SNMP ALG PROTOCOL SEQUENCE ANALYSIS FOR INTRUSION DETECTION SYSTEM

[1]D. PARAMESWARI, [2]Dr. R. M. SURESH

[1]Research Scholar,Mother Teresa Women's University,Kodaikanal-624 101.
[2]Professor & Head, Computer Science & Engineering
RMD Engineering College, Chennai, Tamil Nadu - 601206

ABSTRACT

Network technology smooth the progress of communication system in a sophisticated manner at the same time it braves are increased from the huntsman. In communication process, user's connectivity, violations of policy on access of information are handles through intrusion. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. It focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. However, organizations use Intrusion detection and prevention system (IDPS) for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. Now a days IDPSs have become a necessary addition to the security infrastructure of nearly every organization. In this paper describes about **Simple Network Management Protocol Application Level Gateway (**SNMP ALG) protocol sequences which is used to detect the intrusion on hybrid network and its attributes and recommend the standardized **(**SNMP ALG) protocol for the intrusion detection process.

Keywords: *Simple Network Management Protocol Application Level Gateway (SNMP-ALG) , Network instruction Detection, Protocol Analysis , SNMP ALG –NIDS*

1.0 INTRODUCTION

The modern information and communication Technology (ICT) system developed and facilitated many communication enhancement options for the up gradation of our living standards. The computer network is played vital role as a backbone of ICT. Many challenges are managed in this system. In the communication process, user's connectivity, violations of policy on access of information are handles through intrusion. According to Peter, Intrusion detection is the process of monitoring the events occurring 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, acceptable use policies, or standard security practices.

2.0 INTRUSION DETECTION SYSTEM (IDS)

In recent years, dramatically increase the amount of data (text; images; audio; etc.) that available electronically on the Internet. Therefore, the hackers and intruders had made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure the data over the network and over the Internet.Computer networks are usually protected by anti-virus software, firewall, and encryption, secure network protocols, password protection etc. Since it has been proven that a potential attacker can always find a way to attack a network. These systems are known as Intrusion Detection System (IDS) and are placed inside the protected network, looking for potential threats in network traffic and or audit data recorded by host.

3.0 REVIEW OF LITERATURE

Initially intruder attempts to break into an information system or performs an action not legally allowed, we refer to this activity as an *intrusion* (Graham, 2002; see also Jones and Sielken, 2000). Intruders can be divided into two groups, *external* and *internal*. The former refers to those who do not have authorized access to the system and who attack by using various penetration techniques. The latter refers to those

with access permission who wish to perform unauthorized activities. Intrusion techniques may include exploiting software bugs and system misconfigurations, password cracking, sniffing unsecured traffic, or exploiting the design flaw of specific protocols (Graham, 2002). An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation an organization's information security policy (Jones and Sielken, 2000), which reflects an organization's statement by defining the rules and practices to provide security, handle intrusions, and recover from damage caused by security breaches.

There are two generally accepted categories of intrusion detection techniques: *misuse detection* and *anomaly detection*. *Misuse detection* refers to techniques that characterize known methods to penetrate a system. These penetrations are characterized as a 'pattern' or a 'signature' that the IDS looks for. The pattern/signature might be a static string or a set sequence of actions. System responses are based on identified penetrations. *Anomaly detection* refers to techniques that define and characterize normal or acceptable behaviors of the system (e.g., CPU usage, job execution time, system calls). Behaviors that deviate from the expected normal behavior are considered intrusions (Bezroukov, 2002; see also McHugh, 2001).

IDSs can also be divided into two groups depending on where they look for intrusive behavior: *Network-based IDS (NIDS)* and *Host-based IDS*. The former refers to systems that identify intrusions by monitoring traffic through network devices (e.g. Network Interface Card, NIC). A *host-based IDS* monitors file and process activities related to a software environment associated with a specific host. Some *host-based IDSs* also listen to network traffic to identify attacks against a host (Bezroukov, 2002; see also McHugh, 2001). There are other emerging techniques. One example is known as a *blocking IDS*, which combines a host-based IDS with the ability to modify firewall rules (Miller and Shaw, 1996). Another is called a *Honeypot*, which appears to be a 'target' to an intruder, but is specifically designed to trap an intruder in order to trace down the intruder's location and respond to attack (Bezroukov, 2002).This approached is planned with network based sensors. So the intrusion can be detected based on the observation of protocol and its sequence analysis. Therefore we are going to discuss about various protocol definitions which is used and observed in this research.

4.0 PROTOCOLS

Protocols are set of rules that governing how data is transferred, compressed and presented over networks.There are many protocols, each one governing the way a certain technology works. A **network protocol** defines rules and conventions for communication between network devices. Protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of *packets*. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication. Hundreds of different computer network protocols have been developed each designed for specific purposes and environments.

In general , The Internet Protocol family contains a set of related (and among the most widely used network protocols. Besides Internet Protocol (IP) itself, higher-level protocols like TCP, UDP, HTTP, and FTP all integrate with IP to provide additional capabilities. Similarly, lower-level Internet Protocols like ARP and ICMP also co-exist with IP. These higher level protocols interact more closely with applications like Web browsers while lower-level protocols interact with network adapters and other computer hardware. Here we are going to discuss few protocols which is observed over the network . The following part of the paper provides more details on various protocols and its functional services .

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and

providing address conversion in both directions. This is used to identify and monitor the packet communication across the network. This part of the work try to optimize and construct the ARP sequence to detect the Intrusion.

Hypertext Transfer Protocol (HTTP) : The Hypertext Transfer Protocol (HTTP) is an application level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990.HTTP is a request-response standard typical of client-server computing. In HTTP, web browsers or spiders typically act as clients, while an application running on the computer hosting the web site acts as a server. The client, which submits HTTP requests, is also referred to as the user agent. The responding server, which stores or creates resources such as HTML files and images, may be called the origin server. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels. HTTP is not constrained in principle to using TCP/IP, although this is its most popular implementation platform. Indeed HTTP can be "implemented on top of any other protocol on the Internet, or on other networks." HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used.

Hypertext Transfer Protocol Secure (HTTPS):HTTP can run on top of TLS or SSL for secured transactions, which is called HTTPS. HTTPS is not to be confused with S-HTTP, a security-enhanced version of HTTP developed and proposed as a standard by IETF. HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.

Internet Control Message Protocol (ICMP) is an integrated part of the IP suite. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation. ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problems.CMP[1] relies on IP to perform its tasks, and it is an integral part of IP. It differs in purpose from transport protocols such as TCP and UDP in that it is typically not used to send and receive data between end systems. It is usually not used directly by user network applications, with some notable exceptions being the ping tool and traceroute.

NetBIOS Session Service over TCP/IP (NBSS): NetBIOS Session Services are part of the NetBIOS over TCP/IP (NetBT) family of protocols and is used for server message block (SMB). This is both the port that NULL Sessions are established over and the port that file and printer sharing takes place on.

Network Basic Input Output System (NetBIOS): Network Basic Input Output System (NetBIOS), created by IBM originally, defines a software interface and standard methods providing a communication interface between the application program and the attached medium. NetBIOS, a session layer protocol, is used in various LAN (Ethernet, Token Ring, etc) as well as WAN environments, such as TCP/IP,PPP and X.25 networks.

Real-Time Transport protocol (RTP) provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video or simulation data, over multicast or unicast network services. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. However, RTP may be used with other suitable underlying network or transport protocols. RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network.

Simple Network Management Protocol (SNMP): is the standard protocol developed to manage nodes (servers, workstations, routers, switches and hubs, etc) on an IP network. SNMP enables network administrators to manage network performance, find, solve network problems and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

Spanning-Tree Protocol (STP), as defined in IEEE 802.1D, is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations. Loops occur in networks for a variety of reasons. The most common reason for loops in networks is a deliberate attempt to provide redundancy—in case

one link or switch fails, another link or switch can take over.

TELNET is a TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.TELNET is a client-server protocol, based on TCP, and clients generally connect to port 23 on the host providing the service (though like many protocols in use on the Internet, which port to use is fairly easy to change). Partly because of the design of the protocol and partly because of the flexibility typically provided by TELNET client programs, it is also possible to use a TELNET program to establish an interactive TCP connection to some other service on an Internet host. A classic use of this is telnetting to port 25 (where typically an SMTP server is to be found) to debug a mail server.

VOIP Protocols : Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. Using VOIP protocols, voice communications can be achieved on any IP network regardless of whether it is Internet, Intranet or Local Area Network (LAN). In a VOIP enabled network, the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. VOIP signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities. The key benefits of Internet telephony are the very low cost; the integration of data, voice and video on one network; the new services created on the converged network; and simplified management of end user and terminals.

5.0 EXPERIMENTAL SPECIFICATION

The network consists of wired and wireless with internet, intranet, and extranet using LAN and WAN architectures to provide the services for the students, staff. This network used for file transfer(FTP), Remote access(TELNET), Active Directory Services(DNS), NETBIOS, Print server, IP telephony (Internal),Wireless Fidelity, Bluetooth, VPN , Email(IMAP), SMTP, E-Learning(Web server-HTTP) , PING-ICMP, etc services. While providing the above specified services the network response and its Quality of Services varies due to the protocols which is used for the specific service. To reach the maximum service utilization, existing services are observed based on its protocol in and between the networks.

There are many protocols running over the network to facilitate various requests and services. In this study we considered few services and its related protocol for the observation and analysis to construct the packet sequence to detect the intrusion.

The following diagram show the Network architecture of hybrid academic networkwhich connect three academic department and four non academic departments. This network provides Teaching- learning and educational management service over 3000 students and the faculties in the campus. This consist of LAN and the following technological configurations

This academic network is framed as three clusters to provide the educational services. For the effective administration and maintenance of this network services, the classification and cluster made in the department level. In this study, the academic network structure and its laboratories' setup data communication and transformation architecture is adopted.

The network architecture constructed with modern technological equipments such as cisco switches(Core Switch)- 4503E, SAN-SWITCH-IBM-2005-16B, cisco-routers-1700,2800 series; Firewall-CISCO-ASA-5510, cisco IP phones encompass of CISCO-MCS-7800-KQGCY35-Pentium-D- 2.80GHz call manager. This also integrated with High end servers' such as HP Proliant-DL380 - GB8639NHPS-Xeon 3.4Ghz; IBM-3850-99B5265-Xeon-3.5GHz ; DVR- Proline- DVR-UK; SAN SWITCH- A device that routes data between servers and disk arrays in a storage area network . Its' 800 nodes are typically Conduit with UTP CAT-5, CAT-5E,CAT-6 and Fiber Channel switch made up of fiber multimode channels.

The established infrastructure integrated with wireless fidelity of various manufacturers. The network is enhanced with Video conferencing supported for inter and intra conferencing facility. There are many protocols are observed for the intrusion detection process to frame the sequence formation. But in this paper we are going to discuss the common sequence formation of the SNMP ALG protocol.

6.0 SNMP – ALG

An SNMP ALG should provide transparent IP address translation to management applications. An SNMP ALG must be compatible with the behavior of the SNMP protocol operations as defined by RFC 1157 and RFC 1905

and must not have negative impact on the security provided by the SNMP protocol. A fully transparent SNMP ALG must be able to translate all categories of IP addresses as described above, when provided with the specified OID's and the encoding details.The SNMP ALG requires bi-directional NAT devices enroute, that support static address mapping for all nodes in the respective private realms. When there are multiple private realms supported by a single SNMP ALG, the external addresses assumed by each of the NAT devices must not collide with each other.

6.1 Basic SNMP Application Level Gateway

A basic SNMP ALG is an SNMP ALG implementation in which only IP address values encoded in the IpAddress base type are translated. A basic SNMP ALG implementation parses an ASN.1/BER encoded SNMP packet looking for elements that are encoded using the IpAddress base type. An IP Address value can be identified easily by its tag value (0x40). Once an IP Address has been detected, the SNMP ALG checks the translation table and decides whether the address should be translated. The translation process system represented below diagram. If the address needs translation, the 4 bytes representing the IPv4 address are replaced with the translated IPv4 address and the UDP checksum is adjusted.

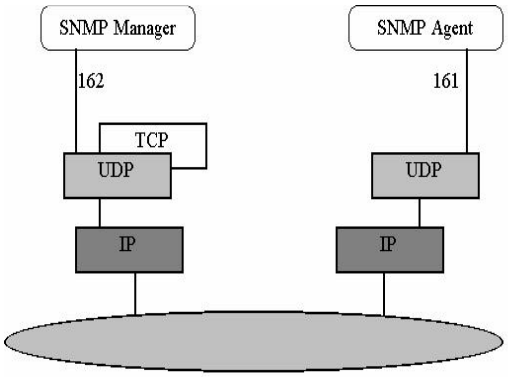

Fig : SNMP Communication –IP Based

The basic SNMP ALG does not require knowledge of any Management Information Base (MIBs) since it relies on the ASN.1/BER encoding of SNMP packets. The MIS bit representation described below table. It is therefore easy to implement.

GROUP	#OBJECTS	DESCRIPTION
System	7	Name, location, and description of the equipment
Interfaces	23	Network interfaces and their measured traffic
AT	3	AddressTranslation
IP	42	IP packet statistics
ICMP	26	Statistics about ICMP messages received
TCP	19	TCP algorithms parameters, and statistics
UDP	6	UDP traffic statistics UDP traffic statistics
EGP	20	Exterior gateway protocol traffic statistics
Transmission	0	Reserved for media-specific MIBs
SNMP	29	SNMP traffic statistics

Table : objects groups of MIB

A basic SNMP ALG does not change the overall messages size and hence it does not cause translated messages to be lost due to message size constraints. However, a basic SNMP ALG is only able to translate IPv4 addresses in objects that use the IpAddress base type. Furthermore, a basic SNMP ALG is not capable to translate IP addresses in objects that are index components of conceptual tables. This is especially problematic on index components that are not accessible. Hence, the basic SNMP ALG is restricted to the first out of the four possible ways to represent IP addresses in SNMP messages.

6.2 Advanced SNMP Application Level Gateway

An advanced SNMP ALG is an SNMP ALG implementation which is capable of handling and replacing IP address values encoded in well known IP address data types and instance identifiers derived from those data types. Hence, an advanced SNMP ALG may be able to transparently map IP addresses. This implies that an advanced SNMP ALG must be MIB aware.

An advanced SNMP ALG must maintain an OBJECT IDENTIFIER (OID) translation table in order to identify IP addresses that are not encoded in an IpAddress base type. The OID strcutre is represented in the below diagram with its functional components. The OID translation table needs to maintain information about the OIDs where translation may be needed. Furthermore, the translation table needs to keep information about instance identifiers for conceptual tables that contain IP addresses. Such an OID translation table may be populated offline by using a MIB compiler which loads the MIBs used within an addressing realm and searches for types, textual conventions and table indexes that may contain IP addresses. The translation function scans the packet for these specific OIDs, checks the translation table and replaces the data if needed. Note that since OIDs do not have a fixed size this search is much more computationally consuming, and the lookup operation may be expensive.

The ability to translate IP addresses that are part of the index of a conceptual table is a required feature of an advanced SNMP ALG. IP addresses embedded in an instance identifier are ASN.1/BER encoded according to the OID encoding rules. Another effect of an advanced SNMP ALG is that it changes the lexicographic ordering of rows in conceptual tables as seen by the SNMP manager. This may have severe side-effects for management applications that use lexicographic ordering to retrieve only parts of a conceptual table. Many SNMP managers check lexicographic ordering to detect loops caused by broken agents. Such a manager will incorrectly report agents behind an advanced SNMP ALG as broken SNMP agents.

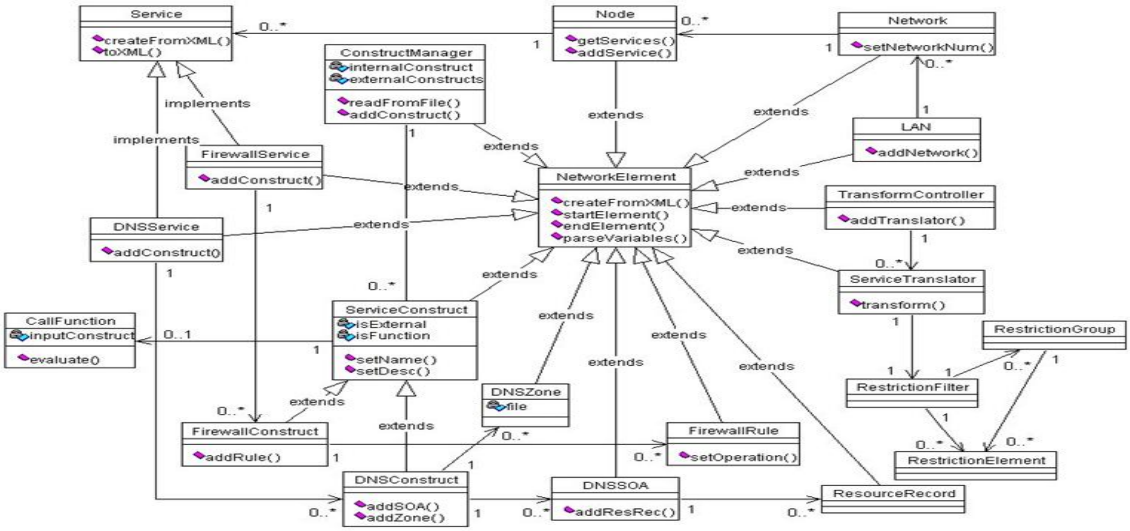

Fig :SNMP ALG - OBJECT IDENTIFIER (OID)

6.3 Translating IP Addresses in SNMP Packets

The static mapping process on SNMP is achieved through translate IP addresses in SNMP packets.SNMP ALG must be capable to translate IP addresses in outgoing and incoming SNMP packets. SNMP messages send over UDP may experience fragmentation at the IP layer. In an extreme case, fragmentation may cause an IP address type to be partitioned into two different fragments. In order to translate IP addresses in SNMP messages, the complete SNMP message must be available. As described in, fragments of UDP packets do not carry the destination/source port number with them. Hence, an SNMP ALG must reassemble IP packets which contain SNMP messages.

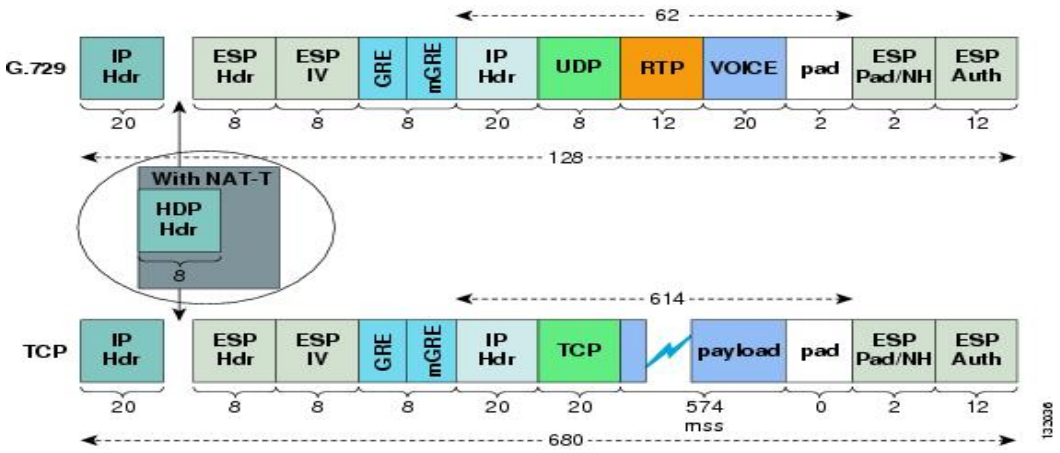

Fig: SNMP – ALG IP translation architecture

SNMP agents are aware of the Maximum Transmission Unit(MTU), and that SNMP packets are usually relatively small. Some SNMP implementations also set the don't fragment (DF) bit in the IP header to avoid fragmentation.

6.4 Standardized 64 byte SNMP ALG protocol strcuture

The above addressed issues are used one way to another to facilitate the communication process effectively . The communication facilitation allows the intrusion attacker to the network . To Monitor and detect the same users , the following sequence are proposed .

From 1-4 bytes (32 bit) Frame Information

1	2	3	4
Frame Info (0-31)			
Time	Number	Length	Capture Length
Link	Data	Data	Data

The first byte represented about the frame information . This provides information about when the packets is travelled at that system or device, as well as number , length and capture of the packet .

5	6	7	8	9	10
Destination Address (32 - 79)					
Broad Cast					
Group Address					
	Multi Cast	Local Address			

The next 48 bit (6 byte) provides the information about the destination. If any of the destination is not listed with the specified network then that device will be blocked from the attached using GA algorithms.

11	12	13	14	15	16
Source (80 - 127)					
Uni Cast Individual					

The next 48 bit (6 byte) provides the information about the source. If any of the socuece not listed with the specified network then that device will be blocked from the attached using GA algorithms.

17	18	19	20	21	22	23	24	25	26
Type SNMP (128 - 143)		ARP (144 - 367)							
		Hard ware Type	Protocol Type			Hard ware Size		Protocol Size	Op Code

This ten byte information provides more details about the SNMP ALG type , hardware and relateed information's .The following sequence will provide data about the MAC address of the sender as well as target device .

27-30	31-36	37-40	41-46
ARP (144 - 367)			
Mac Address	Sender IP	Target MAC	Target IP

47-64
Trailer (368 - 511)

8.0 CONCLUSION

This proposed standardized SNMP ALG 64 byte structure is easy to capture the SNMP ALG from the network. All the required information from the source and the sender as well as sender and target device are captured in this structure. This is not affected the data transformation process but this can be integrated to the monitor the nerwork. This paper is part the instruction detection work using genetic algorithm .

REFERNCES:

[1]. Arizona. URL: http://www.acsac.org/1999/papers/fri-b-1030-sinclair.pdf (30 Oct. 2003).

[2]. Bezroukov, Nikolai. 19 July 2003. "Intrusion Detection (general issues)."

[3]. Bridges, Susan, and Rayford B. Vaughn. 2000. "Intrusion Detection Via Fuzzy Data Mining." *In Proceedings of 12th Annual Canadian Information Technology Security Symposium*, pp. 109-122. Ottawa, Canada.

[4]. Crosbie, Mark, and Gene Spafford. 1995. "Applying Genetic Programming to Intrusion Detection." *In Proceedings of 1995 AAAI Fall Symposium on Genetic Programming*, pp. 1-8. Cambridge, Massachusetts. URL: http://citeseer.nj.nec.com/crosbie95applying.html (30 Oct. 2003).

[5]. David C. Plummer (1982-11). "RFC 826, An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware". Internet Engineering Task Force, Network Working Group. http://tools.ietf.org/html/rfc826.

[6]. http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf Guide to Intrusion Detection and Prevention Systems (IDPS), NIST CSRC special publication SP 800-94, released 02/2007

[7]. http://www.geatbx.com/docu/algindex.html.

[8]. IANA - Ethertype values

[9]. IANA ARP - "Protocol Type"

[10]. Jones, Anita. K. and Robert. S. Sielken. 2000. "Computer System Intrusion Detection: A Survey." Technical Report.Department of Computer Science, University of Virginia, Charlottesville, Virginia.

[11]. Li, Wei. 2002. "The integration of security sensors into the Intelligent Intrusion Detection System (IIDS) in a cluster environment." Master's Project Report. Department of Computer Science, Mississippi State University.

[12]. McHugh, John, 2001. "Intrusion and Intrusion Detection." Technical Report. CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University.

[13]. Miller, Brad. L. and Michael J. Shaw. 1996. "Genetic Algorithms with Dynamic Niche Sharing for Multimodal Function Optimization." *In Proceedings of IEEE International Conf. on Evolutionary Computation*, pp. 786-791. Nagoya University, Japan.

[14]. Paxson, Vern. 1998. "Bro: A System for Detecting Network Intruders in Real-time." *In Proceedings of 7th USENIX Security Symposium*, pp. 31-51. San Antonio, Texas.

[15]. Pohlheim, Hartmut. 30 Oct. 2003. "Genetic and Evolutionary Algorithms: Principles, Methods and Algorithms."Genetic and Evolutionary Algorithm Toolbox. Hartmut Pohlheim. URL:

[16]. RFC 1122, Requirements for Internet Hosts -- Communication Layers, R. Braden (Ed.), Internet Engineering Task Force (October 1989)

[17]. RFC 5342

[18]. Robert Graham. URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html (30 Oct. 2003).

[19]. Roesch, Martin. Nov. 7-12, 1999. "Snort - Lightweight Intrusion Detection for Networks." *In Proceedings of 13th Systems Administration Conf. (LISA '99)*, pp. 229-238.Seattle, Washington.

[20]. Sinclair, Chris, Lyn Pierce, and Sara Matzner. 1999. "An Application of Machine Learning to Network Intrusion Detection." *In Proceedings of 1999 Annual Computer Security Applications Conf. (ACSAC)*, pp. 371-377. Phoenix,

[21]. Sinclair,chris,Lynpierce and Sara Matznel,1999."An application of Machine learning to network intrusion detection", In proceedings of 1999 Annual Computer Society Applications Conference.pp-371-377.

[22]. Softpanorama: Open Source Software Educational Society. Nikolai Bezroukov. URL:http://www.softpanorama.org/Security/intrusion_detection.shtml (30 Oct. 2003).

[23]. Whitley, Darrell. 1994. "A Genetic Algorithm Tutorial." *Statistics and Computing* 4: 65-85.