Internet Protocol Spoofing in VOIP

N.Y Niluka Jayamali¹, M.G.C.M.Munasinghe², I.C Ariyawansha³, Y.A Kumarathilake⁴, W.S.N Gunathilaka⁵, R.D.G Perera⁶ & Dhishan Dhammearatchi⁷

Sri Lanka Institute of Information Technology Computing (pvt) Ltd

Abstract: The main intention of writing this paper is to enable the students, computer users and novice researchers about spoofing attacks. Spoofing means impersonating another person or computer, usually by providing false information (E-mail name, URL or IP address). Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods and types of spoofing: IP, ARP, E-Mail, Web, and DNS spoofing. Internet Protocol spoofing is a method of attacking a network in order to again unauthorized access. We would like to introduce and explain about IP spoofing attacks in this paper .There are no legal or constructive uses for implementing spoofing of any type. Some of the outcomes might be sport, theft, vindication or some other malicious goal. The magnitude of these attacks can be very severe; can cost us millions of dollars. This Paper describes about various spoofing types and gives a small view on detection and prevention of spoofing attacks.

Index Terms -Spoofing, Filtering, Attacks, Information, Trust

I.INTRODUCTION

Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods and types of spoofing. We would like to introduce : (a.)IP Spoofing, (b.)ARP Spoofing (c.), E-Mail Spoofing,(d.)Web Spoofing,(e.)DNS Spoofing

There are no legal or constructive uses for implementing spoofing of any type. Some of the outcomes might be sport, theft, vindication or some other malicious goal. The gravity of these attacks can be very severe, can cost us millions of dollars and should not be overlooked by the Internet security community. There are two types of spoofing attacks, (a.)IP spoofing attack (b.)URI spoofing attack

Internet Protocol spoofing is creation of IP packets with a forged source IP address. The purpose is identity of the sender or impersonating another PC. It also known as on-line camouflage. In this context an attacker gains unauthorized access to a network by making it showing that a malicious message is come from a trusted machine by “spoofing” the IP address of that network.

II.BACKGROUND AND RELATED WORKS

Voice over Internet Protocol (VoIP), there is an existing way of communication over any network. The Users can make the telephone calls over an IP network using this technology. This research paper will describe of security issues and concerns. There are two kinds of spoofing attacks are possible, IP spoofing attack, URI spoofing attack.

The business concerns will be those which are used to affect the Quality of Service (QoS). The network components call processors, gateways and two of the more common architectures are held by VoIP. Voice over Internet Protocol (VoIP) is a form of communication that allows end-user to make phone calls over a broadband internet connection. A special type of adapter is used in some VoIP services which required a computer and a dedicated VoIP telephone. Basically VoIP protocol has been adapted to voice networking. How do they express the Thesis This component they figure out, E.g. (a.)The communications network providers are used to adopt IP in their infrastructure, enterprises are adopting IP for private corporate networks. The communication between employees facilitate by using VoIP technique, whether working at corporate locations, working at home, or travelling. (b.)There are several enterprises which are used to test VoIP, doing a tryout, or engaging in incremental upgrades. The majority of multinational corporations use VoIP instead of remote possibility [1].

Two kinds of spoofing attacks are possible, IP spoofing attack and URI spoofing attack. IP spoofing attack is to forge IP source addresses in order to pretend a trusted user and IP spoofing is the intrinsic security problem in TCP/IP protocol suites and it is not in the scope of our study on VoIP security. URI spoofing attack is a particular case in malformed message attacks. The attacker who hijacked SIP messages between two UAs forges their URI field, so the attacker can hide himself from trackbacks. If spoofed BYE requests (BYE DoS attack) are sent to a victim, the call will be terminated by the attacker.
When considering VoIP service, you should not assume that its features, functionality and options will equal those of traditional landlines; you should be familiar with the requirements, availability and possible service limitations of VoIP service before switching to VoIP as either a primary means of communication or an enhancement to your current services. Threats / Risks: Many of the threats associated with VoIP are similar to the threats inherent to any internet application. Internet users are already familiar with the difficulties of email abuse in the form of spam. VoIP opens yet another pathway for these annoyances, which can lead to spam over internet telephony (SPIT), spoofing and identity theft. Because VoIP spam is unwanted, automatically dialed, pre-recorded phone calls using Voice over Internet Protocol (VoIP). It is similar to E-mail spam [2].

Distributed denial of service is a major threat to the availability of internet services. DDOS attacks are stealthy. The internet service provider finds it when the new technique propose a defense mechanism, stack identification and marking, which the previous approaches are allows the host being attacked, or its upstream ISP, to filter out attack packets and to detect spoofed source IP addresses, on a per-packet basis.

This work proposed Stickpin-Write ahead with a new packet marking scheme based on Pi, and new filtering mechanisms. Stack marking is the similar for TTL marking the packet’s TTL to aggregate the markings from different routers; each router instead treats the IP Identification field as though it were a stack. Write ahead marking All the router needs to do is substitute its own IP address for the last-hop IP address and the next-hop IP address for its IP address when calculating the bits to mark, they need not be repeated for each forwarded packet and also develop a new filter, the PiIP filter, which can be used to detect IP spoofing attacks with just a single attack packet. Stickpin filtering can thus defend against not only DDoS attacks, but also many IP spoofing attacks and multicast source spoofing attacks.

A packet is marked deterministically by routers along its path towards the destination. Packets traveling along the same path will have the same marking so that an attack victim need only identify the StackPi marks of attack packets to filter out all further attack packets with the same marking. In this scheme almost completely eliminates the effect of legacy routers in small quantities and performs 3-5 times better than the existing system. For the filtering mechanism, derive an optimal threshold strategy for filtering with the Path identification marking. Finally, evaluate the Stack path identification’s compatibility with IP Fragmentation, applicability in an IPv6 environment [3].

The wireless network is the self-configuring type of network. The wireless enable nodes can join or leave the network as they want. In this type of network many type of internal as well as external attacks are possible. When the source nodes want to transmit data to the destination nodes, shortest path will be established between them. The secure and shortest path between sender and receiver ensures the reliable data transmission. AODV is the reactive routing protocol which is used to establish the shortest path, on the basis of hop counts. But in the self-configuring type of network many malicious nodes may exits which are responsible for packet dropping.

Diffie-Helman is the algorithm which is used to set up the secure path between the sender and receiver before transmitting the data. In this paper, we propose the novel approach to prevent black hole and IP spoofing attack. In our work, a secure channel is established between sender and receiver for reliable data communications, it will prevent black hole attack. A random number is used with the IP address for the prevention of IP spoofing attack [4].

Spoofing attack is an identity based attack through which a malicious user can spoof the MAC address of a node to create multiple illegitimate identities that highly affect the performance of wireless sensor network. The identification of spoofers and localization of the same is a challenging task in wireless sensor network. This paper presents expository survey of various spoofing attack detection techniques in wireless sensor network [5].

Internet Protocol Spoofing is used to acquire illegal access to a computer. The attacker forwards packets to a computer with a source address representing that the packet is coming from a trusted port or system. Attackers must go through some complicated steps to accomplish the task [6]. They must: Obtain a target; obtain an IP address of trusted machine; Disable communication of the trusted machine we can take SYN flooding as a example for it; Sample a communication between the target and the trusted hosts; Guess the sequences number of the trusted machine; Modify the packet headers and it appear when the packets are coming from the trusted hosts; Authenticated service or port attempt connection to an address; The attacker will plant some kind of backdoor access for future references if it is successful.
Figure 1 illustrate system A impersonates system B by sending B’s address instead of its own. The reason for doing this is that systems attend to function within groups of other “trusted” systems. This trust is implemented in a one-to-one way; system A trusts system B. IP spoofing occurs in the following manner: if system A trusts system B and system C spoofs system B, then system C can gain otherwise reject access to system A. This is all made possible by means of IP address authentication, and poorly configured routers if the packets are coming from external sources. [7]

C never perceives the responses from A that is one of the major drawbacks with IP spoofing. This is completely blind attack, much experience and knowledge of what to expect from the target’s responses is needed to successfully carry out his attack. Immobilize source-routed packets and to disable all outside incoming packets with the same source address as a local host these are some of the most common ways to avoid this type of attack. [7]

Internet Protocol is used for sending of packets across the internet. IP header source and destination IP address filed. There are mainly used for forwarding of a packet to correct destination and for authentication. The source IP address in the header field is used for replying and providing authentication. To replace the actual source IP address with another IP address means spoofing the IP address. Usually trusted IP address. This packet on reaching the destination it checks for the source IP address. Even though it was sent by distrust party but since the IP address is seen to be a trusted one it accepts the packet. Below Fig. 2- shows the IP header fields along with the source IP address field where spoofing occurs mostly.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Address</td>
<td>192.168.30.4</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>192.168.31.2</td>
</tr>
</tbody>
</table>

192.168.31.2 it identifies that the packet is send from the trusted one. [8]

VoIP (Voice over IP) is a method and group of technologies which allow to send multimedia and voice communications over internet protocol networks (IP) such as the internet. The flexibility and low cost associated with VoIP networks have made it very popular among business as well as individuals. However, this popularity of the application of VoIP networks have attracted so many attackers. These attackers, try to gain unauthorized access to the communicated data and information via VoIP. They do this mainly to get financial gains or just for the fun of it. Some of these attacks are: (a) Session Initiation Protocol (SIP) flooding (b) Eavesdropping (c) Spoofing (d) Man in-the-middle [9]

These attackers are a major threat to the end-to-end security of data transmission through VoIP networks. It is believed that most of these attacks are caused by the weaknesses existing in the VoIP security, rather than the talent of the attacker. When IP networks are developed in relation to shared media communications, it exposes the network to security breaches. Before identifying the security issues in VoIP networks, the security components should be known. They are: (a) Security constraints (b) Security requirements (c) Security management [10]

Managing these three aspects of security properly would help to lessen the chances of networks getting attacked. Even the smallest vulnerabilities in any of these three security components would allow attackers to exploit the information transmitted through the VoIP network. Attacks may use a listening device (Ex; packet grabber) on the particular network to which he has access to the TCP/IP (Transmission Control Protocol) network in order listen to conversations of other people. Most vulnerabilities can be seen in data networks. VoIP uses platforms such as Linux and Windows operating systems. Those platforms already have a lot of platforms, therefore, this results in VoIP servers and network to be vulnerable to attacks as well. [11]

Some of the most common threats and vulnerabilities of VoIP networks are: (a) Registration attacks: This is the type of attack where the attacker injects himself to the signal path of the VoIP network through the network vulnerabilities. Some registration attacks are: IP spoofing, theft of service, reflection attack, and Brute force attack. (b)During a call attacks: This is where, when a person is making or receiving a call, the attacker intercepts the route where voice/data packages are sent. Some examples of this type of attacks are: call hijacking, eavesdropping, ARP spoofing (Porter, 2006), connection hijacking, signal protocol tampering. (a)Denial of service attacks: This

As an example for the IP spoofing take that an intruder whose IP address is 192.168.30.12 needs to send a packet to a website with IP address 192.168.30.4. Intruder knows an IP address which is a reliance one to 192.168.30.4 say 192.168.31.2 then 192.168.30.12 before sending the packet will swap IP header field in such a way that the source IP address now is 192.168.31.2 instead of 192.168.31.2. This receiver on seeing the source IP address
type of attack usually is not targeted to gain valuable information. The attacker isolated the network endpoint from the rest of the world by jamming the IP PBX and switches using many rogue requests. (b) Attacks on VoIP components: These attacks are targeted on devices and these attacks have effect on targeted devices easily. Some devices that get attacked are: IP PBX, soft phones and IP phones. Even though the attacks cannot be fully stopped, there are some measures that can be taken to prevent attacks from happening. They are listed below: (1) Using anti-virus and anti-spyware programs (2) Be careful about opening files attached to email messages or instant messages that cannot be trusted. (3) Verify the authenticity and security of downloaded files and new software. (4) Configure the web browser(s) securely. (5) Use a firewall. (6) Identify, back-up, and secure personal and financial data. (7) Use strong passwords only. (8) Patch and update application software. (9) Should not disclose personal information to people not known personally.

Early mobile communication service was developed for voice communication, but as the Internet in the wired environment advanced, demands for mobile service, which provides mobility based on mobile communication service, increased. Accordingly, data networks for providing data communication as well as voice service were added to mobile networks, and voice is processed as VoIP (Voice over Internet Protocol) in accordance with the All-IP communication paradigm. The importance of IP-based data networks is growing gradually. Availability as well as confidentiality are affected at the network layer predominately through spoofing IP addresses of network devices in order to intercept/redirect traffic. The used of malformed packet attacks are also common at the network layer. The IP phone net mask vulnerability is in many ways similar to the ARP cache issue an attacker can change address and mask of a router in order to redirected packets to a device of his choice. The two most common malformed packet attacks are the IP fragmentation or “jolt” attacks. In the IP fragmentation exploit, the attacker creates large packets that will be broken apart before they are sent to the recipient. During reassembly at the receiver an overlap in the data typically complicates the procedure. The results can vary from resource starvation to a system crash. Similarly, in the jolt exploit an attacker sends malformed IP packets to the IP processing stack. Again, the overlap in data results in a processing error or unstable state. [12][13][14].

IP Address Spoofing Attacks: (a) Blind spoofing- This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days. Using the spoofing to interfere with a connection (or creating one), that does not send packets along your cable. (b) Non-Blind spoofing- This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgment numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgment numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection. (c) Man in the Middle Attack- This is also called connection hijacking. In these attacks, a malicious party intercepts a legitimate communication between two hosts to controls the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge. If an attacker controls a gateway that is in the delivery route (d) Denial-Of-Service- conducting the attack, attackers spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic; it is very challenging to quickly block the traffic. IP spoofing is almost always used in denial of service attacks (DoS), in which attackers are concerned with consuming bandwidth and resources by flooding the target with as many packets as possible in a short amount of time.

IP spoofing in brief consists of several interim steps: (a) Selecting a target host (or victim). (b) The trust relationships are reviewed to identify a host that has a “trust” relationship with the target host. (c) The trusted host is then disabled and the target’s TCP sequence numbers are sampled (d) The trusted host is then impersonated, the sequence numbers forged (after being calculated) (e) A connection attempt is made to a service that only requires address-based authentication (no user id or password). (f) If a successful connection is made, the attacker executes a simple command to leave a backdoor.

Controlling IP Spoofing through Inter Domain Packet Filters they propose an inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework works correctly in that it does not discard packets with valid source addresses. Based on extensive simulation
studies, we show that even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers. There simulation results showed that, even with partial deployment on the Internet, IDPFs can significantly limit the spoofing capability of attackers. Moreover, they also help pinpoint the true origin of an attack packet to be within a small number of candidate networks, therefore, simplifying the reactive IP trace back process. [15]

III SOLUTION

Implement the IP encryption
Detecting changed IP packets
Detecting the IP headers
Hiding internal IPs and MAC addresses to the outside
Generate the log reports

Fig.3 virtual firewall

Fig.3 explain the solution for the research problem. Implementing a virtual firewall for avoid spoof attacks in a virtual firewall include: (a.) Implement the IP encryptions (b.)Detecting Changed IP Packets(c.)Detecting the IP Headers (d.)Hiding Internal IPs and Mac addresses to the outside networks’ (e.)Generate Log Reports. This are the main functions of virtual firewall for Identify IP spoofing attacks.

IV FUTURE WORKS

Research future implementation is developing virtual application on virtual server with above features: (a) Implement the IP encryption (b) Detecting changed IP packets (c) Detecting IP headers (d) Hiding internal IPs MAC address to the outside (e)Generate a log report

V CONCLUSION

IP Spoofing is a problem without an easy solution. It is inherent to the design of the TCP/IP network. Understanding how spoofing attacks are used, combined with a simple prevention methods and can help protect the network from a malicious cloaking and cracking techniques. Internet protocol is a network protocol operating at layer 3 network of the OSI model. Two kinds of spoofing attacks are possible, IP spoofing attack and URI spoofing attack. IP spoofing attack is to forge IP source addresses in order to pretend a trusted user and IP spoofing is the intrinsic security problem.

ACKNOWLEDGEMENT

We would like to express our deep and sincere sense of gratitude and indebtedness to our institution - Sri Lanka Institute of Information Technology (SLIIT). We are deeply indebted to our lecture Mr. Dhishan Dhammearatchi who helps us to simulating suggestions, knowledge, experiences and encouragement helped us in all the times of study and analysis of the research paper of this period. We are extremely thankful to our friends for their help and blessing which helped us directly and indirectly in this research paper.

REFERENCES


