IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 1, Issue 1 (May.-Jun 2014), PP 08-14
www.iosrjournals.org

A survey on Stack Path Identification and Encryption Adopted as Spoofing Defense Mechanism to Assist in the Adoption of Electronic Payment Systems

Anne Kaluvu[1], Dr. Wilson Cheruiyot[2], Dr. Joseph Wafula[3]
[1,2,3]*School of computing, Jomo Kenyatta University of Agriculture and Technology, Kenya*

***Abstract**: Spoofing attacks are a constant nag in the information world, so many methodologies have been invented to reduce on its effects but still there is a lot left to be desired. The kind of impact that this attacks have on Electronic Payment Systems is so detrimental to the economic world given that this systems are viewed as performance enhancers on payments. This study elaborates two methodologies a combination of StackPi and Encryption as spoofing defense methodologies. Billions of shillings are lost in this rollercoaster thus giving rise to a situation that deserves undivided attention and should be researched on. A profound argument on the methodologies that have been used in this mission to eradicate spoofing attacks, the limitations that they posses and other methodologies that have been brought in play to succeed them elicits an interesting he strategy of integrating or combining methodologies and the benefits that this strategy contributes to curbing spoofing attacks. With that knowledge underhand, it can be justified why the combination of Stack Pi and Encryption is a recommended solution against spoofing attacks.*

***Keywords:** Electronic Payment Systems, Encryption, Security, Spoofing attacks, Stack Pi*

I. Introduction

The world has changed with the advent of internet and its use has created a revolution in almost all spheres of life. We are heavily dependent upon web based services for even transactions and nobody is complaining as it offers a world of convenience to the payment process.

Since then, e-commerce has been transformed by the emergence of the electronic payment system (EPS), which is rapidly shaping the way business is conducted in the digital world. Bruce (2012), a payment for buying and selling goods or services offered through the internet. According to Hezlin et al. (2011), most e-commerce transactions involve the buying and selling of goods and services and payment for these goods and services. Because traditional payment methods cannot be effectively be used to complete an electronic transaction, EPS has emerged as an attractive alternative because of its features such as security, simplicity, convenience, reliability, privacy, and anonymity.

Consumers have generally been willing to adopt new electronic payment systems because they have confidence in the financial system in general and in electronic operations in particular. The process has though been a silent revolution because these extensive changes have occurred slowly and not necessarily in ways that are obvious. The traditional, trusted and convenient means of effecting payments still have a strong attraction to consumers, who therefore change their economic behavior slowly because of their emotional relationship to money and the payment mechanisms they trust. (Thomas *et al*., 2004)

Although this has been the case the adoption proceedings have been impressive but not satisfactory as there have been a few issues when it comes to entrusting ones financial and personal information that is needed for the implementation of these systems without having doubts of its breach or misuse in the future.

This has created a forum that wants to look into this issue and thus the importance of this survey is to into the aspect of security viewing what its effects are when it comes to adoption of EPS systems. It will give an overview of what forms of security issues are in EPS systems, focusing on spoofing attacks and what forms of solutions can be captured to help curb this issue and in particular it will focus on a combination of Stack PI and Encryption as the main methodologies.

II. Methods

A meta-analysis of seven methodologies that have been used in spoofing attacks is critical for comprehension of general nature of spoofing attacks and the efficiencies of the methodologies employed under the given circumstances.

Ferguson and Senie (1998) proposed to deploy network ingress filtering to limit spoofing of the source IP address. Although it could help by preventing a packet from leaving a border network without a source address from the border network attackers have countered by choosing legitimate border network addresses at random. Also, every ISP had to implement this scheme otherwise there would have been entry points to the

internet. To add to that the additional router configuration that was required and processing overhead to perform the filtering made it a not so much sought after remedy.

Savage et al. (2000), introduced a new scheme for providing traceback data by having routers embed information randomly into packets. They proposed a scheme in which adjacent routers would randomly insert adjacent edge information into the ID field of packets. Their key insight was that traceback data could be spread across multiple packets because a large number of packets were expected. They also include a distance field which allows a victim to determine the distance that a particular edge is from the host. This prevents spoofing of edges from closer than the nearest attacker. The biggest disadvantage of this scheme is the combinatorial explosion.

Park and Lee (2001) propose a router packet filtering (RPF) mechanism against IP address spoofing. RPF relies on Border Gateways Protocol (BGP) routing information to detect spoofed IP addresses. According to Tao et al. (2006), their approach was interesting, but required high levels of router participation. To add to that, it relates to the implementation of RPF in practice. Given that the Internet contains more than 10,000 ASs, RPF would need to be implemented in at least 1,800 ASs in order to be effective, which is an onerous task to accomplish. Moreover, RPF requires modifications to the BGP message scheme (Rekhter and Li 1995), so that source addresses are included in BGP messages. This would significantly increase the size and processing time for BGP messages. The third potential limitation is that RPF relies on valid BGP messages to configure the filter. If an attacker can hijack a BGP session and disseminate bogus BGP messages, then it is possible to mislead border routers to update filtering rules in favor of the attacker. Finally, the filtering rules in RPF have a very coarse granularity, i.e., at the AS level. The attacker can still spoof IP addresses based on the network topology.

Li et al. (2002) proposed the Source Address Validity Enforcement (SAVE) protocol which enables routers to update the information of expected source IP addresses on each link and block any IP packet with an unexpected source IP address. SAVE protocol is geared to provide routers with information about the range of source IP addresses that should be expected at each interface. Similar to the existing routing protocols; SAVE constantly propagates messages containing valid source address information from the source location to all destinations. Hence, each router along the way is able to build an incoming table that associates each link of the router with a set of valid source address blocks.

Morein et al. (2003) proposed a graphic turing test a complementary approach to blocking attack traffic is to limit the rate at which sources can generate requests. If a target service is designed for use by a person, then it may be reasonable to filter all traffic that is generated by an automated source, e.g., an attack zombie. When an unfamiliar source uses a service for the first time, then it must first complete an admission challenge that requires human judgment, such as reading a character string that has been presented as an image Morein et al. (2003). This denies access to automated sources, which would be unable to complete the challenge. Such challenges can be reissued to a source if that source starts to generate a large number of requests, i.e., the person has been replaced by an automated source. A variant on this approach has been proposed for target services that are intended for use by automated sources, e.g., DNS servers. In this case, the admission challenge takes the form of a computational puzzle, which is designed to be easy to set and verify, but hard to solve, e.g., a constraint satisfaction problem, Kandula et al. (2005).

In this case, any additional requests from a source are blocked until the initial challenge has been solved. However, this form of puzzle-based challenge requires compatible client software at the source, which may limit the deployment of this approach. Similarly, admission challenges that require human judgment can create more work for legitimate users, and may not achieve user acceptance. Furthermore, both types of challenge still require some computational resources at the target, which can become a bottleneck during an attack.

SAVE is a protocol that enables the router to filter packets with spoofed source addresses using incoming tables. It shares the same idea with ingress filtering and RPF that the source address space on each link of the router is stable and foreseen. Any packet that violates the expected source address space will be regarded as forged and will be filtered. SAVE outperforms ingress filtering and RPF in that it overcomes the asymmetries of Internet routing by updating the incoming tables on each router periodically. According to Tao et al. (2006) the limitations of SAVE needs to change the routing protocol, which will take a long time to accomplish. Moreover, as SAVE filters the spoofed packets to protect other entities, it does not provide direct implementation incentives. If SAVE is not universally deployed, attackers can always spoof the IP addresses within networks that do not implement SAVE. Moreover, even if SAVE were universally deployed, attackers could still launch DDoS attacks using non-spoofed source addresses.

Sung and Xu (2002) proposed an altered IP traceback approach, where the victim tries to reconstruct the attack path but also attempts to estimate if a new packet lies on the attack path or not. Their scheme was probabilistic and each router either inserts an edge marking for the IP traceback scheme or a router marking identifying the router. Unfortunately, their approach required the victim to collect on the order of 105 attack

packets to reconstruct a path, and once the path is reconstructed, this scheme was likely have a high false positive rate as the routers close to the victim would all lie on some attack path and frequently mark legitimate packets which would then get rejected.

Cryptography is related to computer security. The word cryptography was originally derived from the Greek words of *kryptos* and *graphos*. *Kryptos* is defined as secret whereas *graphos* is defined as writing (Bacard, 1995). Cryptography involves two processes which are encryption (scramble) and decryption (unscramble). Cryptography is a process of converting plaintext into cipher text, and in contrast ciphers text into plaintext (Haney, 2006). Plaintext is a term that refers to an original text. There are certain mathematical formulae or rules that can be used for the encryption and decryption processes. These mathematical formulae or rules are known as cipher.

Cryptographic techniques provide the logical protection of electronic money systems by ensuring the confidentiality, authenticity and integrity of devices, data and communications used in transactions. There are a number of different cryptographic techniques that are used for different purposes in electronic money systems.

Encryption is a technique used to protect the confidentiality of data during transmission or while stored on a device. Encryption is particularly important for certain types of sensitive data used in security processes, such as cryptographic keys. Other information, such as payment amounts or card serial numbers, may not necessarily be transmitted or stored in encrypted form. Firstly, overall cryptography is a long process and it takes a long time to figure out the code to use, if one was to send the code to another person in the past it would take a while to get to that person.

Secondly, the widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wiretaps) and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. Thirdly, encryption also threatens national security by interfering with foreign intelligence operations. The United States, along with many other countries, imposes export controls on encryption technology to lessen this threat. To add to that, cryptography poses a threat to organizations and individuals too. With encryption, an employee of a company can sell proprietary electronic information to a competitor without the need to photocopy and handle physical documents.

Fifthly, electronic information can be bought and sold on "black networks" such as Black-Net with complete secrecy and anonymity a safe harbor for engaging in both corporate and government espionage. The keys that unlock a corporation's files may be lost, corrupted, or held hostage for ransom, thus rendering valuable information inaccessible. Lastly, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned.

According to V. Shyamaladevi et al., (2009) StackPi is an abbreviation Stack Path Identifier, and is where a packet traverses routers on the path towards its destination; the routers deterministically mark bits in the packet's IP Identification field. The deterministic markings guarantee that packets traveling along the same path will have the same marking.

StackPi allows the victim and routers on the attack path to take a proactive role in defending against a DDoS attack by using the StackPi mark to filter out attack packets on a per packet basis. In addition, the victim can build statistics over time relating StackPi marks to IP addresses. Then if an attacker spoofs an IP address, it is likely that the StackPi mark in the spoofed packet will not match the StackPi mark corresponding to the legitimate IP address in the database, thus enabling the victim to tag packets.

The filter simply checks any incoming packet's StackPi mark and compares its IP address to a list of hIP address, StackPi marki tuples to see if there is a match. Like the threshold filtering scheme, the StackPi-IP filter requires bootstrapping however, in this case, with packets bearing non-spoofed source IP addresses. Such a scenario is ideal for a server that has a static set of authorized users.

The metric that best quantifies the performance of the StackPi-IP filter is the probability that a randomly selected attacker will be able to spoof an IP address that will be accepted by the victim. The only way for this to happen is for an attacker to spoof the IP address of an end-host that happens to have the same StackPi mark as the attacker itself. This is hardest for the attacker when the IP addresses of end-hosts in the topology are distributed uniformly over the possible StackPi marks, because no StackPi mark has a large number of IP addresses that map to it and thus there are fewer IP addresses for that StackPi mark that will be accepted by the filter.

III. Integrated Solutions

This sections looks into a combination of techniques because of the many limitations that the standalone. Tao et al. (2006), most approaches focus on detecting and filtering attack traffic near the target of

the attack. The main limitation of this general approach is that the computational and network resources available to the attacker can readily exceed that of the target. This means that the zombies can engage in more complex transactions such as authentication requests or web queries, which are difficult to differentiate from legitimate traffic. In order to respond to this growth in attack power, defenders need a more scalable approach to defense.

1.1 Compressed Anti IP Spoofing Mechanism using cryptography

S.Gavaskar and Dr.E.Ramaraj (2011) proposed a technique of IP spoofing using two way security mechanism compression and encryption. This was a method whose main objective of IP compression is to avoid the overhead, which provides the bandwidth utilization. The IP header compression work initiated ten years ago but still there is some drawback and problem persists. For handling the packet transformation in effective manner they moved to IPv6 but the header size would increase in IPv6. To increase the bandwidth utilizations, avoid the network traffic, congestion, collision, and then the compression technique was adopted. Basically compression was used to minimize the size of file into half. For example if the original file size is 100mb after compression it will reduced into 50mb here the files are decompressed without losing anything. Basic idea behind this was to remove the unwanted data's or information's.

First the original packet was then split by the packet header with the data. Whenever the data transmission happen that time 4tuple information are common for throughout the data transfer. Then the compressions of these things minimized the many space due to that we can utilize bandwidth in optimized manner.

The GRS algorithm was the novel algorithm that was designed for implementation. The concept behind this group of IP address is considered as a single no which is taken as host identification. The next step was applying the cryptography technique which was used because of its simple state. Simple functions in the implementation used transformation function as method. It just modified the one value into another form using add or multiply that value into original no. for example the previous 2 will converted onto 6 adding 4 with 2 . The final thing we have had to send the key value for decryption. Key value added into encrypted value for easy identification similar to the format of IP address 6.4 is the final value that was send to the destination machine likewise all 4tuple's. Again the decryption happened in reverse manner. TABLE 1 represents the algorithm used in S-ARP.

Table 1 Compression and Cryptography

• Split the packet header with data
• Applied the GRS compression algorithm
• Apply the cryptography technique
• Transmit the data
• Decryption
• Decompression
• Original information.
• Split the packet header with data

3.2 Cryptography & Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) involves the process of cryptography. The PGP has commonly been used for electronic mails. Phil (1995) PGP is a software that combined several high-quality; existing public-key encryption algorithms and protocols into one package for secure, reliable electronic mail and file transfer. The PGP concept was created by Phil Zimmermann in 1995 but did not have the unique techniques for encryption Henry (2000). Nonetheless, RSA, IDEA and digital signatures are the frequently used techniques for the encryption process in PGP at present.

Kamarudin and Mohammad (2011), the PGP is widely used due to several advantages it pertain which among them being a freeware, existence on web, and more secure algorithms. In addition, PGP is independent in view of the fact that it is neither in extensive development, nor is it controlled by any government or organizational standards.

Stallings (2002) explained on five operations involved in PGP authentication, confidentiality, compression, email compatibility and segmentation.PGP uses an efficient algorithm that generates a hash code from the user's name and other information about the data to be transmitted. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, then the receiver is sure that the message has arrived securely from the stated sender. A demonstration of this is shown in figure 1.

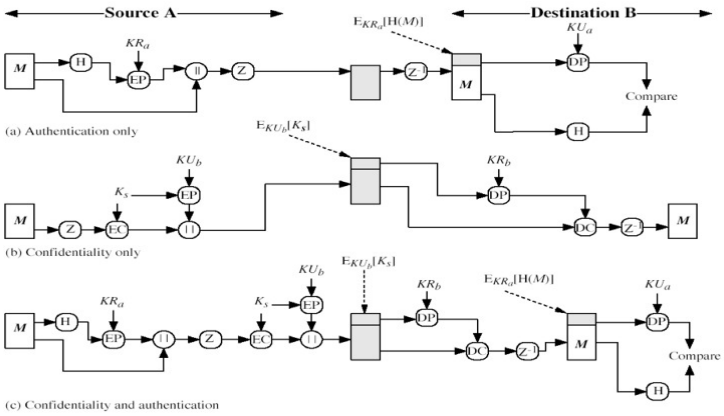

Fig1. PGP integrated with cryptography. Source Kamarudin and Mohammad (2011)

3.3 Secure Address Resolution Protocol

D. Bruschi et al. (2003) used a new approach to prevent spoofing attacks by combining cryptography and Address Resolution Protocol (ARP) to make it more secure and increase results. Secure ARP (S-ARP) extends ARP with an integrity/authentication scheme for ARP replies, to prevent ARP spoofing attacks.

Since S-ARP is built on top of ARP, its specification (as for message exchange, timeout, cache) follows the original one for ARP. In order to maintain compatibility with ARP, an additional header is inserted at the end of the protocol standard messages to carry the authentication information. This way, S-ARP messages can also be processed by hosts that do not implement S-ARP, although in a secure ARP LAN all hosts should run S-ARP.

Hosts that run the S-ARP protocol will not accept non authenticated messages unless specified in a list of known hosts. On the contrary, hosts that run the classic ARP protocol were able to accept even authenticated messages. A mixed Local Area Network (LAN) is not recommended in a production environment because the part running traditional ARP is still subject to spoofing attacks.

S-ARP uses asymmetric cryptography. Any S-ARP enabled host is identified by its own IP address and has a public/ private key pair. A simple certificate provides the binding between the host identity and its public key. Besides the host public key, the certificate contains the host IP address and the MAC address of the Authoritative Key Distributor (AKD), a trusted host acting as key repository. Each host sends its signed certificate containing the public key and the IP address to the AKD, which inserts the public key and the IP address in a local data base, after the network manager's validation

Furthermore, the list of hosts not running S-ARP must be given to every secured host that has to communicate with an unsecured one. The interoperability with the insecure ARP protocol is given only for extraordinary events and should be always avoided. It is intended to be used only during the transition phase to a full S-ARP enabled LAN. A demonstration of the S-ARP is shown in figure 2.

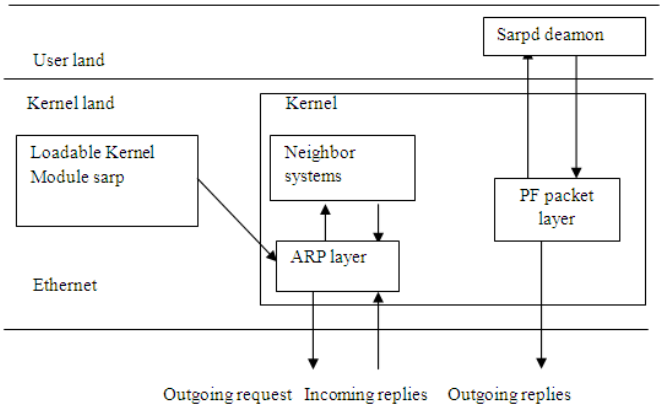

Fig2. The structure of S-ARP. Source Bruschi et al. (2003)

IV. Comparisons between integrated and standalone solutions

My review of standalone solutions and integrated solutions of eradicating spoofing attacks clearly indicates that integrated solutions perform better in comparison to their standalone counterparts. An example of the S-ARP show how cryptography enhances the performance of the normal ARP solution by including an authentication layer that the messages have to go through that requires a cryptographic key to decrypt in order to allow access leading to a more secure alternative in comparison to the normal ARP solution. S-ARP uses asymmetric cryptography. Any S-ARP enabled host is identified by its own IP address and has a public/ private key pair. A simple certificate provides the binding between the host identity and its public key.

Another example is the compressed anti IP spoofing mechanism using cryptography uses the cryptographic feature to also assist in the encryption of the compressed header thus allowing only the data or messages that contain the decrypted key passage thus increasing security in comparison to the compressed anti IP spoofing mechanism that is standalone.

The same case applies to cryptography and pretty good privacy they are both independent methodologies but their combination makes them better performers. Pretty Good Privacy (PGP) concept is applied to increase the level of security for a digital file by enhancing security thus making it difficult for intruders by adding obstacles in order to obtain the files they desire. This is done by ensuring that an exact port number between client and server to add an obstruction for intruders trying to gain access. It increases security by applying of cryptography and compression processes. The intruders would have to necessitate more time period, additional methods and a specific access key because of the difficulties when trying to access the files content as result of cryptography and compression.

Integrated solutions are a combination of two working standalone solutions and instead of having advantages of one methodology we get to have two methodologies working hand in hand to assist in complementing the other methodologies weakness or limitations. Cryptography is one of the most used solutions because it's more robust and can accommodate different methodology platforms. With this in play that is the solid reason why the choice of Stack Pi and Encryption seem like a valid combination to assist in the fight against spoof attacks.

V. Adoption of Stack Pi and Encryption

The results of the combined techniques are an improved version meaning more effective in comparison their stand alone counterparts. In review of all the standalone methodologies that we have seen for curbing of spoofing attacks, cryptography and StackPi stood out as the most effective and thus bound to give better results.

According to Bruce Schneier (2006), cryptography is one of the most important components of fraud prevention in all electronic money systems. Although it bears certain limitations as listed in its previous review it also bears a lot of weight and thus a perfect choice when it comes to integrating it with other methodologies. Also we have seen that Encryption has been paired before with other methodologies giving outstanding results and thus there is guarantee that if we integrate it with another powerful methodology it is to help bridge the gap that limits spoofing attacks.

Stack Pi originated from the *Pi*, a Path Identification algorithm but it had certain limitations which prompted the introduction of Stack Pi. According to Adrian et al. (2002), the original Pi marking is based on the use of the packet's TTL field as an index into the IP Identification field where a router should add its marks. This method is not as lightweight as the StackPi method. Legacy routers have a harmful affect on the original Pi scheme because they decrement the TTL of a packet but do not add any markings. The StackPi scheme is robust to legacy routers and even includes the write-ahead scheme to incorporate markings for single legacy routers in the path.

With the reviews a combination of these methods will mean an ultimate product that will not only curb spoofing attacks but will also enable the victim to track down the perpetrator involved in the action. This will guarantee an increase in the users of EPS systems confidence and thus they can perform their services to the best of their abilities saving both the supplier and the consumer billions of shillings in savings.

VI. Conclusion

In this work we present a survey of standalone methodologies versus integrated solutions that are a combination of two working standalone techniques. We justify through a comparison of both solutions the added advantage that these integrated solutions posses which supports the justification of the work that we want to undergo of integrating Stack Pi and Encryption as our methodologies of choice.

Acknowledgement

I would like to thank my supervisors, Dr. Wilson Cheruiyot and Dr. Joseph Wafula for their many suggestions, generous help and constant support during my research. I feel grateful for the support I have received from the Jomo Kenyatta University of Agriculture and Technology with their scholarship for my

Masters studies. Finally I wish to thank my family Mr. & Mrs. Kaluvu, John, Jones, Lucy, Betty and Declan for their continued support throughout this endeavor it's an honor to have you as my support system.

References

[1] Bruce J, Summers, Payment Systems: Design Governance and Oversight (Central Banking Publication Ltd London, 2012).
[2] Hezlin Harris ,Balachander Krishnan Guru and Mohan V. Avvari, Evidence of Firms' Perceptions toward Electronic Payment Systems (EPS) in Malaysia. International Journal of Business and Information, 2011.
[3] Thomas P. Vartanian, Robert H. Ledig and David L. Ansell, "Role and Security of Payment Systems in an Electronic Age," IMF Institute Seminar on "Current Developments in Monetary and Financial Law" June 1, 2004
[4] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. RFC 2267, January 1998.
[5] Savage, S., Wetherall, D., Karlin, A., And Anderson, T. Practical network support for IP traceback. In Proceedings of the 2000 ACM SIGCOMM Conference August, 2000.
[6] Heejo Lee and Kihong Park, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In Proceedings IEEE Infocomm 2001, April 2001.
[7] Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems." Department of Computer Science and Software Engineering. The University of Melbourne Australia, 2006.
[8] Rekhter, Y. and T. Li, (eds.), A Border Gateway Protocol 4 (BGP-4)," RFC 1771 (Standards Track), March 1995.
[9] Li, J., Mirkovic, J., Wang, M., Reither, P., and Zhang, L., Save: Source address validity enforcement protocol. In Proceedings of IEEE INFOCOM 2002, NewYork, NY, USA, 2002 1557-1566.
[10] Morein, W. G., Stavrou, A., Cook, D. L., Keromytis, A. D., Misra, V., and Rubenstein, D., Using graphic turing tests to counter automated ddos attacks against web servers. In Proceedings of the 10th ACM International Conference on Computer and Communications Security (CCS). Washington D.C.2003
[11] Kandula, S., Katabi, D., Jacob, M., and Berger, A. W., Surviving Organized DDoS Attacks That Mimic Flash Crowds. In 2nd Symposium on Networked Systems Design and Implementation (NSDI). Boston, MA. 2005.
[12] Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems." Department of Computer Science and Software Engineering. The University of Melbourne Australia, 2006.
[13] Sung Minho and Xu Jun (2002), "IP traceback-based intelligent packet filtering: A novel technique for defending against internet DDoS attacks," In Proceedings of IEEE ICNP 2002, Nov. 2002.
[14] Bacard, A. The computer privacy handbook (Berkeley, CA: Peachpit Press, 1995).
[15] Haney, J.D., The use of cryptography to create data file security: with the Rijndael cipher block. Journal of Computing Sciences in College. 21 (3), 2006, 30-39.
[16] V. Shyamaladevi , Dr. R.S.D Wahidabanu, K.S.Rangasamy, Analyze and Determine the IP Spoofing Attacks Using Stackpath Identification Marking and Filtering Mechanism. IJCSNS International Journal of Computer Science and Network Security, 8(10), 2008, 339
[17] Tao Peng and Christopher Leckie and Kotagiri Ramamohanarao, Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems, Department of Computer Science and Software Engineering. The University of Melbourne Australia,2006.
[18] S.Gavaskar and Dr.E.Ramaraj., A Compressed Anti IP Spoofing Mechanism using Cryptography, Madurai Kamraj University, Madurai, 2011
[19] Philip Zimmerman, PGP Source Code Internals, (Boulder, Colarado: MIT Press 1995).
[20] Henry, K. (2000). Getting started with PGP. Crossroads: The ACM magazine for students. 6(5). doi:10.1145/345107.345119, http://dx.doi.org/10.1145/345107.345119.
[21] Kamarudin Shafinah& Mohammad Mohd Ikram, File Security based on Pretty Good Privacy (PGP) Concept. Faculty of Agriculture and Food Sciences, Universiti Putra Malaysia Bintulu Sarawak Campus (UPMKB), 2011.
[22] Stallings, W. Network security essentials: application and standards. (2nd ed.). New Jersey: Prentice-Hall, 2002.
[23] D. Bruschi, A. Ornaghi, E. Rosti, S-ARP; A secure address resolution protocol. In proceedings of the 19th Annual Computer Security Application Conference (ACSAC) Las Vegas, Nevada, 2003.
[24] Schneier Bruce Caller ID spoofing. schneier.com. 2011.
[25] Adrian Perrig, Dawn Song , Abraham Yaar, StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks. School of Computer Science Carnegie Mellon University 2002.