International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Current Network Security Issues and Solutions

Jaspreet Kaur[1], Mandeep Singh[2]

[1]*University College Of Computer Applications, Guru Kashi University, Talwandi Sabo (Punjab)*

[2]*DAV College, Bathinda (Punjab)*

ABSTRACT

With the evolution in nature and requirement of network security there are many factors contributing to these changes, most important is the shift in focus from so called network level threats such as connection oriented intrusions and Denial of services (DoS) attacks to dynamic, content based threats such as viruses, worms, Trojans, spyware and phishing that can spread quickly and indiscriminately and require sophisticated levels of intelligence to detect. This paper provides an overview of the most common network security threats and its solution which protects you and your organization from threats hackers and ensures that the data travelling across our network is safe.

Keywords- Audit, Firewall, Security, Vulnerability

I. INTRODUCTION

Computer and network security is new and fast moving technology and as such is still being defined and most probably will always "still defined". Security threats and incidents are arising on daily basis or year by year. As the complexity of network attacks and threats increased so the security measurement is required to protect networks. Securing a modern business network and information technology infrastructure demands protective measures associated to network security vulnerabilities.

Today security problem becomes one of the main problems for computer network and internet developing. However there is no simple way to establish a secure computer network. In fact we cannot find a network in the world which does not have a security holes now-a-days. The infrastructure of cyberspace is vulnerable due to three kind of failure: complexity, accidents and hostile intent. Hundreds of millions of people now appreciate a cyber context for terms like "VIRUSES", "DENIAL OF SERVICES", "PRIVACY", "WORMS" more generally attacks so far have been limited.

Protecting infrastructure systems involves five coupled stages first it's necessary to attempt to deter potential attackers, second if attacked the need is to prevent damage, third since success cannot be guaranteed in prevention next stage is to limit the damage as much as possible, fourth stage having sustained some level of damage from attack the defender must reconstitute the pre-attack state of affairs and last step is for defender to learn from failures. The more specific defense to be discussed may be useful portioned in to two forms:

Passive defense- Essential consists in target hardening.

Active defense- In contrast, imposes some risk or penalty on the attacker. Risk or penalty may include identification and exposure investigation and prosecution or pre-emptive counter attacks of various sorts.

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

II. NETWORK SECURITY AND PREVENTION TECHNIQUES

There are several major drivers that are shaping the new security landscape:

A. *Increasing complexity of networks:* Where a network 10 years ago might have consisted of a LAN connected to the Internet through a WAN connection, and maybe a few remote access or site-to-site VPN tunnels, the reality today is much more complex. A common environment today will have multiple access mechanisms into the network, including 802.11 wireless LAN (with myriad Client devices including portable computers, PDAs and Smart Phones), web portals for partners and customers, FTP servers, email servers, end-users using new communication platforms (such as Instant Messaging) and peer-to-peer applications for file-sharing. An example of such a network, and the threats that are present, is illustrated in Fig. 1. In addition, the workforce is becoming more mobile. From telecommuter's who work from a home office to mobile workers who are never in a single location for more than a day, this growing "distributed" model adds a significant amount of risk to the network. To help mitigate these risks, the IT manager must ensure that all remote locations and remote clients are protected with the same level of security as is present in the corporate network. Finally, threats are just as likely to come from inside the local network as they are from the Internet. One trend alone overshadows all others in this regard users are taking their laptops home at night and over the weekend, where they are at increased risk of becoming infected or compromised. When the laptops are brought back into the office, the entire network is at risk since the user entered the network "behind the firewall". This is one of many reasons that an emerging "best practice" in secure network design is to segment the network into separate "security zones" (by physical or logical segmentation) such that attacks can be contained in the event of an outbreak.

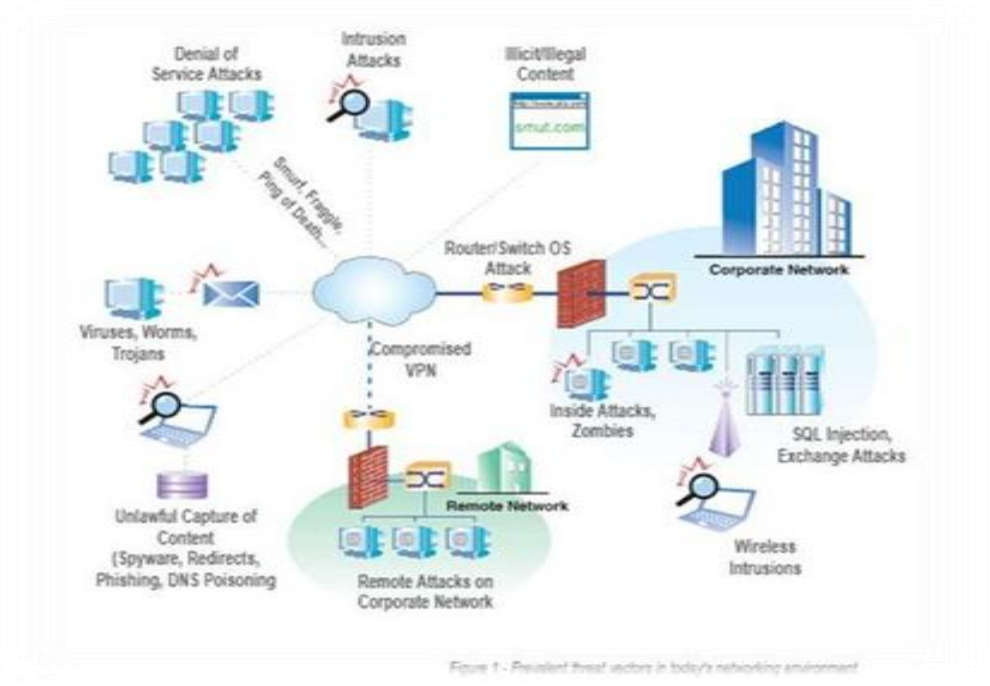

Fig. 1: ***Prevalent threat vectors in today's networking environment***

B. Increasing sophistication of applications and attacks: Applications are growing in complexity. Where Windows NT launched with 5million lines of code in 1994, Windows Vista has over 50 million more than 1000% growth! With this increased complexity comes increased vulnerability, particularly in server systems, which must be patched on a regular basis. While applications are becoming more sophisticated, so are the attacks. A "serious" attack in the early 2000's might have consisted of a simple indiscriminate DoS attack aimed at restricting or temporarily disrupting network access. Today's serious attacks target applications themselves, and in many cases have goals of significant criminal intent, as is demonstrated by the Sasser worm described.

C. Intrusion Attacks, Worms and Trojans: The "grand-daddy" of them all, the universe of Intrusion attacks is wide and deep. Intrusion attacks are modern threats that target applications and application layer protocols (e.g. using the SMTP protocol to exploit a buffer overflow on an Outlook Exchange server), rather than the networks they are transported on (e.g. DoS attacks that utilize ICMP echo and TCP SYN floods). Examples of common intrusion attacks are Worms, Trojans, web site cross-scripting, SQL injection and tampering, Outlook Exchange server attacks, Apache/IIS buffer overflow attacks, file-path manipulation etc. The Sasser worm, described below, is a classic illustration of an Intrusion attack carried out by a worm. As the Sasser example shows, modern threats are designed to bypass traditional firewalls completely, and instead require an entirely new set of technologies to detect and stop them. An interesting side-note: Sasser also eluded majority of Anti-Virus scanners, which is one example of why AV alone is no longer sufficient protection for Worms and Trojans. As discussed later in this paper, the new technology required to protect against modern threats is Deep Packet Inspection (DPI). DPI gives a security appliance the ability to look not only at the packet headers (like a firewall) but at every bit in the packet payload itself, often across multiple thousands of packets, to detect threats.

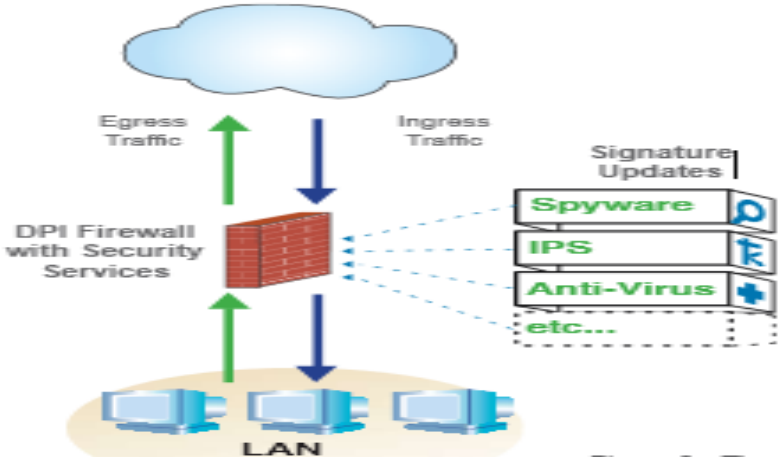

Fig. 2 ***The security appliance is now a dynamic system that requires regular signature updates***

D. *Viruses:* Viruses (and Worms) are a class of attack whereby an infected attachment or download causes damage to a host system or network. The damage can range from minor (client DoS attack) to catastrophic (full-

blown corruption of critical stored information or system registries). A critical trend that is resulting from the increased sophistication of Viruses is the rapidly decreasing "window of infection". In July of 2001, it took the Code Red virus just under 6 hours to infect 359,000clients. Just eighteen months later, the Slammer worm infected 75,000 clients in under 30 minutes. The threats are real… and spread fast. Security vendors have responded by trying to decrease their own "windows of inoculation" which is the time it takes to detect a threat, issue a patch release, and download it to its host systems under management.

There is also a new class of virus-related attack called a 'blended threat'. A blended threat is a 'perfect attack' whereby a virus is accompanied by a number of other attack and intrusion techniques to maximize penetration and damage. A good illustration of this type of attack is the So Big virus detailed below. So Big and Sasser are good examples of how complicated it has become to detect and prevent sophisticated application-layer attacks. To protect against these types of attack, it is mandatory to have IPS and Gateway Antivirus (GAV) installed and activated in the network, whether it is provided by a Deep Packet Inspection.

E. *Financial rewards for hackers with the advent of Spyware and Phishing:* The Internet has evolved from being a general information source to a critical enabler of international commerce. Because of the sensitive type of information that now flows freely over the Internet, a new breed of threat aims at obtaining this information sometimes honestly and sometimes with malicious intent. Because the information obtained in these types of attacks has value, hackers are being financially compensated for their work, often by major public corporations; sometimes by organized crime. This is a particularly disturbing trend, since it is attracting the best and the brightest one-time programmers into the black-hat world of hacking and malware generation.

F. *Spyware:* Spyware (and Adware) is one of the most misunderstood of the new generation of application-layer threats because there is no consensus on what defines a threat(or more appropriately, what the difference is between 'annoying' Adware and a true threat). There are three general classes of Spyware:

- Harmless-but-annoying: Generally consists of actions such as changing the default home page of your browser, or unsolicited/untargeted pop-up ads.
- Information-collecting: Cookies are the most common type of information collecting mechanism, but simple keystroke and activity loggers are becoming more common. This class of Spyware is generally interested in collecting basic information about you, the sites you visit, and other preferences so that a 3rd party can send you targeted ads or promotions. There is generally not malicious intent, but many would call this an invasion of privacy.
- Malicious: Full keystroke logging and collecting private information with the intent of sending the information to a collection server. The information is collected and sold to 3rd parties who have varying interests. Even today, this type of Spyware can be downloaded instantly on a Client device simply by visiting a URL no further clicking necessary. This type of Spyware is illegal and critical for an organization to detect and stop. To further add to the complexity, there are three major Spyware delivery mechanisms:

A. *Embedded Installs:* The most 'honest' of the three mechanisms, embedded installs are typically Spyware/Adware elements that are embedded into programs or services that are downloaded from the web. For

example, BigCorp.com might pay a bundling agreement with Claria (Gator eWallet), where they pay Claria $1per client install.

B. *Drive-by Installs***:** In this method, a banner ad or popup attempts to install software on a PC, usually through the ActiveX controls distributed within Windows and by default enabled in Internet Explorer. Depending on the security settings on the PC browser, the Spyware downloads silently or was downloaded when the user clicked 'Yes' in the installer dialogue box. In many cases, Drive by's also take advantage of browser exploits that can force an unsuspecting PC browser to automatically download and execute code that installs.

C. *Browser Exploit:* As described above, targets vulnerabilities in the web browser code to install Spyware. A classic example is the Internet Explorer iFrame vulnerability. Because IE is such a targeted browser, many IT departments are migrating to alternate browsers such as Mozilla's Firefox. This is only putting off the inevitable, however, as every browser that gains in popularity will eventually be the target of Spyware attacks.

Spyware is difficult to stop because it requires so many technologies to detect and prevent the exploit. A robust Spyware prevention architecture will consist of both client/server and gateway-based elements. Client and server based Anti-Spyware software will detect and try to prevent users from accessing known bad sites, and to a limited extent provide more advanced functionality to detect suspicious behavior from actual downloads and ActiveX controls. The software will also inspect individual system memory, system registries, start-up files and other stored items to detect and remove Spyware. While necessary, client and server based Anti-Spyware software is not enough. Since Spyware is carried by so many delivery mechanisms and is getting so sophisticated, an additional gateway-based Anti-Spyware element is required. The gateway element not only reinforces URL filtering to prevent access to known bad sites, but provides thorough IPS functionality that detects abnormal behavior from ActiveX Controls and Java Applets and the like, and also provides Anti-virus functionality that inspects attachments for malicious code that installs Spyware. The gateway is also an effective tool for scanning both Instant Messaging (IM) and peer-to-peer protocols/programs, which are a growing target for Spyware and other attacks. Perhaps most importantly, a gateway-based Anti-Spyware solution mitigates the harmful outbound effects of pre-infected client and server devices (that might be attempting to contact a collection server on the Internet to deliver sensitive personal or company data, for instance).

G. *Security as a tool to increase workforce productivity:* One of the most profound impacts of security is how it is utilized across all types of organizations to increase operational efficiencies through enhanced work force productivity. There are two main technologies that are helping achieve this:

- Web Security and Policy Enforcement: It is no longer a secret that a good amount of an average employee's day can be spent online doing non-work-related activities. Web surfing, online shopping, online gambling, stock trading and even online dating are a few of the more common uses of company Internet resources.
- In what many employees might consider a breach of privacy, the company employing URL filtering technology can monitor and report on individual Internet usage, and can also set scheduled restrictions on what types of sites employees are allowed to access throughout the day. If the company is using this type of technology, eSoft highly recommends that the HR department make public notice that this technology is

being used, and also clearly state (in the employee handbook, for example) the rules and restrictions of employee Internet usage. The figure above shows a typical screen end user will see when they are trying to access a site that was banned by an IT department employing eSoft Site Filter technology, described later in this document.URL filtering is also a necessary tool for reducing liability that stems from illegal and unethical use of the Internet in public places or organizations. A classic example of this is where an employee (or Internet café patron, for that matter) is accessing a porn site, and another person walks by, witnesses the activity, and uses the company for emotional distress or a hostile work environment. Libraries and schools, by their very nature, MUST have this type of technology deployed. In addition to workforce productivity and liability protection, URL Filtering technology is also the first line of defense at preventing users from accessing Spyware sites. As noted in the previous section, however, Spyware is a much more complicated problem than URL filtering alone can handle.

- Spam: Spam has grown into a major problem for all companies and organizations. Spam is especially problematic for public email addresses (listed on a website, for instance), or for common email addresses (support@your_company.com). Spam is also the primary delivery mechanism for Phishing attacks, so its importance has grown over the years. In 2006, over 86% of all e-mail was classified as spam. Over 63% of this spam originates from new or unknown sources. Spam is best dealt with at the security gateway. The reason for this is simple…once Spam emails are inside the network, they are already consuming precious network resources (such as storage, bandwidth and mail server CPU cycles).If prevented before they ever get to a mail server, Spam can become a more manageable nuisance and threat. Another reason Spam is best dealt with at the security gateway is the sophistication of the tools and techniques that are possible to implement at the gateway. Technologies such as word filtering, Bayesian filtering, black and white lists, real-time blackhole lists (RBLs), DNS MX record lookups, reverse DNS lookups, sender policy framework (SFP) compliance and other techniques are all mandatory for effective Spam mitigation. A good gateway Spam filter will reject Spam in such a way that the Spammer will eventually remove the target from their Spam list. For many technologies such as Bayesian filtering, it is necessary to have many, many samples of known spam, and known ham (non-spam) to begin the heuristic process of self-learning. This is another advantage of Anti-Spam technology at the gateway, where there is visibility into every email coming into or exiting the network.

III. FOCUS ON SECURITY

The network security program emphasizes to secure a network. The following background formation in security helps in making correct decisions some areas are concept oriented:

*Attack reorganization: Recognize common attacks such as spoofing denial of service, buffer overflow, etc.

*Encryption techniques: Understand techniques to ensure confidentiality, authenticity, integrity. There must be understood as protocol and at least partial at mathematics or algorithm level in order to select and implement the algorithm matching the organizations need.

*Network security Architecture: Configure a network with security appliances and software such as placement firewalls, intrusion detection system and log management.

To secure a network certain skills must also be practiced:

A. *Protocol analysis:* Recognize normal from abnormal protocol sequences using sniffers. Protocols minimal include IP, ARP, ICMP, TCP, UDP, HTTP and encryption protocols SSH, SSL, IP

B. *ACLs (Access Control Lists):* Configure and audit routers and firewalls to filter packets accurate and efficient by dropping ,passing or protecting packets based upon their IP and/or port addresses and state. Intrusion detection/Prevention systems

C. *(IDS/IPS):* Set and test rules to recognize and report attacks in timely manner

D. *Vulnerability Testing*: Test all nodes (routers, server and clients) to determine active application via scanning or other vulnerability test tools and interpret results

E. *Application Software Protection*: Program and test secure software to avoid backdoor entry via SQL injections, buffer overflow etc

F. *Security Evaluation*: Use risk analysis to determine what should be protected and at what cost

G. *Security Planning:* Prepare an audit Plan and report

H. *Legal Response*: Understanding and interpreting the law regarding responding to computer/network attacks corporate responsibility and computer forensics

I. *DoS Attacks*: DoS attacks today are part of every Internet user's life. They are happening all the time and the entire internet user as community has some part in creating them suffering from them or even loosing time and money because of them. DoS attacks don't having anything to do with breaking into computers taking controls over remote hosts over the internet or stealing privileged information like credit card numbers using the internet way of speaking DoS is neither a hack nor a crack . The sole purpose of DoS attacks is to disrupt the services on the internet. Dos attacks are real vandalism against internet services.

Some solution to DoS Attacks: The way DoS and DDoS attacks are perpetrated, by exploiting limitations of protocols and applications is one of the main factor why they are continuous evolving and because of presenting new challenges on how to combat or limit their effects. Even if all of these attacks cannot be completed avoided some basic rules can be followed to protect the network against some and to limit to extent of attack:

- Make sure the network has firewall up that aggressively keeps everything out except legal traffic
- Implement router filter this lessons the exposure to certain denial of service attacks
- Install patches to guard against TCP/IP attacks. This will substantially reduce the exposure to these attacks but may not eliminate the risk entire
- Observe the system performance and establish baselines for ordinary activity. Use the baseline for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage or network traffic

IV. CYBERSPACE IS VULNERABLE

The infrastructure of cyberspace is vulnerable due to three kind of failure: complexity, accident, and hostile intent. Very little of it was designed or implemented with assurance or security as primary considerations. Bad things can be done either via network infrastructure or to the infrastructures themselves. These bad things can be characterized by a lot of words destroy, damage, deny, disable, disrupt, distort, degrade, delay and disconnect. We lack a comprehensive understanding of these vulnerabilities.

Absolute defense against cyber attack has rare if ever been achieved in large complex, geographically distributed networks. The complexity of such systems and modes of attack are such that we don't know precisely how to assess and secure them are and this lack of understanding forces defenders to protect themselves in overlapping and in multiple stages. Risk or penalty may include identification and exposure investigation. There will be other tradeoffs, e.g. between detailed and potential cost of individual transaction and waiting to identify and punish attackers over the longer term.

Government will pursue policies that focus on longer term, aspects of protection, seeking to reduce cumulative losses, protecting economies and national security and maintaining law and order.

Protecting Network Boundaries with Firewalls: A Firewall is mechanism by which a controlled barrier is used to control network and out of an organizational internet. Firewall is basically application specific routers. The firewall process can be tight control what is allowed to traverse from one side to another side. Firewalls can range from fairly simple to very complex.

As with most aspects of security, deciding what type of firewall to use will depend upon factors such as traffic levels services needing protection and complexity of rules required. The greater number of services that must be able to traverse the firewall the more complex the requirement become. The difficult for firewalls is distinguishing becomes are distinguishing between legitimate and illegitimate traffic. What do firewall protect against and what protection do the not provide?

If firewalls configured correctly they can be reasonable form of protection from external threats including some denial of services attacks. If not configured correctly then it can be major security holes in organizations.

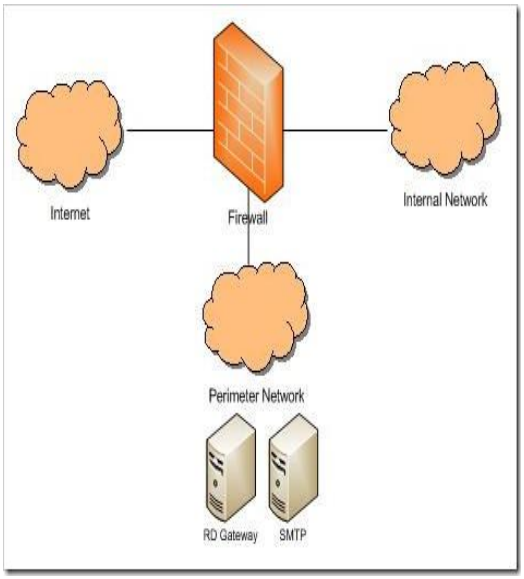

Fig. 3

V. PREVENTING AN ATACK

There are at least three ways to prevent an attack and all three are ultimately formed of active defense. One is to deter the attacker by having demonstrated capabilities to punish the attackers. This implies that attacker understand the risk of being identified and located that the defender is seen as credible in a resolve to punish and

that the cost of punishing is acceptable to defender. A simple situation is when the attacker suffers a large front end loss through discovering during the probe phase and defender can accomplish that discover cheap. When the cost to develop ways of discovering attackers. But the more common situation is when the relatively high costs of legal persecution of single attacker are returned in reduced losses over the longer term.

Second way is to prevent an attack is through establishing cyber attacks as unacceptable behavior among the community of nation.

Third way to prevent an attack is to pre-empt the attacker in ways that the result in abandoning the attack. This implies a great deal by way of national surveillance capabilities to be able to provide strategic warning. So stealth are cyber attacks so widespread is the ability to plan and launch them, so inexpensive are the tools of attacks that pre-emption would not appear to be a practical option at this point. But Should responsible norms of behavior in cyberspace becomes better established the detection and identification of abnormal behavior may become easier.

VI. THWARTING AN ATTACK

While preventing attack is largely based on government authority and responsibility the detailed knowledge need to thwart an attack on cyber system to prevent damage rests primarily with its owner. The least complicated case is where the system owner acts individually. Not only must the owner be concerned with defense from outsider, but also need to be recognized that not all authorized users of system may have the owner's interests at heart. There are many ways of defending system against cyber attack and some minimal number must probably employed for the owner to demonstrate due diligence.

This technique such as requiring authorization to center, monitoring the use of system to detect unauthorized activities, periodic checking on the integrity of critical software and establishment and enforcing policies governing System security and responses to unexpected event will be necessary. Owner can limit authorization activities through compartmenting information within the system and maintaining need to know discipline. Owner can provide themselves substantially more rights to monitor inside user by covering access through contractual terms with employees and vendors.

VII. RECONSITUTING AFTER AN ATTACK

Short term recognizaton is set of first steps taken to meet the most urgent threats to life and property. They include assessing damage and implementing an appropriate cover plan. System is restored from backup where possible and residual resources may have to ration. It's possible that additional capacity can be generated as facilities that are idle or in maintenance are brought on line. Online status reporting dispatching of emergency personally and repair equipment notification of users possible lost transaction, an ability to adjust plans in near real time and procedure for secure emergency communication will be required.

VIII. HALTING CYBER ATTACKS IN PROGESS

Along with the sharing of information system administrator also need procedure the can use to assist in ending attack already under ways. This need is particularly evident in DoS attacks, which can be of extended duration

and which can shut down business operations while they occur. To aid in ending an attack system administrators would profit by working with infrastructure operators to trace the attack to its source and then to block the attacker. Methods for halting attacks in progress as well as those for investigating attacks are constrained by the inability to easily identify and locate attackers. In the case of internet because packet source addresses are easily forged the only way to identify and locate attackers with confidence is to trace the path by packet through the routing infrastructure.

IX. CONCLUSION

The security issues in our networked systems as described in this paper identify some of the work to be done and the urgency with which concern need to be addressed. Dependence on some of the IT-based infrastructures in several countries is such that serious national consequences could result from the exploration of their vulnerabilities and as the density of network increases the necessity for transnational participation in improving network security increases. The changing technologies and the potential for changing threats is taxing our understanding of threats and how to deal with them. Due to complexity and entanglement among networks and communities internationally an increase in network security must involve the concentrated efforts of as a many nation as possible.

REFERENCES

[1] "Google Query-serving Architecture" at national conference sponsored by NACC by dixit @ DR.R.K.DIXIT

[2] Intrusion Control in computer network; Published in National seminar sponsored by higher education of M.P.

[3] www.abanet.org/scitech/computercrime/cybercrimeobject.html

[4] Batista E; IDC; Tech Bucks; Hack threats Up Wired news; 23 December 2002

[5] Council of Europe, convention on cyber crime; ETS no: 185- Explanator report (Article 2 section 2); 23 November 2001: http://conventions.coe.int/treat/en/reports/html/185.html