# A Novel Holistic Grading for Network Security

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

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

## Abstract

***Global research trends indicate a growing desire to provide a holistic view of network security. Accordingly, this paper proposes a grading scale for overall security of the network. We propose a method to analyze various vulnerabilities that exist in the network, the security solutions implemented, the cyber security policies promulgated, the extent of enforcement of these policies, the training level of the persons running the network, the end users, and security specialists. The proposed grading scale looks at the capability of the organisation to respond to threats and any disaster recovery plans that are existing in the enterprise network. Finally, we propose a three level grading based on the effectiveness of People, Process and Technology forming the network..***

**Keywords:** Security Grading, Security Metrics, Computer Networks, Grading scale, Information security

## 1. INTRODUCTION

The neural system for most of the enterprises is the network. With the emergence of social networking, video streaming, peer-to-peer technology, cloud computing and SaaS, it's safe to say that modern enterprises are only as good as their networks especially in terms of the bandwidth and security they provide. The banks have to secure their data against thefts, the business organisations have to secure their network against security threats and the militaries have to worry about the loss of strategic information. There is always the lurking threat of getting breached, compromised and damaged by an unknown zero-day intruder. The continuous evolution of intrusion techniques has made the task of ensuring network security increasingly difficult in spite of becoming all the more critical. Experienced information security professionals are growing increasingly cynical. We may win the occasional battle but we are losing the war against hackers, fraudsters, organised criminals, terrorists, pirates, plagiarists, industrial spies, unethical insiders and other adversaries. Metrics are a substantial part of the answer to today's information security management challenges [1][2]. We cannot continue throwing money at security, guessing at what needs to be done or implementing shiny new products while hoping for the best. If you enter the phrase, “Network Security Metrics” into your search engine, you will probably get less than one page of links [3].

A key tenet of network security is "know thy system" [4]. A computer network comprises of the People, Process and Technology. Designing and running networks requires not just technology, but a disciplined team of administrators & users with systematic approach & strict adherence to processes. This includes policies about escalation management, knowledge sharing, risk, as well as the day to day operations. It also requires that all persons using the network are aware of the security instructions and are adequately trained. A network is as strong as the weakest link. Section II of the paper looks at the existing types of network and the threats posed by environment to them. Section III outlines the proposed grading methodology..

## 2. TYPES OF NETWORKS AND THREATS POSED

Let’s first see the various types of networks that exist and the threats faced by them which are analyzed in the subsequent paragraphs.

### 2.1 Local Area Network (LAN)

LAN is a relatively small network that is confined to a small geographic area, such as a single office or a building. Laptops, desktops, servers, printers, and other networked devices that make up a LAN are located relatively close to each other. A key characteristic is that all the equipment that constitutes a LAN, is owned by a single entity. From a security context, LANs are the point at which trusted users typically access your network and server resources. Often, enterprises extend too much trust to users (People) in LANs who have otherwise unrestricted access to information resources. Consider the plight of an organisation that fires an employee, but permits the employee to return to their computer under the guise of removing personal data. With unrestricted access to network resources, the disgruntled employee has the ability to delete or tamper with information that is critical to the organisation. Even satisfied & trustworthy employees can be a critical threat to information security. An employee who is tricked into installing malicious software or accidentally introduces a computer virus or worm to an organisation can cause immeasurable damage if he is granted access to critical systems.

For example, an employee of a large corporation was able to delete all the programs that ran the company's engineering operations. This former system administrator turned disgruntled employee, who had been fired from the company, planted the logic-bomb shortly before implementing his attack. As a result the company lost $12 million in revenue and had to lay off 80 employees to cover up their losses. It is easy to identify employees as the potential inside threat, with all others in the external threat category. The problem with this classification method is that LAN users are not always employees. The contractors, business partners, vendors, and students are all examples of people who might use a company LAN but are not trusted with limitless access to information resources. It is thus important to consider all access to LAN resources when evaluating the internal threat to an organisation & not just traditional users.

### 2.2 Metropolitan Area Network (MAN)

MAN is typically used to describe a network that spans a citywide area or a town. MANs are larger than traditional LANs and predominantly use high-speed media, such as fiber optic cable, for their backbones. MANs are common in organisations that need to connect several smaller facilities together for information sharing. This is often the case for hospitals that need to connect treatment facilities, outpatient facilities, doctor's offices, labs and research offices for access to centralized patient and treatment information. MANs share many of the same security threats as LANs, but on a larger scale. The plight of an administrator in a central location granting access to countless offices that are scattered within a city is a difficult one that demands strict access control mechanisms to protect against unauthorised information access.

### 2.3 Wide Area Network (WAN)

A WAN covers a significantly larger geographic area than LANs or MANs. A WAN uses public networks, telephone lines and leased lines to tie together smaller networks such as LANs and MANs over a geographically dispersed area. Connecting devices in different geographic areas together for information sharing, WANs are an important piece of enterprise networks.

Each of the above mentioned networks require a different method of protection. Ideally, each network must implement an independent level of protection, that too in a layered manner.

## 3. GRADING MODEL

The threats to any network are handled by people, process and the technology forming part of the network. Therefore it is proposed to grade the Network Security on the basis of the Metrics (M) related to these verticals. Mathematically,

NS = f {M(people)+M(process)+M(tech)}

(where NS is the Overall Security Grading.)

### 3.1 People

The most important part of the network security is the people. One person downloading an unauthorised file and bringing it into the system can cause havoc on the network. The measures that we use in grading the network under this head are given in the Table below.

**Table 1**: Metrics for people

| Parameter | Weightage (%) |
|---|---|
| Whether a Security Knowledge Examination (SKE) is laid down by the network owner (written test compulsory for all). | 10 |
| Percentage of people qualifying in the SKE and conduct of refresher training on matters related to network security. | 20 |
| Average technical qualification of network administrator (100 marks for persons with doctorate, 80 for persons with post-graduation, 70 for persons with graduation, 60 for diploma-holders and 50 for university recognized certificate courses in computer related subjects). | 20 |
| Average qualification of network/system users (100 marks for persons with doctorate, 80 for persons with post-graduation 70 for persons with graduation and 50 for university recognized certificate courses in any subjects). | 20 |
| Average qualification of incident response team other than those forming part of network designers and administrators. No credit if no such persons are earmarked, 100 marks for persons with doctorate, 80 for persons with post-graduation, 70 for persons with graduation, 60 for diploma-holders and 50 for university recognized certificate courses in any subjects. | 10 |
| Qualification of nonuser of the network system in the organisation (same scale as Network / system users) | 10 |
| Percentage of personnel who underwent in-house training courses or pre-induction course. (No credits if such courses are not conducted by the organisation) | 10 |

### 3.2 Process

The process which handles the network and the people forming part of it comes next in deciding the security of the network. This metric has strong correlation with the technology used in the network. However to form an independent metric, generalized parameters are proposed to form a holistic metric.

**Table I1**: Metric for process

| Parameter | Weightage (%) |
|---|---|
| Organisation owner has laid down a security policy, or adopted an international state of the art policy [5][6]. | 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 up gradation, 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 |

### 3.3 Technology

It is often said that the weakest link of a system is the people in the systems however; the entire infrastructure is on the platform of technology. The most difficult vertical to find a metric is the technology since it is mutant in matter of months and what was considered as secure few months back becomes weak in a near future. However since TCP IP is the predominant technology, the metric proposed follows TCP IP layers. It is pertinent to note that the security measure taken at one layer may not compensate for the lack of security at another layer, therefore a cumulative grading calculation based on the score of all the layers is proposed for the Technology vertical.

**Table III.** Metric for technology: physical and data link /network access layer

| Parameter | Weightage (%) |
|---|---|
| Ratio of number of nodes in the network / system to the openings to the external network / world. For example, connection through internet on shared media (through secure / unsecure medium), employees / customers given remote access to the network using media not owned by the organisation etc. Lower ratio gets higher credits. | 5 |
| Average of number of encrypted communication links (e.g. VPNs using Internationally recognized open standard encryption) routed outside the organisation-owned premises of the system to total number of such links. | 5 |
| Inverse of ratio of number of wireless links with high level of security & MAC-binding to the total number of nodes in the network. | 5 |

| Parameter | Weightage (%) |
|---|---|
| Physical security for all components including media outside organisational premises as per the Internationally recognized standards. | 5 |
| Ratio of No of hosts whose access to network resources is bound to its hardware address (MAC binding etc) to total no of host in the network/system. | 5 |

**Metric for technology: network layer**

| Parameter | Weightage (%) |
|---|---|
| Use of the state-of-art network layer protocol e.g. IP ver. 6. | 5 |
| Centralised control for network address distribution bound to hardware address e.g. MAC binding of IP addresses using a DHCP server for a domain. | 5 |
| Network layer security devices installed e.g. Firewall, IPS, IDS etc and configured to the state of the art settings with respect to each geographically separated network / nodes. Average for the whole organization to be calculated | 10 |
| Percentage of hosts configured with address spoofing prevention methods at network or MAC layer. | 5 |
| Percentage of links (both logical and physical) encrypted with state of the art network layer encryption protocol. | 5 |

**Metric for technology: transport layer**

| Parameter | Weightage (%) |
|---|---|
| Percentage of sockets created using state of the art Transport Layer Security (TLS) protocol. Sockets created should include sockets created for web service , mail service, data base service, directory service, virtual private networking etc. | 10 |

**Metric for technology: application layer**

| Parameter | Weightage (%) |
|---|---|
| Centralised access control for network resources and application services e.g. Domain Controller and Active Directory with minimum administration rights to the end-users. | 5 |
| Percentage of application services with user rights based authentication and role-based access. | 5 |
| Percentage of data used for business / organisation support and decision making kept in encrypted format to total data stored (using state of the art encryption standard and tools). | 5 |
| Percentage of data used for business / organisation support and decision making stored in a centralised setup e.g. using SANs rather local drives and removable media. | 5 |
| Number and types of back-ups for critical data ( minimum three factor back-up for maximum max credit e.g. RAID1, back-up server in different room, geographically isolated Disaster Site (DR) etc). | 5 |

**Metric for technology: evaluation parameter common to all layers**

| Parameter | Weightage (%) |
|---|---|
| Homogeneity of the network / system. If the network or the system is homogeneous in terms of the technology used between nodes across geographical locations then it gets highest credit. If more than one technology is used than a normalized ratio of number of nodes to number of technology is used to calculate the credit. | 5 |
| Average vintage version of technology used in the system. If the technology is less than two years old, it gets full sub weightage and technology more than two years old which has better replacement be awarded as per number of years while technology more than five years vintage without | 5 |

| Parameter | Weightage (%) |
|---|---|
| replacement will be given no credits. | |

## 4. SECURITY TEMPLATE

Under each vertical i.e. People, Process and Technology, score will translate to grade as per following template:-

**Grading template**

| Score | Grading |
|---|---|
| 70 and above | A |
| 60 to < 70 | B |
| 50 to <60 | C |
| <50 | D |

Example if an organisation scores 61 in People vertical, 48 in Process vertical and 73 in Technology vertical then the overall grading of the organisation will be ‘BDA’.

## 5. CONCLUSION

The security metric architecture of networks has been viewed previously from different angles[7]. However, the grading methodology proposed in this paper is designed in simplistic and generic terms with the aim of creating a metric for comparing network systems comprising of varied technologies. The proposed metric is also holistic and not narrow to give any undue weightage to technology specific parameters. The model also gives equal weightage to the three verticals of People, Process and Technology for ensuring holistic security of any cyber system. The model can be translated and calibrated using mathematical formulae and spread-sheets. The grading will also enable the organisation in understanding their own weaknesses; find their position in the environment and take suitable measures to overcome the shortcomings so as to ensure minimum losses in case of any crisis.

## 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 Lowans GIAC 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.

## AUTHORS

Lieutenant General Rajesh Pant, Ati Vishisht Seva Medal, Vishisht Seva Medal, was commissioned into the Corps of Signals, Indian Army on 23 Dec 1973. He is one of the foremost authorities in the field of a variety of technologies related with Info Communication Technology and Information Warfare. He has been a panel member in many national level technical seminars on these subjects, with an illustrious career of 40 years of rare operational experience combined with triple post graduate degrees.

C N Khairnar is currently serving in the Faculty of Communication Engineering, Military College of Telecommunication Engineering (MCTE), Mhow (M.P). He received his Bachelor of Engineering (Electronics), from Pune University and Master of Technology (Electronics), from Visvesvaraya Regional Engineering College (Now VNIT), Nagpur. He is Ph.D. in the field of Electronics and Telecommunication Engineering. He has about 18 years’ experience of academic institutions and industry. His areas of interest are Low-power mobile computing, Software Defined Radios and Cognitive Radios.