Steganography Based Authentication to Prevent IP Spoofing

Nosheen Fayyaz [1], Imranuddin[2], Rahatullah[2], Syed Usman Anwar[2], Lala Rukh[2]

[1.] Department of Computer Science, University of Peshawar, Khyber-Pakhtunkhwa, Pakistan.
[2.] Department of Computer Science, IBMS, University of Agriculture Peshawar, Khyber-Pakhtunkhwa, Pakistan.
imrandin@yahoo.com

Abstract: The idea of the ancient Steganography technique is used for the prevention of IP spoofing. Previously the steganography was used by the hackers or intruders, but here it is used for a positive purpose to authenticate the user at the time of handshake and prevent the Denial of Service (DOS) attack and resolve the open connection problem. The Steganography authentication is applied within a domain, and is successful in the rejection of unauthorized packets. The system is used and recommended for the inter-domain operations, especially on gateways machines, in order to prevent unauthorized packets from entering into the Internet highway. The Steganography filters inside the domains and router-based filters in Internet can minimize the IP spoofing. By stopping IP spoofing, many attacks are either automatically incomplete or the attacker is forced to use legal machine, which can be traced back easily. This study is performed on the TCP (Transport Control Protocol)/IP (Internet Protocol) communication handshake technique to prevent IP spoofing.
[Fayyaz N, Imranuddin, Rahatullah, Anwar S.U, Rukh L. **Steganography Based Authentication to Prevent IP Spoofing** *Life Sci J* 2013;10(12s):673-677] (ISSN:1097-8135). http://www.lifesciencesite.com. 108

Keywords: IP Spoofing, Hand Shake, steganography, DOS attack

1. Introduction

Millions of public and private networks are connected by using a standard Internet Protocol Suite (also known as TCP/IP). In 1982, TCP/IP was standardized and the concept of Internet was introduced [1]. Networks are prone to threats and current Intrusion Detection Systems (IDS) could not provide the ultimate solution, though it can present the real picture of a network to the administrator [2].These IDS cannot trace the hacker within a domain. When two or more computers communicate, they establish a connection by an initial process known as three-way hand-shake [3]. The connection is then opened between the client and the server, and the service-specific data can be exchanged, if handshake fails, no further communication takes place.

IP Spoofing is a hijacking technique in which an attacker masquerades as a trusted host to hide his identity and gain access to a network. It is also known as IP address forgery [4]. "This spoofing attack involves forging one's source address. It is the act of using one machine to impersonate another." [5]. In case of IP Spoofing, the hacker sends a SYN packet to server, forging its IP as that of an authorized client. The server will send SYN-ACK back to the sender (authorized client), which in turn will send RESET packet to the server, stating that it has no knowledge of any SYNC sent to server, and so the server resets the connection [6]. This information is vital for an attacker. This attack can be initiated again when the authorized client is offline. The hacker will send SYN to the server, that will sends SYN/ACK to authorized client. After some interval, the hacker sends a forged ACK packet to the server again forging the IP Address, making the server think as if packet was legal, and false handshake is completed. Now the hacker has access to a server connection which can be exploited illegally [6].

Steganography is a technique of hiding a message such that no one except the sender and the recipient know about it. It is a Greek word which means "Concealed Writing". In Steganography the message will be hidden in something just like images and list of items [7]. The secret message is covered or embedded in a cover and transmitted such that the existence of the message is undetectable. Steganography is used for secret data transmission because it provides more security. It is used for both legitimate and illegitimate purposes. It can even be used by hackers, or terrorists, but it can also be used for something good such as authentication, sending secret messages, transmitting secure data over the internet [8], controlling log forensics and tracing back the hacker by observing his/her behavior [9].

Usually the steganography and cryptography are implemented together resulting in increased security [10]. Cryptography is a technique that is also used to hide messages, but Steganography has an advantage over it. Cryptography hides the message but cannot hide the parties, and the message which is encrypted using cryptographic algorithms, no matter how strong the encryption is, will cause attention to itself. The main difference between steganography and cryptography is the suspicion factor. Steganographic process can be explained by the following formula:

Cvr1 + Msg2+ S-key3 = Cvr + H_ MSG4 (1)
1Cvr: Cover: A medium that can be an image, a shopping list, a newspaper/ article or an audio/video file etc.
2Msg: Message: The information we want to hide in the Cover.
3S-key: Steganographic key to encrypt the hidden message.
4H_MSG: Hidden Message

Digital images, videos/audios or any other digital file can be used as a carrier of steganography information and are called Covert objects. The digital file is merely a binary file containing a binary representation of the colour or light intensity of each picture element (pixel) comprising the image, or each audio bit, or pixel information of frames of a video. The simplest steganography technique LSB (Least Significant Bit) insertion can hide bits by changing the least significant bit at the cost of changing roughly 50% of the original [11].

Current studies about IP spoofing concentrated mostly on router based filtering that is the egress filtering and ingress Filtering [6]. Apart from filtering, the hop count technique discard the packets coming from a network using the IPs of another Network, checking the hop distance on the packet [12]. There is no mechanism to authenticate the IP. The window size, the TTL (Time to Live), and sequence numbers were considered a source for authentication, but this consideration fails when sniffer is present within the network for packet analysis.

1.1. Problem Summery

- IP Authentication techniques exist, but all have limitations and weaknesses.
- IP spoofing inside a domain is not stopped; rather it should be identified and discarded before exiting from the domain.
- Techniques that are suggested for Inter-domain packet authentication can be easily analyzed by the sniffing software, which make them useless.

1.2. Objectives

- To create a mechanism for IP Authentication at the time of handshake
- To create random codes, and steganography combinations making it difficult to analyze if sniffer is present.
- To avoid the network being populated by spoofed packets.

2. Literature Review

For the first time in 1985, creation of half open connection in UNIX BSD was described as a security weakness in TCP/IP protocol stack. It focused on the design of the TCP/IP and BSD 4.2 implementation that allowed users on un-trusted hosts by masquerading IP's [13]. The system had no mechanism to verify the IP's, but the security analysts did not give much attention to the problem at that time. In 1995, Tsutomu Shimomura's machine was hacked by Kevin Mitnick, a "Computer outlaw" to get some unauthorized files from the system, and this was reported to CERT (Computer Emergency Response Team). CERT described the reasons of server buffer overflow by creating half open connections and suggested router filters (egress and ingress) to minimize IP-Spoofing attacks on a network [14]. Nelson and Paul also suggested the ingress and egress filters, but in combination with fire walls, Secure Bridges, TCP wrapper classes to reduce the attacks [15]. Different methods for detecting spoofed packets are categorized as *Active*, *Passive* and *Router-based*. *Router-based* methods require the entire defense on routers, but they fail if the attacker and forge address belong to the same network, when *router-based* approaches fail, *Active* and *Passive* techniques come into action. The active techniques are the techniques which require some responsive action for verification of the source addresses by the recipient. The techniques categorized as active are TTL, Direct TTL probes, IP identification number, OS Fingerprinting, flow control and trace route etc., while in *Passive* methods the packet information is analyzed. The passive TTL and OS idiosyncrasies are Passive methods to prevent IP Spoofing [6].

The spoofed packets can be filtered, assuming to follow a single path from source to destination i.e. p(s,d). A certain number of selected routers exchange filtering information with their neighboring routers. If a packet is illegally injected into the network, its path changes and its p(s,d) is different, then it is discarded [16]. But getting the g*lobal* routing information to create filters is not feasible. To stop IP Spoofing, different techniques had been proposed. These includes Hop count filtering [12], ANTID technique with a unique path fingerprints in packets[17], the Clouseau System based on RBF to carefully select AS [18], a technique known as LIPS (Lightweight permit system for packet source origin accountability [19], tagging the packets by routers [20], proposing firewall rules for stopping the DOS attack in MANETS [22]. The problem that the hacker should be stopped at the initial stages, and specifically when he/she is spoofing the IP from his/her own network. Duan extended the idea of *route-based packet filters* [16] by introducing Inter Domain Packet Filters (IDPF), based on local Border Gateway Protocol (BGP) updates [21]. This can localize the origin of the attack to a small number of candidate networks [23], but the problem in this technique is to get the information of best R(s,d) on every node, which is not possible. The deployment of

IDS with virtual agent as EADS (Exception Agent Detection System) shows the correctness of packet filtering [24]. But it works during the attack from unknown IP. To check IP spoofing at Access Routers, the trustworthiness of AS is computed by judge router. The technique has low false positive and false negative rates [25], but it needs an extra router and the AS and judge router can also come under attack. The IDPF constructed on the information and functions performed by AS, i.e network reachability information and the size of feasible R(s,d) does not require global routing information and work correctly as long as AS propagates network reachability information according to rules [26].

3. Material & Methods

This technique is a modification to the Normal TCP/IP handshake with the introduction of steganography. Stopping IP Spoofing at the time of handshake will prevent the network being populated by spoofed packets, besides being secured from attacks. In the proposed technique, when a client asks for a connection by sending SYN packet, the server on receiving does not insert any information in the buffer, instead it generates an 8 bit random number (code) and an array of 8 non-repeating random numbers (position-array), for simplicity, we kept the range of array up to 48 numbers but this could be extended. The Ethernet packet pay-load is set to 46 bytes. The code and position-array are encrypted using the DES encryption algorithm and sent back to client in the pay-load, with SYN-ACK flag. The client decrypts the information and populates the 8bit code on random 8 positions (according to position-array) in the first 48 bits of payload. This data along with code and position-array is then encrypted again and sent back to the server with ACK flag. The server decrypts the data and checks if the code bits are in correct places inside the pay-load. If it is found correct, the connection is established with entry in a connection buffer; otherwise the packet is considered malicious and is discarded. The illegal injected packets must be encrypted using a key, which is only known to sender and receiver and could be gained only by social engineering. Guessing about the code and position-array makes the process also difficult or time consuming, because both of them are based on random numbers. Constructive research technique is adopted to develop a test bench using machine/OS independent application to work on multiple machines on a network or on a single machine with multiple Ethernet cards installed supporting multiple platforms. The test bench is composed of three components/actors which are SERVER, CLIENT, and HACK_MACHINE.

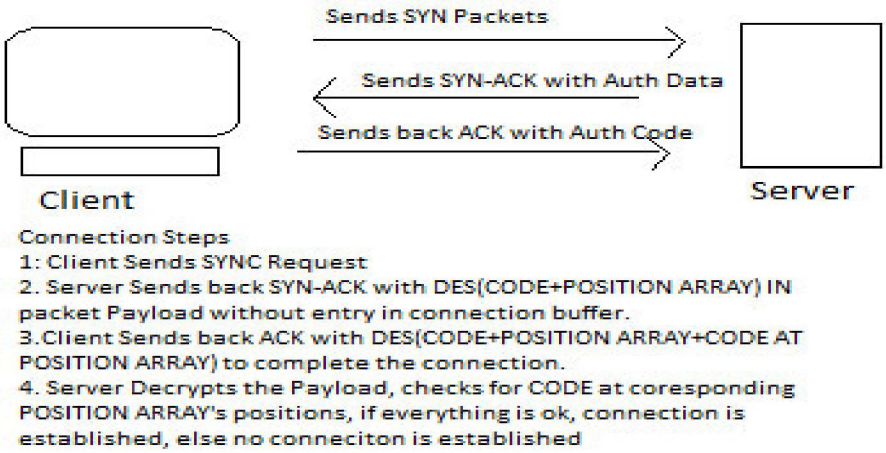

Figure1. Client Server Steganography based Authentication Procedure

3.1. Security Modes

We have defined three main security modes in SERVER and CLIENT machines.

1. Normal Mode: Normal TCP/IP operational mode without any security features. It will simulate how the real world internet makes connections.
2. Firewall Mode: In this mode, firewall operations are simulated, and any MAC address can be banned/ blocked. In this mode, when Client with blocked MAC address tries to establish a connection, the packets are discarded and MAC based filtering is performed. If that machine is black listed, every packet from that machine is discarded.
3. Steganography Mode: For this mode, Steganography and cryptography are used to detect MAC and IP forging, and don't let the

SERVER buffer to overflow. Therefore the network is not populated with spoofed packets.

There is a secret KEY shared by both, the SERVER and the CLIENT, which is used to encrypt the scattered code and generate a cipher text.

4. Results

The suggested technique for TCP/IP three-way handshake functioned by using our custom test bench in various scenarios, for devices working together inside a single domain.

Following scenarios were tested:

1. Scenario2: Attacking Server in Normal situation to overflow the buffer of SERVER.
2. Scenario3: Attacking SERVER with Activated Firewall.
3. Scenario 4: Attacking SERVER's Firewall with MAC spoofing.
4. Scenario 5: Normal Handshake in Steganography Mode.

   Scenario 6: Attacking SERVER in Steganography Mode with IP Spoofing followed by MAC Spoofing.

Table 1. Results of the above scenarios

Spoofing Type	Security Mode	Buffer Status	Attack Status
IP Spoofing	Normal	Chocked	Success
IP Spoofing	Firewall	Normal	Fail
MAC Spoofing	Firewall	Chocked	Success
IP Spoofing	Steganography	Normal	Fail
MAC Spoofing	Steganography	Normal	Fail

5. Conclusions & Recommendations

Steganography is an old technique but with a new adoption which can provide inter-domain security in both the IP Spoofing as well as MAC spoofing**.** The information flowing in the network, if sniffed, is useless to the hacker, and may be very difficult for the cryptanalysis and steganalysis. The proposed technique is a proactive technique. Server is saved from DOS attack as it is not keeping any record of the client until a handshake is completed. The server would need a separate buffer for maintaining information about random numbers. It has low number of false positive detections. The encryption keys used should be protected from social engineering. Fast systems are recommended as the random number generation causes systems to slow down if complex techniques are used.

The study can be further extended by incorporating key distribution system which automatically sends the machines their keys for each communication. To apply Stress testing on the server, as the random number buffer can also overflow but this should not let the server down. The steganographic technique can also be used for defense against other types of attacks.

Corresponding Author:
Imranuddin.
Department of Computer Science,
Institute of Business & Management Sciences, University of Agriculture Peshawar, Khyber Pakhtunkhwa, Pakistan.
E-mail: imrandin@yahoo.com

References

1. Wikipedia, History of Internet. http:/www.wikipedia.org/wiki/history of internet. (2012)
2. Shipley G.1999, ISS Real Secure pushes past newer IDS player. Network Compute(May 17). http:/www.network computing.com/1023/1023f1.html. (1999)
3. Steven R., "Three way Handshake" Unix Network Programming Third Ed, (2004). Tanase M. "IP Spoofing, An Introduction" online: http://www.symantec.com/connect/articles/ip-spoofing-introduction(2003)
4. Sharma K. "IP Spoofing" Linux Gazette, 2001, Issue 63, http:/www.linuxgazette.com/issue63/sharma.html (2001)
5. Steven J. Templeton. Levitt K.E "Detecting spoofed packets" DARPA Information Survivability Conference and Exposition, 2003. Volume: 1, on page(s): 164- 175. (2003)
6. Wikipedia, What is Steganography. http://en.wikipedia.org/wiki/Steganography, (2012).
7. H S Manjunatha Reddy, K B Raja, 'High capacity and security steganography using discrete wavelet transform' International journal of computer science and security(IJCSS),volume 3, Issue 6,2009, page 462-472. (2009)
8. Ya-Ting Fan,"Intrusion Investigations with Data-hiding for Computer Log-file Forensics", Future Information Technology (FutureTech), Taiyuan, Taiwan, May 2010 pp 1-6
9. A.Joseph Raphael,V Sundaram,"Cryptography and Steganography : A Servey", Int. J. Comp.

Tech. Appl., June 2011,Vol 2 (3), 626-630 ISSN:2229-6093 (2011)
10. Gary C. Kessler,' An overview of Steganography for Computer Forensics Examiner', forensics Science communications, volume 6, July 2004. Number 3.(2004)
11. Jin C., Wang H., Shin K., "Hop-count filtering: an effective defense against spoofed DDoS traffic". In CCS 2003. Washigton: ACM Press, 30 – 41, ISBN:1-58113-738-9 (2003)
12. Moris T. R. "A Weakness in the 4.2 BSD UNIX TCP/IP Software",. AT&T Bell Labs. (1985)
13. Computer Emergency Response Team (CERT), "TCP SYN Flooding and IP Spoofing Attacks" CA-1996-21.html. http://www.cert.org/advisories/#1996. (1996)
14. Neslson E. H., and Mclean, P. M. "TCP/IP Spoofing Fundamental".: Proceedings, IEEE Phoenix Conference on Computers and Communications, (1996).
15. Park K and H.LEE "On the effectiveness of rout-based packet filtering for distributed Dos attack prevention in power-law internets" In SIGCOMM 2001. San Diego ACM Press 2001, 15-26.(2001)
16. Yuan L. F., Shieh S., "Defending against spoofed DDoS attacks with path fingerprint" (2005). National Chiao Tung University, Hsinchu 30010, Taiwan 28 March 2005, @ Science Direct. (2005)
17. Mircovic J., Jevtic, Reiher P. "Practical IP spoofing defense through route based filtering" Maximum Security third edition by SAMS publishers, chapter 4, page 50, 2001. (2001)
18. Dong Y., Choi C., Zhang Z. "LIPS: A lightweight permit system for packet source origin accountability" Computer Networks 50 (2006) 3622–3641 @Science Direct. (2006)
19. Craig A. Shue,Gupta M., Davy M. "Packet Forwarding with Source IP Verification". Computer Networks: The International Journal of Computer and Telecommunications Networking. Volume 52, Issue 8 doi>10.1016/j.comnet.2007.11.023 Pages 1567-1582 (2008)
20. Akram, S.; Zubair, I.; Islam, M.H.,"fully distributed dynamically configurable firewall to resist Dos attacks in manet", IEEE conference publication 2009,pp 547-549 DOI: 10.1109/NDT.2009.5272096 (2009)
21. Duan Z., Yuan X., Chandarshaker J. "Controlling IP spoofing through Inter-domain Packet Filtering" IEEE Transaction on Dependable and secure computing. Vol 5. No.1 2008. San Diego, Pages: 15 – 26, ISBN: 1-58113-411-8. (2008)
22. Zhenhai Duan; Xin Yuan; Chandrashekar, J.," Controlling IP Spoofing Through Inter Domain IP Filters", IEEE Transactions on Dependable and Secure Computing, Volume: 5, Issue: 1, DOI:10.1109/TDSC.2007.70224 , 2008, Pp 22 – 36 (2008)
23. Manusankar, C.; Karthik, S.; Rajendran, T., "Intrusion Detection system with packet Filtering for IP Spoofing", Communication and Computational Intelligence (INCOCCI), 2010,pp 563-567 (2010)
24. Gonzalez, J.M.; Anwar, M.; Joshi, J.B.D.,"A Trust based approach against IP Spoofing Attacks", In: PST 2011, Pp 63 – 70, DOI: 10.1109/PST.2011.5971965 , (2011)
25. Aluvala, S.; Rao, P.S.,"Constructing Inter Domain Packet Filters to Control IP Forging", ICECT 2011, Volume 5, Pp 292 – 295, DOI: 10.1109/ICECTECH.2011.5942005 (2011).

12/2/2013