IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 27-32
www.iosrjournals.org

A Secure Cryptographic Puzzle based Approach Ensuring Total Security for transmitted Information with IP Tracing

Sruthy R.S.
(Dept. of Computer Science and Engineering, Mahatma Gandhi University, Kerala, India)

***Abstract*:** *Today internet is extremely affected by several attacks such as Denial-of-Service attacks. The source IP address in a packet can be falsified. Thus IP Protocol fails to determine the originator. The attacker performs IP Spoofing and creates attacks. Thus for determining the real source of the attacker several IP Traceback schemes come forward. The available schemes have their own advantages and disadvantages. Computational Complexity is considered as common drawback. With the aim of overcoming the drawback an IP Traceback Digital Signature Algorithm is used for ensuring security for the transmitted data using Socket communication As all the available methodologies for IP Traceback, the current approach also focuses only on tracing attacker. With the aim of ensuring a Total security, a Cryptographic puzzle based scheme is also incorporated along with the new approach for preventing Hackers. Here certain puzzles are also used for encrypting the message along with the available methodology. Here the opponent cannot solve the puzzle until the encrypted packet reaches the destination. . The scheme is implemented based on a share market based application. The security of the scheme is also analyzed.*

***Keywords*:** *Cryptographic puzzle hiding scheme, Denial-of-Service (DoS) attacks, Digital Signature Algorithm (DSA) , IP Traceback , IP Spoofing.*

I. Introduction

As the internet grows at a widespread, several security issues also emerge. The malicious attackers and hackers can create serious damages on network. Normally the network traffic may include the source information. An Internet Protocol (IP) provides a header field for all packets which includes a source IP address to identify the origin of packet. The lack of security in TCP/IP specification may lead to IP Spoofing. Due to the datagram technique available in IP Protocol the attackers can spoof the source IP address and remain anonymous during the attack. Here the attacker may fake the source IP address with another IP address, thereby misleading the server. One IP Spoofing attack is a Denial-of-Service (DoS) attack. It is an attempt to make a computer or network unavailable for its intended users. The attack mainly floods up network with useless traffic. Ideally the attackers play their role by spoofing the server IP address; thereby a normal network connection may be prevented. The need for the identification of real source of attacks becomes a major target in this situation. Several IP Traceback schemes [1] come forward with the aim of tracing the source of attacker's the first step their came an Ingress filtering approach [2] configures routers to block the packets with a fake source IP address. The scheme requires a powerful router to check the source IP address and also a better ability to differentiate between the fake and original IP address. For the scheme both the network and router overhead is high. Burch and Cheswick propose a Link testing scheme [3]. The scheme starts at the router near the victim and test the incoming links until the attacker traffic is obtained. The method works based on the assumption that the attacker remains active until the tracing get completed. The scheme is ineffective for tracing an ongoing approach. As the next step a Packet logging, logs packet at the key routers and uses data mining techniques to determine the path by the packet traversed. An advantage with this scheme is that it can trace an attack long after the attack has completed. Here the complexity increases as there is a need for huge resources.

Packet marking [4] is yet another approach, where the trace details are inserted in to the packets and marked in to the upcoming routers in the path. The scheme works with a packet marking algorithm. The approach is a bit insecure if there occurs a false marking. Packet marking and Logging schemes can be used as a combined approach to overcome the problem of false marking by using marking and logging algorithm. Here security is ensured for the data by logging the trace data into a hash table, but the scheme is a bit complex and the scheme seems insecure if the architecture of the network get changed. Available traceback schemes have their own advantages and disadvantages, but they are analyzed by considering complexity as the parameter. A new approach is introduced which ensures security for the transmitted data with Digital Signature Algorithm. Here the trace data from source to destination is marked into the upcoming routers and to avoid false marking, the trace data is encrypted with digital signatures. A client server communication is enabled and a socket communication is used to establish a connection between the communicating parties. The scheme proceeds with the assumption that the agents with registered MAC is participating in the communication. For the new scheme

the problem of computational complexity is resolved. All the available traceback schemes including the new approach only focuses on tracing the IP of attacker.

For these reasons, a cryptographic puzzle based scheme is used as an additional security feature for preventing hackers along with the attacker and thereby a total security is ensured for the transmitted data. Here certain puzzles are used with the key for encryption. Here the recipient must solve certain puzzles to determine the secret of communication. The highlight is that the puzzle is only known to the client and server. The puzzle solving depends on the power of the solver. The scheme is being implemented at real time. The whole scenario offers 1) complete security from the malicious attacker and hacker 2) computational complexity can be reduced.

The rest of the paper is organized as section II .Related work, section III deals with the proposed scheme, section IV deals with the security analysis of the scheme. Conclusion and reference in rest of the sections.

II. Related Work

IP traceback is the name given to any method for reliably determining the origin of packets in the internet. Several traceback schemes come forward with the aim of tracing the source of attacker with certain protection measures. Existing IP traceback schemes can be categorized into single packet [5], packet logging [5] and packet marking[5]. In packet logging the digest of the packet is stored in the routers, the method can trace single packet and considered efficient. SPIE[5] is proposed with the idea of packet logging, which has the ability to trace even a single packet is stored with bloom filters, thereby space efficiency can be improved. Packet marking[6][7][8] is a method that write the identification information into packet heading. Here the overhead arises due to the lack of sufficient storage space in the header field. Flexible deterministic packet marking is one such concept connected with packet marking, here the marking field do not consume much space, thereby excess bandwidth and excess network overload can be reduced.

Packet marking provides transparency and packet logging needs storage requirement for storing packet details and has sufficient ability to trace a single packet. Taking advantage of both the approach lead to yet another scenario, which solve the storage problem. As the first step, Kihong Park and Heejo Lee [6][7][8] proposed a technique called Probabilistic based packet logging and packet marking for DoS attacks. Here in the method, the attackers in the network are analyzed and tracks spoofed packets, thereby DoS attacks can be minimized. Here every packets are spoofed and the probability of each packet is detected and packet cannot be tracebacked. Here the chances of attacks can be minimized. So while considering the combined scenario the need for a new approach is sufficient. Gong and Sarac [8] proposed a Hybrid IP Traceback (HIT) approach, shown in Fig 1. The scheme works by first of all creating a homogenous or heterogeneous network. In HIT the packet trace details are marked at every upcoming routers deterministically and logs at the router alternatively and the router information is mapped into a hash table. The inter-logging distance between routers are designed by a carefully designed marking approach.

HIT works as follows, First of all create a homogenous or heterogeneous network. Then Apply pre shared key exchange between the router and the sender using: Here certain Assumptions are followed that is Sender node has already registered with the router and got the pre-shared key. Process: 1) Sender node sends a request to egress for sending data packets to destination node using the function sendPacket (req). 2) Egress Router now will send challenge response acknowledgement to sender node chaAck (). 3) Now Sender node will send the new packet encrypted with pre-shared key to the ingress router. This packet need to be a tcp/syn packet making sure that further authentication of packets is not required in that session for the same node. sendPacketv (TCP/SYN(msg)). 4) Now egress router will use the compare (Hcs,Hcr). Where Hcs is the sender msg and Hcr is the message created by ingress router. 5).If comparisons are true then call the function forward (msg) to forward the packets else reject (req) , reject the request. As the final step apply the following algorithm for the packet marking as shown: IR (Marking Info. Of _Attack Packets).

For Pass I 1) for each subset of routers that marked certain packet (P). a) if (P end-list router is not in the table) i) add new entry for P end-list router ii) add P remaining routers to the predecessor list of P end-list router b) else add P remaining routers to the predecessor list of P end-list router **Pass II** 1) for each end-list router E Rx in the table a) if (E Rx appears in the predecessor list of any other end-list router E Ry) i) append predecessor list of E Rx _ to the Predecessor list of ERy. Ii) Remove ERx and its predecessor list from the table. The scheme is an efficient technique for trace backing the source IP address. But the technique cannot be used if the network architecture changes and also cannot gather sufficient information from the packets. Here there will be marking and logging issues and also by considering computational complexity and network overhead as an issue, a new concept is introduced and the proposed work is somewhat related to but different from the previous works The proposed scheme is an IP traceback scheme based on MAC address verification, here Digital Signature Algorithm is used to ensure security for the transmitted data. The transmitted information is marked in the upcoming routers and the digital signature provides security for the transmitted data. For the new approach the

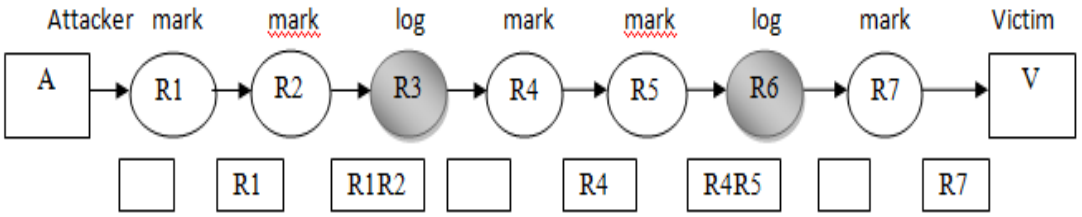

Fig. 1. Hybrid single-packet IP traceback. In this example, the marking field of packet can accommodate the identification information of two routers. Routers *R*3 and *R*6 log the packet, the other routers mark the packet

computational complexity is not a matter and has real time significance. The connection between the communicating parties is through socket communication.The scheme ensures fewer networks overhead and can be deployed in any network architecture. As compared to all the available traceback schemes, the new approach also works with the aim of tracing the attacker. As an additional feature, a better security from a malicious hacker is also a sufficient need for attaining a total security in secret transactions. A hacker is a person who enters the computer or network to view files or attain knowledge. He just want to know exactly how things works or how things can be done. They don't want to cause any harm, but rather explore, experiment and gain knowledge. An attacker is someone who wants to exactly attack a computer or cause harm. An attacker will view the data and can cause serious damage to the computers as well as personal profiles in the internet.

Several packet hiding schemes come forward with the aim of preventing the hackers. One such approach is the usage of cryptographic puzzles. Rivest et.al. put forward the use of cryptographic puzzles, which are used to enable "future decryption". Here encrypting a message so that decryption is possible only after a particular amount of time[9].The idea is termed as Time-Release Cryptography (TRC) and an alternative way connected with the approach is the usage of third party server [9]. Here the puzzles are termed as Time-lock-puzzles and the properties are:

- Puzzle solving is intrinsically sequential process
- The puzzle generator must have a short-cut way to find solutions.

The application involve e-Voting. Furthermore TRC approach doesn't provide confidentiality; here any one can get the message after solving the puzzles. So achieving confidentiality and delayed decryption is very essential in every application. Another interesting approach is encapsulated key-escrow technique [9] where both the confidentiality and delayed decryption are essential, but the puzzles need not be parallelizable. Also Internet Service Providers (ISP) may need to escrow (session) keys of its customers to the government agencies. Puzzles are used to prevent the agencies from involving in massive wire-tapping. The current approaches against hackers are not treated in a formal way.

A much formal and thorough approach is necessary in this situation. A new cryptographic puzzle-based hiding scheme is proposed. The main aim of puzzles is to force the recipient of puzzles to execute certain predefined computations to attain certain secrets in communications. The time required for solving the puzzles depend on the computational ability of the solver and the hardness of puzzles. The advantage of the scheme is that the security of the scheme doesn't depend on any parameters. Here the cryptographic puzzles are used to hide the data from the hackers. Here the puzzles are only known to the senders ad receivers. A cryptographic puzzle hiding algorithm is used in this context. The proposed scheme serve as an additional security for the transmitted information send.

III. Proposed Scheme

IP traceback based on DSA algorithm is less complex approach in tracing the source IP of a packet, here the secrecy in the transmitted data is achieved using Digital Signature Algorithm (DSA), the encrypted data transferred from client to server is marked at the upcoming routers in the path., the router interface information is then logged into the table. Thereby on retrieving the information from the table the tracepath can be reconstructed to analyze the source IP. The approach proceeds with the assumption that the participants with a registered MAC address is participating in the transactions. On considering certain parameters such as network overhead, router over head, computational complexity and timing problems, the current approach seems to be considerably a better one as compared with the existing IP trace back approaches. In the current approach to ensure the security of the data Digital Signature Algorithm (DSA) algorithms are used. A Digital Signature is a construct which helps achieve non-repudiation of Origin (ie. Origin Integrity) of data. By digitally signing the document, the person who signs it assures that he is the author of the document or the message that was signed.

Two main Security considerations should be taken into account when implementing Digital Signatures i) Sign the message and then encrypt the signed message ii) Sign the Hash of the message instead of the entire message. Here the whole scheme is done based on a socket communication between the client and server. In socket communications a socket is created at the client and server side and further communications are by writing to and reading from the socket. The scheme retains the confidentiality of data. A secure data transfer is ensured in the current IP traceback scheme. To provide security for the transmitted data, the algorithm works as follows:

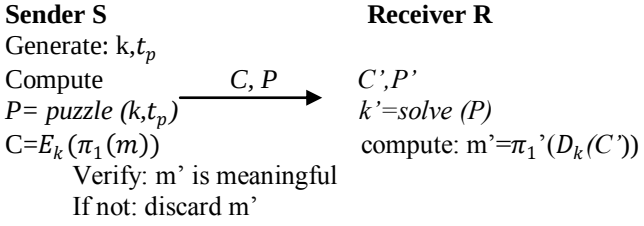

Fig. 2. Cryptographic puzzle-based hiding scheme

Example if two parties namely Ram and Renu wishes to transfer a confidential meaasge $m. If Ram has agreed to transfer $m to Renu, then there had to be a way for Renu to be sure that: i) It was Ram who performed the transaction and not someone else impersonating Ram (Authentication) ii) The amount agreed by Ram is $m (Integrity) iii) Ram could not dispute his statement of transacting $m to Renu (Non-Repudiation of Origin) These concerns were addressed with a solution known as Digital Signatures. With the above considerations, the algorithm below can be used for implementing public key cryptography in Java.

- Encrypt the message using a symmetric key.
- Concatenate the symmetric key + Hash of symmetric key + Hash of message.
- Encrypt the concatenated string using the receiver's public key.
- Sign the data to be transmitted (Encrypted symmetric key + Hash of the key + Hash of message).
- Validate the Signature.
- Decrypt the message using Receiver private key to get the symmetric key.
- Validate the integrity of the key using the Hash of the key.
- Decrypt the actual message using the symmetric key which has been decrypted and parsed and checked for integrity.
- Compute MessageDigest of data.
- Validate if the Message Digest of the decrypted text matches the Message Digest of the Original Message.

To attain a total security for the transaction the existing scenario is incorporated by a cryptographic puzzle hiding scheme. The new approach offers confidentiality for the transmitted data. Certain puzzles are used at both the client and server side. At the client side the puzzles are binded with the key thereby encryption process is established; Here the recipient of the message must solve the puzzle to retain the secrecy in the transmission. The time required for solving the puzzle depends on the computing ability of the receiver [9]. Here in this approach the security doesn't rely on any physical layer parameters Cryptographic puzzles are used to temporary hide the transmitted data. A packet m is transmitted to the receiver. Here the packet is encrypted using a randomly selected key of size s The key k is binded using a puzzle. The opponent cannot solve the puzzle until the encrypted version of message m reaches the destination Shown in Fig.2.Here the sender has a packet named m for transmission. The sender selects a random key k $\in \{0,1\}^s$, of a particular length s. S generates a puzzle named $P= puzzle\ (k,t_p)$, where *puzzle()* denotes a puzzle generator function and t_p denotes the time for solving the puzzle. t_p is measured in terms of time. After generating the puzzle P, the sender broadcast (C,P), where C = $E_k(\pi_1(m))$. At the receiver end any receiver R solves the received puzzle P' to recover key k' and then calculates m'=$\pi_1'(D_k(C'))$. If the decrypted packet m' is meaningful, the receiver accepts m=m', otherwise discards m'.

Cryptographic puzzles are certain primitives for establishing a secure communication. It's a better way to hide the transmitted packets from the hackers. Cryptographic puzzles have good computational efficiency. Client puzzles[10] use one-way hash function with partially disclosed inputs to force puzzle solvers search through a space of a precisely controlled size. Here in the work the sender selects a random key k with k =k_1 ‖ k_2., the corresponding length of k_1 and k_2 are s_1 *and* s_2. Then computes C=$E_k(\pi_1(m))$ and transfer (C, $k_1, h(k)$). To obtain k any recipient needs to calculate on average 2^{n_2} hash operations. Thus the puzzles cannot be solved until the encrypted version of m reaches the destination.

Table 1: Qualitative Comparison of Existing Schemes

Schemes	Management overhead	Network overhead	Router overhead	Distributed capability	Post-mortem capability	Preventive/ reactive
Ingress Filtering	Moderate	Low	Moderate	N/A	N/A	Preventive
Link Testing *Input debugging* *Control flooding*	High Low	Low High	High Low	Good Poor	N/A N/A	Reactive Reactive
ICMP traceback	Low	Low	Low	Good	Excellent	Reactive
Logging	High	Low	High	Excellent	Excellent	Reactive
Marking	Low	Low	Low	Good	Excellent	Reactive
Proposed scheme	Low	Low	Low	Excellent	Excellent	Reactive

IV. Security Analysis

Current IP traceback scheme is analyzed and compared in accordance with the available traceback schemes. Several methods come forward to reduce the damages caused by IP spoofing. Table 1. Provides a subjective comparison of these methods in terms of management overhead, network load, router overhead, and ability to trace multiple attacks, ability to trace an attack at the completion stage and also on whether they are preventive or reactive. The proposed scheme is also characterized with the same criteria mentioned above. An additional feature in accordance with the proposed IP traceback namely cryptographic puzzle hiding scheme to trace a hacker is also analyzed in this section.The security of the scheme is analyzed at different stages of execution. An opponent may try to classify message m after the successful completion of P. The task is being performed by crypt analyzing cipher text C=$E_k(\pi_1(m))$.

The selection of the key of sufficient length is enough to solve these cipher text only attacks. In this approach the security of the transmission rely on the puzzles, which are blinded with the key. After the transmission of P, there will be chances for the opponent to recover the key used in transaction. Here security is offered by the notion that, for every puzzle P, a time period is already assigned in such a way that none of the opponents can never tract the key, unless every bit of puzzles reaches the destination, thus security is offered. The cryptographic puzzles never depend on any physical layer parameters. is also applicable to the wireless systems.

V. Conclusion and Future Work

Several IP traceback schemes are surveyed and by taking several parameters in to consideration, a comparatively new and less complex scheme is introduced for IP traceback, incorporating Digital Signature Algorithm to ensure security from attackers and as an additional security feature, a cryptographic puzzle hiding scheme is also included, thereby a total protection from both the attackers and hackers can be obtained. The whole scenario is being implemented in a share market based application, where security is offered for share details. All the proposed IP traceback methods have their own advantages and disadvantages. Currently no single solution is not available for fulfilling the need for an effective trace back. The proposed method is based on an application and as a future enhancement; the total security measure should be enhanced for a wide range of application in the real internet. All the Traceback schemes including the commercially available products are only implemented in commercial basis, so as a future enhancement; there should be a new scheme where the whole IP trace back approach can be implemented throughout the real internet.

References

[1]. S.C. Lee and C. Shields, "Tracing the Source of Network Attack: A Technical, Legal and Societal Problem," Proc. 2001 IEEE Workshop on Information Assurance and Security, IEEE Press, 2001, pp. 239–246.

[2]. P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," Internet Eng. Task Force RFC 2827, May 2000.

[3]. H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. of USENIX Systems Administration Conference, (New Orleans, LA, USA), December 2000.

[4]. Stefan Savage and David Wetherall, "Network Support for IP Traceback" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.9, NO.3, JUNE 2001.

[5]. Ming-Hour Yang and Ming-Chien Yang,"RIHT:A Novel Hybrid IP Traceback Scheme",IEEE Transaction on Forensic,VOL.7.NO.2,APRIL 2012.

[6]. Chao Gong and Kamil Sarac,student member,"A More Practical Approch for Single-Packet IP Traceback using Packet Logging and packet Marking"

[7]. Dong Yan, Yulong Wang, Sen Su And Fangchun Yang "A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging", Journal Of Information Science And Engineering 28, pp. 453-470 , 2012.

[8]. C. Gong and K. Sarac, "IP traceback based on packet marking and logging," in Proc. of IEEE ICC, (Seoul, Korea), May 2005.

[9]. R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedreleasecrypto. Massachusetts Institute of Technology, 1996.

[10]. A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks,"Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999.