Capabilities of existing network architecture model and ways to mitigate cyber attacks

Prof. Partha Shankar Nayak
Dept. of Computer Application
Bengal School of Technology and Management
Chinsurah, Hooghly, WB, India
psnayak2007@gmail.com

Mr. Shrikant Sharma, Mr. Shashi Kumar Sharma
Bachelor of Computer Application
West Bengal University of Technology
Kolkata, India
shrik36@gmail.com, shashi.2302@gmail.com

***Abstract*— Focus on robustness and capabilities of existing network models and its implementation in banking, military and other organization to withstand cyber attack. Our detailed diagram/model is a new approach to secure the network by covering the entry vaults and effectively mitigating attacks. We will also discuss about how MAC address of every devices or user on network can be useful in preventing attacks.**

***Keywords-network access model; computer network; cyber attack; network security; cyber attack mitigation*.**

I. INTRODUCTION

Detecting the vulnerabilities and loop holes in the existing network is the only way of making network system secure. Ageing of the existing network architecture and technologies of the devices have limited the securities of the existing system [1]. Vulnerabilities have increased and network is becoming more prone to attacks today. The most hazardous deeds over the network are happening today when almost the whole world is moving towards network based system (for example, Cloud Computing) and many of them who are already digitalized are working on protecting them. But more or less, the architecture and protocols upon which this network is established is same. This implemented architecture has been designed keeping its application is mind and unfortunately, not the security [4]. We can see the data collected from the report of Yves Younan, Senior Research Engineer, Sourcefire Vulnerability Research Team (VRT) 1988-2012 that as the dependency over the network increased, its vulnerabilities also increased along with the benefits [2]. This is now taking the organization into significant or data mishandle loss.

According to the "12th CSI computer crime and securities" report published in 2009-10, 45.5% of the respondents were the victim of at least one target attack. Of all the attack all around the world, 33% cases are from financial organization like banks and 23% are from hospitality industry. This accounts more than half of the total cyber attacks [3]. Report also says that in order to target customers, home or general user, fake antivirus programs were created and made available on the Internet. 40% of the antivirus programs that were created in 2010 were fake ones. This caused attack to 5.4% of the PCs. This illustrates deficiency in existing network model devices, firewalls, and protocols to withstand attack and provide network security.

There is a need of thorough research into network access models as current system and protocols are ageing. Development and upgrading are done upon the existing system which is making easy for the attackers. Upgrade of the existing network system is done to manage the loop holes in the existing system, and on the existing system, ways or options are less i.e. managing here acts as patch up the existing system, which will only help in saving the system from further attacks. This is not the perfect or concrete solution to the present system. We know the problem, and so do the attackers. If we overcome or secure it by patching up the existing system, then we must also think, for how long it is going to hold the attackers away.

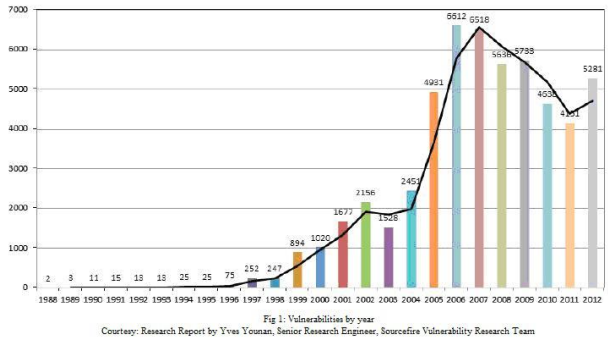

Fig. 1. Vulnerabilities by year

Source: Research report by Yves Younan, Senior Research Engineer, Sourcefire Vulnerability Research Team

The National Computer Security Centre, USA, the official evaluator for the US Defense Department, maintains record of an Evaluated Products List of commercial systems that it has rated according to the criteria [5]. According to them, a network access model should follow a verified design, which has formal top-level specification and verification, formal covert channel analysis and informal code correspondence

ISBN: 978-81-923777-9-7

demonstration. We will be following this NCSC criterion for developing our network access model.

TABLE I. NUMBER OF ATTACKS DISCOVERED IN YEAR 2012
COURTESY: WWW.HACKMAGEDDON.COM

Months(in 2012)	Cyber Crime (in percentage)	Hacking Activities (in percentage)	Cyber Warfare (in percentage)	Spying (in percentage)
Dec	47	46	4	3
Nov	69	28	2	1
Oct	58.8	37.7	2.9	1
Sept	55	42	3	1
Aug	58	36	3	3
July	55	31	11	4
June	72	18	6	4
May	61	30	5	4
Apr	51	39	7	2
Mar	68	28	3	1
Feb	59	39	2	0
Jan	53.3	42.6	2.3	1.6
Total (Percentage in 2012)	**58**	**34.775**	**4.266**	**2.133**

II. DEFINITIONS

Computer Network

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

Computer Security

Computer security is what keeps the users on the network safe from any threats, prevent from attacks or unauthorised access, ensures faster transmission with no or least loss of data and maintenance of data integrity.

III. OUR APPROACH

To adhere the securities and data integrities our network model is an approach to benefit by securing areas like financial organization, military, hospitality. This new approach will:

- Make the networks secure.
- Identify the valid user.
- Identify potential threat.
- Have a self managing monitoring system; also explore the capabilities and use of MAC address to authenticate a user.

Our contribution in this paper is to, find the potential attacks and loop holes in the existing system, and also provide a new approach for securing the network [Fig. 3].

We represent the Threat Level (TL) and Data Packet as follows:

Fig. 2. Threat Level (TL=1) + Original Data Packet = New Data Packet

In Fig. 3, the handling of data packets along with allotted Threat Levels at different servers is shown.

An intelligent system is installed on each server over the network. A user is registered to an ISP server. Whatever request user makes through his device, request passes through his ISP server. This request packet is analyzed by the program present on the server. The software program retrieves the packet, checks whether threat level is attached to the data packet or not. If not, then the program understands that this packet is coming from user connected to this server [Fig. 4(a)]. Then server analyses the data packet for any threat on the basis of its artificial intelligence and the threat record present inside the database.

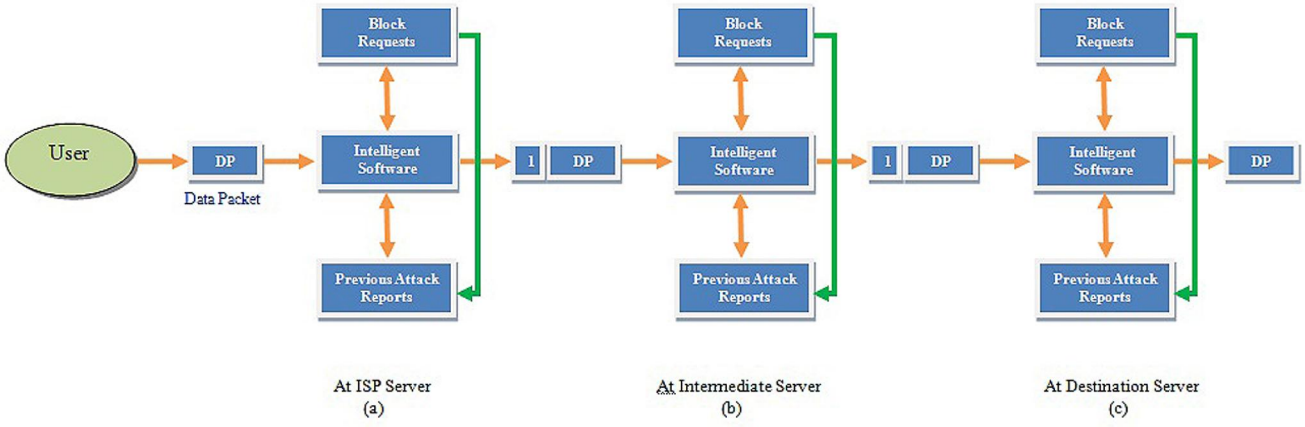

Fig. 3. The proposed Network Access Model

ISBN: 978-81-923777-9-7

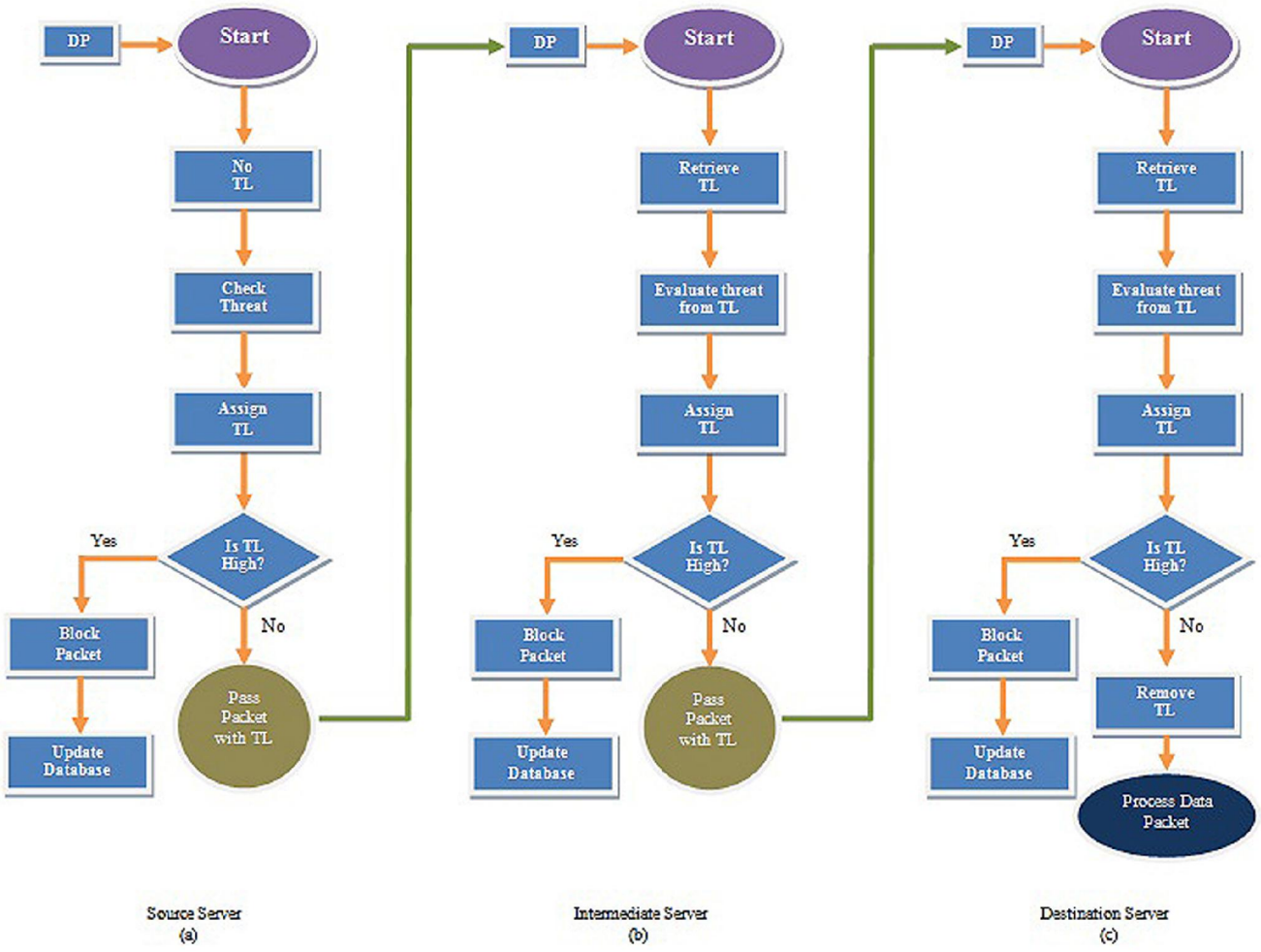

Fig. 4. Decisions taken at various servers

After analyzing, a threat level (TL) is attached to the data packet. This threat level is then checked whether it is high or not; if the TL is high, the program blocks the request and updates the database. In case the TL is low, the program passes the data packet towards its destination along with its TL packet.

When the data packet and its TL packet reach any intermediate server [Fig. 4(b)], the program present inside the server retrieves the packet and evaluates threat possibilities on the basis of the retrieved TL and the threat record present inside the database. After analyzing, the new threat level is attached to the data packet. This TL is then checked whether it is high or not; if the threat is high then software blocks the request and updates its database. In case the TL is low, the program passes the data packet towards its destination along with its TL packet.

When the data packet and its threat level packet reach the destination server [Fig. 4(c)], the program present inside the server retrieves the packet and evaluates threat possibilities on the basis of the retrieved TL and the threat record present inside the database. After analysing, this TL is checked whether it is high or not; if the threat is high then the program blocks the request and updates the database. In case the TL is low, the threat packet is removed from the data packet and the request is then processed by the server.

IV. Determining Threat Level

TABLE II. Attack Table Acknowledgment

Attack	Percentage	Lower and upper bound	Attack level
A1	27	20-29	3
A2	13	10-19	2
A3	40	40-49	5

ISBN: 978-81-923777-9-7

This table contains record of different types of attacks, attack percentage and a bound column that determines the level of attack. The bound column is from 0 to 99, subdivided as 0-9 as 1, 9-19 as 2, 20-29 as 3, 30-39 as 4, 40-49 as 5, 50-59 as 6, 60-69 as 7, 70-79 as 8, 80-89 as 9, 90-99 as 10. Here 1, 2, 3… 10 are different attack levels.

TABLE III. DAMAGE TABLE

Damage Name	Damage Type	Damage Level
D1	Data loss	9
D2	Server damage	8

This table holds the record of damage, its type and level. Damage level is assigned to each damage name according to the damage/loss done to the system.

Threat level TL= (A_x * D_y)

Where x >0 and x<= 10 and y>0 and y <=10.

It will depend upon the Server Administrator or the software developer to set a value for TL between 1 and 10, 1 being the lowest and 10 being the highest Threat Level. When a data packet will reach any intermediate or destination server, it will always hold a threat level with it.

Suppose a data packet is having threat level value as 12. The factors of 12 are {2,3,4,6}, 1 is excluded as because 1*12 not possible.

TABLE IV. THREAT LEVEL CALCULATION

Damage Level	*	Attack Level	Threat Level
2	*	6	12
6	*	2	12
3	*	4	12
4	*	3	12

If attack level value is 2 then damage level value will definitely be 6. So here, our intelligent system can make a very good and precise prediction. Suppose if 6 is the damage level value for data loss and attack level 2 is for SQL injection then software can greedily analyze whether data packet will "damage data saved on server" or not.

V. DISCUSSION

There is a need of software based on Intelligent System that can protect from any new attack. The existing security systems used to protect the systems in the network are developed after the attack events have occurred. Firewalls and antivirus programs have the updates of the attacks that have occurred already. These software programs cannot protect the system from any new attack. Then how will the system be saved from new attack? Here, need of an intelligent system exists. The system we are approaching through this paper has the capability to learn from the previous attacks and implement its intelligence in mitigating any new attacks. There may be possibility that our software may delay the data transfer rate of the server. A server takes time to resolve next address of the data packet leaving the packet idle. We can utilize this idle time in analyzing the data packet to ensure from any threat.

As our dependency on network is increasing, its attack is also increasing. This is making the system insecure, vulnerable tending towards great financial and data loss. There is a need of focusing and determining the capacity and capabilities of the existing system and protocols. These protocols have been designed keeping its application in mind, not the security. The number of the Internet users is increasing every day. This expansion is also increasing vulnerability and chances of attack. So there is a need to think and build up a network system which is reliable, secure, robust, ability to withstand attack, identify them and take appropriate preventive measures. Network access model is also one of the major areas to be focused; every user is connected to the network through the Internet Service Provider that also assigns an IP to a user.

As of now, when an attack happens, we can only identify the attacker through its IP address. What happens in case the attacker has changed its IP address? Here, MAC address can be one of the best data to recover attacker details no matter how much IP is changed. MAC address is unique to a machine. For getting attacker through MAC address, a global database should be maintained which will have MAC address, serial numbers, and details of the user. This can be an approach to dilute the possibilities of attack.

Along with the software for monitoring the network ports and users accessing the network, a more intelligent software program is required which will be helpful in monitoring every request (usual and unusual). This will help the Network Administrator to look for any possible loop hole before any damage.

REFERENCES

[1] http://www.infoworld.com/d/security/news, INFO WORLD, Aging networking protocols abused in DDoS attacks.

[2] Y. Younan, “25 years of vulnerabilities: 1988-2012”, Sourcefire Vulnerability Research Team (VRT™), 2013.

[3] CSI Computer Crime and Security Survey 2010/11 report by Computer Security Institute, 350 Hudson Street, Suite 300, New York, NY 10014. Aired on December 2, 2010.

[4] W. Odom, Official exam certification guide, Second Edition, CCIE NO-1624, ISBN-978-81-317-1572-7, pp. 8-14, ciscopress.com.

[5] US Department of Defense Standard, DoD 5200.28-STD Supersedes CSC-STD-00l-83, Library No. S225, 7ll, p. 18, August 1983.

ISBN: 978-81-923777-9-7