JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Issues in WA networks and Protection Related Phenomena

[1]Chinu Mog Choudhari, [2]Sunita Debbarma

[1,]Assistant Professor, Department of Computer Science and Engineering, TIT, Narsingarh, Tripura, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, TIT, Narsingarh, Tripura, India

***Abstract*—Advent of huge present networks and their proper usages at the end users have become real challenges. The protection and services to the organization have never been in its level. Users are demanding high bandwidth in the network service and the exchange of more potentially sensitive information within these services. Firstly, in any organization there is definite requirement of the network access [3-4]. In order to enable users to go beyond the limitations of space and time to acquire net savvy works; in order to provide excellent access environment for greater freedom and greater choice of acquiring activities, this paper serves the problem at its network kingdom. It is related to the quality and level of their savvy work. All organizations have plenty works to be done, viz. research, management, communication, compilation with the outside world. Therefore, the issue of network protection has become a priority to WA (Widened Area) network management. Obviously, the current Internet is convenient but at the same time it is unsafe. While using network services, it is very access venerable . This paper represent the current protection status of the WA network, analyze protection threat to organization and describe the strategies to maintenance of network protection, so as to maintain an effective as well as robust network system. There is always Protection threat [1] in the WA network. So, high firewall and security steps are not ample enough to resolve the present huge network. This paper will also introduce various current network informationprotection problem and its solutions.**

***Keywords*— Widened Area network, Network protection, access venerable, Protection threat, Firewalls, security steps.**

I. INTRODUCTION

Exchange of information among people had been very important role from the age of civilization. No matter how the exchange may be, but there had been always an effort to protect the information. Similar to ancient era network protection threat it had been a regular serious issue and is very crucial. As we are aware about the present network, which include, internet connected devices like multi cellular, wireless router, cell phone, PDA (Personal digital assistant)[1-5], smart TV which are being connected via WiFi, Bluetooth or a physical connection like a USB cable. An organization network is an autonomous network under the management of commercial organization or within a local geographic area such as a business park, a government institution, a research centre, or a medical centre. While the network may be managed by a single entity, it may be used by different organizations. The organization network has matured and grown more complex than ever. Often, a organization network provides and access path into a larger network, such as a metropolitan area network or the Internet. To build a stable, safe, efficient, convenient wireless organization network has become the inevitable trend of development and construction of organization network.

Computer network administrator faces many challenges in the process of maintaining high availability, good performance, and protection. In a network there are several user groups which have different set of resource accessibility. Network operators may wish to allow only certain users access to various parts of the network; they may also aim to prevent certain sensitive data from “leaking” between different parts of the network, or from the internal network to the global Internet. It is difficult for network administrator to translate these types of high-level policy and design goals at level of individual devices, not based on a global perspective of the network.

There are two primary goals to design a data sharing system in organization network: First, from a user's perspective, users must have control on their data sharing system through which they can decide which web site they want to share and should also be aware of what happened to their data. Second, in organization network design, existing infrastructure must be utilized.

With the rapid expansion of the organization network connectivity, the network applications have increased rapidly, at the same time, the

organization network information protection has caused more attention today. Two areas where high-level problem is particularly acute are access control (defining who has access to what information and services on the network) and information flow control (defining where on the network, various information should be allowed to travel).

Almost no protection measures has been taken in the existing network and application systems, and above this, protection vulnerabilities in the host operating system and application system are also without any processing. There are many problems within system management; all of these formed a serious protection problem, thus seriously threatening the safety of the organization network. In the recent network monitoring, system and the host was found to attempt to be invaded by others, a large number of protection vulnerabilities exists in the system, and there are many protection vulnerabilities which are difficult to avoid and eradicate. Also, a virus transmitted through the network severely affected the normally running of the organization network . Network traffic consumption attacks are another serious threat for network management. These attacks (e.g. Distributed Denial of Service attacks, Smurf Attack, TCPSYN Flood attack) are passive network attacks where network traffic is consumed up by unnecessary flow of data, preventing legitimate user to use network path. In this attack speed of network traffic is slow down to such a level that user cannot use network resource.

Poor network protection means that an external hacker break into a computer. on network, then they can access the rest of the internal network more easily. This would enable the attacker to read and possibly leak confidential emails and documents; trash computers, leading to loss of information; and more. The University network must be kept secure. Protection concerns involve protection of central data files, host computers and the network itself. Tracking of virus infections, compromised computers, and collaborating with other sites to isolate problems is an ongoing task. The technique most often used when problems occur is to quarantine the problem computer from the remainder of the University network by disabling its network port. This happens daily and sometimes many times each day during virus outbreaks. Clearly, a single-port model minimizes the interruption of services in a protection incident. With network authentication, it will be possible to contact the person responsible for the computer to announce that the device has been quarantined, thereby saving time and confusion for the user. The organization network faces a serious protection

situation. The organization network has been acongregation of hackers. This is because the virus and hacker tools are spreading and most users are unconscious about protection.

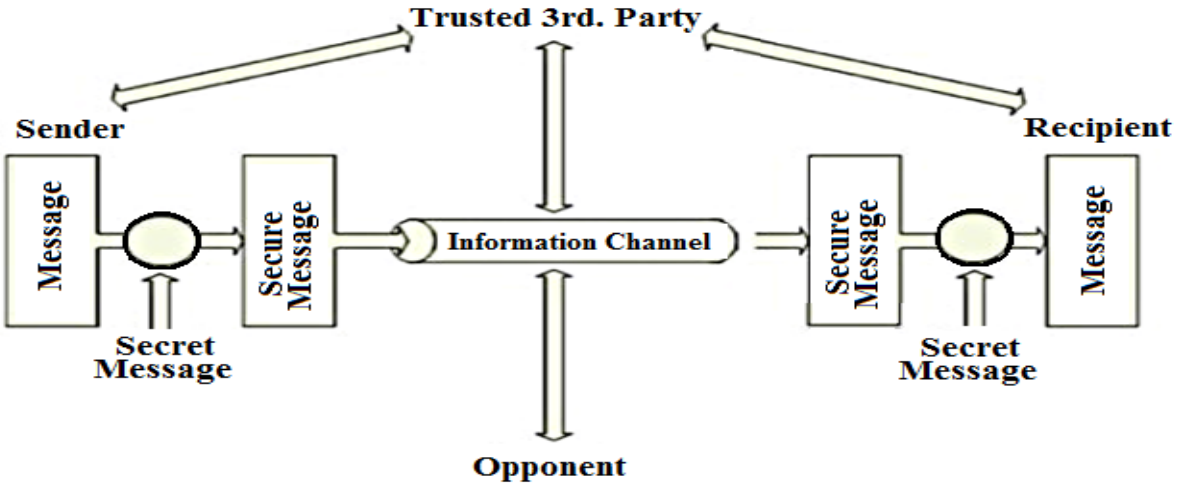

Fig. 1 Network protection plan

II. CHALLENGES IN ORGANIZATION NETWORK

The access of vulnerable organizational networks are the type of media to be used between Wide Area Networks [6] (WAN), network hotspots, outside cable specifications, rights-of-way, avoidance of natural barriers, underground or aerial cabling requirements, line of site for inter organizational wireless transmissions, and protection problem. Figure 1 shows classification of protection threats. In organization network if cable is open than it can be tapped or cut. A user within the company can access many internal resources. There may be no any bypass firewalls or other protection mechanisms which prevent non-trusted sources, such as Internet users, to access the internal network. Such type of internal users can be equipped with hacking skills, and they can successfully penetrate and achieve remote administrative network rights. In fact number of network attacks originates from inside the firewall.

In addition, college students are energetic and curious about new things. They have high intelligence and passion, but lack of the responsibility for the results of their behaviour. Malicious attacks of organization network are from the internal network. Wireless link makes the network more vulnerable from passive eavesdropping to active interference have variety of attacks. Since wireless networks transmit data through the electromagnetic waves in the air, within the transmitter coverage area all of the wireless.

Network users in organization can access to these data, as long as the frequency with the same receiver may get the message. In Organization WLAN, the threat that can be encountered mainly in the following areas:

information disclosure, integrity destruction, denial of service and theillegal use of it. In general, network traffic is non- encrypted format, the attackers can easily monitor and crack wireless network communication packets. Intrudersdo not need to trap the eavesdrop or analytical equipment physically access the network, so the threat has become one of the biggest problems of wireless local area network.

III. PROPOSED SOLUTIONS FOR ORGANIZATION NETWORK INFORMATION PROTECTION

To build more protection robust organization network, we should analyze protection risk, and on the basis of that, prepare unified plan to take action. We should adopt more and more advanced technology generously in our network e.g. Firewall technology[3-7], virtual Local Area Network (VLAN), encryption technology, Virtual Private Network (VPN), multiple operating system atserver side, etc.

In organization network we can use virtual private network (VPN) technology which uses special software on each computer (i.e. VPN client), to encrypt network traffic from that computer to a VPN concentrator on the institution's network. Generally, we do not use VPN on- organization, as the functionality that VPN provides is already present on organization. However, it would be more theft and misuse proof on Wireless Network. It can also be used to authenticate via VPN. Through VPN, member of organizationcomputer can connect securely.

WLAN (Wireless Local Area Network) technology played an important role in promoting the development of organization information technology, and it is an important component in organization network. WLAN reduce the workload of the network cabling. Once it is completed, itbecomes very easy to the users to access the network at any location in the organization.PKI technology, and achieve centralized configuration, monitoring, management. Finally, we should strengthen formulating of systems and specifications about the network protection.

Any user, user group, or department wants to establish its own local area network or to establish connectivity to external data communications networks must assign a member of that user group or department to coordinate with Network Services and obtain approval.Colleges and Administrative units may create sub domains within organization network. Sub domains usually encompass multiple departments which have a need to share common information. System [8] should automatically alert the protection event to the user, if protection problem is detected as well as user should be isolated to the recovery area or block the data flows according to the user ID Computer viruses and worms are the most common protection problems in organization network, and these viruses are written for any operating system to exploit protection flows. Different viruses are written for different operating system that can run on particular type of operating system (For example Linux-Unix, Microsoft Window, MAC OS etc.). Therefore two types of operating systems (having different kernel architecture) should be used in server centre in pipeline, allowing all traffic to go through this pipeline and activity analysis should be done on both systems separately. Unused port should always be closed on server. Improper use of the protection settings will also increase the protection vulnerabilities.

In addition the operating system's protection problems generate from the virus threats. Hackers [5-7] penetrated the network to destruct the data. Network antivirus tools must be effective and kept updated to protect all possible virus entry from the internet. Anti-virus program should be installed for online virus detection and the virus clean-up or tracking. Intrusion detection sensors should be placed at the organization border to identify computers[9-11], generating infected and malicious traffic entering or leaving the organization computing network. A network honey pot should also be placed on an unused network segment to

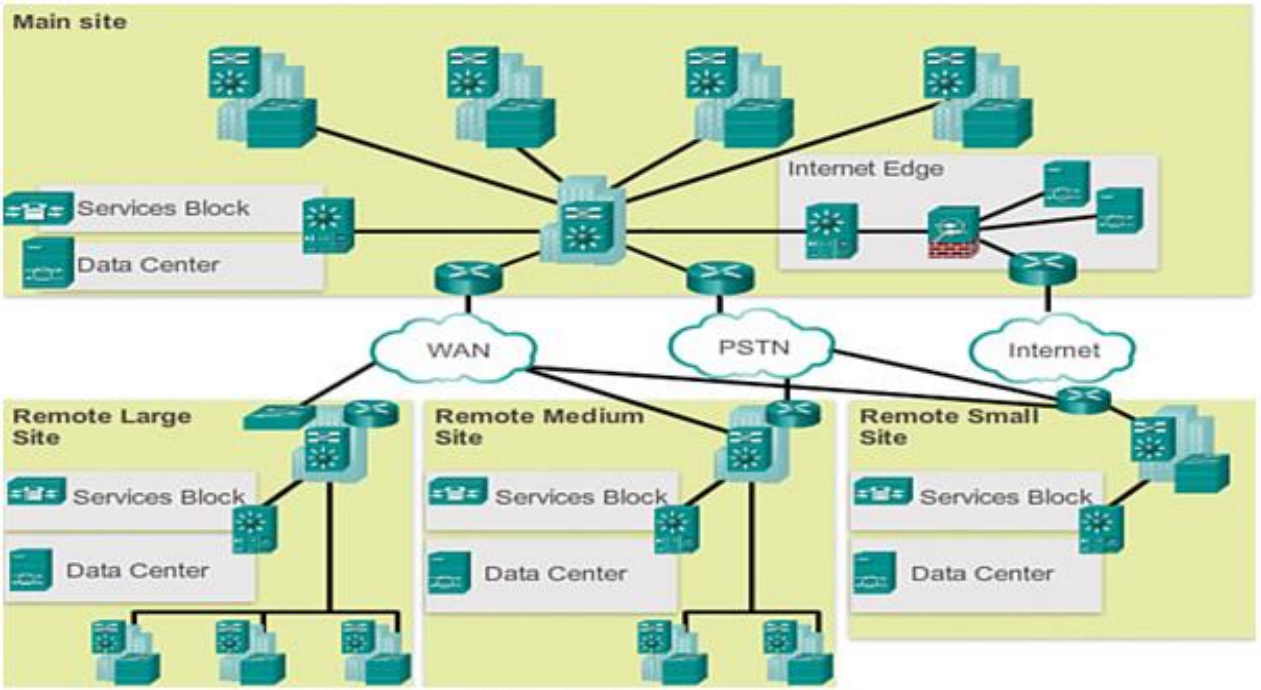

Fig. 2 Hierarchical Network Design

identify infected computers attempting to scan or connect to

non-existent hosts. Figure 2 shows a Hierarchical network design for organization network establishment

The network protection must be all-around the organization. More network protection measures must be in the important areas such as network outlet, data center, and servers. After that both the access or backbone equipment must be equipped with strong defense ability, and the deployment of protection policies must not affect the network performance or cause single point failure. Overall the protection must be deployed globally to cover every aspect, from access control, detailed detection of protection events, and collaboration of existing protection equipment, to accurate location of threat source and isolation and recovering according to user ID, further the entire protection structure of the network is formed from internal to external network.

Therefore, in the protection deployment some key areas like outlet, protection measures shall be extended to the whole network to make a big move beyond the equipment level protection, rather than enforce the protection strength of single local points.

IV. CONCLUSION

In short, by providing network protection in organization, the users can work; achieve performance, research at anytime, anywhere in organization. A secure network plays a vital role for promoting the development of organization information and digital organization construction. This paper proposed a viewpoint from access control, data sharing management, content filtering, data encryption, user management, permissions distribution, log auditing, and several other protection issues. As network protection has become more and more important, the proper protection have to be built to achieve the open and secure network environment we aimed for.

REFERENCES

[1] Saadat M. Network Protection Principles and Practices (CCIE Professional Development) (CCIE Professional Development) (Hardcover) [M].Cisco Press, 2020: 52-78.

[2] William S. Network Protection Essentials: Applications and Standards (3rd Edition) (Paperback) [M]. Oxford:Blackwell business, 2016: 15- 47.

[3]Mark R, Roberta B, Keith S. Network Protection: The Complete Reference [M]. Osborne: McGraw-Hill Osborne Media, 2017- 11-17.

[4]Kwot T.Fung Network Protection Technologies, Second Edition [M]. AUERBACH,2014/10/28, 11-123.

[5]Joel S, Stuart M, George K. Hacking Exposed: Network Protection Secrets & Solutions [M]. McGraw-Hill, April 2021:23-126B. Harris, R. Hunt. TCP 1 IP protection threats and attackmethods .Computer Communications, 2015, (22) :Page.885-897 .

[6]Venter H S, Eloff J H P. Data packet intercepting on the internet: how and why? A closer look at existing data packet -intercepting tools .Computers & Protection, 2021, 17(3):683-692 .

[7]SHEN ChangXiang, ZHANG HuangGuo et al. Survey of information protection. SHEN ChangXiang et al. Sci China Ser F - Inf Sci I June 2017 I vol. 50 I no. 3 I 273-298

[8]Yong Yu, Wireless Distribution System Management ,WHUT,2020.5

[9] N.A. Giacobe, Application of the JDL data fusion process model for cyber security[J]. Proc Spie 7710(5), 1–10 (2010)

[10] Goodall J R. Introduction to visualization for computer security[A]. The Workshop on Vizsec[C]. DBLP, 2018.1-17.

[11] Z. Li, J. Taylor, E. Partridge, et al., UCLog: A unified, correlated logging architecture for intrusion detection[J] (Telecommunication Systems – TELSYS, 2014), pp. 12–27