ISSN 2229-5518

Evaluation of security risk associated with different network layers

Arshad Ali, Dr. Mohd. Rizwan Beg, Shish Ahmad, Azhar Ali

Abstract— Managing the security of enterprise information systems has become a critical issue in the era of Internet economy. As any other process, security cannot be managed, if it cannot be measured. The need for metrics is important for assessing the current security status, to develop operational best practices and also for guiding future security research. In this paper we evaluated the different security attacks on the different OSI layers with the help of some operational metrics. In this paper we proposed a model for evaluating the security risk and calculated the high and low probability of risk on each and every layer.

Index Terms— System security, security metrics, vulnerabilities, security management, different threats and attacks, OSI layers.

1 INTRODUCTION

A Network attack or security incident is defined as a threat, intrusion, denial of service or other attack on a network infrastructure that will analyse the network and gain information to eventually cause the network to crash or to become corrupted. In many cases, the attacker might not only be interested in exploiting software applications, but also try to obtain unauthorized access to network devices. Unmonitored network devices are the main source of information leakage in organizations. In most organizations, every email message, every web page request, every user logon, and every transmittable file is handled by a network device. Network attacks cut across all categories of software and platform type. There are at least two types of network attacks —

1.1 Active Attacks

Active Attacks: Active attacks are attacks in which attacker is not only being able to listen to the transmission but also being able to actively modify or generate false data. Types of Active attacks are:-

1.1.1 Masquerade

A Masquerade takes place when one entity pretends to be different entity. A Masquerade Attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place thus enabling an authorized entity with few privileges by impersonating an entity that has those privileges.

1.1.2 Replay

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

1.1.3 Modification of messages

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or recorded, to produce an unauthorized effect. For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts".

1.1.4 Sniffing

Packet sniffing is the interception of data packets traversing a network. A sniffer program works at the Ethernet layer in combination with network interface cards (NIC) to capture all traffic traveling to and from internet host site. Further, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating by anywhere near the internet host site. A sniffer placed on any backbone device, inter-network link or network aggregation point will therefore be able to monitor a whole lot of traffic. Most of packet sniffers are passive and they listen all data link layer frames passing by the device's network interface. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion. The key to detecting packet sniffing is to detect network interfaces that are running in promiscuous mode. Sniffing can be detected two ways: **Host-based**: Software commands exist that can be run on individual host machines to tell if the NIC is running in promiscuous mode.

Network-based: Solutions tend to check for the presence of running processes and log files, which sniffer programs consume a lot of. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files. The best countermeasure against sniffing is end-to-end or user-to-user encryption.

1.1.5 Hijacking (man in the middle attack)

This is a technique that takes advantage of a weakness in the TCP/IP protocol stack, and the way headers are constructed. Hijacking occurs when someone between one and other person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of

- *Arshad Ali, M.Tech Student,CSE Dept., Integral University, Lucknow, UP, India, ,arshad.a.14@gmail.com*
- *Dr. Mohd. Rizwan Beg, Professor & Head ,CSE Dept., Integral University, Lucknow, UP, India, 9839384611 , rizwanbeg@gmail.com*
- *Shish Ahmad, A.P., CSE Dept., Integral University ,Lucknow, UP, India, shish_parv@rediffmail.com*
- *Azhar Ali, M.Tech Student,CSE Dept., Integral University, Lucknow, UP, India, , azhar786.ali@gmail.com*

the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you, because the attacker might be actively replying as you, to keep the exchange going and gain more information

1.1.6 Mapping (Eavesdropping)

Before attacking a network, attackers would like to know the IP address of machines on the network, the operating systems they use, and the services that they offer. With this information, their attacks can be more focused and are less likely to cause alarm. The process of gathering this information is known as mapping .In general, the majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Counter measures are strong encryption services that are based on cryptography only. Otherwise the data can be read by others as it traverses the network.

1.1.7 Denial of Service attack (DoS)

A denial of service attack is a special kind of Internet attack aimed at large websites. It is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Denial of Service can result when a system, such as a Web server, has been flooded with illegitimate requests, thus making it impossible to respond to real requests. Yahoo! and e-bay were both victims of such attacks in February 2000. A Dos attack can be perpetrated in a number of ways. There are three basic types of attack: Consumption of computational resources, such as band width, disk space or CPU time, Disruption of configuration information, such as routing information, Disruption of physical network components.

The consequences of a DoS attack are the following: Unusually slow network performance, Unavailability of a particular web site, Inability to access any web site, dramatic increase in the amount of spam receive in email account. Common forms of denial of service are-

1.1.7.1 Buffer Overflow Attacks

The most common kind of DoS attack is simply to send more traffic to a network address than the programmer's expectation on size of buffers. A few of the better known attacks based on the buffer characteristics of a program or system include:

Sending e-mail messages that have attachments with 256 character file names to Netscape and Microsoft mail programs, Sending over sized Internet Control Message Protocol (ICMP) packets, Ending to a user of an e-mail program a message with a "From" address longer than 256 characters.

1.1.7.2 Smurf Attack

In this attack, the perpetrator sends an IP ping request to a receiving site. The ping packet specifies that, it is broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, which is the target site that is to receive the denial of service attack. The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

1.1.7.3 SYN floods

When a computer wants to make a TCP/IP connection to another computer, usually a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The computer requesting the connection, usually the client's or user's computer sends a TCP/SYN packet which asks the server if it can connect. If the server is ready, it sends a TCP/SYN-ACK packet back to the client to say "Yes, you may connect" and reserves a space for the connection, waiting for the client to respond with a TCP/ACK packet. In a SYN flood, the address of the client is often forged so that when the server sends a TCP/SYN-ACK packet back to the client, the message is never received from client because the client either doesn't exist or wasn't expecting the packet and subsequently ignores it. This leaves the server with a dead connection, reserved for a client that will never respond. Usually this is done to one server many times in order to reserve all the connections for unresolved clients, which keeps legitimate clients from making connections.

1.1.8 Distributed Denial-of-Service attacks (DDoS)

A distributed denial of service attack (DDoS) occurs when multiple compromised systems or multiple attackers flood the band width or resources of a targeted system with useless traffic. These systems are compromised by attackers using a variety of methods.

In DDoS attacks, the attacker first gains access to user accounts on numerous hosts across the Internet. The attacker then installs and runs a slave program at each compromised site that quietly waits for commands from a master program running, the master program then contacts the slave programs, instructing each of them to launch a denial-of-service attack directed at the same target host. The resulting coordinated attack is particularly devastating, since it comes from so many attacking hosts at the same time.

Here also ingress filtering only can control DoS attack and that too to a small extent.

1.2 Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are

1.2.1 Release of message contents

The Release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

1.2.2 Traffic Analysis

A second type of passive attack, traffic analysis is subtler. Suppose that we had a way of masking the contents of message or other information traffic so that opponents, even if they captured the message, could not extract the information

from message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

2 NETWORK RISK BACKGROUND

For every organization there is some combination of optimum loss prevention and reasonable cost. The purpose of risk management is to find that combination. Simply stated, risk management seeks to avoid or lesson loss. Loss implies injury to, denial of access to or distraction of assets. The opportunity for a threat to impact an asset adversely is called vulnerabilities. Risk is present when an access is vulnerable to threats. Assets associated with IT include, data, hardware, software, personal and facilities. Facilities consists of computer sites, the communication network plant and associated subsystem installations.

Many authors have discussed the varied threats to it resources. Following these are threats and shows that they may originate from physical sources, unauthorized access and authorized access. Further, threats from internal and external sources. The threats arising from authorized access are the most difficult to find and access. Following are potential threats to IT:-

2.1 Physical threats

Equipment Failure, Power interruption, Contaminants in the air, Weather, Fire, Humidity, Destruction or damage to facility or equip ment by human, Death or injury to key personnel, Personal turnover

2.2 Unauthorized physical or electronic access

Microcomputer theft, Theft of data, Disclosure, Modification and/or destruction of data, Hackers, Viruses, Bombs, Worms,EDI fraud,Phantom nodes on network,Voice mail fraud,Software piracy

2.3Authorized physical or electronic access

I/S applications portfolio may be outdated or obsolete, Increase in end user computing, Increased end user access to corporate data, Proliferation of end user developed applications.

Three types of threats affect the confidentiality, integrity, reliability & availability of computer network services.

Computer Security =Confidentiality + Integrity + Avaiability

2.3.1 Confidentiality

Intentially, Inadvertently

2.3.2 Integrity

Accurate, Complete, Consistent, Authentic, Timely

2.3.3 Availability

2.4 Accepted Levels

Threats to computer networks are defined as entities, events or circumstances with the capability to inflict harm or distort normal security operations by exploiting vulnerabilities in system. Harm is defined as the abuse or break of the Confidentiality, Integrity or Availability of computer networks, in the form of destruction, disclosure, modification, interruption of data and/or denial of service.

An asset is defined as anything that is a value and importance, to the owner, which includes information, programs, data network and communication infrastructures.

Threats classification ─ Threats to computer networks comprise of the following:

2.5 Network errors

Deliberate software threats includes, worms, viruses, macros and denial of service according to CSI/FBI Annual computer crime & security survey.

Natural disaster (wildfire, flooding, earthquakes, tidal waves tsunami), Cyber threats (Terrorism, political warfare)

Insider threats caused by disgruntled employees.

That risk is fundamentally about uncertainly in work performance and the resulting out comes. Most of the risk conceptualization into three categories:-

2.6 Risk components

Different types of negative outcomes:-

Risk factors leading to loss or source of risk factors. Risk as probability of negative outcomes, Risk as difficulty in estimating outcome, Risk undefined or discussed using a different term such a problem of threat.

2.6.1 Risk factors, Risk components source

Financial risk, Security risk, Technology risk, People risk, Information risk, Business process risk, Success risk, Business risk, System security risk, Project risk, Competitive risk ,Transition risk, Monetary risk, Environmental risk

Probability of negative outcomes

3 RELATED WORK

3.1 Key metrics: IT security metrics can be obtained at different levels within an organization. Detailed metrics, collected at the system and network level, can be aggregated and rolled up to progressively higher levels, depending on the size and complexity of an organization. If measurements are instantaneous snapshots of a particular measurable parameters, then metrics are more complete pictures, typically comprised of several measurements, baselines, and other supporting information that provide context for interpreting the measurements.

Good metrics are goal-oriented and should have the following features: specific, measurable, comparable, attainable, repeatable, and time dependent.

3.2 Metrics to Evaluate the Security Vulnerabilities: One such model is the Common Vulnerability Scoring System (CVSS) which was designed to provide the end user with an overall composite score representing the severity and risk of a vulnerability. The score is derived from metrics and formulas. The metrics are in three distinct categories that can be quantitatively or qualitatively measured. Base metrics contain qualities that are intrinsic to any given vulnerability that do not change over time or in different environments. Tem-

poral metrics contain vulnerability characteristics which evolve over the lifetime of vulnerability. Environmental metrics contain those vulnerability characteristics which are tied to an implementation in a specific user's environment. The particular constituent metrics used in CVSS were identified as the best compromise between completeness, ease-of-use and accuracy. They represent the cumulative experience of the model's authors as well as extensive testing of real-world vulnerabilities in end-user environments.

3.3 There are seven base metrics which represent the most fundamental features of vulnerability:

3.3.1 Access vector (AV) measures whether the Vulnerability is exploitable locally or remotely.

3.3.2 Access complexity (AC) measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system (high or low).

3.3.3 Authentication (A) measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability. (required or not required)

3.3.4 Confidentiality impact (CI) measures the impact on confi dentiality of a successful exploit of the vulnerability on the target system. (none, partial or complete)

3.3.5 Integrity impact (II) measures the impact on integrity of a successful exploit of the vulnerability on the target sys tem. (none, partial or complete)

3.3.6 Availability impact (AI) measures the impact on avail abilty of a successful exploit of the vulnerability on the target system. (none, partial or complete)

3.3.7 Impact bias (IB) allows a score to convey greater weighting to one of three impact metrics over the other two. The value can be normal (CI, II and AI are all assigned the same weight), confidentiality (CI is assigned greater weight than II or AI), integrity (II is assigned greater weight than CI or AI), or availability (AI is assigned greater weight than CI or II)

The temporal metrics which represent the time depend-ent features of the vulnerability are:

Exploitability (E) measures how complex the process is to exploit the vulnerability in the target system. The possible values are: unproven, proof of concept, functional, or high.

Remediation level (RL) measures the level of an available solution. (official fix, temporary fix, workaround, or un available)

Report confidence (RC) measures the degree of confidence in the existence of the vulnerability and the credibility of its report. (unconfirmed, uncorroborated, or confirmed)

The environmental metrics represent the implementation and environment specific features of the vulnerability.

Collateral damage potential (CDP) measures the potential for a loss of physical equipment, property damage or loss of life or limb. (none, low, medium, or high)

Target distribution (TD) measures the relative size of the field of target systems susceptible to the vulnerability. (none, low, medium, or high)

Scoring is the process of combining all the metric values according to specific formulas.

Base Score is computed by the vendor or originator using the following formula:

BS= round (10 * AV * AC * A *((CI*CIB) + (II*IIB) + (AI*AIB)),

Once is set and published, the BS score is not expected to change. It is computed from "the big three" confidentiality, integrity and availability. This is the "foundation" which is modified by the Temporal and Environmental metrics. The base score has the largest bearing on the final score and represents vul nerability severity.

Temporal score is also computed by vendors and coordina tors for publication based on the following formula:

TS= round (BS * E * RL * RC).

It allows for the introduction of mitigating factors to reduce the score of the vulnerability and is designed to be re-evaluated at specific intervals as a vulnerability ages. The temporal score represents vulnerability urgency at specific points in time.

Environmental score is optionally computed by end-user organizations and adjusts combined base-temporal score based on the following formula:

ES= round ((TS + ((10 – TS)* CDP))* TD),

This should be considered the final score and represents a snapshot in time, tailored to a specific environment. User organizations should use this to prioritize responses within their own environments

CVSS differs from other scoring systems (e.g. Microsoft Threat Scoring System, Symantec Threat Scoring System, CERT Vulnerability Scoring or SANS Critical Vulnerability Analysis Scale Ratings) by offering an open framework that can be used to rank vulnerabilities in a consistent fashion while at the same time allowing for personalization within each user environment. As CVSS matures, these metrics may expand or adjust making it even more accurate, flexible and representative of modern vulnerabilities and their risks.

4 PROPOSED WORK

In this paper we have analysed different possible attacks on each layer of Network model using different possible categories of Basic, Temporal and Environmental matrices.

4.1 Different kinds of possible Security Attacks on OSI layers

4.1.1 Physical Layer

According to our analysis there are different types of attacks are possible on physical layer. In Physical layer we use combination of Base Metric Group and Environmental Metric group. Following attacks and formulas are:-

Attacks

Cable disconnected, Physical threats, Equipment Failure, Power interruption, Contaminants in the Air , Weather Fire, Humidity, Destruction or damage to facility or equipment by human, Death or injury to Key personnel, Personal turn over.

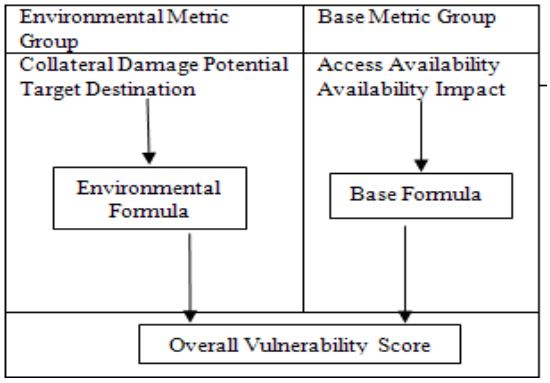

Fig. 1

1. Environmental Formula= Collateral Damage Potential +Target Destination
2. Base Formula=Access Availability + Availability Impact
3. Overall Vulnerability Score= Base Formula+ Environmental Formula

.4.1.2 Data Link Layer

In Data link layer we use combination of Base Metric Group and Temporal Metric group. In Data link layer there are different types of possible attacks and formulas are:-

Attacks

MAC modifications, MAC attack, MAC flooding, ARP attack, STP (Spanning Tree Protocol) Attack, VLAN Hopping attack , Active Attacks - Sniffing, Host-based, Network based attacks.

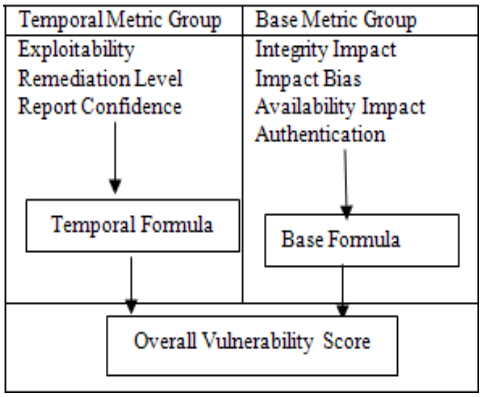

Fig. 2

1. Temporal Formula= Exploitability + Remediation Level + Report Confidence
2. Base Formula= Integrity Impact + Impact Bias+ Availability Impact + Authentication
3. Overall Vulnerability Score= Base Formula+ Temporal Formula

Network Layer

In Network Layer we use combination of Base Metric Group and Temporal Metric group. In Network Layer there are different types of possible attacks and formulas are:-

Attacks

IP modification, DHCP attack, ICMP attacks and so on.

Passive Attacks Interception- Release of message contents, Traffic Analysis, DoS, Spoofing (Identity spoofing or IP Address Spoofing) Smurf Attack, Buffer Overflow Attacks

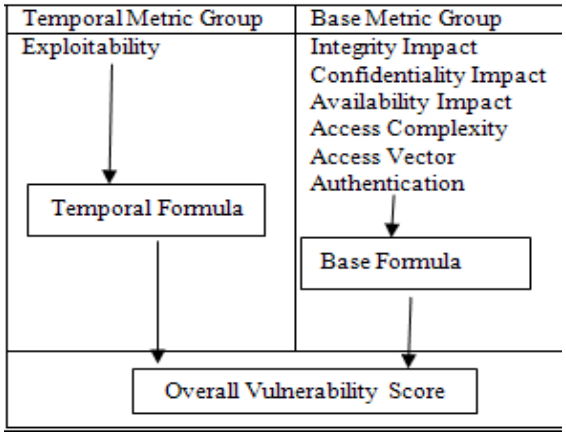

Fig. 3

1. Temporal Formula= Exploitability
2. Base Formula= Integrity Impact + Confidentiality Impact + Availability Impact + Access Complexity+ Access Vector+ Authentication
3. OverallVulnerability Score= Base Formula+ Temporal Formula

4.1.4 Transport Layer

In Transport Layer we can use combined form of Base Metric Group and Environmental Metric group. In Transport Layer there are different types of possible attacks and formulas are:-

Attacks

TCP sync flooding, UDP flooding, scanning and so on, it affects serious damage on network devices and servers on overwhelming loads.

Equipment Failure, Power Interruption, Containments in the air, Weather, Fire, Humidity, Destruction or damage to facility or equipment by human, Mapping (Eavesdropping), SYN floods

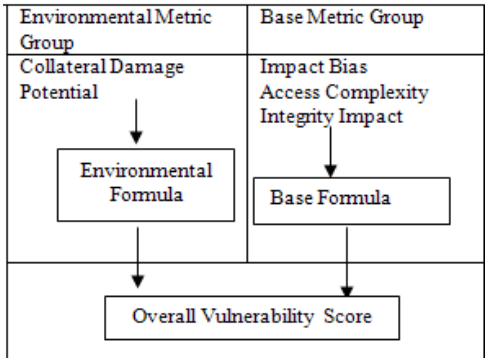

Fig. 4

1. Environmental Formula= Collateral Damage Potential
2. Base Formula= Integrity Impact + Access Complexity+ Impact Bias
3. Overall Vulnerability Score= Base Formula+ Environmental Formula

4.1.5 Application Layer, Presentation Layer, Session Layer

According to our research in Application Layer, Presentation Layer and Session Layer mostly attacks are common. We can

use the combination of Base Metric Group, Temporal Base Group and Environmental Metric group. The formulas and attacks are:-

Attacks

Virus, Worms, Trojan horse, Buffer overflow, APP/OS weakness. Authorized physical or electronic access,I/S applications portfolio may be outdated or obsolete,Increase in end user computing,Increased end user acces to corporate data,Proliferation of end user developed applications,,Increased end user acces to corporate data,Proliferation of end user developed ,Applications

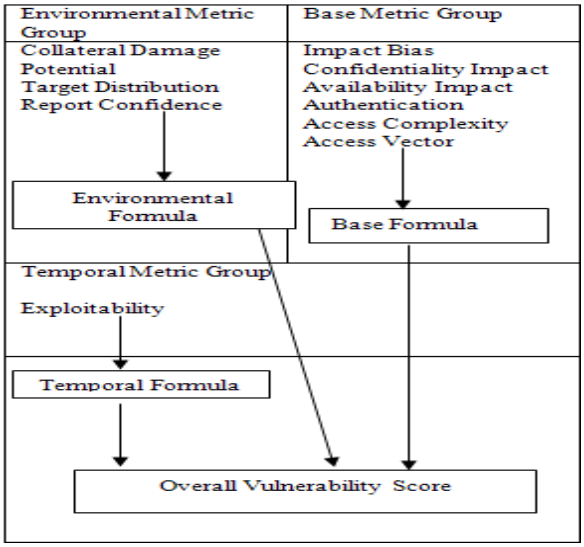

Fig. 5

1. Environmental Formula= Collateral Damage Potential + Target Distribution+ Report Confidence
2. Temporal Formula=Exploitability
3. Base Formula= Impact Bias+ Confidentiality Impact+ Availability Impact+ Authentication + Access Complexity+ Access Vector

4.2 Following are the formulas of different category matrices based on CVSS:-

4.2.1 CVSS Base Score Equation

BaseScore = (.6*Impact +.4*Exploitability-.5)*f(Impact), Impact = 10.41*(1-(1-ConfImpact)(1-IntegImpact)*(1-AvailImpact)), Exploitability =20*AccessComplexity*Authentication*AccessVector, f(Impact) = 0 if Impact=0; 1.176 otherwise

Different types of Access Complexity:- high: 0.35, medium: 0.61,low: 0.71, **Different types of Authentication:-** Requires no authentication: 0.704, Requires single instance of authentication: 0.56, Requires multiple instances of authentication: 0.45, **Different types of Access Vector:-**Requires local access:.395, Local Network accessible: .646, Network accessible: 1, **Different types of Confidentiality Impact :-** none: 0, partial: 0.275, complete :0.660, **Different types of Integrity Impact:-** none: 0, partial: 0.275,complete: 0.660, **Different types of Availability Impact :-** none: 0, partial: 0.275, complete: 0.660

4.2.2 CVSS Temporal Equation

TemporalScore=BaseScore*Exploitability*RemediationLevel*ReportConfidence

Different types of Exploitability:- unproven: 0.85, proof-of-concept: 0.9, functional: 0.95, high: 1.00, not defined 1.00 **Different types of Remediation Level: -** official-fix: 0.87, temporary-fix: 0.90, workaround: 0.95, unavailable: 1.00, not defined: 1.00, **Different types of Report Confidence:-** unconfirmed: 0.90, uncorroborated: 0.95, confirmed: 1.00, not defined 1.00

4.2.3 CVSS Environmental Equation

Environmental Score= (Adjusted Temporal+ (10-AdjustedTemporal)*CollateralDamagePotential) * TargetDistribution, AdjustedTemporal = TemporalScore recomputed with the Impact sub-equation replaced with the following AdjustedImpact equation, AdjustedImpact = Min (10, 10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq)))

Different types of Collateral Damage Potential :- none: 0, low: 0.1, low-medium: 0.3, medium-high: 0.4, high: 0.5, not defined: 0, **Different types of Target Distribution:-** none: 0, low: 0.25, medium: 0.75, high: 1.00, not defined: 1.00,**Different types of Confidentiality:-** Impact Low: 0.5, Medium: 1, High: 1.51, Not defined: 1,IntegReq = case IntegrityImpact of Low: 0.5, Medium: 1, High 1.51, Not defined: 1, **Different types of Availability Impact**:- Low: 0.5, Medium: 1, High: 1.51 Not defined:

According to our analysis we can define some formulas for different network layers which are use for finding risk. The formulas are:-

5.1 Physical Layer

Environmental matrices and Base matrices can be calculated as follows-

EF=CDP+TD, BF=AA+AI

Overall Vulnerability Score is-

OVS=BF+EF

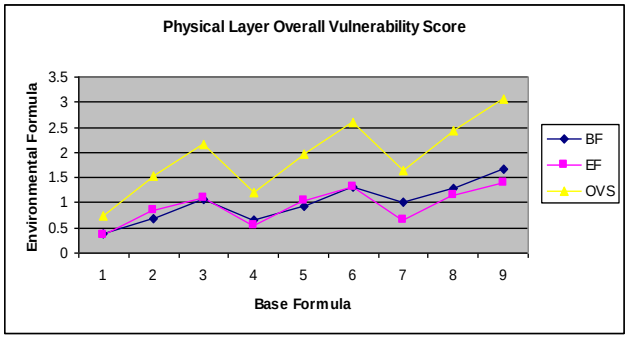

Fig. 6

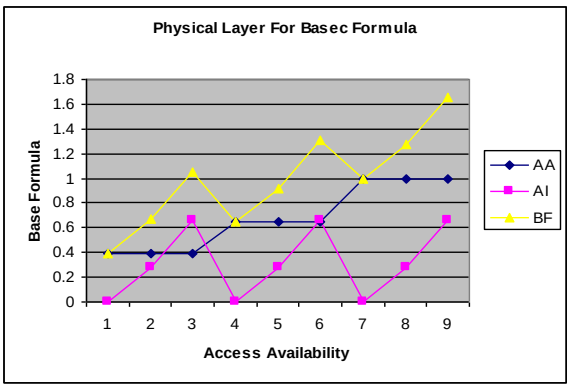

Fig. 7

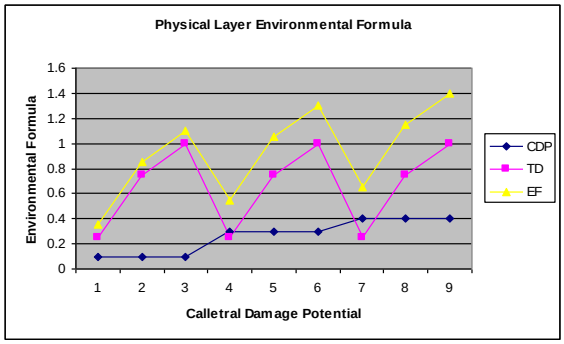

Fig. 8

5.2 Data Link Layer

Temporal matrices and Base matrices can be calculated as follows-

TF=E+RL+RC, BF=II+IB+AI+A

Overall Vulnerability Score is-

OVS=BF+TF

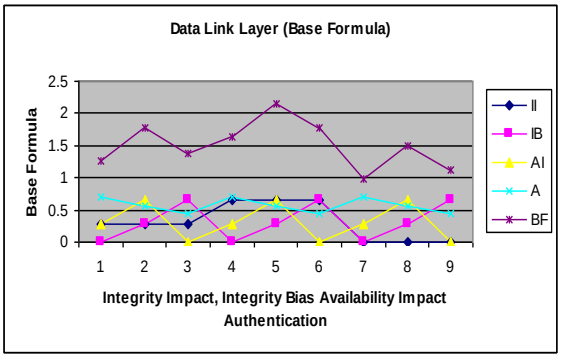

Fig.9

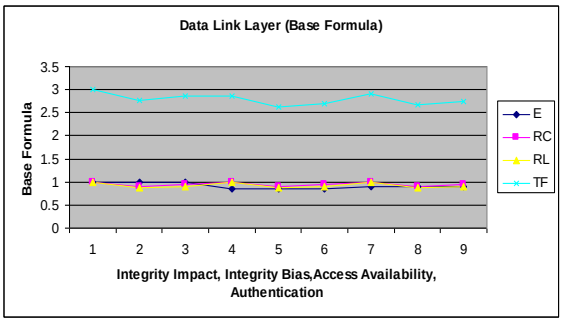

Fig.10

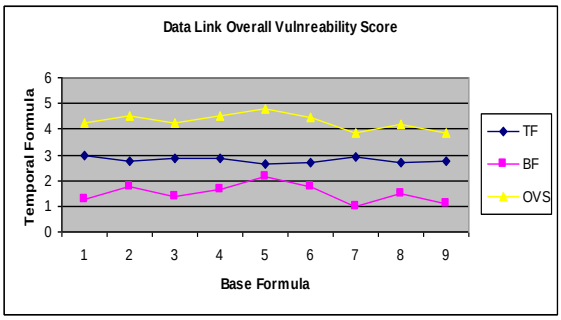

Fig.11

5.3 Network Layer

Temporal matrices and Base matrices can be calculated as follows-

TF=E, BF=II+CI+AI+AC+AV+A

Overall Vulnerability Score is-

OVS=BF+TF

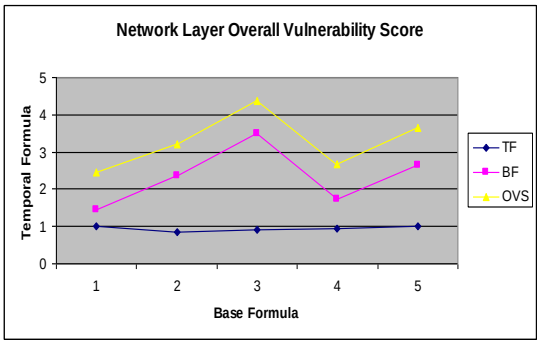

Fig.12

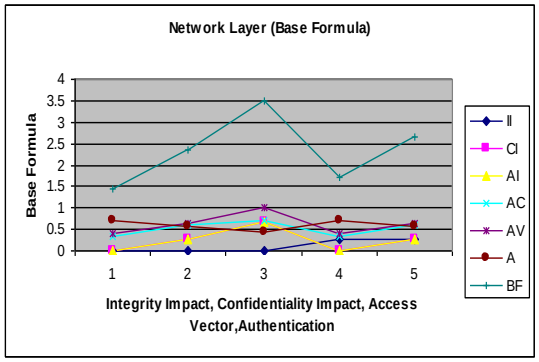

Fig.13

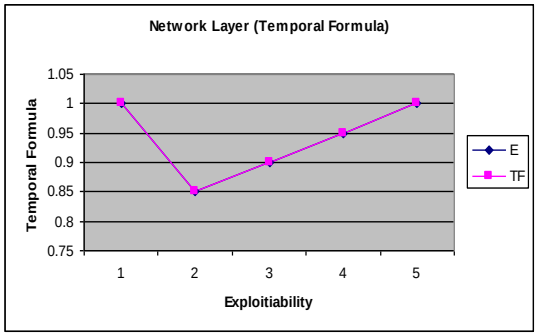

Fig.14

5.4 Transport Layer

Environmental matrices and Base matrices can be calculated as follows-

EF=CDP, BF=II+AC+IB

Overall Vulnerability Score is-

OVS=BF+TF

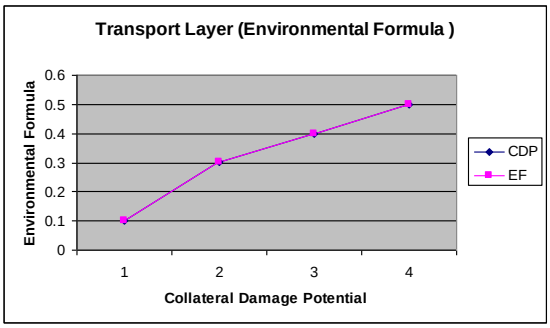

Fig.15

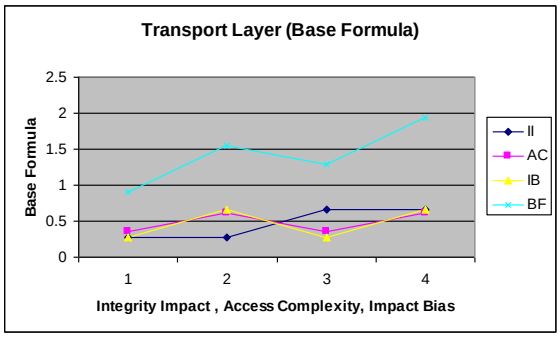

Fig.16

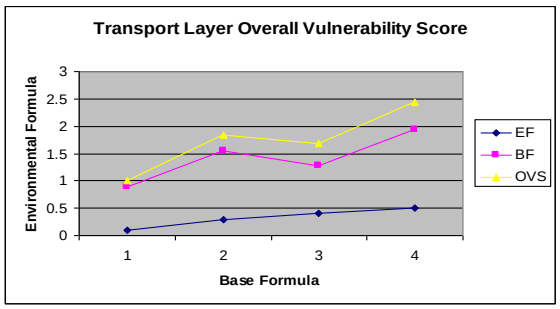

Fig.17

5.5 Application Layer, Presentation Layer, Session Layer

Environmental matrices , Temporal matrices and Base matrices can be calculated as follows-

EF=CDP+TD+RC

TF=E, BF= IB+CI+AI+A+AC+AV

Overall Vulnerability Score is-

OVS=BF+TF+EF

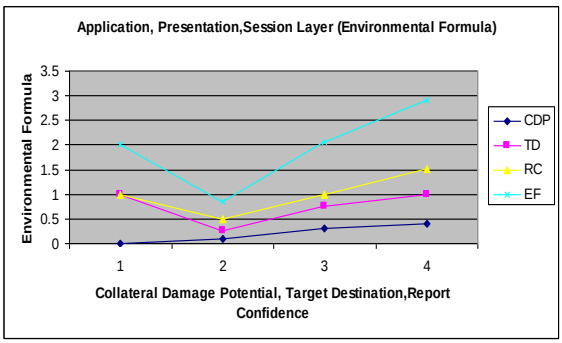

Fig.18

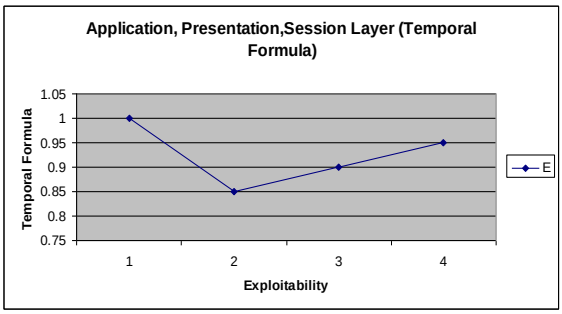

Fig.19

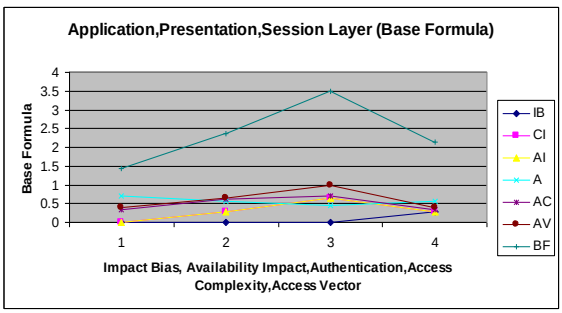

Fig.20

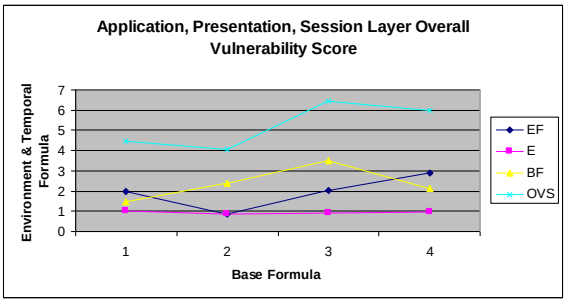

Fig.21

5 CONCLUSION

Metrics are central for measuring the cost and effectiveness of complex security controls. Security metrics, at least such metrics trying to define a measure for the security of an entire organization, are a quite new area of research.
In this paper we have analyze risk at different layers using Base metric, Temporal metric and environmental metric and result shows that we can control the risk at each and every layer by controlling the different parameters of each metrics. We have also found that the data link layer have probability of higher risk

REFERENCES

[1] Victor-Valeriu PATRICIU, Iustin PRIESCU, Sebastian NICOLAESCU Security Metrics for Enterprise Information Sysems 2007

[2] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison Wesley, 2006

[3] Gerald L. Kovacich, Edward Halibozek, Security Metrics Management: How to Measure the Costs and Benefits of Security, Butterworth-Heinemann, 2005

[4] Marianne Swanson P & others, Security Metrics Guide for Information Technology Systems, NIST pecial Publication 800-55, 2003(http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf)

[5] Ron Ross, & others, Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, 2005(http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf)

[6] SystemsSecurity Engineering-Capability Maturity Model Group, SSE-CMM – Model Description Document version 3.0, In ternational Systems Security Engineering Association, 2003 (http://www.sse-cmm.org/docs/ssecmmv3final.pdf).

[7] Mike Schiffman, Cisco CIAG, A Complete Guide to the Common Vulnerability Scoring System (CVSS), Forum Incident Response and Security Teams (http://www.first.org/)

[8] VV Patriciu, I. Priescu, S. Nicolăescu, Security Monitoring-An Advanced Tactic for Network Security Management, communications 2006 Conference, Bucharest, Romania, 2006

[9] VV Patriciu, I. Priescu, S. Nicolăescu, Operational Security Metrics for Large Networks, International Conference on Computers, Communications & Control (ICCC 2006)

[10] ISO/IEC.InformationTechnology–SecurityTechniques, Code of practice for information security management (final draft), ISO, 2005.

[11] British Standard Institute, Information Security Management.Code of Practice for Information Security Management (BS 799-1), British Standard Institute, 1999.

[12] Basel Committee on Banking Supervision, Working Paper on the Regulatory Treatment of Operational Risk Bank for International Settlements, Basel Committee, 2001.

[13] CERT, CERT/CC Statistics 1988-2005, CERT, 2005 (http://www.cert.org/stats/)

[14] US President's Information Technology Advisory Committee – "Cyber Security: A Crisis of Prioritization", Report to the President, National Coordination Office for Information Technology Research and Development, 2005

[15] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, "CVSS: A Common Vulnerability Scoring System", National Infrastructure Advisory Council (NIAC), 2004.

[16] Microsoft Corporation. Microsoft Security Response Cen ter Security Bulletin Severity Rating System. November 2002 [cited 16 March 2007].URLhttp://www.microsoft.com/technet/security/bulletin/rating.mspx

[17] United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006 [cited 16 March 2007]. Available from URL: http://www.kb.cert.org/vuls/html/fieldhelp

[18] SANS Institute. SANS Critical Vulnerability Analysis Archive. Undated [cited 16 March 2007]. Available from URL: http://www.sans.org/newsletters/cva/.

[19] http://nvd.nist.gov/cvss.cfm?calculator