INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

EFFECTIVE TWO-WAY AUTHENTICATION MECHANISM TO CONTROL IP SPOOFING USING IDPF

D.Srinath
Associate Professor / Department of Computer Science and Engineering
Panimalar Institute of Technology, India

ABSTRACT---In this developing world Internet is most important thing to be considered and there are many problems in this internet that has been solved and there are some problems which have to be solved. In the past years the consideration for security is very less and many people all over the world faced severe problem on man-in-the-middle attack, "MIME" and Distributed Denial of Service, "DDOS" especially for those who uses online banking. Every largest bank in the world faces this problem where there is a loss in customer confidence on online banking. The main purpose of MIME is to steal personal information and account information of the customer. DDOS plays vital role in denying the service in the Internet. Several mechanisms have been implemented to control these types of attacks. Attackers use IP spoofing, to make the target network to contain heavy burden in it and to make the attacking packet policed. In our paper, we construct an Inter Domain Packer Filters [IDPF] that can reduce IP Spoofing over the internet. The main aspect of our paper is to produce IDPF, with the available information in BGP, which is implemented network border routes and it does not requires Global Routing Information's. IDPF does not reject the packets with valid source addresses and they also help in finding the origin of the packet. More priority is given for the protection of customer information and to maintain trust relationship with the customer in banks and in any service related to finance. So this can be achieved my establishing 2-way Authentication.

KEYWORDS: *IP spoofing, DDoS, BGP, network-level security and protection, Routing*

I. INTRODUCTION

An intruder propels information to a system by IP address suggesting that the information is approaching from the faithful host. This mechanism is called IP spoofing because the intruder wants to gain the unofficial access from the computers. To employ as a hacker the intruder will develop many techniques to extract the trusted host address. After extracting the address, the hacker will change the packet header. So, that it looks like a message coming from the trusted host. It turns into risk for computer network community and the Internet. Then onwards, the Internet is undergoing from the quantity of huge scale attacks. In this attack, alternative of IP spoofing be utilize.

As a research done by the Internet sites and infrastructure,[1][7] DDOS attack is a serious threat. Frighteningly on large networks, DDOS attacks are observed. This will reduce the effect ness of the source-based packet filtering. The IP spoofing is exposed more in Internet. In an authentication system, from small space of possibilities human clients will prefer the low entropy passwords. For cryptographic secrets the protocols are designed to security but when using the passwords the protocols become insecure especially to on-line dictionary attacks[2]. To reduce these attacks, this research introduces the two server authentication mechanism where the password is spitted into three

and one part is maintained by the user and other two parts are maintained by the server and the hidden server. When user giving the password, the server will match the part of the password with its part and with the hidden server. When it matches, the user is an authenticated one. This is how the process works in the research.

1.1 MOTIVATION

The authenticated user and the server should not be cheated by the hacker who acts as an original server to the user and original user to the server. The threats should not attack the network, and so the user should feel safe when they transfer files to the network.

1.2 OUR CONTRIBUTION

In our system, we are using the IDPF (Inter Domain Packet Filters). The main idea of the IDPF (Inter Domain Packet Filtering) is finding the association among the topology and effects due to the route based filtering. The packet filters are constructed by the global routing. With the IDPF we are using the two server authentication for authenticating the user. The password will be divided into three parts where one part is maintained by the user and other two parts are maintained by the server. When user gives the password, it matches with the server's password and the user is authenticated.[3]

2. RELATED WORK

The Distributed Denial-of-Service (DDoS) attack is a serious threat for Internet usage. Attackers identify the sensitive communications between user and server and they send seemingly authentic e-mails asking user to verify their personal information. Intruders make use of this and have an access over the user data. By spoofing, users are associated to the attackers and lose his connectivity to the authenticated server which leads to non-privacy. To avoid this state, we propose a mechanism is called IDPF with two server authentication [4]. Two-way authentication also comes up short in shielding server and their users from Man-in-the-middle (MITM) attacks.

2.1 BORDER GATEWAY PROTOCOL

The main idea of the IDPF (Inter Domain Packet Filtering) is finding the association among the topology and effects due to the route based filtering. The packet filters are constructed by the global routing. The small number of ASes significantly limited the IP Spoofing. To construct the filters by using the local BGP updates are more effective. From the local BGP update we can make the effective filters.

2.2 PSEUDO RANDOM PASSWORD

The Hash function used here is one way. It can practice a letter to create a strong image known as a message digest. To find the integrity of the message this algorithm is used. If any changes occur in message with high probability, it will affect the results in the message digest. With a generation of random numbers this method is used to verify and generate message authentication codes and digital signature.

2.3 IP SPOOFING

Spoofing the IP address of a particular machine is the main purpose of this attack. By using IP spoofing the hackers can hide their hacking source in the attack. (Used in Denial of service) and maintain a good association with machines with hope. Here that we explain the Internet Protocol Spoofing.

3. BACKGROUND

In TCP/IP set that IP as unreliable network protocol and as well as connectionless. This is the two 32-bit title fields to grasp address message. To route packets in the region of the network is work of the IP's. This gives no device for accountability or reliability. Just the IP is hopes that create its intact and this will try to send the information. If this fails the packet is consider as lost packet but it will try to send a bug message that is ICMP message back to the foundation. That IP is not assurance release. IP does not maintain any connection state information because this is connectionless [5]. The information is easy to adjust the IP stack to let randomly select IP address into the basis fields makes IP susceptible to various attacks.

3.1 BGP AND AS INTERCONNECTIONS

Each node owns one or multiple network prefixes. Nodes exchange BGP route updates, which may be announcements or withdrawals, to learn of changes in reach ability to destination network prefixes. A route announcement contains a list of route attributes associated with the destination network prefix.

3.2 POLICIES AND ROUTE SELECTION

Each node only selects and propagates to neighbors a single best route to the destination, if any. Both the selection and the propagation of best routes are governed by locally defined routing policies. Two distinct sets of routing policies are typically employed by a node: import policies and export policies[7]. Neighbor-specific import policies are applied upon routes learned from neighbors, whereas neighbor-specific export policies.

3.3 RELATIONSHIPS AND ROUTING POLICIES

The specific routing policy that an AS internally employs is largely determined by economics: connections between ASs follow a few commercial relations. A pair of ASs can enter into one of the following arrangements:

- Provider to customer. In this arrangement, a customer AS pays the provider AS to carry its traffic. It is most common when the provider is much larger in size than the customer.[6]
- Peer to peer. In a mutual peering agreement, the Ass decides to carry traffic from each other (and their customers). Mutual peers do not carry transit traffic for each other.
- Sibling to sibling. In this arrangement, two ASs provide mutual transit service to each other. Each sibling AS can be regarded as the provider of the other AS.

4. METHODOLOGIES

In this system, three different types of prototypes are discussed; they are a SS (service server) which is the two server model for the public server, back-end server which is called as CS (Control server) and the peers. Here, peers can able to converse with service server (SS) and there is no need to know about Control Server(CS).To provide peer endorsement, a peer u is having password in which it is converted to clandestine of two big sum, both which will be detained through control system (CS) and service system(SS) correspondingly. When peer logins, based on the corresponding shares, control server (CS) and service server (SS) jointly authenticate the peers. A passive challenger manages the control server and an active challenger manages the service server corresponding to malicious attacks of offline dictionary to peer secrets, since there is no collision (Alternatively, SS is associated).

4.1 TWO SERVER WITH SECRET SAFETY EVALUATION

The double system secret verification system measures the total amount of exponentiations at the same time as evaluation measure, exponentiations lead single person evaluation fixed cost.

The integer next "/" indicate amount of exponentiations that can be computed offline and the integer before "/" indicate the full amount that exponentiations make by every party. Single-path message transfer is one in circles. Two sets of rules and regulation measures are reasonably provident in way of information transfer to all with the evaluation.

The table 1.1 planned under show the calculation presentation in conditions of success rate and time between single server authentication and the two server password authentication. Solitary system secret verification mechanism and Evaluation calibration through double server is done.

Password Security Scheme	Time of Authenticity (MilliSecond)	Success Rate (Percentage)
Two Server	10	97
Single Server	8	86

Table 1.1 Solitary system secret verification mechanism and Evaluation calibration through double server

4.2 MOTIVATION IDPF

Every node should contain the best of source node and destination node even though the route-based packet filtering is true. At present, as inter-domain packet routing protocol, the BGP will be used by the Internet architecture and there is gathering of data. The local resolution in BGP is the route assortment which is other wise known as the superior source node and destination node is computed by the source‘s’ based on the routing table routes and the favorite of AS contains the source‘s’. For the nodes in the superior source and destination nodes the information will not obtainable.

5. IDPF WITH BGP

Through the consideration, we can modify the process of the presentation of IDPF with the updates of BGP and the points of non-overlapping. Then the following section we can point-out the process of collation of the other limits like the exact information route and also the points of overlapping.

5.1 SECURITY CONCERNS IN BGP

The main aim of BGP network was mention as the process like the surrounding of the previous network can treated equally and the homogeneous as moderately. The basic describe distance of the vector comparison is a large process of the casual model that can associated with the propagation of information to produce the correct and reliable result. The network is like a rumor network. There are some demerits in the BGP[8]

- The process of secure honesty, source genuineness and the new innovation of BGP message cannot have any mechanism, which are the first demerits.
- Then BGP cannot provide any type of device for the verification and the authentication of address and the starting point of AS in the routing system.
- At last the protocol cannot provide any way to assure the given BGP message can be quality and right.

5.2 STRENGTHENING PASSWORDS

The password is a reusable, understandable, low entropy protocol PIN and it has techniques like challenge response which is based on the hash concept which is found in the weaker protocols. The server-side SSL - authenticated connection is the better approach for sending a password and password hash. The approach was realized and started from the benefits of zero-knowledge there will be a exchange of encrypted key. To provide an authentication procedure in which the password should not be known to other parties. This research line will be in several instructions continued and in the client-server protocols; there will be a momentous improvement.

5.3 MULTIPLE SERVER USE

The server password protocols are proposed from many zero-knowledge. A basic username-password authentication is provided by the Multi-server protocols which has collection of servers which does not have

particular hardware or key storage in client side. The threshold number of servers which is not corrupted, there will no improvement in the naive guessing strategy by an attacker even in the for low-entropy passwords.

5.4 PROVABLE SECURITY

The cryptographic scheme the protocol is valuable, where it is the provable security analysis, is realized. Tools are provided by the secure multi-party manipulation and threshold cryptography results where the protocols are paying attention is included in the complexity theoretic foundations is the security proof techniques are used.

The asymptotic security definitions and security proofs are presented by the framework. A concreted security analysis is required for deployment of the protocol.

6. IDPF WITH TWO SERVER AUTHENTICATION

The process can simply tell us the connection establishes between the source and the destination, for all the available node and the node which is selected and analyzed for the path selection process, the neighbor node of the select node can also process. The both selection and the analysis process are done by defined local route policies. In our proposals we are using IDPF, to control the IP spoofing and non privacy of user, while establishing the connection between authenticated server and the user.[9]

- Global routing information is not required to IDPF architecture which can also mitigate the level of IP spoofing.
- Inter domain packet filter are constructed from the data in BGP (Border Gateway Protocol) route modernize and then organize in the network border routers.
- During the selection of best route, first it finds the feasible upstream nodes. Two-way authentication also comes up short in shielding server and their users from Man-in-the-middle (MITM) attacks.
- In 2-way authentication method, the server creates a hidden server itself. The server randomly generates a secret key and splits the key into three parts and shares the key with user and hidden server.
- Limits the spoofing capability of attackers

7. COMPARISON OF EXISTING WITH PROPOSED PROTOCOL

7.1 EXISITNG PROTOCOL

Initially, from the legitimate traffic harder an isolating attack is made from the IP spoofing. Packets will be appearing like it is from the source address in the Internet by spoofing. By using Border Gateway Protocol (BGP) each AS can communicate with its neighbors. Some locally defined routing policies will guide the AS for best route from source to its destination selection and propagated by the BGP where it is a policy-based routing protocol.

DISADVANTAGE

Knowledge of global routing information is required for route based packet filter which is hard to merge in the current Internet routing infrastructure is considered to be the most challengeable thing.

7.2 PROPOSED PROTOCOL

Inter Domain Packet Filter (IDPF) is given as a result of route-based packet filters. Based on the BGP updates this filter is constructed.

ADVANTAGE

1. IP spoofing is avoided.
2. Secure Communication.
3. Attacker's ability for spoofing packets will be limited.

Here the information cannot be retrieved easily by the intruders because the system is based on the frond end server and the control hidden server. For increasing the system security, even the authorized persons also get through this security features for accessing the system. The intruders will access both the servers for extracting the password is called single point of vulnerability will also be eliminated. Due to these features, when comparing to

other systems, this two server authentication is a secured way. Thus the table 2 gives a comparative result with various protocols.

VALUES/PROTOCOLS	BGP updates	IDPF
Security Level	Low	High
Throughput	Medium	High
Route Selection	Long route	Short Route

Table 2 Comparison of Values with existing protocols

8. IMPLEMENTATION AND VALIDATION

This section discusses other design issues and implementation details of proposed novel based Technique for the IP spoofing with two server authentication. It also discusses the implementation of this technique in java with a performance in comparison to the proposed technique.Fig1 gives the Performance Graph of the existing methodology with the proposed two server mechanism.

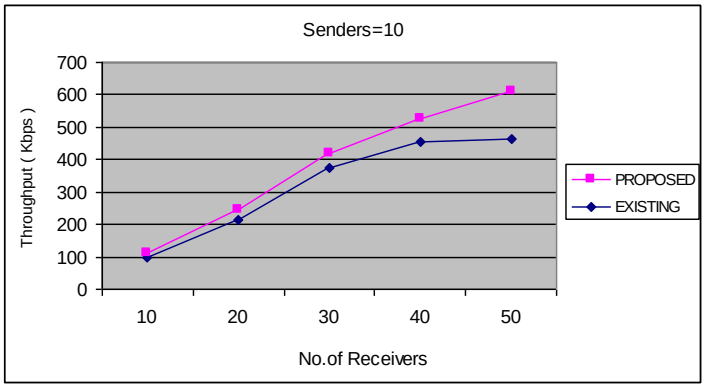

Fig 1 Performance Graph of the existing & proposed two server mechanism

9. CONCLUSION

In this research, we proposed a password-based authentication and key exchange system that is built upon a novel two-server model, where it consist of two server, one will be hidden and the other server which is visible to the user to communicate. In the DDOS attack where the IP address can be changed by the hacker and the request is send to the system and reply to hacker.

Here, we defined the two server authentication user gives the one third of the password; the server will match it with its own password and the hidden server password. If all password matches, the server allows the user. Otherwise, it won't allow the user to access. Our system has more advantages than the current available solution, which includes avoidance of PKI, high efficiency and elimination of a single point of vulnerability. In the difference obtainable multi server password systems and that system has huge possible for sensible request. This will directly apply to secure accessible standard individual-server password request, for example Web applications and FTP. This is using in the associate enterprise location there is an only one control server backup which will support many service servers.

The safety system essential our planned protocols presume that to manage server may only be prohibited with a passive adversary. Because we contain maintain, this supposition is fairly logical in view of the positioning in this model, and the applications of the form to associate enterprises.

10. REFERENCES

[1] FengQiaojuan and Wei Xinhong "A new research on DoS/DDoS security detection model" IEEE International conference on Computer Engineering and Technology, Vol.3, 2010.
[2] Bin Wang "The research of BGP convergence time" IEEE joint international conference on Information Technology and Artificial Intelligence,Vol.2,Pp.354-357.
[3] Lu Xuanmin; Shan Chang and Moses "Research on IP Address Replacement Technology Based on Iptables" IEEE international conference on Wireless Communications, Networking and Mobile Computing, Pp.1-3,2011.
[4] Yong Wang,Dawu Gu,Junrong and XiuXia Tian "Research on Multi-dimensional Cellular Automation Pseudorandom Generator of LFSR Architecture" IEEE International Symposium on Information Engineering and Electronic Commerce,Pp.11-15, 2009
[5] Velmayil and Pannirselvam "Detection and Removal of IP Spoofing Through Extended-Inter Domain Packet Filter Architecture" International Journal of Computer Applications ,Vol. 49,No.17,Pp.37- 43 , 2012
[6] Bremler-Barr and Levy, "Spoofing prevention method" IEEE International Conference on wireless networks, March 2005

[7] Srinath.D and Janet.J "A Survey of Routing Instability with IP Spoofing on the Internet "Asian Journal of Information Technology, Vol.9, No.3, Pp.154-158, 2010.

[8] Ramesh Babu, Lalitha and Sathyanarayana "A Comprehensive Analysis of Spoofing" International Journal of Advanced Computer Science and Applications, Vol. 1, No.6, 2010

[9] Sharmin.R and Subhra Prosun P, "Proposed Methods of IP Spoofing Detection & Prevention" International Journal of Science and Research, Volume 2 Issue 8, August 2013