Detecting and preventing attacks using network intrusion detection systems

MeeraGandhi meera.gandhi@gmail.com
Department of Computer Science and Engg.,
ResearchScholar,
SathyabamaUniversity,

S.K.Srivatsa profsks@hotmail.com
Professor, ICE, St.Joseph's College of Engg., Chennai,

Abstract

Intrusion detection is an important technology in business sector as well as an active area of research. It is an important tool for information security. A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action. Today computers are part of networked; distributed systems that may span multiple buildings sometimes located thousands of miles apart. The network of such a system is a pathway for communication between the computers in the distributed system. The network is also a pathway for intrusion. This system is designed to detect and combat some common attacks on network systems. It follows the signature based IDs methodology for ascertaining attacks. A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. It has been implemented in VC++. In this system the attack log displays the list of attacks to the administrator for evasive action. This system works as an alert device in the event of attacks directed towards an entire network.

Key words*:* intruders, information security, real time IDS, attacks, signature

1. INTRODUCTION

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of attacks and secures the networks. Main purpose of IDS is to find out intrusions among normal audit data and this can be considered as classification problem. Intrusion detection systems (IDS) are an effective security technology, which can detect, prevent and possibly react to the attack. It performs monitoring of target sources of activities, such as audit and network traffic data in computer or network systems, requiring security measures, and employs various techniques for providing security services. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before.

Symantec in a recent report [1] uncovered that the number of fishing attacks targeted at stealing confidential information such as credit card numbers, passwords, and other financial information are on the rise, going from 9 million attacks in June2004 to over 33 millions in less than a year .One solution to this is the use of network intrusion detection systems (NIDS) [2], that detect

attacks by observing various network activities. It is therefore crucial that such systems are accurate in identifying attacks, quick to train and generate as few false positives as possible.

This paper presents the scope and status of our research in misuse detection [2, 3]. Experimental results have demonstrated that this model is much more efficient in the detection of network intrusions, compared with network based techniques. Section 2 describes an overview of frequently occurring network attacks and discusses related research done so far, also presents the experimental results. Finally, section 3 provides the concluding remarks and future scope of the work. Section 4 briefs the references.

2. NETWORKING ATTACKS

A Network Intrusion Detection System is used to monitor networks for attacks or intrusions[5,6] and report these intrusions to the administrator in order to take evasive action. A large NIDS server can be set up on a backbone network, to monitor all traffic; or smaller systems can be set up to monitor traffic for a particular server, switch, gateway, or router. It has been shown in fig. 1.

Intrusion detection is needed in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. The environment is constantly evolving and changing field by new technology and the Internet. Intrusion detection products are tools to assist in managing threats and vulnerabilities in this changing environment. Threats are people or groups who have the potential to compromise your computer system. These may be a curious teenager, a disgruntled employee, or espionage from a rival company or a foreign government [4].

Attacks on network computer system could be devastating and affect networks and corporate establishments. We need to curb these attacks and Intrusion Detection System helps to identify the intrusions. Without an NIDS, to monitor any network activity, possibly resulting in irreparable damage to an organization's network

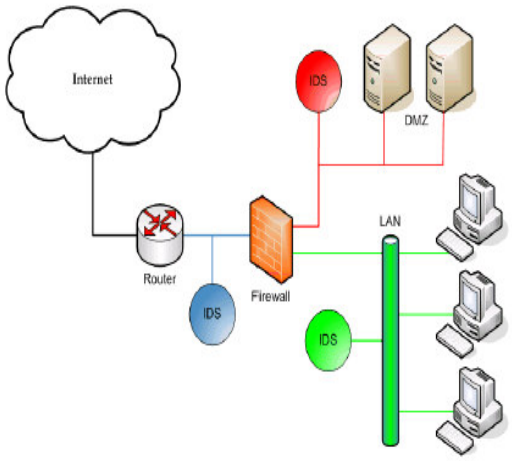

FIGURE 1: Computer network with Intrusion Detection Systems

Intrusion attacks [7, 8, and 9] are those in which an attacker enters your network to read, damage, and/or steal your data. These attacks can be divided into two subcategories: *pre intrusion activities and intrusions.*

2.1 Pre intrusion activities

Pre intrusion activities are used to prepare for intruding into a network. These include port scanning to find a way to get into the network and IP spoofing to disguise the identity of the attacker or intruder.

- **Port scans**: A program used by hackers to probe a system remotely and determine what TCP/UPD ports are open (and vulnerable to attack) is called a scanner. A scanner can find a vulnerable computer on the Internet, discover what services are running on the machine, and then find the weaknesses in those services. There are 65,535 TCP ports and an equal number of UDP ports. Stealth scanners use what is called an IP half scan, sending only initial or final packets instead of establishing a connection, to avoid detection.
- **IP spoofing**: This is a means of changing the information in the headers of a packet to forge the source IP address. Spoofing is used to impersonate a different machine from the one that actually sent the data. This can be done to avoid detection and/or to target the machine to which the spoofed address belongs. By spoofing an address that is a trusted port, the attacker can get packets through a firewall.

Various *intrusions* into the network are given as follows:

- **Source routing attack**: This is a protocol exploit that is used by hackers to reach private IP addresses on an internal network by routing traffic through another machine that can be reached from both the Internet and the local network [7, 8]. TCP/IP to allow those sending network data to route the packets through a specific network point for better performance supports source routing. Administrators to map their networks or to troubleshoot routing problems also use it.

- **Trojan attacks**: Trojans are programs that masquerade as something else and allow hackers to take control of your machine, browse your drives, upload or download data, etc. For example, in 1999, a Trojan program file called Picture.exe was designed to collect personal data from the hard disk of an infiltrated computer and send it to a specific e-mail address. So-called Trojan ports are popular avenues of attack for these programs.
- **Registry attack**: In this type of attack, a remote user connects to a Windows machine's registry and changes the registry settings. To prevent such an attack, configure permissions so that the every one group does not have access.
- **Password hijacking attacks**: The easiest way to gain unauthorized access to a protected system is to find a legitimate password. This can be done via social engineering (getting authorized users to divulge their passwords via persuasion, intimidation, or trickery) or using brute force method.

2.2 System Description

2.2.1 Packet Sniffer

This module involves capturing all traffic passing through the network. The sniffer will be installed on the end system in a network on which the traffic has to be captured. The sniffer[10] captures all network traffic by operating the network adapter in promiscuous mode.

2.2.2 Determination of attack signatures

Attack Signatures [13, 14] refers to the pattern of attack traffic. Signatures are modeled based on the packet header pattern a particular attack follows. It involves a count of packets from a particular target or a particular source or destination port or it may even be modeled with the help of other details in the packet such as header size, Time to Live (TTL), flag bits, protocol.

2.2.3 Identification of attacks

This involves extracting useful information from captured local traffic such as source and destination IP addresses, protocol type, header length, source and destination ports etc and compare these details with modeled attack signatures to determine if an attack has occurred.

2.2.4 Reporting attack details

This involves reporting the attack to the administrator so that he may take evasive action. Reporting involves specifying attack details such as source and victim IP addresses, time stamp of attack and more importantly the type of attack.

2.3 Experimental Results

2.3.1 Signature based intrusion detection

Signature-based IDSs operate analogously to virus scanners, i.e. by searching a database of signatures for a known identity – or signature – for each specific intrusion event. In signature-based IDSs, monitored events are matched against a database of attack signatures to detect intrusions.

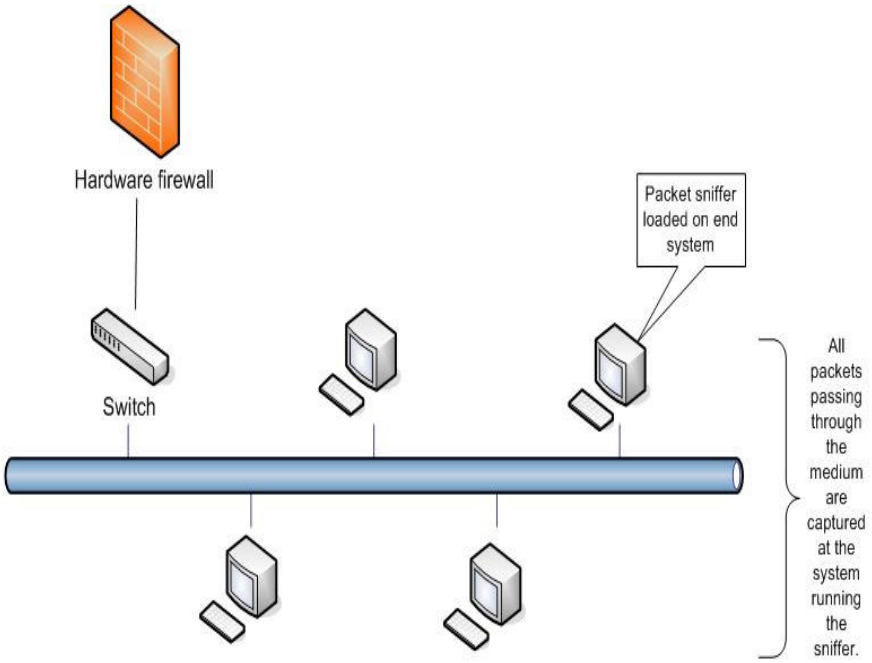

FIGURE 2: IDS in Promiscuous mode

Signature-based IDS [15] are unable to detect unknown and emerging attacks since signature database has to be manually revised for each new type of intrusion that is discovered.

In addition, once a new attack is discovered and its signature is developed, often there is a substantial latency in its deployment across networks [13]. The most well known signature-based

IDS include SNORT [14], Network Flight Recorder [16], NetRanger [17], RealSecure [18], Computer Misuse Detection System (CMDS™) [20], NetProwler [21], Haystack [22] and MuSig (Misuse Signatures) [23].

This system follows the signature based IDs methodology for ascertaining attacks. A signature based IDS will monitor packets on the network and compare them against a database of signatures [19] or attributes from known malicious threats.

Most intrusion IDS are signature based. This means that they operate in much the same way as a virus scanner, by searching for a known attack or signature for each specific intrusion event. And, while signature-based IDS is very efficient at sniffing out known attack, it does, like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker technique.

Because signature based IDS can only ever be as good as the extent of the signature database, two further problems immediately arise. Firstly, it is easy to fool signature-based solutions by changing the ways in which an attack is made. This technique simply skirts around the signature database stored in the IDS, giving the hacker an ideal opportunity to gain access to the network. This can be overcome by using defense in depth technique.

Secondly, the more advanced the signature database, the higher the CPU load for the system charged with analyzing each signature. Inevitably, this means that beyond the maximum bandwidth packets may be dropped. We have overcome these problems in our IDS system by using capture drivers that support network of up to 1 GBPS (Giga bits per second).

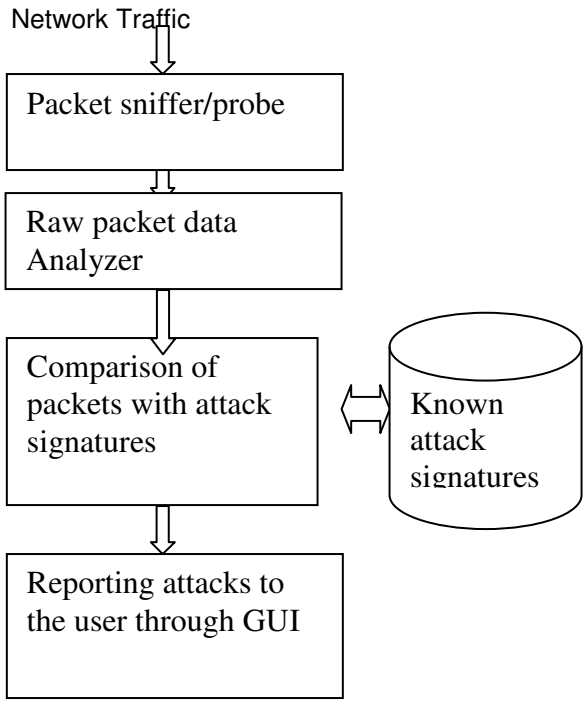

FIGURE 3. – Implementation Architecture

2.3.2 Packet sniffing and promiscuous mode

Packet sniffers generally require that a network interface is in promiscuous mode. The packet sniffer normally requires administrative privileges on the machine being used as a packet sniffer,

so that the hardware of the network card can be manipulated to be in promiscuous mode is given in Figure 2.

This system uses a network probe to capture raw packet data and then we use this raw packet data to retrieve packet information such as source and destination IP address, source and destination ports, flags, header length, checksum, Time to Live (TTL) and protocol type. We then use this data and compare it with known attack signatures to identify threats to the network, shown in figure 3.The experimental results have been shown through screen shots in the figure 4 and 5

2.3.3 Attacks captured by software

IGMP KOD

An IGMP based denial-of-service attack that depletes the stack's large envelopes and also has source IP address spoofing. KOD (Kiss of Death) is a denial-of-service attack, which results in "Blue Screen" error message (so called "blue screen of death") or instantaneous reboot of computer. KOD send to victim's computer malformed IGMP (Internet Group Management Protocol) packets causing TCP/IP stacks to fail.

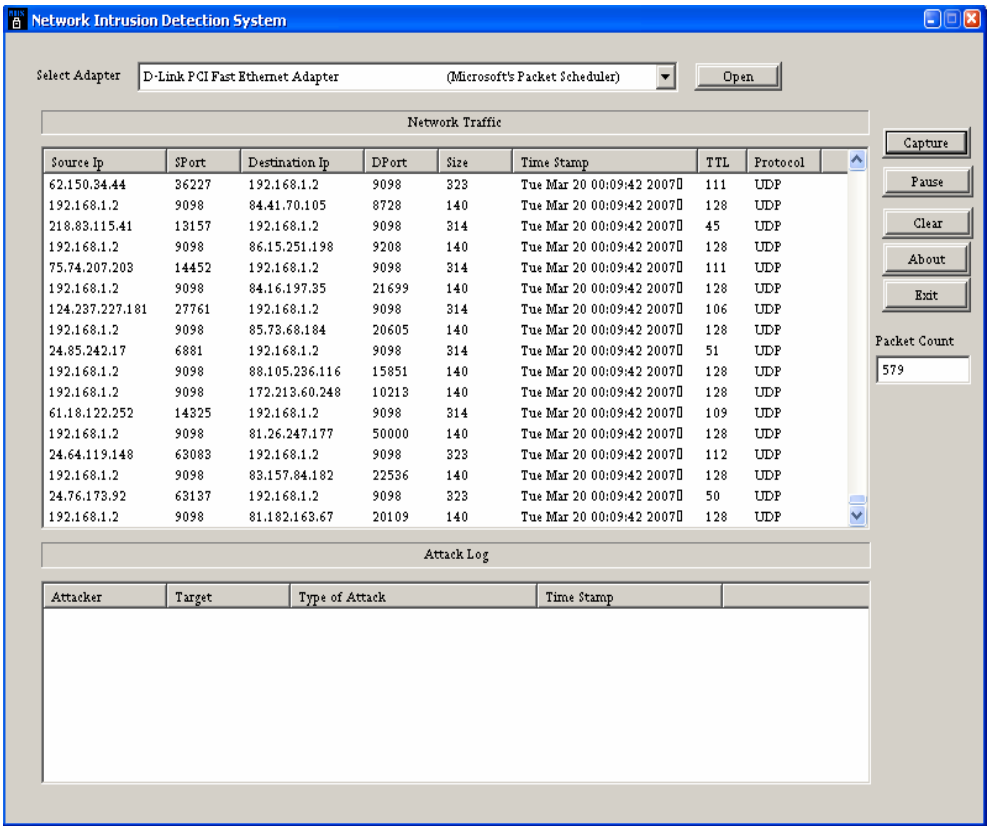

FIGURE 4: Screen shots 1

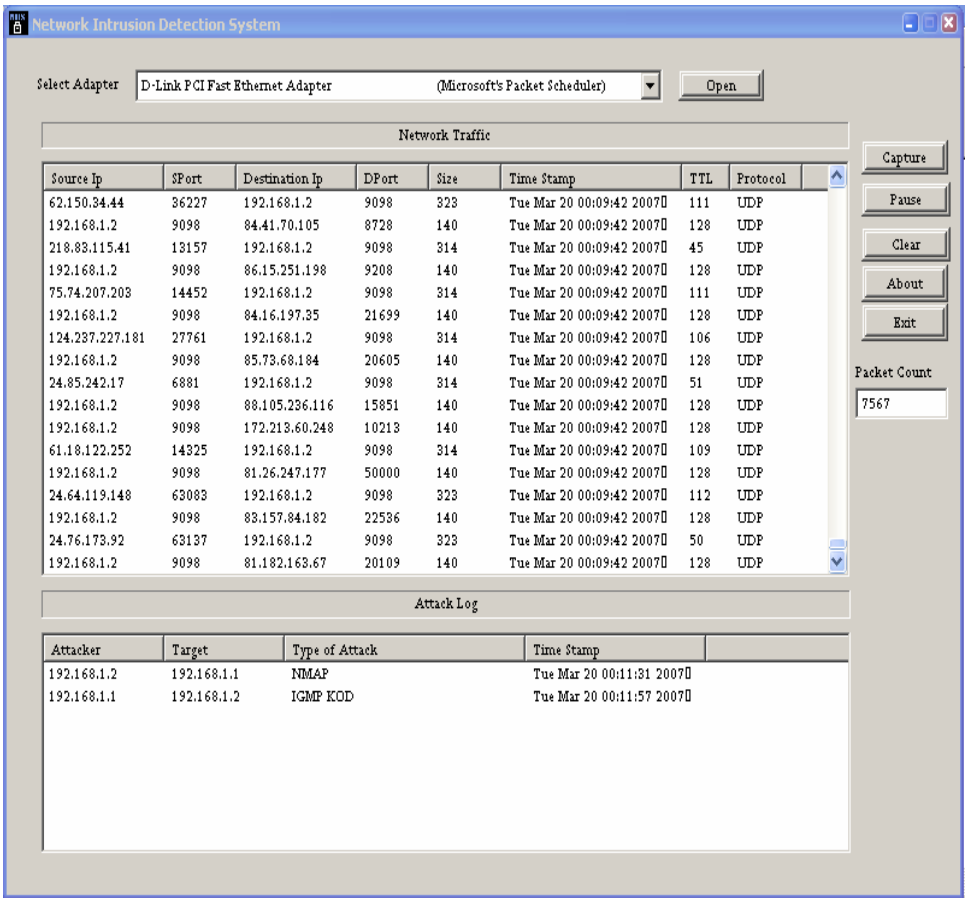

FIGURE 5: Screen shots 2.

DOS attack

In computer security, a denial-of-service attack (DOS) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the internet. It is a computer crime that violates the Internet proper use policy as indicated by the internet Architecture Board (IAB).

DOS attacks have two general forms:

i) Force the victim computer(s) to reset or consume its resources such that it can no longer provide its intended service.
ii) Obstruct the communication media between the intended users and the victim so that they can no longer communicate adequately.

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- flooding a network, thereby preventing legitimate network traffic;
- Disrupting service to a specific system or person.

- Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System Servers.
- Consumption of computational resources, such as bandwidth, disk space, or CPU time

DOS conseal

Vulnerability exists in the conseal firewall product that causes the vulnerable system to reboot or lock up when a large number of spoofed UDP packets are received by the firewall. The way this attack kills the machine happens in 2 ways

- If Conseal is set for "learning" mode the flooding packets from all the different IPs and ports will cause the program to continuously attempt to write more and more new rules. This eventually uses up all the resources and results in a freeze and eventually a reboot.
- If Conseal is set to log attacks, once again because of the number of packets the system resources are eaten up and the machine dies.

DOS bloop

It is a denial Of Service attack that sends random spoofed ICMP packets. ICMP flooding is probably the most common type of Denial of Service attack, since nearly all websites reply to ICMP packets, its easy to use ICMP flooding to shut them down. The result of the attack is freezes the users machine or a CPU usage will rise to extreme lag potential.

ICMP flooding works by sending a lot of ICMP packets to the target machine, for each packet sent the remote computer has to reply to each one, meaning it would exhaust the machines bandwidth so a legitimate user could not access the server. ICMP packets are better known as “Pings”, they are used to see if a remote computer is online.

NMAP

NMAP was the source of strange new scan patterns started being detected by the SHADOW ID Systems located throughout the Internet. This scan’s signature is characterized by SYN packets sent to apparently random destination ports over some discreet range of values. At the end of these scans we typically see several packets to high numbered TCP and UDP ports, followed by a small number of packets to a common destination port. The two basic scan types used most in NMAP [8,9] are TCP connect () scanning and SYN scanning also known as half-open, or stealth scanning.

DNS solinger

Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols that provides an openly re-distributable reference implementation of the major components of the Domain Name System. BIND SOLINGER vulnerability could allow remote attackers to hang the service for periods up to 120 seconds by initiating abnormal TCP connections to the daemon. In some systems, it is possible to set the system wide solinger timeout to a lower value, however this may have unexpected consequences with other applications.

2.4 Testing tool

We have used Karalon traffic IQ professional [11, 24] for testing our software with intrusion attacks. Traffic IQ Professional provides a unique industry approved software solution for auditing and testing the recognition and response capabilities of Intrusion detection systems.

Features include

- Traffic Replay
- Traffic scan list
- Reporting
- Traffic file editor
- Command prompt

- Traffic library

3. CONCLUSION

We have successfully created a network based intrusion detection system with signature IDS methodology. It successfully captures packets transmitted over the entire network by promiscuous mode of operation and compares the traffic with crafted attack signatures. The attack log displays the list of attacks to the administrator for evasive action. This system works as an alert device in the event of attacks directed towards an entire network It has functionality to run in the background and monitor the network.

It also incorporates functionality to detect installed adapters on the system, selecting adapter for capture, pause capture and clearing captured data is shown in *the screen shots*. It may be incorporated with further signatures for attacks. This 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. The types of attacks share the characteristic that upon their initiation and while they are in progress, Global attack and of distributed intrusion detection processes produce sufficient network traffic (e.g. port scanning) so that local detectors can find sufficient evidence of the attack and report the attacks.

4. REFERENCES

[1] "Symantec-Internet Security threat report highlights (Symantec.com)", http://www.prdomain.com/companies/Symantec/newreleases/Symantec_internet_205032.htm

[2] Symantec Security Response, W32.ExploreZip.L.Worm, http://securityresponse.symantec.com/avcenter/venc/data/w32.explorezip.l.worm.html , January 2003.

[3] Komninos T., Spirakis P.: Dare the Intruders, Ellinika Grammata and CTI Press (2003).

[4] E. Biermann, E.Cloete, L.M. Venter, A comparison of Intrusion detection systems, *Computers and* Security, 20(2001)8, 676–683.

[5] P. Ning and D. Xu. Hypothesizing and reasoning about attacks missed by intrusion detection systems. ACM Transactions on Information and System Security, 7(4):591– 627, November 2004

[6] Herringshaw, C. (1997) 'Detecting attacks on networks', IEEE Computer Society Vol.30, pp.16 – 17.

[7] International Standard IS0 7498.2, Information processing system - Open system interconnection – Basic reference model, PaR *2:* Security architecture, 1989.

[8] D. Oollmann, *Cornpuler Security,* John Wiley & Sons, 1999.

[9] R.G. Bace, *Intrusion* Detection. Macmillan Technical Publishing, 2000

[10] http://www.winpcap.org/ - Obtained drivers for packet capture with wpcap.dll and packet.dll driver.

[11] http://www.karalon.com - Obtained Karalon IQ professional tool for testing our network intrusion detection system.

[12] http://www.securityfocus.com – White papers for intrusion detection techniques and methodologies.

[13] R. Lippmann, The Role of Network Intrusion Detection, In *Proceedings of the Workshop on Network Intrusion Detection*, H.E.A.T. Center, Aberdeen, MD, March 19-20, 2002.

[14] SNORT Intrusion Detection System, www.snort.org, 2004.

[15] Snort-Wireless Intrusion Detection, http://snort-wireless.org, 2003.]

[16] NFR Network Intrusion Detection, http://www.nfr.com/products/NID/, 2001.

[17] Cisco Systems, Inc., NetRanger-Enterprise-scale, Real-time, Network Intrusion Detection System, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/netrangr/, 1998.

[18] Internet Security Systems, Inc., RealSecure, http://www.iss.net/prod/rsds.html, 1997.

[19] Intrusion.com, Intrusion SecureHost, white paper available at: www.intrusion.com/products/hids.asp , 2003.

[20] J. Van Ryan, SAIC's Center for Information Security, Technology Releases CMDS Version 3.5,

http://www.saic.com/news/may98/news05-15-98.html, 1998.

[21] N. Weaver, V. Paxson, S. Staniford and R. Cunningham, A Taxonomy of Computer Worms, In Proceedings of the The Workshop on Rapid Malcode (WORM 2003), held in conjunction with the 10th ACM Conference on Computer and Communications Security, Washington, DC, October 27, 2003.

[22] Wheel Group Corporation, Cisco Secure Intrusion Detection System,

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm , 2004

[23] Patwardhan, A. Parker, J., Joshi,A., Karygiannis, A., and Iorga,M. “Secure Routing and Intrusion Detection in Ad Hoc Networks”, *Third IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, Hawaii, 2005.

[24] Komninos T, Spirakis P., Stamatiou et.al..: A Software Tool for Distributed Intrusion Detection in
Computer Networks (Helena) (Best Poster presentation in PODC 2004).