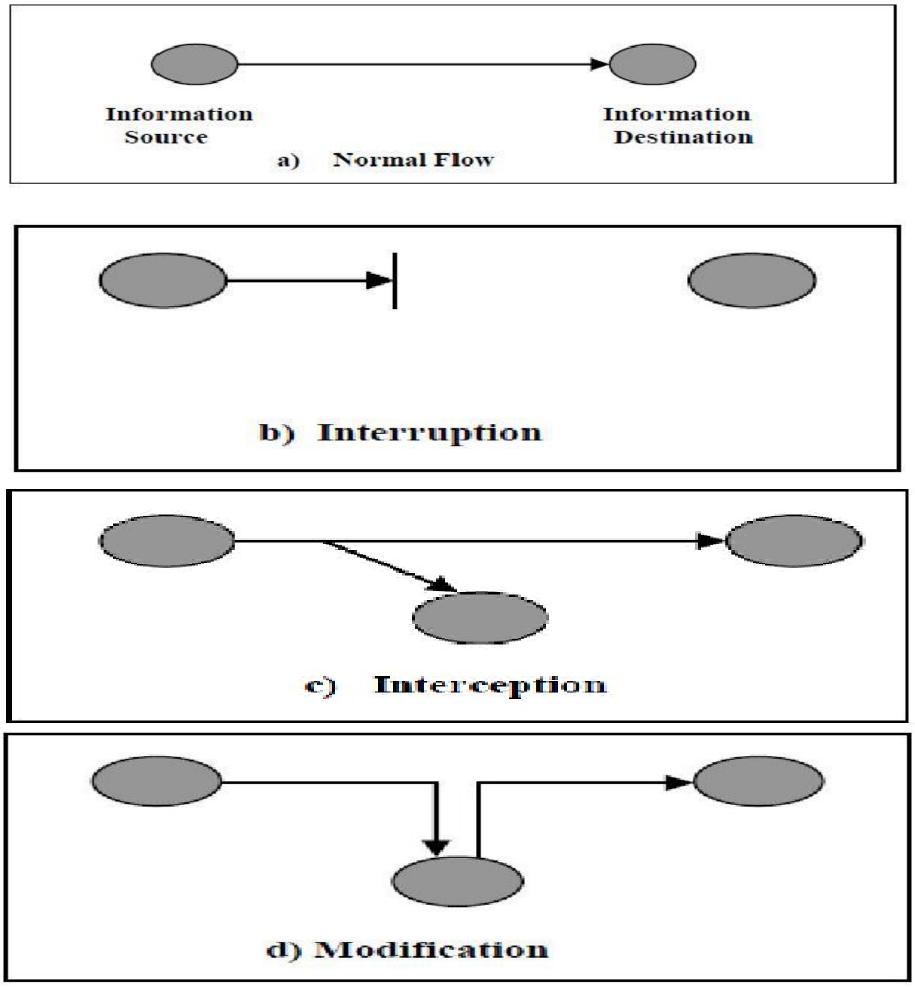
Threats can be seen as potential violations of security and exist because of vulnerabilities, i.e. weakness, in a system. There are two basic types of threats: **accidental threats** and **intentional threats**.

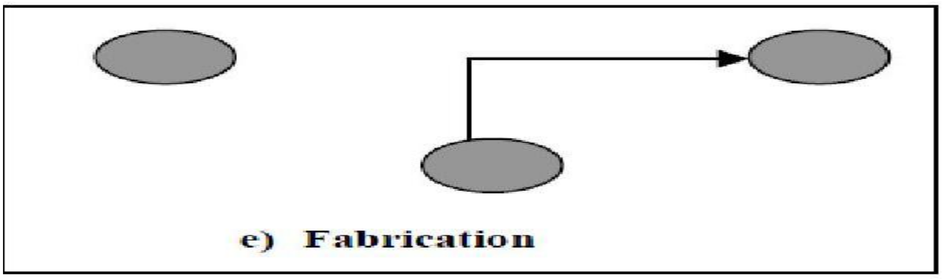
1.2.1 Accidental Threat:

An accidental threat can be manifested and the result is either an exposure of confidential information or cause of an illegal system state to occur i.e. modification of an object. Exposures can emerge from both hardware and software failures as well as from user and operational mistakes thus resulting in the violation of confidentiality. It can also be manifested as modification of an object, which is the violation of object integrity. An object here can be both information and resource.

1.2.2 Intentional Threat:

An intentional threat is an action performed by an entity with the intention to violate security. Examples of attacks are interruption, modification, interception and fabrication of data as shown in the figure.





e) Fabrication

2. Need for INTRUSION DETECTION

A computer system should provide *confidentiality*, *integrity* and *assurance* against denial of service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. These subversion attempts try to exploit flaws in the operating system as well as in application programs and have resulted in spectacular incidents like the Internet Worm incident of 1988.

There are two ways to handle subversion attempts. One way is to prevent subversion itself by building a completely secure system. We could, for example, *require* all users to identify and authenticate themselves; we could protect data by various cryptographic methods and very tight access control mechanisms. However this is not really feasible because:

I. In practice, it is not possible to build a completely secure system. Miller gives a compelling report on bugs in popular programs and operating systems that seems to indicate that (a) bug free software is still a dream and (b) no-one seems to want to make the effort to try to develop such software. Apart from the fact that we do not seem to be getting our money's worth when we buy software, there are also security implications when our E-mail software, for example, can be attacked. Designing and implementing a totally secure system is thus an extremely difficult task.

II. The vast installed base of systems worldwide guarantees that any transition to a secure system, (if it is ever developed) will be long in coming.

III. Cryptographic methods have their own problems. Passwords can be cracked, users can lose their passwords, and entire crypto-systems can be broken.

IV. Even a truly secure system is vulnerable to abuse by insiders who abuse their privileges.

V. It has been seen that that the relationship between the level of access control and user efficiency is an inverse one, which means that the stricter the mechanisms, the lower the efficiency becomes.

The history of security research has taught us a valuable lesson – no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in.

We thus see that we are stuck with systems that have vulnerabilities for a while to come. If there are attacks on a system, we would like to detect them as soon as possible (preferably in real-time) and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than pro-active agent. It plays the role of an informant rather than a police officer.

3. Background on INTRUSION DETECTION

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as to *prevent* unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called **Intrusion Detection.**

A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant). The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the "signatures" of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks are further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

Intrusion detection techniques while often regarded as grossly experimental, the field of intrusion detection has matured a great deal to the point where it has secured a space in the network defense landscape alongside firewalls and virus protection systems. While the actual implementations tend to be fairly complex, and often proprietary, the concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack.

4. Types of IDS

For the purpose of dealing with IT, there are three main types of IDS:

4.1 Network intrusion detection system (NIDS)*:* is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

4.2 Host-based intrusion detection system (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. Examples of HIDS are Tripwire and OSSEC.

4.3 Stack-based intrusion detection system (SIDS)

This type of system consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This fact makes its implementation to be dependent on the Operating System that is being used. Intrusion detection systems can also be system-specific using custom tools and honey pots.

5. History of INTRUSION DETECTION

1980: James Anderson gave the foundation of IDS by writing the paper Computer Security Threat Monitoring and Surveillance
1985: Early IDES evolved by the support of the U.S. Defense System
1989: Todd Heberlein presented Network System Monitor introducing NIDS

1999: Presidential Decision directive presented final Federal Intrusion Detection Network to protect national infrastructure

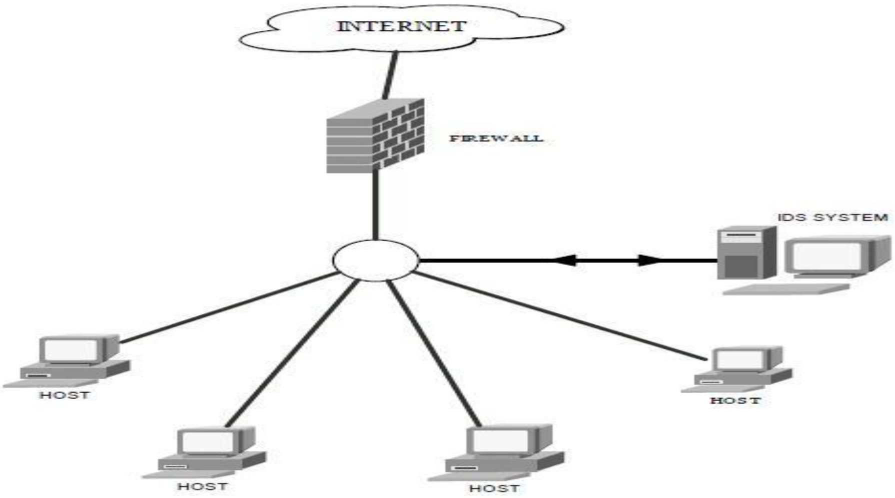
5.1 Characteristics of IDS:

1. Runs constantly without human supervision

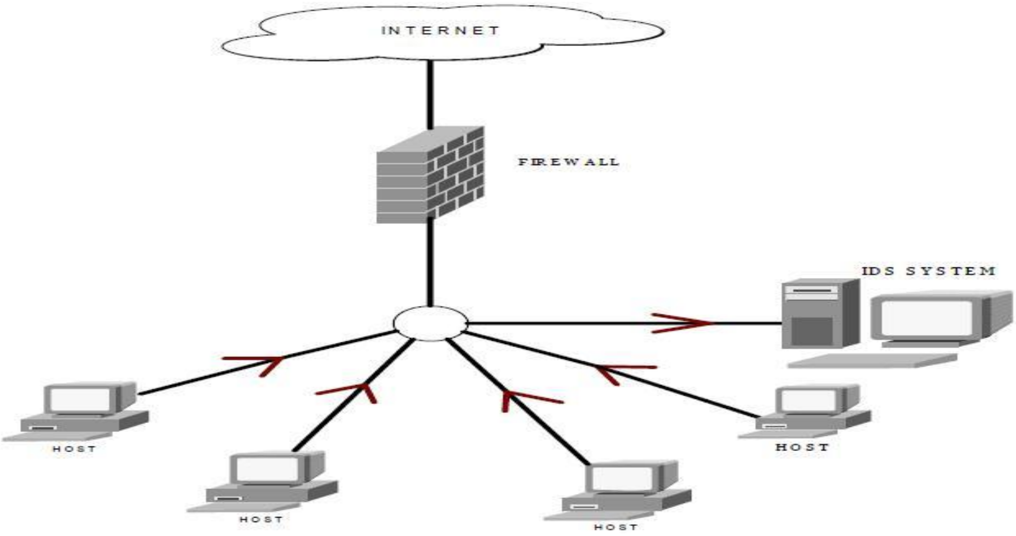
2. Survives with system crash and must be fault tolerant

3. Enforces least overhead on the system
4. Observes deviations from normal behavior
5. Adaptability of system with technologies
6. System errors cannot be overlooked by IDS

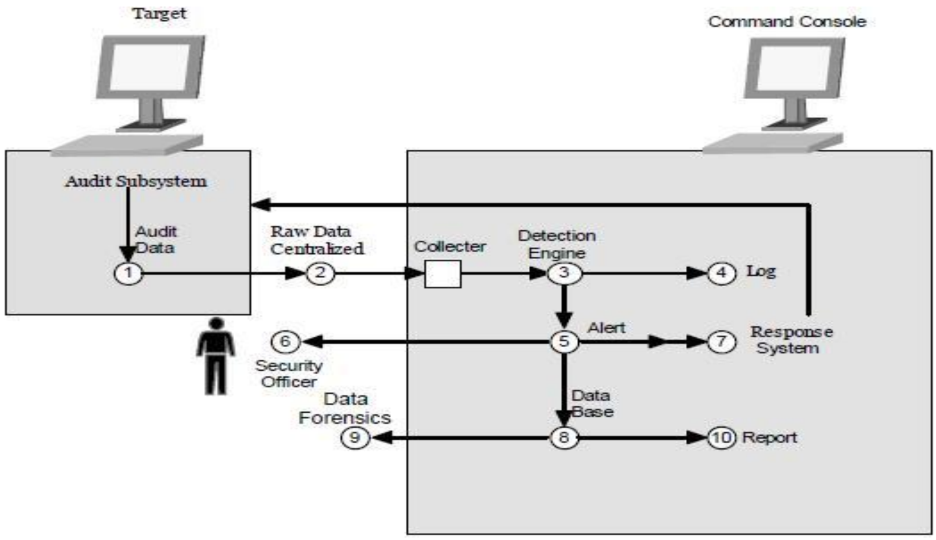
6. Architecture of NIDS



7. Architecture of HIDS



8. Centralized Host Based HIDS



9. CONCLUSION

The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. It is important to note that absolute security is an abstract concept – it does not exist anywhere. All networks are vulnerable to insider or outsider attacks, and eavesdropping. No one wants to risk having the data exposed to the casual observer or open malicious mischief. Regardless of whether the network is wired or wirelesses, steps can and should always be taken to preserve network security and integrity.

We have said that any secure network will have vulnerabilities that an adversary could exploit. This is especially true for wireless ad-hoc networks. Intrusion Detection can compliment intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to improve the network security. However new techniques must be developed to make intrusion detection work better for the wireless networks.

We have shown that an architecture for better intrusion detection in wireless networks should be distributed and cooperative by applying Mobile Agents to the network and given few of the implemented approaches for intrusion detection. Currently, the research is taking place in developing new architecture for wireless networks for better security.

REFERENCE

[1] Lidong Z., Zygmunt J. H., *"Securing ad hoc networks"*, IEEE Network, Vol. 13, No. 6, 1999, pp. 24-30.
[2] Sundaram A., "An Introduction to Intrusion Detection", http://www.acm.org/crossroads/xrds2-4/intrus.html
[3] Marti S., Giuli T.J., Lai K. Baker M., "*Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*", Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM 2000, pp 255-265.
[4] Arbaugh W., Shankar N., Wan Y.C.J., *"Your 802.11 Wireless Network Has No Clothes"*, University of Maryland, 30-Mar-2001.
[5] Yongguang Z., Wenke L., "*Intrusion Detection in Wireless Ad- Hoc Networks*", Proceedings of the Annual International Conference on Mobile Computing and Networking, MobiCom 2000, pp 275-283.
[6] Andrew B.Smith, An Examination of Intrusion Detection Architecture for Wireless Ad-Hoc Networks.
[7] C. Krugel, T.Toth. , Applying Mobile Agent Technology to Intrusion Detection
[8] Kumar's "Classification and Detection of Computer Intrusion.