iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VIII **Month of publication:** August 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Closing the Location of IP Spoofers Using Greedy Algorithm

S.Srithar[1], Deepthi C J [2], R Dinesh Kumar [3], S. Jeevarekha [4], Sneha Varghese[5]
[1]Assistant Professor, [2, 3, 4,5]UG Student
Department of Information Technology, RVS College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract— Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs. The system implementation mainly focusing disclosing the Locations of IP Spoofers from Path Backscatter using the passive IP trace back (PIT) that bypasses the deployment difficulties of IP trace back techniques. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofer's based on public available information (e.g., topology). In this way, PIT can find the spoofer's without any deployment requirement. This paper illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofer's through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood. Though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an Internet-level trace back system has been deployed in real. Instead of proposing another IP trace back mechanism with improved tracking capability, we propose a solution algorithm, named Greedy algorithm to bypass the challenges in deployment. Routers may fail to forward an IP spoofing packet due to various reasons,exceeding. In such cases, the routers may generate an ICMP error message and send the message to the spoofed source address.
Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers. Greedy Algorithm exploits these path backscatter messages to find the location of the spoofers. With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks. PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic.
Key words -PIT, Greedy algorithm, ICMP message.

I. INTRODUCTION

As a network security systems refers to the long known attackers may use forged source IP address to conceal their real locations. To capture the spoofers, a number of IP Trace back mechanisms have been proposed. However, due to the challenges of deployment, there has been not a widely adopted IP Trace back solution, at least at the Internet level. As a result, the mist on the locations of spoofers has never been dissipated till now. This paper proposes passive IP trace back (PIT) that bypasses the deployment difficulties of IP Trace back techniques. PIT investigates Internet
Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information. In this way, PIT can find the spoofers without any deployment requirement. This paper illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood. Though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an Internet-level trace back system has been deployed in real.

II. LITERATURE SURVEY

A. C. Snoeren et al.,.[5] This paper present a hash-based technique for IP traceback that generates audit trails for traffic within the network, and can trace the origin of a single IP packet delivered by the network in the recent past. the system is effective, space-efficient (requiring approximately 0.5% of the link capacity per unit time in storage), and implementable in current or next-generation routing hardware. We present both analytic and simulation results showing the system's effectiveness.
S. M. Bellovin, [1] describes the TCP/IP protocol suite, which is very widely used today, was developed under the sponsorship of the

Department of Defense. Despite that, there are a number of serious security flaws inherent in the protocols, regardless of the correctness of any implementations. We describe a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks. We also present defenses against these attacks, and conclude with a discussion of broad-spectrum defenses such as encryption.

Y. Xiang, W. Zhou, and M. Guo,[14] paper we present a novel and practical IP traceback system called Flexible Deterministic Packet Marking (FDPM) which provides a defense system with the ability to find out the real sources of attacking packets that traverse through the network. While a number of other traceback schemes exist, FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments; it also adaptively changes its marking rate according to the load of the participating router by a flexible flow-based marking scheme.

III. PROBLEM DEFINITION

The main problem with IP spoofing is that even if you are able to send a data to the server, making it believe that the data came from fake, then the server will reply to the spoofed IP address and not your real IP address. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for denial-of-service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack. The problem of finding the source of a packet is called the IP traceback problem. IP traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path(s).

A. Overview Of The Project

In this project we focus on transaction that should satisfy the requirements of the customer to cover the entire transaction process. The nodes are arranged in a consecutive manner which is used to transfer data effectively. Nodes should be reorganized in a way if an attacker is identified in that particular path.

This paper describes four modules using dot net programming language. First module illustrate customer authentication. In the first module present If you are the new user going to use the service then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

In the second module pin authentication represents the customer going to use the service then they have to register first by providing necessary details. After successful completion of process, the customer has to login into the application by providing Customer ID and PIN Number. The Admin has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

In the third module IP spoofer processes can able to retrieve their data from the IP Address, similarly can able to find their data from that storage area.

In the final module admin processes can be done. The implementation of final module based on the greedy algorithm.

IV. SYSTEM ANALYSIS

A. Existing System

In the existing system are users and applications passive IP Trace back(PIT) that bypasses the deployment difficulties of IP trace back techniques. It is not so sufficient if there is heavy interaction between branches. It can be classified into five main categories: packet marking,ICMP testing, overlay and hybrid tracing. Existing trace back mechanisms are either not widely supported by current commodity routers or will introduce considerable overhead to the routers generation especially in high-performance networks.

1) Drawbacks

a) Not so efficient if there is heavy interaction between branches

b) Data should be carefully maintained

B. Proposed System

A Proposed algorithm(Greedy algorithm) will add found the view and find the attacker. It is used to identify the location of the IP spoofer The users uses applications passive IP trace back techniques.PIT investigates Internet Control Message Protocol error messages(named path backscatter)triggered by spoofing traffic, and tracks the spoofers based on public available information. Based on the successive transaction, the nodes are uniformly distributed.

Through the performance analyses we show that our system is efficient than the existing protocol with reliable transaction

1) Advantages

a) This techniques is very efficient if there is heavy interaction between branches

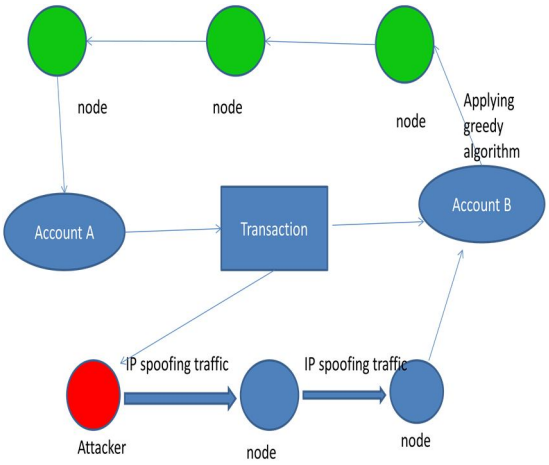
b) We can store the data normally and efficiently

V. SYSTEM DESIGN

A. System Architecture

In this architecture the transaction between the two accounts (ie) account A and account B is based on the IP spoofing traffic with in each node that is between these two accounts.

The IP spoofing traffic facilitates each node that to determine the path of the transaction. Accordingly this will minimize the time required for transaction. If the attacker is found in that path then there involves Greedy algorithm, which involves challenging role to find the alternate path By Greedy algorithm, the path is concentrated by the consecutive nodes that forward to the further nodes.



Transaction is proposed because of its network scalability many nodes can be added or removed from the network without significantly affecting the performance.Greedy algorithms have some research challenges in finding an attacker- free path.

VI. SYSTEM IMPLEMENTATION

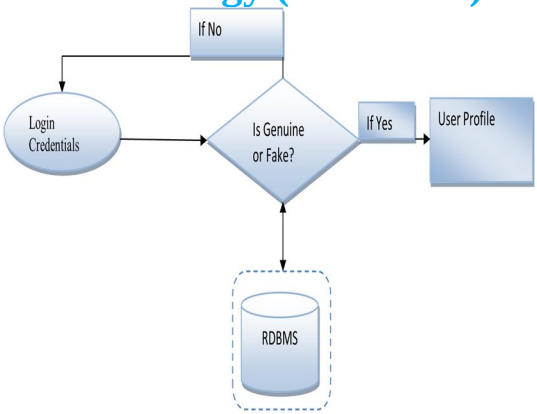
A. Node Creation

Each node is created with unique node-ID in the same system the two or more nodes can communicate each other using this node-ID. We make use of six nodes in our implementation. The number of connections to establish between each pair of nodes in a network is dependent on the size and configuration of the system.

B. Customer Authentication

If you are the new user going to use the service then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

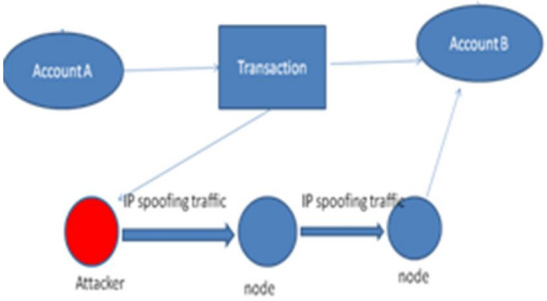


C. Pin Authentication

If you are the customer going to use the service then they have to register first by providing necessary details. After successful completion of process, the customer has to login into the application by providing Customer ID and PIN Number. The Admin has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

D. IP Spoofer Process

IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines. For example, it is common on some corporate networks to have internal systems trust each other, so that users can log in without a username or password provided they are connecting from another machine on the internal network (and so must already be logged in). By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authentication.



E. Passive IP Traceback(PIT)

IP trace back can be used to find the origin of anonymous traffic; however, Internet-scale IP trace back systems have not been deployed due to a need for cooperation between Internet Service Providers (ISPs). This article presents an Internet-scale Passive IP Trackback (PIT) mechanism that does not require ISP deployment. PIT analyzes the ICMP messages that may scattered to a

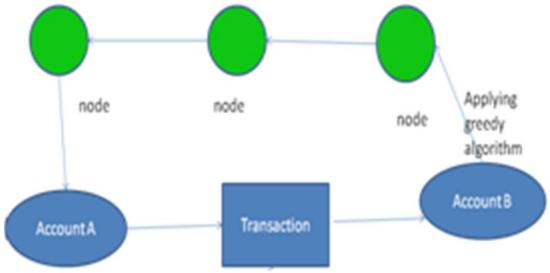
network telescope as spoofed packets travel from attacker to victim. An Internet route model is then used to help re-construct the attack path. Applying this mechanism to data collected by Cooperative Association for Internet Data Analysis (CAIDA), we found PIT can construct a trace tree from at least one intermediate router in 55.4% the fiercest packet spoofing attacks, and can construct a tree from at least 10 routers in 23.4% of attacks. This initial result shows PIT is a promising mechanism.

F. Greedy Algorithm

A greedy algorithm is a mathematical process that looks for simple, easy-to-implement solutions to complex, multi-step problems by deciding which next step will provide the most obvious benefit.

Such algorithms are called greedy because while the optimal solution to each smaller instance will provide an immediate output, the algorithm doesn't consider the larger problem as a whole. Once a decision has been made, it is never reconsidered.

Greedy algorithms work by recursively constructing a set of objects from the smallest possible constituent parts. Recursion is an approach to problem solving in which the solution to a particular problem depends on solutions to smaller instances of the same problem. The advantage to using a greedy algorithm is that solutions to smaller instances of the problem can be straightforward and easy to understand. The disadvantage is that it is entirely possible that the most optimal short-term solutions may lead to the worst possible long-term outcome.



VII. CONCLUSION AND FUTURE ENHANCEMENTS

A. Conclusion

We try to dissipate the mist on these locations of spoofers based on investigating the path backscatter messages. In this article, we proposed Passive IP Trace back (PIT) which tracks

spoofers based on path backscatter messages and public available information. We illustrate causes, collection, and statistical results on path backscatter. We specified how to apply PIT when the topology and routing are both known ,or the routing is unknown, or neither of them are known .We presented two effective algorithms to apply PIT in large scale networks and proofed their correctness. We demonstrated the effectiveness of PIT based on deduction and simulation .We showed the captured locations of spoofers through applying PIT on the path backscatter dataset. These results can help further reveal IP spoofing, which has been studied for long but never well understood.

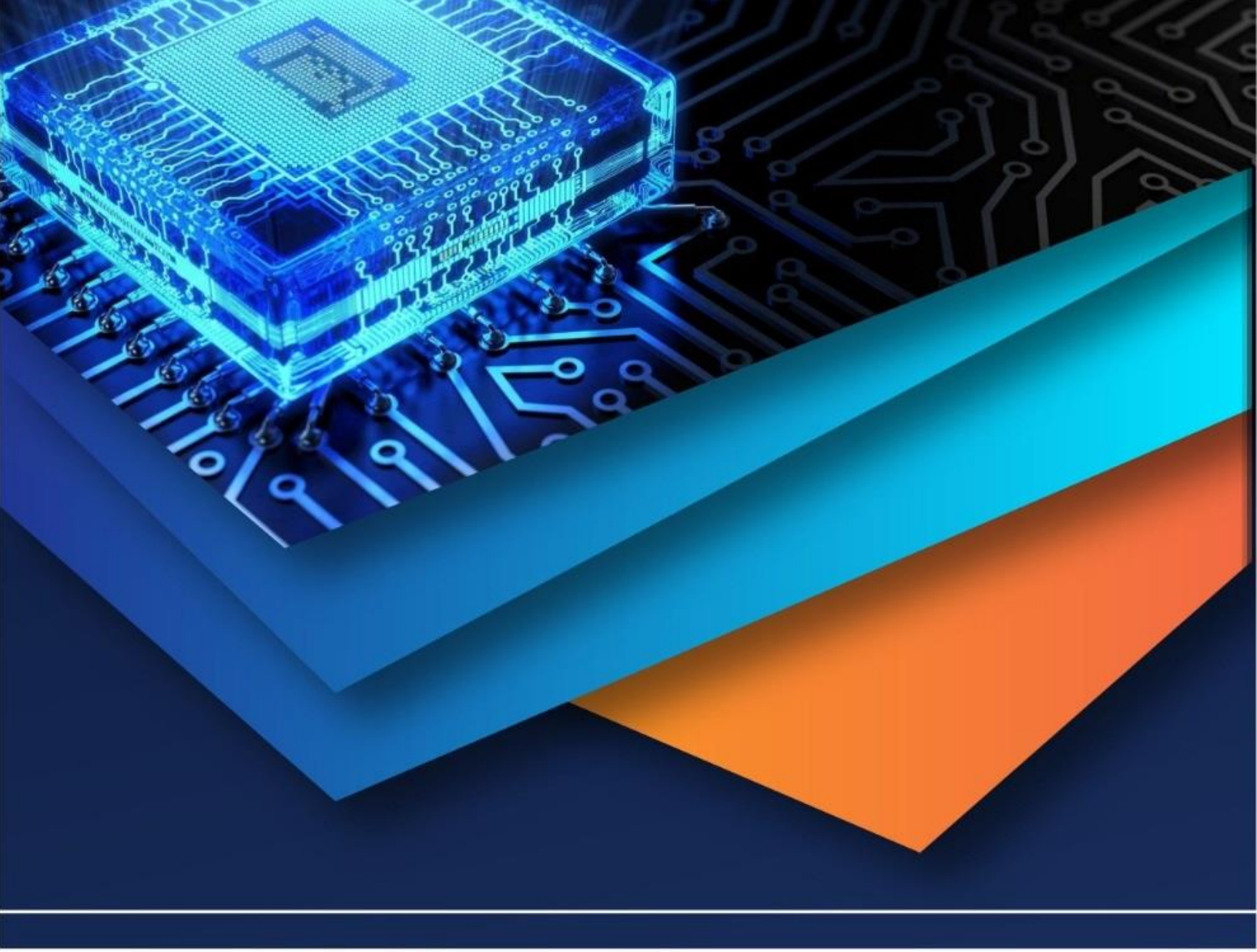
B. Future Enhancement

In future this work includes the implementation of more effective secure transaction processes using passive IP trace back mechanism followed by Greedy Algorithm.

REFERENCES

[1] S. M. Bellovin, "Security problems in the TCP/IP protocol suite,"ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48,Apr. 1989.
[2] ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008,Mar. 2006.
[3] C. Labovitz, "Bots, DDoS and ground truth," presented at the 50th NANOG, Oct. 2010.
[4] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP trace back," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.
[5] A. C. Snoeren et al., "Hash-based IP trace back," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.
[6] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage,"Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006.
[7] M. T. Goodrich, "Efficient packet marking for large-scale IP trace back,"in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117–126.
[8] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP trace back," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.
[9] A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet trace back," in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM),vol. 2. Mar.

2005, pp. 1395–1406.
[10] J. Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient IP trace back," Comput. Netw., vol. 51, no. 3,pp. 866–882, 2007.
[11] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP trace back under denial of service attack," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.
[12] M. Adler, "Trade-offs in probabilistic packet marking for IP trace back,"J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.
[13] A. Belenky and N. Ansari, "IP trace back with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.
[14] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking:An IP trace back system to find the real source of attacks," IEEE Trans.Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, Apr. 2009.
[15] R. P. Laufer et al., "Towards stateless single-packet IP trace back," in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007,pp. 548–555.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY