iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** II **Month of publication:** February 2016

DOI:

www.ijraset.com

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

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

Security to Protect From Cybercrime and Security Incidents Used To Commit Cybercrime in Cyberspace

Dr.P.B.Pathak
Assistant Professor& Head, Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded, Maharashtra, India

Abstract— Security is the key to preventing or detecting Computer and Computer Network related criminal activity. Cybercrime is possible because Computers and Networks are not properly secured. Security Incidents have greatly increased over the years, where the attackers have increasingly improved in devising attacks towards a specific target. Cyber Incidents have created a global threat, both in defending local and global Computer Networks. Attacks are becoming more sophisticated and possess the ability to spread in a matter of few seconds.
Keywords— Security; Security Incidents; Confidentiality; Integrity; Availability; Identification; Authentication; Nonrepudiation

I. INTRODUCTION

Most criminals look for easy victim. Most attacks against Computers and Networks exploit well known vulnerabilities. In many cases these vulnerabilities can be fixed with a minimal change in the configuration. These simple security measures costs nothing. Yet computer users and network administrators are as reluctant in protecting their valuable data. The fact that these known exploits still work. Most of the time shows that most individuals and companies are not performing due carefulness in protecting their IT assets before connecting them to the Internet. There are many reasons for this behavior:

Lack of knowledge of Security and Security issues.

Lack of time.

Psychological denial that it can't happen to me.

None of these reasons is good enough to justify the potential loss due to Cybercrime, and those fact costs lots, after the network and its data have been compromised. It is important to realize that it is not just individuals or small businesses on tight budgets that neglect their security needs. Human nature is such that it often takes a tragedy to motivate people in charge to take action.[1,2]

II. SECURITY

Computer Security and in particular Computer Network Security is based on three pillars: Confidentiality, Integrity, and Availability. Confidentiality means keeping information secret from all except the intended readers. Integrity means to protect information from being altered by unauthorized persons. Availability means to protect the information from becoming unavailable either by accident or sabotage. [3]

Some references also include Identification and Authentication, Nonrepudiation, Access Control, and Accountability in their description. Identification and Authentication is the verification of a claimed identity. Nonrepudiation is the process of ensuring that the author of a document cannot later claim not to be the author. Access Control encloses any mechanism of granting access to data or performing an action, and the access control mechanism grants and revokes privileges based on predefined rules, and finally Accountability means to track and record events occurring in a system and all these are important aspects of information security. [4]

A. Confidentiality

Confidentiality refers to any method that keeps the contents of the data secret. Confidentiality means encrypting data to prevent unauthorized persons from understanding what the data says even if they intercept it. In a high security environment, where network communications necessarily involve information that should not be shared with the world, it is important to use strong Encryption mechanism to protect the confidentiality of sensitive data.

B. Integrity

Data integrity is ensuring that the data was not changed after it left the sender, that the data that was sent is exactly the same as the

data that is received at the final destination. It is essential to be able to count on data integrity in network transactions such as e-commerce.

C. Availability

Availability ensures the uninterrupted service to authorized users. Service interruptions can be either accidental or maliciously caused by denial-of-service attacks. Assets should be available to those who need them at the times when they need them. If someone has access rights to a resource, they should be able to access it. Availability equates to the ability to access an information resource and the data that is stored within that resource. More specifically, availability is about information being accessible as needed, when needed, where needed. The responsiveness and capacity of the information resource and the communications pathways that connect information resources serve as indicators of the system's capability to execute the requests made to the information resource. The objective of availability is to enable access to authorized information or resources.

D. Identification And Authentication

Identification and Authentication is one of the most fundamental mechanisms. Most other protection mechanisms are useless if identification and authentication is not working effectively. By identifying and authenticating all users of a system we are able to control what different users are able to do with the system and what information they're allowed to access. It also gives us the opportunity to track and record these actions for later reference. Authentication is the process of establishing whether someone or something is who or what its identifier states it is. The key benefit of electronic authentication is that it enables electronic transactions to take place in an environment of trust and confidence. Various methods can be used to authenticate a user's identity. Generally, the user is asked to provide something that is associated with his or her user account that could not easily be provided by someone else. The requested credential is generally one or more of the following: Password, Smart Card, Biometric, Logon, and Remote Access.

E. Nonrepudiation

Nonrepudiation is closely associated with authentication. This is a means of ensuring that whoever sends a message cannot later claim that he or she didn't send it. Nonrepudiation just goes a step further than authentication.

F. Access Control

Access control requires identification and authentication in order to be useful. Access control is often implemented in the form of an Access Control List (ACL) for each object in the system, listing the authorized users and what actions they are allowed to take on the object. In military systems access control is often implemented using formal rules, where all users and all objects are allocated different security classes. A user's ability to take a specific action on an object is completely determined by applying the formal access roles on the class allocations. Access control is used to control what actions a user is allowed to take on the objects in a system.

G. Accountability

Accountability is a security requirement, since holding a legitimate user accountable for their actions increases security and avoids nonrepudiation. Accountability functions intended to record exercising of rights to perform security relevant actions. Accountability is ensuring that access to systems and information by users is appropriately recorded. There are multiple ways to enforce accountability for activities taking place. The components of accountability are Availability of Resources to Enforce Security, Monitoring of Activities and Logging.

Accountability for cyber attacks that cause serious damage is essential. The ability to accurately and precisely assign responsibility for cyber attacks to entities or individuals to deter future attacks and motivate evolutionary improvements in relevant policies and engineering technology.

III. SECURITY DEFINED

Security may be defined variously as:

Security is the prevention of or protection against access to information by unauthorized recipients, or intentional but unauthorized destruction or alteration of that information.

Security is keeping anyone from doing things you do not want them to do to, with, or from your computers or any peripherals.

Information Security is the protection of three properties: Confidentiality, Integrity and Availability.

Computer System Security is about much more than just keeping out malicious users and preventing attacks. It is also about maintaining and providing access to resources for authorized users, and it is about maintaining the integrity of the data and the infrastructure. [5-7]

IV. SECURITY INCIDENTS

An information security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Incidents contain activities such as:

Unauthorized access to a system or its data

Unwanted disruption or denial of service

Unauthorized use of a system for the processing or storage of data

Unauthorized changes to system hardware, firmware, or software

There exit more than one ways of categorizing the incidents. Incident Classification must possess some criteria's like it should be Accepted, Mutually Exclusive, Comprehensible, Complete/Exhaustive, Unambiguous, Repeatable, Terms Well Defined, and Useful. When an attack takes place, there is a possibility it uses several vectors as a path to a full blown cyber attack. An attack vector is defined as a path by which an attacker can gain access to a host. This definition includes vulnerabilities, to launch a successful attack it may require several vulnerabilities like Misconfigurations, Kernel Flaws, Buffer Overflow, Insufficient Input Validation, Symbolic Links, File Descriptor, Race Condition, Incorrect File/Directory Permission, and Social Engineering.

Operational Impact is the ability for an attack to culminate and provide high level information known by security experts, as well those less familiar with cyber attacks. Mutually Exclusive operational impacts are Misuse of Resources, User Compromise, Root Compromise, Web Compromise, Installed Malware and Denial of Service of various types [8]

Various strategies a defender can employ to remain vigilant in defending against pre and post attacks. These strategies include both Mitigation and Remediation. Prior to vulnerability exploitation or during an attack, there are several steps a defender can use to mitigate damage an attack has caused, or has the potential to cause. Mitigation involves lessening the severity of the attack by Removing from Network, White listing, and Reference Advisement. In the presence or prior to vulnerability exploitation, there are resolution steps that are available to a defender to prevent an attack. Remediation would involve taking the appropriate steps to correct the situation prior to or during an exploitation by using System Patch and Correct Code.

An attack on a targeted system has potential to impact sensitive information in various ways. A committed resource must be able defend information warfare strategies in an effort to protect themselves against theft, disruption, distortion, denial of service and destruction of sensitive information assets. Attack impacts are Distortion, Disruption, Destruction, Disclosure and Discovery. Various attacks target a variety of hosts, leaving the defender unknowingly susceptible to the next attack. These targets are Operating System, Network, Local Computer, User and Application. Broadly the incidents are categorized as intrusion and attacks.[9]

A. Intrusion

There are numerous ways for attackers to obtain illicit access to computer systems. This kind of access is often called Intrusion, and the first thing an intruder does is usually trying to obtain special/administrative privileges i.e. a root access on that system. Having a root access is very important for the attackers, since this means that they can do whatever they want on the system, including covering their tracks, strengthening their hold and doing damage. In general, there are three main ways to intrude into a system: Physical Intrusion, System Intrusion, and Remote Intrusion.

1) *Physical Intrusion*: This kind of intrusion happens when an intruder has a physical access to the target machine. This might allow the intruder to gain full control of the system.
2) *System Intrusion:* In this case, it is assumed that the intruder has already got low level privileges on the system. They then exploit unpatched security vulnerabilities in order to escalate their privileges to administrative level.
3) *Remote Intrusion:* With remote intrusion, an attacker tries to get into the system remotely through the network. They initially do not have any privileges to the system, but one way or another.

Intrusion do some damage to a system in that an underlying system or sub process would be disrupted or modified as the end result of the intrusion or as a step in a series of penetration activities. Intruders may also seek to change important data in an attempt to

either cover their tracks or to cause people or other processes to act on the changed data in a way that causes a cascading series of damages in the physical or electronic world. Intrusion is an effective step in gaining additional access and knowledge by intruders. There are various common forms of network intrusion, such as Port Scans, LAND attacks, Ping of Death, UDP bombs, Out of Band attacks.[10]

In order to minimize intrusion, many organizations install Intrusion Detection Systems (IDS). Such a system inspects inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. There are several IDSs available.[11]

B. Attacks

A Computer Network Attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. However, CNA may also occur when an attacker uses stolen information to enter restricted computer systems. CNA disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to output errors. Computer hackers opportunistically scan the Internet looking for computer systems that are misconfigured or lacking necessary security software. Once infected with malicious code, a hacker can remotely control a computer, via the Internet, send commands to spy on the contents of that computer or attack and disrupt other computers. [12]

Cyberattacks usually require that the targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, that the malicious code can exploit. Broadly CAN are of two forms as Active attacks and Passive attacks.

1) *Active Attacks:* Active Attacks attempt to cause harm typically through system faults or brute force, and attempt to overload the victim's computer to the point that it either slows to an unusable crawl, hangs, or completely crashes.
2) *Passive Attacks :* Passive Attacks are in the nature of eavesdropping on, or monitoring of transmissions where the goal of the attacker is to obtain the information that is being transmitted i.e. interception. These attacks can be used by a trespasser to degrade the anonymity of the clients. [13]

3) Predecessor Attack: In this attack, the attacker targets any one particular node, and observes it from the receiver point of view. The attacker keeps track of all the clients who initiate a request to send, and identifies the client who appears the most number of times. This is possible because, in an anonymous environment, the list of all available nodes changes whenever an existing node leaves or when a new node joins. So, the client has to make a new connection, and to do so, it might contact the same node (which the attacker is observing) for a new request. But the probability of success is very less because there is very small chance that the client initiates the new request with the same node that is being observed.

4) Denial Of Service Attack: There is a high chance that an attacker might act as a malicious node in the anonymous group. So, if that malicious node plays the denial of service attack on the directory server which provides the clients with the list of available nodes or routes, then no other client's request can be processed. As a result, the entire network fails. [14,15]

5) Distributed Denial Of Service Attack: Distributed Denial-of-service attacks are a major threat. In recent years distributed denial-of-service attacks are used, which expand the vulnerability of Web sites. Attackers use hundreds or thousands of compromised systems in order to harm commercial Web sites.

Attackers use multiple ways to harm their victims. They manipulate the target networks or target servers directly by using a lack of protocols and standards to force failures and shutdowns. Or they try to deplete resources like bandwidth, memory, or processing capacities. With both strategies, attackers try to hinder or interfere with legitimate users of the Web site. Damages from DDoS attacks against a Web site can range from inconvenience for legitimate users and customers, to a lack of reliability of the site and finally to a shutdown of the server and some delay until Web services are continued.

Scanning and infecting computers is usually automated by script programs. These programs scan systems connected to the Internet for known security holes. Another way of recruiting agents for a DDoS network is the use of malicious programs called worms, which are sent via e-mail attachments. After infecting a target with malicious code, a worm sends copies of itself to further recipients. To increase the credibility of such harmful and unsolicited messages, worms use sender addresses and entries of electronic address books of already infected systems for their activities. A group of handlers may be established as intermediaries to avoid direct and traceable connections between the attacker and its agents. Typically, attackers consider those systems for the role of handlers that can be utilized inwardly. Agents subscribe to the commands of handlers who give the starting signal for the attack at a later point. Finally, the agents execute the attack against the target server.

6) Sybil Attack: This is an extension of the denial of service attack. An attacker creates multiple virtual identities, and all act as malicious nodes. Within a time period, all these malicious nodes flood the server with the requests of joining the group, and by doing so; they obstruct the legitimate clients from joining the groups.

7) Local Eavesdropping: When a client wants to communicate with others, it initiates a new connection. So, an eavesdropper sitting there can detect it, but he/she cannot determine the content due use of encryption technology. However, the initiator's/sender's anonymity will be compromised, and the attacker can determine the probable list of the recipients by using the timing of the sender's message.[16]

8) Attack On Critical Information Infrastructure Protection (CIIP): There is a growing misuse of electronic networks for criminal purposes or for objectives that can adversely affect the integrity of national critical information infrastructures. As threats can originate anywhere around the globe, the scope of the problem is inherently international. CIIP is universally acknowledged as a vital component of national security policy.

Critical Infrastructure consists of those indispensable resources that are required for a country to conduct its day-today business. In its basic form those resources include Power/Energy, Information & Telecommunications, Financial Services/Banking, Transport, Emergency Services, Water, Public Administration/Government, Agriculture, Food, Public health, Defense Industrial Base, Chemical Industry & Hazardous Materials, Government, Postal & Shipping, Government and Real Estate [17,18] Four Pillars of Critical Information Infrastructure Protection are Prevention and Early Warning, Detection, Reaction, Crisis Management.

a) *Prevention and Early Warning:* Prevention and early warning aim to reduce the number of information security breaches. A goal is to ensure that critical infrastructures "are less vulnerable to disruptions, any impairment is short in duration and limited in scale, and services are readily restored when disruptions occur."

b) *Detection:* In close collaboration with technical experts from Computer Emergency and Response Teams (CERTs), the CIIP unit should identify new technical forms of attacks as soon as possible. Furthermore, non-technical analyses of the general risk situation are needed.

c) *Reaction:* Reaction includes the identification and correction of the causes of a disruption. Initially, the CIIP unit should provide technical help, and support to the targeted company. However, the CIIP unit cannot take on the management of incident response for these companies. The CIIP unit usually provides advice and guidance on how to tackle an incident, rather than offering complete solutions.

d) Crisis Management: Minimizing the effects of any disruptions on society and the state has always been a major task of protection, so the CIIP unit must be embedded in the national crisis management structure. It should be well positioned in order to have direct access to decision makers, because a key function of the CIIP unit is to alert the responsible people and organizations. In case of a national crisis, the CIIP unit must be able to offer advice directly to the government.

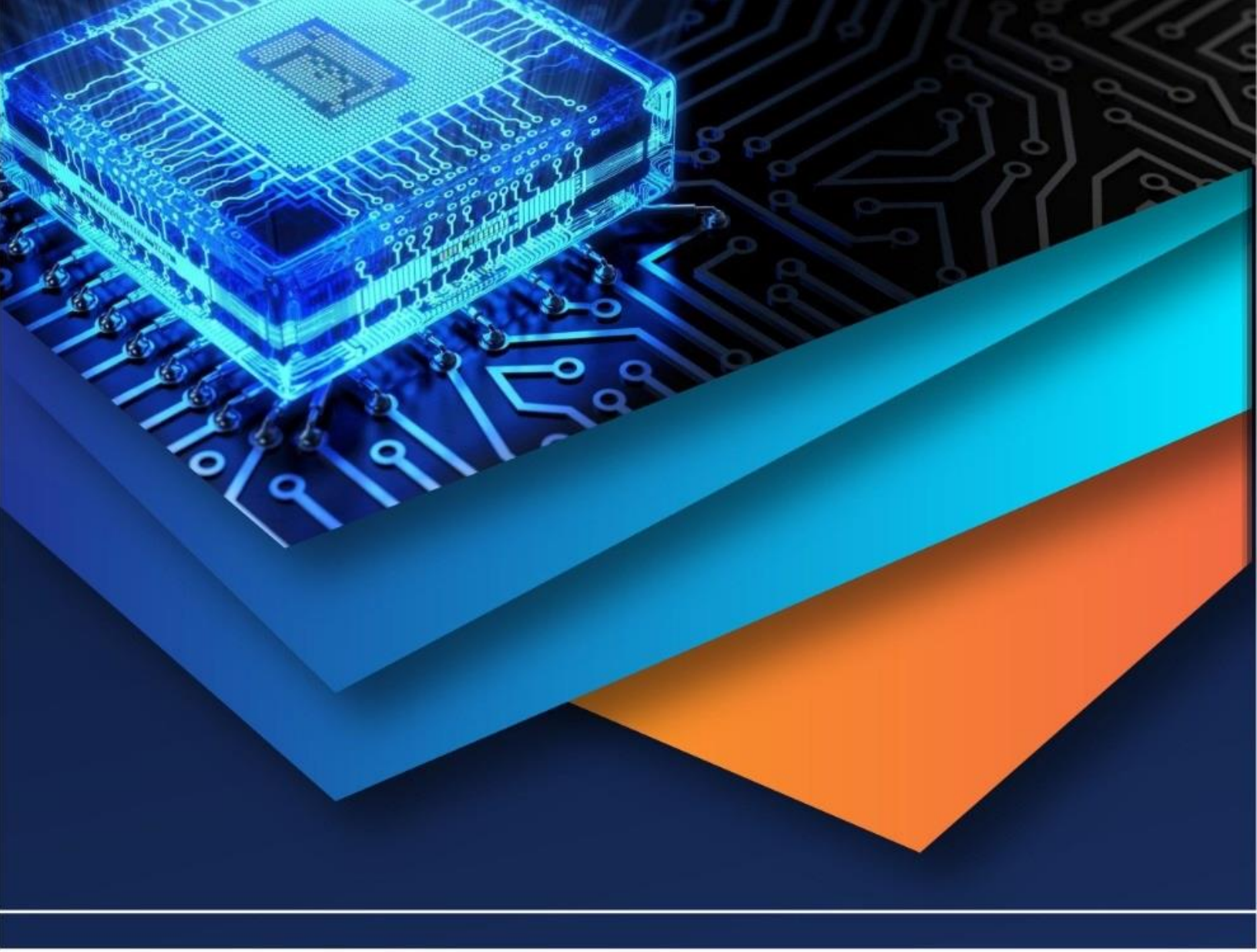
V. CONCLUSIONS

With the start of the 21st century, modern societies have a growing dependency on information and communication technologies that are globally networked. However, with this growing dependency, new threats to network and information security have emerged. There is a growing misuse of electronic networks for criminal purposes. In this paper concepts related to Security and Security Incidents are discussed including Security components Confidentiality, Integrity, Availability, Identification and Authentication, Nonrepudiation, Access Control, Accountability, Various definitions of Security, Security Incidents as Intrusion and Attacks.

REFERENCES

[1] Lehtinen R., Russell D., Gangemi G.T. (2006) "Computer Security Basics" 2nd Ed, O'Reilly, Sebastopol CA.
[2] Rothke B. (2005) "Computer Security: 20 things every employee should know" 2nd Ed, McGraw-Hill, USA.
[3] Australian Computer Emergency Response Team, (2004), "Computer Crime and Security Survey", Queensland University, Brisbane, Australia.
[4] Berger M.A. (2003), "Password Security is a Must for Any Organization", Computers in Libraries
[5] Loeb M., Gordon, L. (2004) "CSI Computer Crime and Security Survey: The 2004 Annual Computer Crime and Security Survey." Computer Crime Research Centre. PRnewswire. http://www.crimeresearch.org
[6] "Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime." Council of Europe Octopus Program. http://www.coe.int
[7] Poulsen, Kevin. (2004) "US Defends Cybercrime Treaty. Security Focus." The Register. http://www.theregister.co.uk
[8] Rae A & Wildman L (2003). "A Taxonomy of Attacks on Secure Devices." Proceedings of the Australia Information Warfare and Security Conference 2003. Adelaide: Australia.
[9] Kjaerland M.(2005) "A taxonomy and comparison of computer security incidents from the commercial and government sectors" Computers and Security.
[10] Maria (2004) "Analyzing Cyber Incidents"
[11] Maria Kjaerland "Approaches For Analysing Cyber Incidents"

[12] Hansman S., Hunt R., (2005) "A taxonomy of network and computer attacks". Computer and Security
[13] Pfleeger, Charles P., and Pfleeger, Shari Lawrence (2003). "Security in Computing" – 3rd Edition. Upper Saddle River, NJ: Prentice Hall.
[14] Mirkovic J., Reiher P. (2004) "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM CCR
[15] C. Douligeris , A. Mitrokotsa, (2004) "DDoS Attacks and Defense Mechanisms: Classification and State-of-theart," Comp. Networks
[16] Jones, Andy. (2004) "Anonymous Communication on the Internet." http://www10.cs.rose-hulman.edu
[17] Carfano James (2008). "Combating Enemies Online: State-Sponsored and Terrorist Use of the internet." http://www.heritage.org
[18] "Critical Infrastructure Threats and Terrorism." (2009). http://www.fas.org



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY