CHANDIGARH GROUP OF COLLEGES
Campus : Jhanjeri, Mohali

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

Existing Vulnerability Scoring Methodologies and the Scope of Improvement

Gagandeep Chawla[1]
Dr. Neeraj Sharma[2]
Dr. Narender Kumar Rawal[3]

Abstract:

Vulnerabilities in Software or Computer network pose a critical risk to any Software company or Organization. The digitalisation of various departments, institutes and our day to day chores have made us dependent on software's. But, are these software secure? Are they not vulnerable to threats? Yes, they are vulnerable. But there exists methods by which we can safeguard ourselves from these vulnerabilities. Vulnerability is the inability of a system or a unit to withstand the effects of a hostile environment. But to find remedial solutions to these vulnerabilities with greatest risks they need to be prioritised and ranked according to their impact on the IT systems. This means to finally find a remedy for vulnerability and the impact it can put it need to be scored. There are a lot many rating systems devised for prioritisation and ranking of the vulnerabilities. This paper briefly discusses the types of scoring methods with Common Vulnerability Scoring System (CVSS) in particular. A brief literature survey is done on the scoring method and equations. This paper further shows the need for research to get a new vulnerability scoring methodology in order to improve the score of the vulnerabilities.

Keywords: Vulnerability, CVSS, Software, Scoring method, scoring equations.

1.Research Scholar, Punjab Technical University, Kapurthala, India.
2.Dean & Professor, GianJyoti School of Management, Banur, District Patiala, India.
3. Assistant Professor, H.N.B Garhwal University, Uttarakhand, India

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

I.INTRODUCTION

There is an exponential growth in the number of vulnerabilities alongwith the increase in number of software's and our dependency on them. This growth in number of vulnerabilities poses a big challenge to the organisations, software merchants and IT security managers.The security vulnerabilities in software can arise from a variety of problems, like errors in design,misconfigured systems, or defects, commonly known as bugs. These vulnerabilities could be exploited by one or more threats which can harm the confidentiality, the reliability and the availability of the system [1, 2]. This means they can harm a system to a great extent and leave the system totally or partially useless and put its information under stake.

In order to safeguard and protect against the vulnerabilities with greatest risksthey need to be prioritised and ranked according to their impact on the IT systems. This can help organisations and software vendors find remedial solutions for them. Any vulnerability needs ranking according to which it can be scored assessed and then have remedial action for it. This means to finally find a remedy for a vulnerability, it needs to be scored, to find the impact it can put. There are a lot many rating systems devised for prioritisation and ranking of the vulnerabilities. These have mostly been given by the software vendors and researchers. These rating methodologies can be broadly categorised as:

1) Qualitative

2) Quantitative

II. COMMON VULNERABILITY SCORING SYSTEM (CVSS)

The Common Vulnerability Scoring System (CVSS), version 1 [2], CVSS version 2 [9, 1] and CVSS version 3(Preview released in December 2014,has given time for public feedback till February 2015, final version will be released later)[17], US-CERT's

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

vulnerability scoring system [11], and the PVL metric [12] are the quantitative systems available for vulnerability scoring.

Quantitative methodologies are better than qualitative as they give proper score. From the list of the quantitative methods available CVSS is the one which is a free and open vulnerability evaluation criteria. It also provides insight into how scores are calculated [1, 13] that means the formulas are available to the public. It is also of our interest so, further we focus on CVSS and since CVSS version 3 has only the PREVIEW released we aim at CVSS version 2 for further focus. Even the National Vulnerability Database (NVD) uses CVSS for measuring the severity of vulnerabilities. NVD is a vulnerability database maintained by the U.S. government and consists of 68,054 vulnerabilities recorded till 15/01/2015 [14].

CVSS has three metric groups (where each metric group gives a score and is furthera set of metrics). It gives scores between 0 to 10 where 0 means no vulnerability and 10 indicates the highest possible value of vulnerability score.The three metric groups of CVSS v2(as shown in Figure 1)are:-

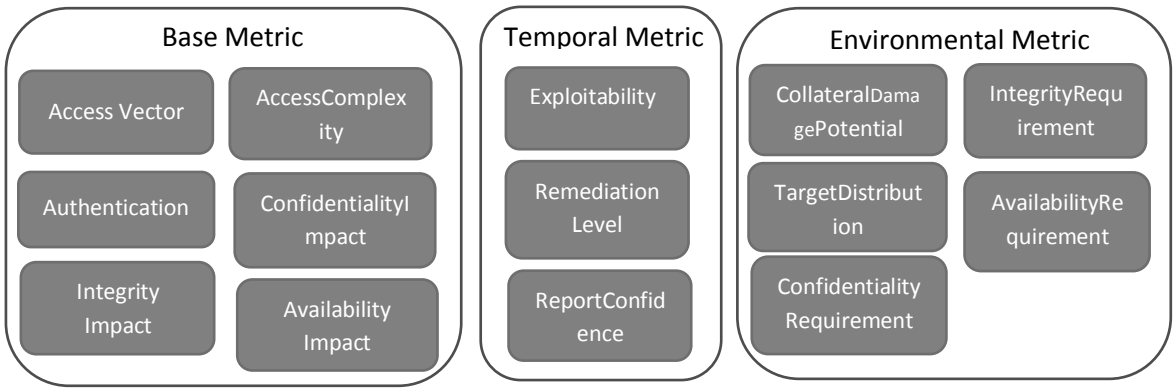
1. Base: It represents the type of vulnerability that are fundamental and intrinsic to it. It is basically of static type that means it doesnot change over time and environment. In CVSS Version 2 there are 6 base metrics i.e. Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact and Availability Impact.

2. Temporal: This represents characteristics of vulnerabilities that changes over time but not over the environment.Three factors that are covered under temporal metric are Exploitability(E), Remediation Level (RL) and Report Confidence(RC).

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

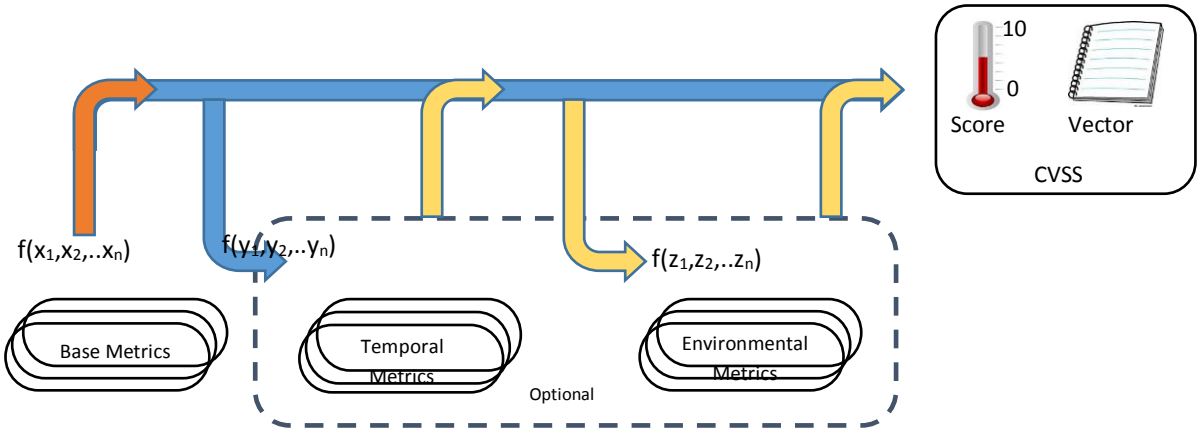
3. Environment:These representscharacteristics that are unique to each user's environment.The CVSS environment metric group comprises of Collateral Damage Potential (CDP), Target Distribution (TD),and Security Requirements(CR, IR, AR)[1, 2].

Figure 1: Metric categories of CVSS Version 2



CVSS calculates base scores for any vulnerabilities and takes temporal and environment metrics as optional (both version 2[1] and version 3[18] as per preview). However, if temporal and environment scores are to be computed, they are inclusive of base scores as depicted in the Figure 3.

Figure 3: Direction of Score Calculations in CVSS Version-II.



International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

The base equation is the foundation of CVSSscoring.

The scoring in CVSS Version 2 is as follows:

The base equation is:

BaseScore6 = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)–1.5)*f(Impact))

Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))

Exploitability = 20* AccessVector*AccessComplexity*Authentication

f(impact)= 0 if Impact=0, 1.176 otherwise

Table 1.The weights of the base metrics in CVSS version 2.

Metric Name	**Metric Values**	**Metric Weights**
Access Vector	Local, Adjacent Network,	0.395, 0.646, 1
Access Complexity	High, Medium, Low	0.35, 0.61, 0.71
Authentication	Multiple, Single, None	0.45, 0.56, 0.704
Confidentiality	None, Partial, Complete	0.0, 0.275, 0.660
Integrity Impact	None, Partial, Complete	0.0, 0.275, 0.660
Availability Impact	None, Partial, Complete	0.0, 0.275, 0.660

The Temporal Equation is (CVSS v2):
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
*RemediationLevel*ReportConfidence)

Table 2. The weights of the Temporal metrics in CVSS version 2.

Metric Name	**Metric Values**	**Metric Weights**
Exploitability	Unproven/proof-of- concept/ functional /high/not defined	0.85/0.9/0.95/1.00/1.00
Remediation Level	Official-fix/temporary-fix/ workaround/ unavailable/not	0.87/0.90/0.95/1.00/1.00
Report Confidence	Unconfirmed/uncorrobated / confirmed / not defined	0.90/0.95/1.00/1.00

The Environmental Equation is (CVSS v2):

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

EnvironmentalScore = round_to_1_decimal((AdjustedTemporal + (10-AdjustedTemporal)* CollateralDamagePotential) *TargetDistribution)

AdjustedTemporal = TemporalScore recomputed with the BaseScore's Impact subequation

replaced with the AdjustedImpact equation

AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)

*(1-AvailImpact*AvailReq)))

Table 3.The weights of the environment metrics in CVSS version 2.

Metric Name	**Metric Values**	**Metric Weights**
CollateralDamagePotential	None/low/low-medium / medium-high / high/ not defined	0/0.1/0.3/0.4/0.5/0
TargetDistribution	None/low/medium / high/ not	0/0.25/0.75/1.00/1.00
ConfRequirement	low/medium / high/ not defined	0.5/1.0/1.51/1.0
IntegRequirement	low/medium / high/ not defined	0.5/1.0/1.51/1.0
AvailRequirement	low/medium / high/ not defined	0.5/1.0/1.51/1.0

III. BRIEF LITERATURE SURVEY

A large number of vulnerabilities rating systems have been presented since 1998. As already said, these are categorised as systems giving scores quantitatively or qualitatively. But most of these systems have not publicised their formulas [3, 4, 5, 6, 7].

CVSS is an open scoring system which gives its formula.CVSS has become a standard and has been widely adopted by the IT community. But, still there is a scope of improvement in CVSS. There are many researchers across the globe who are working on it like [15, 16,19, 20, 21]. Out of these, the one of our interest is [16] by Spanos et al. who have proposed a methodology called Weighted Impact Vulnerability Scoring System (WIVSS). WIVSS methodology puts its focus on base metrics and uses the same 6

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

factors that CVSSv2 (Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact and Availability Impact) but they have assigned different weights to the three impact metrics (refer Table 4) unlike CVSSv2 (refer Table 1). The reason for different weights given by them as per literature [9, 12] is that Integrity Impact is more severe than Availability Impact.Similarly Confidentiality Impactis more severe than Integrity and Availability Impact.

So, accordingly WIVSS assigns the weights in the following manner

Weight of Confidentiality Impact > Weight of Integrity Impact > Weight of Availability Impact

Table 4.The weights of the base metrics in WIVSS [16].

Metric Name	**Metric Values**	**Metric Weights**
Access Vector	Local, Adjacent Network,	0.395, 0.646, 1
Access Complexity	High, Medium, Low	0.35, 0.61, 0.71
Authentication	Multiple, Single, None	0.45, 0.56, 0.704
Confidentiality	None, Partial, Complete	0.0, 1.5, 3.0
Integrity Impact	None, Partial, Complete	0.0, 1.2, 2.4
Availability Impact	None, Partial, Complete	0.0, 0.8, 1.6

They[16] experimented with WIVSS Score and CVSS v2 scores for a given set of vulnerabilities and showed improvement in both score's diversity. However,Spanos et al. has put focus on Base Metrics only but [8] shows that environment has an impact on scores and for vulnerabilities with same base scores, given the different environments, the scores will differ.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

In [15] Wang et al. has considered the environment factor, but unlike CVSS which has a different set of Environment Metric. Wang et al. found that evaluation methods for some subjective evaluation factors are too difficult to quantify and also temporal and environment metric score of one host have no reference value for another host. So, they added a metric factor into the base metric itself, which can reflect the host environment. They took the "Type of host status" and "OS of the host" as a factor into the base metric and gave weights to them as shown in Table5. Hence, their base matrix comprised of Access Vector, Access Complexity, Authentication, Confidentiality Impact and Availability Impact, Server Type and OS Type. Their Experimentation and Analysis gave better scores.

Table 5.Metric Factors in Host Environment of methodology in [16].

Host Environment factors			
Metric	**Description**	**Metric Value**	**Reference Value**
Server Type	Type ofhost status	Common Client/ Business Host/Server Host	0.5/0.8/1.0
OS Type	OS of host	Linux system/ Only windows system/ Windows and other systems	0.6/0.9/1.0

The work in this research will be in line with [16] and will include an Environment Representative into the base metric as in [15]. However, it will be different from them as it will combine the concept of both [15,16] and will introduce a new factor "Vulnerability Type" into it. The weight assigned may also differ.Hence, our base metric will comprise of more factors than theirs and will have its own scoring mechanism.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

IV. NEED FOR RESEARCH

As per the literature review certain gaps have been found, which pave way for research. It has been found that none [15, 16] dealt with "Vulnerability Type" as a factor to be included in the metric to compute the score which we feel is equally important. This will affect, enrich and improve the scoring to check the impact of vulnerability and hence help to draw proper mechanism to safeguard from them.

So, this leave possibility for research in proposing an improvedVulnerability Scoring Methodology (combining with the advantages and disadvantages of CVSS) that will assign different weights to all the metrics as per their severity and also consider an "Environment Representative" and "Vulnerability Type" in base metric to finally become the part of the score which will show "How vulnerable the vulnerability is?"

V. FUTURE SCOPE

As this research is considering 'Environment Representative' and 'Vulnerability Type' factors into the base score itself therefore this research will lead to a methodology that will provide better score for vulnerability. This means by just looking at the base scores better judgement could be drawn regarding the impact and risk level of a vulnerability. Hence, it will help the Software merchants, IT managers, Organisations and the concerned to find a better remedial solution as a security measure for the software.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

REFERENCES

[1] Mell, P., Scarfone, K., &Romanosky, S. June, 2007. A complete guide to the common Vulnerability scoring system version 2.0. Available at:
http://www.first.org/cvss/cvssguide. html

[2] Schiffman, M., & Cisco, C. I. A. G. June, 2005. A complete guide to the common Vulnerability scoring system (cvss). Available at: http://www.first.org/cvss/v1/guide.

[3] IBM. X-Force frequently asked questions. Available at
http://www.935.ibm.com/services /us/iss/xforce/faqs.html .

[4] Microsoft. May, 2012. Security Bulletin Severity Rating System. Available at: http://technet.microsoft.com/en-us/security/gg309177.aspx

[5] Cox, M. February 2004. Classification of Security Issues. Available at: http://www.redhat.com/rhecm/rest-rhecm/jcr/repository/collaboration/jcr:system/jcr:versionStorage/5e76ea2e7f000001397bc9e8eb926b37/1/jcr:frozenNode/rh:pdfFile.pdf

[6] Mozilla Foundation. March, 2013. Mozilla Foundation Security Advisories. Available at: http://www.mozilla.org/security/announce/.

[7] Qualys. Severities KnowledgeBase. Available at http://www.qualys.com/research/knowledge/severity/.

[8] Ibidapo, A.O. , Zavarsky, P. ; Lindskog, D. ; Ruhl, R.(2011). An Analysis of CVS v2 Environmental Scoring, Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom), 1125 – 1130.

[9] Mell, P., &Scarfone, K. (2007). Improving the common vulnerability scoring system.IET Information Security, 1(3),119-127.

[10] Available at: http://www.first.org/_assets/downloads/cvss/cvss-v30-preview2-metricvectorstring-december-2014.pdf

[11] US-CERT. Vulnerabilities Notes Database Fields Descriptions. Available at: http://www.kb.cert.org/vuls/html/fieldhelp.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

[12] WANG, Y., & YANG, Y. (2012). PVL: A Novel Metric for Single Vulnerability Rating and Its Application in IMS.Journal of Computational Information Systems, 8(2), 579-590.

[13] Karen Scarfone and Peter Mell. (2009) An Analysis of CVSS Version Vulnerability Scoring. National Institute of Standards and Technology(NIST).

[14] Available at :https://nvd.nist.gov.in

[15] Wang,R.,&Gao, L. (2011). An Improved CVSS- based vulnerability scoring Mechanism.Inpoceedingsof IEEEThirdInternational Conference Multimedia Information Networking and Security (MINES).China.352-355.

[16]Spanos, G. &Sioziou,A. (2013).WIVSS: a new methodology for scoring information systems vulnerabilities, In Proceedings of the ACM 17th Panhellenic Conference on Informatics.83-90.

[17] Available at :http://www.first.org/cvss/v3/development.

[18] Available at : http://www.first.org/_assets/downloads/cvss/cvss-v30-preview2-formula-december-2014.pdf.

[19] Fruhwirth,C. &Mannisto, T. (2009).Improving CVSS- based vulnerability prioritization and response with context information. In proceedings of IEEE Third International Symposium on Empirical Software Engineering and Measurement.535-544.

[20]Tripathi, A. & Singh U.K. (2011).On Prioritisation of Vulnerability Categories Based on CVSS Scores.in proceedings of IEEE 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT).692-697.