2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing

An Analysis of CVSS v2 Environmental Scoring

Ayodele Oluwaseun Ibidapo, Pavol Zavarsky, Dale Lindskog, Ron Ruhl
Department of Information Systems Security Management
Concordia University College of Alberta
7128 Ada Boulevard, Edmonton, Alberta, Canada T5B 4E4.
aibidapo@yahoo.com, {pavol.zavarsky, dale.lindskog, ron.ruhl}@concordia.ab.ca

Abstract—**This paper analyses the effect of the environmental metrics on the CVSS v2, and it shows that the environmental metrics impact the CVSS base score values in more ways than can be gleaned from the CVSS calculator provided by the NVD. This paper also unveils unexpected anomalies of "negative" calculated results of the Overall CVSS score when the base score is subjected to the environmental metrics. It also reveals that base scores of equal values do not necessarily remain equal when subjected to the environmental metrics. The presented results are based on a theoretical analysis of tthe formulas used in the CVSS v2 calculations. An approach to calculating the Overall CVSS score that eliminates the occurrence of "negative" values, and keeps the values within the range (0.0 – 10.0) as defined in the guide for scoring vulnerabilities in the CVSS v2 is also suggested in this paper.**

Keywords-CVSSv2; environmental metrics; base score; risk management; Overall CVSS score

I. Introduction

Common Vulnerability Scoring System (CVSS) has metamorphosed from an emerging standard to become the de-facto standard for communicating and documenting the major characteristics of vulnerabilities, and also for measuring potential impacts of exploitation of these vulnerabilities[1],[2],[5]. Providing standardized information, using an open framework to enable organizations prioritize mitigation of vulnerabilities was the motivating factor behind the development of CVSS. In the IT community, CVSS is widely embraced and adopted. It is a mandated requirement used worldwide for evaluating the security of payment card systems. The National Vulnerability Database (NVD) [7] maintained by the U.S. government is a repository of over forty-five thousand, and counting known vulnerabilities based on the CVSS. It is also mandated for use in the Security Content Automation Protocol (SCAP) by the U.S. government [6].

CVSS is the only open specification amongst other schemes for scoring vulnerabilities, and it is designed to be quantitative to ensure analysts do not undertake qualitative evaluations when scoring vulnerability severity. It also provides visibility into how scores are calculated [6].

To properly and effectively quantify vulnerabilities for prioritization purposes, an organization cannot rely solely on the base score generated by the NVD. Rather, organizations are required to add the contextual information so as to have a true picture and properly prioritize the response process that can be selected to mitigate the vulnerabilities [3]. In line with guidelines stated in the technical and operational requirements of the Payment Card Industry Data Security Standard (PCI/DSS) which states that for a component to be considered compliant, it must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0 [8]. When this score is subjected to the environmental (contextual) metrics which reflect the user environment, research shows that, depending on the environment, the Overall CVSS score value can have a range of values significantly lower or higher than 4.0; implying that the base score of 4.0 should not just be taken at face value.

The current calculator provided by the NVD for calculating vulnerability impacts is limited to calculating one Overall score for one combination of environmental metric group at a time. However, the improved calculator in [1] can instantaneously calculate a range of possible Overall score values for one combination of environmental metrics; immediately arming an IS professional tasked with the responsibility of mitigating vulnerability risks with the required information to make appropriate decisions. Utilizing this new calculator and the formulas in [2], this research discovered that CVSS v2 base scores when subjected to the environmental metric group in some cases generated "negative" Overall scores, contrary to CVSSv2 specifications.

II. Background

Three metric groups make up CVSS namely, Base, Temporal and Environmental, each consisting of a set of metrics. CVSS assigns vulnerability scores on a scale of 0 to 10, where 0 indicates no vulnerability, and 10 indicates the highest possible value of vulnerability score. The "Base" metric group represents the characteristics of vulnerability that are fundamental and intrinsic to it. These characteristics are constant with time and across user environments. The "Temporal" metric group represents how the severity of vulnerability changes over time, but not within the user environment. The "Environmental" metric group reflects the characteristics of vulnerability with reference to a specific environment [2]. The base metric can be used independently or in combination with the other two metrics, temporal and environmental, based on mathematical equations formulated by P. Mell et al [2]. Temporal vulnerability scores are calculated using both the base score and temporal metric

978-0-7695-4578-3/11 $26.00 © 2011 IEEE
DOI

values as parameters. Environmental scores are computed using an equation that is based on both the temporal score and the environmental metric values as parameters [1].

Environmental metrics group contextualizes vulnerability, thus reflecting the imminent threat to a particular environment. Three different characteristics of vulnerability are measured by this group: (1) Collateral Damage Potential (CDP) impact, which measures the degree of loss to information, revenue, life or physical assets, through damage as a result of exposure to a particular vulnerability; (2) Target Distribution (TD) impact, which measures the percentage of systems within a particular environment affected by the vulnerability; (3) the three security requirements, i.e. Confidentiality Requirement (CR), Integrity Requirement (IR), and Availability Requirement (AR) impacts. These three help to customise the CVSS score depending on the requirement of affected IT assets relative to confidentiality, availability, and integrity within the user's organisation [2].

CVSS, in its most prominent application in the U.S. National Vulnerability Database as a severity metric, does not take into consideration the information pertaining to the context (environment) of the exploit victims. It is a known fact amongst IS researchers and IT managers in the industry that for the same vulnerability, severity varies considerably from one organizations environment to the other. Therefore the base CVSS scores provided by NVD alone are not sufficient for prioritizing vulnerability in practice. To improve the quality of their prioritization, security managers will need to address this deficiency by adding the missing contextual information themselves. It is however unclear for them if this potential improvements worth the extra effort [3]. This research helps to address this issue by showing the impact the environmental metrics have on the base score.

Using the mathematical equations used in generating the CVSS scores, it can be seen that the values of the environmental metric group changes the degree of potential impacts and exploitability of vulnerabilities in various IT environments.

The foundation of CVSS scoring is the base equation as shown below.

BaseScore = Round_to_1_decimal(((0.6 * Impact) + (0.4* Exploitability) – 1.5) * f(Impact)) (1)

Impact = 10.41*(1 - (1 - ConfImpact) * (1 - IntegImpact) *(1 - AvailImpact)) (2)

Exploitability = 20 * AccessVector * AccessComplexity * Authentication (3)

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

BaseVector: AV:[L,A,N] / AC:[H,M,L] / Au:[M,S,N] / C:[N,P,C]/I:[N,P,C]/A:[N,P,C]

Confidentiality impact (C), integrity impact (I), and availability impact (A) can each have values of none, partial or complete as shown in Table 1.

TABLE I. BASE METRICS

Access Vector (AV)	Local	(L)	0.395
	Adjacent Network	(A)	0.646
	Network	(N)	1.000
Access Complexity (AC)	High	(H)	0.350
	Medium	(M)	0.610
	Low	(L)	0.710
Authentication (Au)	Multiple	(M)	0.450
	Single	(S)	0.560
	None	(N)	0.704
Confidentiality Impact (C) Integrity Impact (I) Availability Impact (A)	None	(N)	0.000
	Partial	(P)	0.275
	Complete	(C)	0.660

III. RELATED WORK

In [6], Scarfone and Mell extensively looked into the theoretical and experimental analysis of the base score on CVSS v2 by performing theoretical and experimental analysis of the base metric group. They generated theoretical scoring distributions for CVSS v2 by considering all the possible sets of metric values and calculating the corresponding scores and frequency of each score. There are 101 possible base score values ranging from 0.0 to 10.0, with increments of 0.1. They identified a total of 702 possible combinations of the base score metric values and analyzed 75 possible base scores which corresponded to the impact and exploitability sub scores in the CVSS v2. This research focused primarily on the base score, leaving out the environmental metrics group.

However, as earlier highlighted, in addition to the base score values generated by the NVD, it is required that an organization add the contextual (environmental) information. This gives the organization a true picture of how the vulnerability affects their environment, and helps them to properly prioritize the response process that can be selected to mitigate vulnerabilities. Fruhwirth and Mannisto in their research proposed that the temporal and the environmental metrics can be used to achieve this [3].

Laurent G in [4] attempted to directly analyze the impact of the environmental metric group on the CVSS v2. The scope of this research was however limited to the analysis of the impact of the security requirements of the environmental vector on the CVSS scores. This meant that of the five metrics that make up the environmental group, only three were taken into consideration, leaving out TD and CDP. Another limitation of [4] was that it was based on simulations, not the actual data from the CVSS v2 calculated values. The author concluded that the environmental score calculation is subject to certain difficulties which are yet to be proven.

A. Assad et al in [1] reported in the development of a new practical calculator for the CVSS v2 that, for any given vulnerability, the environmental metric group can have a total of 1920 possible combinations of values. That is, for each base score value, there are 1920 corresponding environmental values. However, due to the importance of mitigation of possible impacts and exploitability of vulnerabilities to IT risk management processes, the selection process can be a very difficult and time consuming process. This is due to the large number of possible combinations of temporal and environmental metric values.

This new calculator has expanded the functionality of available CVSS v2 calculators, making the estimation of possible overall CVSS v2 scores more manageable, considerably helping security managers and organizations make better informed risk management decisions.

IV. Methodology

The focus of this research is the environmental metrics and how they impact the base score value. As discussed, the environmental metrics group give meaning to the base score, enabling the IT manager directly map the value of the base score to his/her IT environment. To compute these scores the following equations are used:

EnvironmentalScore = round_to_1_decimal((
(AdjustedTemporal + (10 - AdjustedTemporal) *
CollateralDamagePotential) * TargetDistribution) (4)

where 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))) (5)

As shown in the Table II below, Confidentiality requirement (CR), integrity requirement (IR), and availability requirement (AR) can each have values of low, medium high or not defined.

Using the above environmental equations and the calculator developed in [1], this research investigated the effects of the environmental metrics on the base score by dividing the metrics into two groups; the security metrics group, comprising of confidentiality requirement, integrity requirement, and availability requirement; and a second group, the environmental metric group, comprising of the security metric group (AR, IR, and CR), and the target of distribution (TD) and collateral damage potential (CDP).

The first division is to give an insight into how the security metric group of the environmental metrics impacted the overall CVSS base score and the second classification was to investigate how the totality of the environmental metrics group affected the overall CVSS base score.

TABLE II. ENVIRONMENTAL METRICS

Collateral Damage Potential (CDP)	None	(N)	0.00
	Low	(L)	0.10
	Low-Medium	(LM)	0.30
	Medium-High	(MH)	0.40
	High	(H)	0.50
	Not Defined	(ND)	0.00
Target Distribution (TD)	None	(N)	0.00
	Low	(L)	0.25
	Medium	(M)	0.75
	High	(H)	1.00
	Not Defined	(ND)	1.00
Confidentiality Requirement (CR) Integrity Requirement (IR) Availability Requirement (AR)	Low	(L)	0.50
	Medium	(M)	1.00
	High	(H)	1.51
	Not Defined	(ND)	1.00

Environmental Vector:
CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/IR:[L,M,H,ND]/AR:[L,M,H,ND]

A. Security Metric Group

In this analysis neither the collateral damage potential (CDP) nor the target of distribution (TD) metrics were taken into consideration. The focus was on the security requirements (CR, IR, and AR). The purpose is to show the customizability of the CVSS and its mapping to confidentiality, integrity and availability for the user organization. This makes the CVSS a useful tool for administrators to map the CVSS scores to the security policy of the organization.

The theoretical distribution of the security metric group was analyzed by calculating the possible values of all the one-to-many values of the possible base scores. For each base score, there was a total of 64 different security environmental metric. These values reflect the different combination of ways the security metrics can be combined to increase, maintain or decrease the Overall CVSS value.

B. Environmental Metric Group

This analysis incorporated TD and CDP metrics alongside the security metrics. This analysis gives the total picture of how all the environmental metrics of the CVSS impact the corresponding base score value, further giving insight into the one-to-many mapping of the CVSS scores as outlined in the equations in [2]. Depending on how critical a system is and the risk exposure, the analysis of this group can help management decide to accept the risks and take no further action, or by selecting proper remedial actions, informed decisions can be made to mitigate risk.

In this group each base score value corresponds to 1920 possible values, giving the different combination of ways the environmental metrics can be combined to either increase, maintain or decrease the base score (overall CVSS) value.

V. Results

Rather than show all the results obtained in the course of this research, only the significant observations will be discussed.

Observations that stand out in this research include the following:

- Impact of the environmental metrics on the Overall CVSS score.
- Occurrence of negative Overall CVSS scores.
- Impact of Target of Distribution (TD) and Collateral Damage Potential (CDP) on Overall CVSS score
- Analysis of recurring base scores

A. Impact of the environmental metrics on the Overall CVSS score

Using the CVSS v2 formulas and the calculator in [1], it was confirmed that the environmental (contextual) factors significantly modify the base score and highlight a range of possible adjusted impact and Overall CVSS scores. Using the graph in Fig. 1 below for illustration, it can be shown that when a base score of 4 is subjected to the environmental

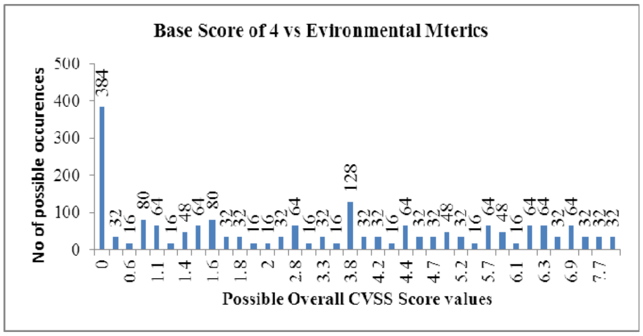

Figure 1. Impact of environmental metrics on base score of 4 when exploitability is 1.9 and impact subscore is 6.9

metrics, depending on the environmental characteristics of the IT environment, the score results can be modified accordingly to optimize the mitigation process.

An IT environment following the guidelines of the PCI/DSS to meet compliance requirements requires that the base score for a component must be less than 4.0 to be compliant. Fig 1 shows that when taken contextually, that is, when exposed to the environmental metrics, the Overall CVSS score can actually be as high as 8.1, and as low as 0.

Fig. 1 also shows a combination of ways to adjust the Overall CVSS score value. For instance, to bring a base score from a medium of 4 to a low of 1, figure 1 shows that there are 80 possible ways of achieving that using the filtering and refinement characteristics of the environmental metrics.

B. *Occurrence of negative overall CVSS scores*

Fig. 2 is the score distribution for a base score of 0.8 subjected to the environmental metrics. It shows the Overall CVSS scores and the corresponding number of possible outcomes. According to [2], the Overall base score value is expected to range from 0 to 10. Having a negative value is however unexpected. As shown in Fig 2, these negative values account for 5% of the total Overall CVSS score values, bringing to question the validity of the formula for calculating the CVSS v2 scores.

An environment that has an Overall CVSS score of zero (0) implies that no vulnerability exists in that environment, or that environment is not susceptible to the vulnerability.

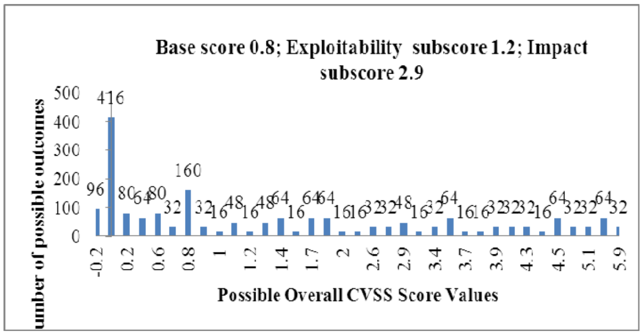

Figure 2. Impact of environmental metrics on base score of 0.8

This research further investigated this occurrence by calculating all the possible Overall CVSS Score values for each of the possible base scores. Fig. 3 below shows the Overall CVSS score distribution and their corresponding frequencies when subjected to the environmental metrics.

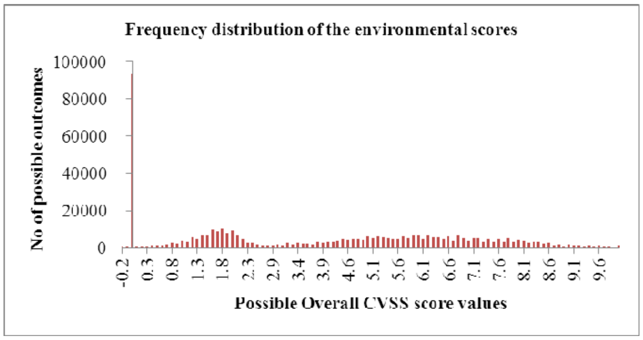

Figure 3. Overall CVSS Score distribution of CVSS v2 Environmental metrics

According to P. Mell et all in [6], there are 75 possible base scores corresponding to the impact and exploitability sub scores in the CVSS v2. The Overall Score distribution shows that when these values are exposed to the environmental metrics, that number rises to 99 possible Overall CVSS scores. The one value that never occurred within the 0 to 10 range was 9.9.

To solve the problem of negative-valued Overall CVSS scores and keep all Adjusted Base Score values in the interval (0.0,10.0), it is suggested that the coefficients 1.5 and f(Impact) = 1.176 in the equations in [2] be substituted with coefficients 1.32 and f(Impact) = 1.15, respectively. This modification would lead to 97 distinct values of the Adjusted Base Score, all within the 0.0 to 10.0 interval.

The "all positive" distinct values of the modified Adjusted Base Score are:

TABLE III. "ALL POSITIVE" ADJUSTED BASE SCORES

0.0	0.1	0.3	0.4	0.5	0.6	0.7	0.9	1.0
1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9
2.0	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8
2.9	3.0	3.1	3.2	3.3	3.4	3.5	3.6	3.7
3.8	3.9	4.0	4.1	4.2	4.3	4.4	4.5	4.6
4.7	4.8	4.9	5.0	5.1	5.2	5.3	5.4	5.5
5.6	5.7	5.8	5.9	6.0	6.1	6.2	6.3	6.4
6.5	6.6	6.7	6.8	6.9	7.0	7.1	7.2	7.3
7.4	7.5	7.6	7.7	7.8	7.9	8.0	8.1	8.2
8.3	8.4	8.5	8.6	8.7	8.8	8.9	9.0	9.1
9.2	9.3	9.4	9.6	9.7	9.8	10		

Of this new score distribution, 0.2, 0.8, and 9.9 will not be possible. Prior to this modification, only a base score of 9.9 was not possible to achieve.

C. *Impact of Target of Distribution (TD) and Collateral Damage Potential (CDP) on Overall CVSS score*

By definition, TD is an environment-specific metric which gives an approximate percentage of systems that could be affected by vulnerability. This is done by measuring the proportion of vulnerable systems. CDP on the other hand measures the potential for loss of life or physical assets through damage or theft [2].

From the environmental equations, TD and CDP can both have a value of zero. A TD of 0 implies that no target systems exist, effectively meaning, the environment is not at any risk. Likewise, a CDP of 0 implies that there are no threats to life, physical assets, productivity or revenue.

Incident prevention and management teams typically aim at keeping vulnerabilities within the IT environment to a bare minimum. Using the base score values coupled with the environmental metrics, they are able to prioritize accordingly.

TD does have a significant impact on the Overall CVSS score value as it is capable of single-handedly bringing the Overall CVSS Score value from whatever value down to 0. This in itself is logical in that if there is no target environment, then there is no risk. However, while the TD is not equal to 0, the CDP when combined with the security metric groups (CR, IR, and AR) can bring the Overall CVSS score down to 0. This can be illustrated thus; we may have a vulnerability existing in an environment (TD>0), where exploitation will have *some* impact (e.g. CI), in an environment where there is a corresponding *requirement* (CR). Yet the CVSS produces a severity score of 0. It implies some error in the formulation of the scoring system, however small the severity might be.

In contrast, it was discovered that at no point could the security metric group (CR, IR and AR) act on the base score as an independent group to bring the Overall CVSS score to 0. It was discovered that the security metric group of the environmental metrics can effectively only change the Overall CVSS score by a margin of 2.6 at its maximum. This means that irrespective of the IT environment, the security metric group of the environmental metrics can only effectively change the Overall CVSS score by a margin of 2.6. This is of significant use to the IS professional tasked with the responsibility of mitigating vulnerability risks.

However, as reported by Ali et al in [1], when subjected to the environmental metrics, each base score can have a total Overall CVSS Score of 1920. Of these 1920 Overall CVSS Scores, 384 – 512 were 0 and below, for every calculated base score value. This accounts for 20% – 26.7% of the possible values of the Overall CVSS score.

With CVSS being a standard for documenting and measuring the impacts of vulnerability exploitation within an IT environment, it would be expected that the CVSS v2 equations better reflect vulnerability scores that have a direct impact on the IT environment. For instance, the TD score distribution should be more evenly distributed so as to match more closely to realistic values. Allocating more than 20% of scoring resources to situations that will never or hardly occur does not give good mathematical justification.

D. *Analysis of recurring base scores*

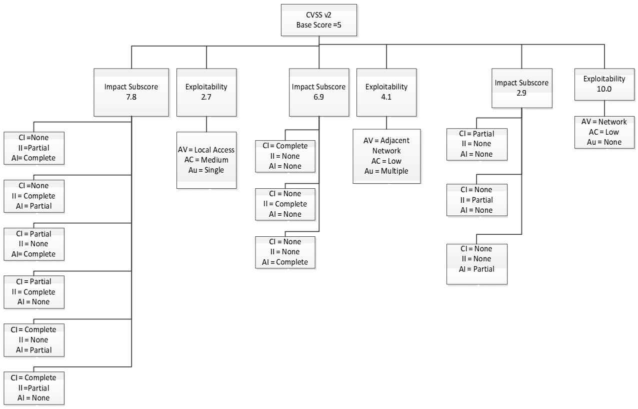

Figure 4. Base Score 5 and the relationships between Impact Subscore and Exploitability

Fig. 4 above shows the impact subscore and exploitability subscores which together generate a base score value of 5. These base score values of 5 are taken from the low end, midrange, and high end of the base score range. Research shows that when these base score values of 5 are each subjected to the environmental metrics, each of them behaves differently, generating differing values.

Fig. 5 – 7 show possible base scores of 5 generated by differing combinations of impact subscore and exploitability. These figures show the following:

Impact subscore = 6.9 and Exploitability = 4.1 Overall CVSS score range = 0.6 – 8.6;

Impact subscore = 7.8 and Exploitability = 2.7 Overall CVSS score range = 0.6 – 8.3;

Impact subscore = 2.9 and Exploitability =10.0 Overall CVSS score range = 1.0 – 8.0.

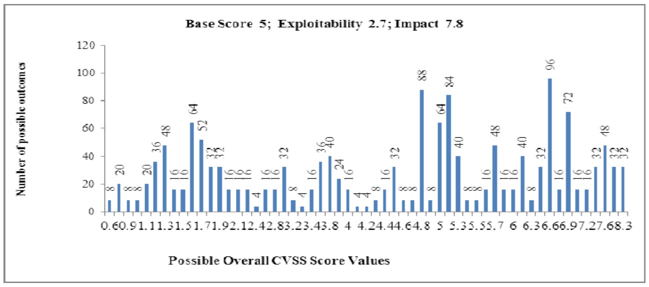

Figure 5. Impact of environmental metrics on base score of 5 when exploitability is 2.7 and impact is 7.8

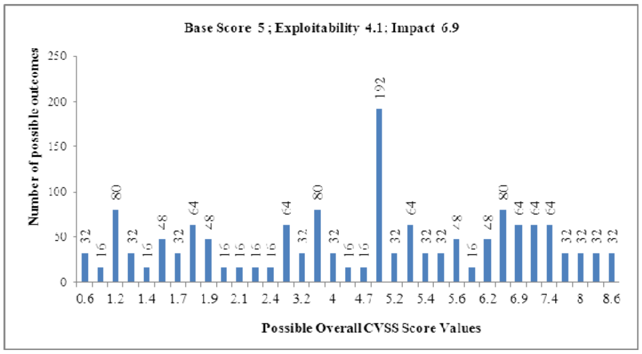

Figure 6. Impact of environmental metrics on base score of 5 when exploitability is 4.1 and impact is 6.9

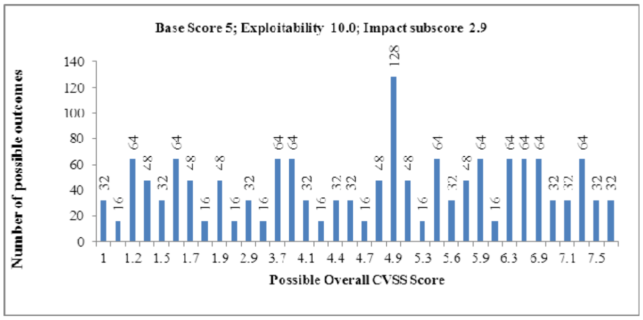

Figure 7. Impact of environmental metrics on base score of 5; exploitability of 10.0 and impact of 2.9

This implies that for a combination of impact subscore and exploitability subscore that generate the same base value, Overall CVSS score varies considerably. Figure 5 - 7 above also show the probability of obtaining a particular Overall CVSS score when a base score is exposed to the environmental metrics.

Fig. 5 – 7 show that vulnerabilities with a base score of 5 and above account for 43.75% - 48.1% of the total Overall CVSS scores.

The low vulnerability range (0 – 3.9) account for 36.5 – 39.6% of the Overall CVSS scores; the median range (4 – 7.9) account for 54.2 – 61.5% of the Overall CVSS scores and the high range (8-10) account for 2.1 – 6.25% of the Overall CVSS scores.

VI. CONCLUSION

In the present day IT environment, risk management is an on-going activity due to the number of vulnerabilities discovered on a daily basis. The CVSS being an important tool in prioritizing risk mitigation activities is heavily depended upon for this purpose. This research however showed that over-reliance on the CVSS base score value alone may not necessarily be the true reflection of the vulnerability state in the user environment. Rather, to get a true value of vulnerability, the base score should be subjected to the environmental metrics, contrary to the optional reference of the authors in [2].

This research looked into the analysis of the effect of the environmental metrics on the CVSS v2. All combinations of the base scores were subjected to the environmental metrics and all the possible Overall CVSS score calculated. This research revealed a fundamental flaw in the CVSS v2 calculation whereby negative Overall CVSS scores were generated, contrary to the design. It was also revealed that base scores of equal values when subjected to the environmental metrics have differing Overall CVSS scores.

In this paper an approach to eliminating the negative values from the Overall CVSS score was suggested. However, it would be suggested that the effect of the target of distribution (TD) on the Overall CVSS be looked into. It was shown that this metric contributed largely to the Overall CVSS value being zero (0) (20 – 26.7%). This is considered to be quite significant, considering the fact that the CVSS is for quantifying real risk to an IT environment. Allocating more that 20% of resources to conditions that might never occur is not a sign of good resource management.

ACKNOWLEDGMENT

The first author would like to heartily thank the research team of Concordia University College of Alberta for all their positive criticism, guidance and support in carrying out this research. He would also like to thank his parents and siblings for their love and support throughout his studies. The first author also thanks God Almighty for the privilege of going through MISSM program, and surrounding me with some of the best minds.

REFERENCES

[1] Assad Ali, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl, " A Software Application to Analyze Affects of Temporal and Environmental Metrics on Overall CVSS v2 Score", Concordia University College of Alberta, Edmonton, Canada, October 2010.

[2] Peter Mell, Karen Scarfone, and Sasha Romanosky, "CVSS: A complete Guide to the Common Vulnerability Scoring System Version 2.0", National Institute of Standards and Technology, June 2006.

[3] Christian Fruhwirth and Tomi Mannisto, "Improving CVSS-based vulnerability prioritization and response with context information", Helsinki University of Technology, Finland, October 2009.

[4] Laurent Gallon, "On the impact of environmental metrics on CVSS score", The Second IEEE International Conference on Privacy, Security, Risk and Trust, Minneapolis, Minnesota, USA, August 2010

[5] Ramaswamy Chandramouli, Tim Grance, Rick Kuhn, and Susan Landau, "Common Vulnerability Scoring System", IEEE Computer Society, November 2006.

[6] Karen Scarfone and Peter Mell, "An analysis of CVSS Version 2 Vulnerability Scoring", National Institute of Standards and Technology (NIST), October 2009.

[7] National Vulnerability Database, http://nvd.nist.gov/, (current 03/2011)

[8] "Technical and Operational Requirements for Approved Scanning Vendors (ASVs) Version 1.1", Payment Card Industry Data Security Standards Council, September 2006.