International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 4, April 2014 ISSN 2319 - 4847

# A Cumulative Security Metric for an Information Network

**Rajesh Pant[1], CN Khairnar[2]**

[1]ECE , JJTU, Rajasthan, India
[2]MCTE, MHOW, MP, India

## Abstract

***The proliferation of networks to a large population has increased network accessibility for a large section of hackers to abuse. Stronger security methods such as advanced encryption algorithms, efficient authentication process and 'defense in depth' approach are being used to address these threats. This paper gives a brief overview of various vulnerabilities associated with each layer of the OSI Model. Issues related to the "eighth layer" have also been elucidated. The authors proposes to carry out performance analysis of the cumulative effect of employing security mechanisms maintained at all layers of the network.***

**Keywords :** Cyber Security, Information Network, Cumulative Effect, Eighth Layer, Vulnerabilities, Network Security Metrics.

## I. INTRODUCTION

Increasing lapses of cyber security in both defence, non-military networks, a growing threat of embedded malware, cyber attacks from inimical elements and nations has brought to fore the immense importance of network security. Simultaneously, the proliferation of networks to a large population has increased network accessibility for a large section of hackers to abuse, which is finally being addressed by stronger security methods such as advanced encryption algorithms, efficient authentication process and 'defense in depth' approach. Every network administrator ensures building adequate security measures at his level. Since all system administrators work in a disjoint manner and manage security solutions at different layers of OSI model, the global picture builds up a scenario, where the sender finds his data going through some encryption/security process at all levels starting from Application layer down to Physical layer and a decryption process at all layers at the receiver end. This paper makes a proposal to carry out performance analysis of the cumulative effect of employing security mechanisms at all layers of the network.

## II. MATERIAL AND METHODOLOGY

THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL AND VULNERABILITIES The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the International Organisation for Standardisation (ISO). The model groups similar communication functions into one of seven logical layers. A layer serves the layer above it and is served by the layer below it. The usage of OSI Model is so wide that it defines the way IT industry should design networking protocols. In this model, each layer can communicate with the layer above and below it. Each layer is developed independently which allows flexibility and development in one layer to progress without delay from any other layer. As information passes through each layer relevant information from that layer is attached - this process is commonly known as Encapsulation. Following is the brief overview of various vulnerabilities associated with each layer.

**Physical Layer Vulnerabilities:-** These include Loss of Power, Loss of Environmental Control, Physical Theft of Data and Hardware, Physical Damage or Destruction of Data and Hardware, Unauthorized changes to the functional environment (data connections, removable media, adding/removing resources), Disconnection of Physical Data Links, Undetectable Interception of Data, Keystroke & Other Input Logging. The security issues become more pronounced when the network is based on a wireless media. A comparatively powerful transmission at same frequencies can easily affect the quality of service; if not fully deny the service to the user. The chances of passive attacks on wireless media are more as it is more susceptible to interception.

**Datalink Layer Vulnerabilities:-** A device running in promiscuous mode and a packet filter could be helpful or harmful tools at OSI Layer two. Allowing flow analysis, problem determination and code debugging can be helpful. However, in the wrong hands the ability to copy datagrams poses a threat. An example of a layer two threat is Libpcap, a packet capture driver that forces an NIC into promiscuous mode, allowing it to absorb traffic destined to other machines. Various known threats at layer 2 are:- Content-Addressable Memory (CAM) table overflow, VLAN hopping, Spanning-Tree Protocol Manipulation, Media Access Control (MAC) Address Spoofing, Address Resolution Protocol (ARP) attack, Private VLAN attack and DHCP starvation.

**Network Layer Vulnerabilities:-** The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network (in contrast to the data link layer which connects hosts within the same network), while maintaining the quality of service requested by the transport layer. The IP address allows a system to contact the outside world and allows the outside world to contact the host. It is logical to consider this border to our system vulnerable. The following are the key security risks at the Network Layer associated with the IP:- IP Spoofing, Routing (RIP) Attacks, ICMP Attack, PING Flood (ICMP Flood), Ping of Death Attack, Teardrop Attack and Packet Sniffing.

**Transport Layer Vulnerabilities:-** One way the Transport Layer ensures that there is reliability and error checking is through the Transport Control Protocol (TCP). Another protocol used at Layer 4 is UDP (User Datagram Protocol). Finding a system on the Internet requires knowing the public IP address assigned to it. To target a specific application on a system, an intruder would need to know the IP address to locate the system and the port number assigned to the application, collectively referred to as a socket. A computer system has 65535 ports. These ports can be further broken down into three categories: well known, registered and dynamic. This is where Layer 4 security is applied. Many applications utilize well known TCP and UDP ports. An attacker will gather information about a system using TCP and UDP. There are many ways in which TCP and UDP are used to infiltrate, deny services, or scan networks. The key security risks associated with transport layer are:- TCP "SYN" Attack, SSL Man-in-the-Middle Attacks, Land Attack, TCP Connecting Hijacking, UDP Flood Attack and Port Scan Attack.

**Session Layer Vulnerabilities:-** The 'session' is created using the three-way handshake. When a client establishes a connection to a server, the client sends a SYN request; the server responds with a SYN/ACK packet and the client validates the connection with an ACK (acknowledgement) packet. A TCP connection cannot be established until these 3 steps have been completed. The vulnerabilities associated with session layer are:- DNS Poisoning, TCP Session Hijacking, SYN Attack and SSH Downgrade Attack.

**Presentation Layer Vulnerabilities:-** The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer. Encryption services are associated with the Upper Layers of the OSI model, specifically the Presentation Layer. When the data is received, what form will it take? Encryption techniques allow us to scramble the packet contents, requiring a special code to reveal them. The more sophisticated the encryption algorithm, the harder it is to gain access to the data. Obviously, this intense processing function could affect system performance. Proper planning is necessary to calculate security needs and balance them with resource limitations. Vulnerabilities at this layer often originate from weaknesses or shortcomings in the implementation of the presentation layer functions. Continuing on the theme of taking advantage of the original atmosphere of implicit trust and simple functionality that systems were (and continue to be) built in, attackers feed unexpected or illegal input into presentation-layer facilities, gaining results that are undesired or contrary to what the original designers intended. Some methods used are:- Buffer Overflows, Format String Vulnerabilities and Attacking the NetBIOS.

**Application Layer Vulnerabilities:-**. This OSI layer is closest to the end user, which implies that both the OSI application layer and the user interact directly with the software application. Application-layer functions typically include identifying communication partners, determining resource availability and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. Similar to the physical-layer, the open-ended nature of the Application Layer groups many threats together at its end of the stack, some of which are as below:- Backdoor Attacks, Authentication Attacks, Phishing Attacks and Access Attacks.

**The Eighth layer – Human Layer and Vulnerabilities:-**A common misconception about the Open Systems Interconnection model is that it contains only seven layers. However, there exists an eighth layer above "Application" commonly titled "User" or "Human Layer". This is also called the Neuman's Layer. This eighth layer must be considered when troubleshooting a network issue, as many times it can prove to be more of a common cause than the physical layer. A mistake or a deliberate tampering with any of the above layers by this eighth layer component can play havoc with the network. Common causes for failures at the Eighth layer of the OSI model include ID10T errors and policy-related issues. Seeing as to how the eighth layer interacts directly with the application layer, a problem at the eighth layer can cause problems at other layers at varying severity, depending on network security and privilege settings. Many layer 8 errors even cause failures at the physical layer, which is a fairly common occurrence. Indeed, the eighth layer can be in many cases very difficult to troubleshoot, but if kept within consideration all along the process of troubleshooting other layers, then a layer 8 issue may reveal itself to the troubleshooter without going through all of the layers in between. Common causes of layer eight issues are:- Users who think they are changing a critical setting to make something "better" or

"faster" without the slightest clue about what the setting actually does, e.g. changing TCP/IP settings, a user who unplugs a network cable for "security" then can't connect the next day and a user who demonstrates the "clicking syndrome", which causes such a wide array of problems that we couldn't possibly list them all here.

## III. RESULTS AND TABLES

**ANALYSIS AND METHODOLOGY**

**ANALYSIS :-**

In view of the threats listed above, there exists a void in establishing a compact model which also includes the 'eighth layer'. Further, no research exists on a cumulative assessment of the security solutions implemented at individual levels. This paper therefore intends to create an evaluation criteria which takes into account the security solutions implemented in all the layers of the network. The author is therefore of the view that in any network the security assurance can only be evaluated based on an index that is a mathematical function of individual layer security indices.

**METHODOLOGY:-**

It is proposed that each layer of the OSI model, including the Eighth Layer, be assessed for any given network. Depending upon the quality and quantity of security mechanisms employed for that particular network, certain marks will be awarded to each layer. These would be weighted against the threat sensitivity of that particular layer, implying that for any compromise in that particular layer, what would be the impact of loss of information in that network.

Once each layer has been graded and weighted, the individual layer values will be added and again normalized as a percentage. This final percentage will finally be assigned an alphabet grading, eg A is over 90, B is over 80 and so on. This would be the final gradation of the network under test. An example of 'Policy' layer table is given below.

| Parameter | Weightage (%) |
|---|---|
| Organisation owner has laid down a security policy, or adopted an international state of the art policy. | 10 |
| Periodical Testing (i.e. PT on Policy, minimum yearly) of users in their understanding of the laid down policy is being carried out. | 10 |
| Performance of the users in the PT on Policy. | 10 |
| Performance of the organisation in the yearly audit of adopted cyber security policy including regular and latest updates to software applications, Operating Systems, their upgradation, use of antivirus measures, firewalls with effective rules and other cyber security infrastructure. This audit should ideally be conducted by either an outside independent agency with expertise in cyber audit or an in-house dedicated section meant for this purpose only. | 30 |
| Ratio of number of Incidents reported to number of System-users in the organisation. To avoid embarrassment to the organisation there is a tendency to subdue the reports of the violations or under-report their numbers but it can result in catastrophic compromises. Higher ratio gets higher credits. This parameter is to curb this tendency and can encourage organisation to report and mitigate incidents at the initial stages of crisis. | 5 |
| Number of external audit carried out by the organisation in five years (credits as per the number of external audits carried out). | 5 |
| Disciplinary actions and corrective actions taken for violations reported in a year and on the cyber-audit report. | 15 |
| Ratio of number of external employees (without administrative control of the organisation's system) who **manage the system / network** to the number of internal employees who manage the system. | 5 |
| Ratio of number of external employees (without administrative control of the organisation's system) who **use the system / network** to the number of internal employees who use the system / network. | 10 |

## IV. CONCLUSION

Recent literature has indicated that the global trend is towards adopting a holistic approach to Network Security. Accordingly extensive research is currently in progress to analyse and model network flows. The current paper is anticipated to create a new benchmark in this important area of network security metrics. While the readers are familiar with indices for (say) financial soundness of AAA CRISIL grading, there is no simplistic grading for Information Security. This paper outlines a methodology to achieve the same, by assessing People, Process and Technology and grading these parameters to present a simplistic grading for the Information Network.

## References

**[1]** Scarfone, K. &Mell, P. (2009). The common configuration scoring system (CCSS): Metrics for software security configuration vulnerabilities (Draft). Gaithersburg, MD: National Institute of Standards and Technology. Available at http://csrc.nist.gov/ publications /drafts/nistir-7502/Draft-NISTIR-7502.pdf.

**[2]** Swanson, M. (2001). Security self-assessment guide for information technology systems. Gaithersburg, MD: National Institute of Standards and Technology.

**[3]** Implementing a Network Security Metrics Program By Paul W LowansGIAC available on 23 Sep 13 at url - http://www.giac.org/paper/gsec/1641/ implementing-network-security-metrics-programs/103004

**[4]** Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, I., & Hatfield, A. (2004). Current trends and advances in information assurance metrics. Proceedings of PST2004: The Second Annual Conference on Privacy, Security, and Trust. Fredericton, NB.

**[5]** NIST SP 800-55 (Revision 1).

**[6]** ISO / IEC 27004 and ISO / IEC 15939.

**[7]** Huang, Yan and Yang (2009).Research of Security Metric Architecture for Next Generation Network. Proceedings of IC-NIDC2009.