

An Analysis of CVSS Version 2 Vulnerability Scoring

Karen Scarfone

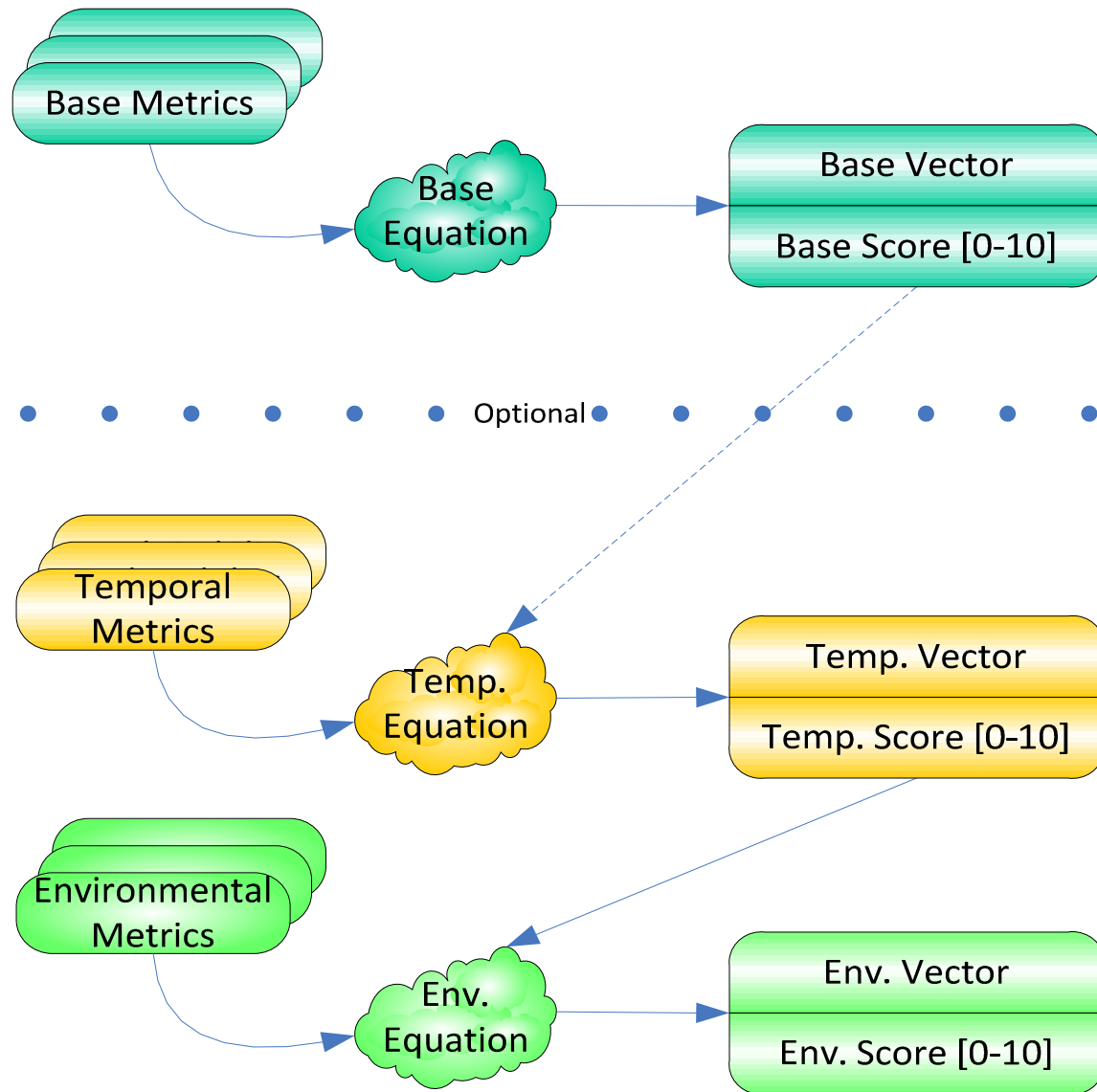
Peter Mell

National Institute of Standards and Technology

Background

- The Common Vulnerability Scoring System (CVSS) is a specification for documenting the major characteristics of vulnerabilities and measuring the potential impact of vulnerability exploitation through scores
- CVSS provides standardized information that organizations use to prioritize their mitigation responses to new vulnerabilities
- CVSS is developed and maintained by the CVSS Special Interest Group (CVSS-SIG) under the Forum for Incident Response and Security Teams (FIRST).

Metrics and Scores



CVSS Version 1 and 2

- CVSS version 1 published October 2004
- CVSS version 2 published June 2007
- National Vulnerability Database repository (<http://nvd.nist.gov>)
 - 39101 CVSS v2 base scores as of 9/30/09

[Update Scores](#) [Reset Scores](#) [View Equations](#)




CVSS Base Score	7.5
Impact Subscore	6.4
Exploitability Subscore	10
CVSS Temporal Score	Undefined
CVSS Environmental Score	Undefined
Overall CVSS Score	7.5

Base Score Metrics

Exploitability Metrics

AccessVector	Network 
AccessComplexity	Low 
Authentication	None 

Impact Metrics

ConfImpact	Partial 
IntegImpact	Partial 
AvailImpact	Partial 

NVD CVSS Calculator

<http://nvd.nist.gov/cvss.cfm>

Goals for CVSS v2

- Produce higher mean and median scores
- Increase score diversity
 - Avoid inappropriately mapping different vectors to the same score
- Change input metrics to better characterize security relevant aspects of vulnerabilities
- Fix scoring inconsistencies
 - (not part of our research as this was fully tested by the CVSS v2 team)

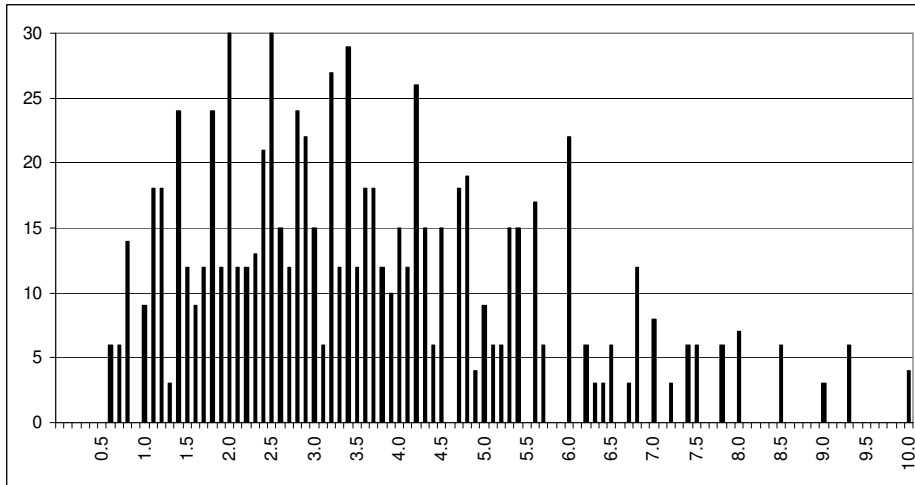
CVSS v2 Creation

- Identify input metrics
 - 6 metrics with 729 possibilities
 - Divided metrics into 3 exploit related and 3 impact related
- Create lookup tables with expert input
 - Exploit table with 27 entries
 - Impact table with 27 entries
- Combine tables .4 for exploitability and .6 for impact
- Create equation to approximate lookup table
 - Includes weighting metric values
 - Deviated from lookup tables to adjust score distribution upwards

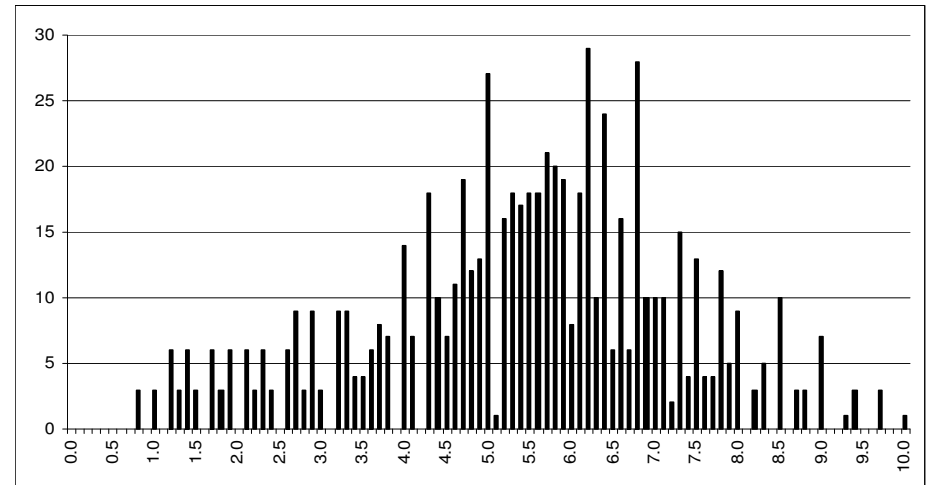
The Analysis Method

- Focused only on CVSS Base Scores
- Theoretical Analysis
 - Consider all possible sets of metric values
 - V1 has 864 and v2 has 729
- Experimental Analysis
 - 11012 vulnerabilities in Common Vulnerabilities and Exposures (CVE) dictionary
 - All CVEs between June 20, 2007 and April 30, 2009
 - Scoring done by the National Vulnerability Database (<http://nvd.nist.gov>)

Theoretical Score Distribution



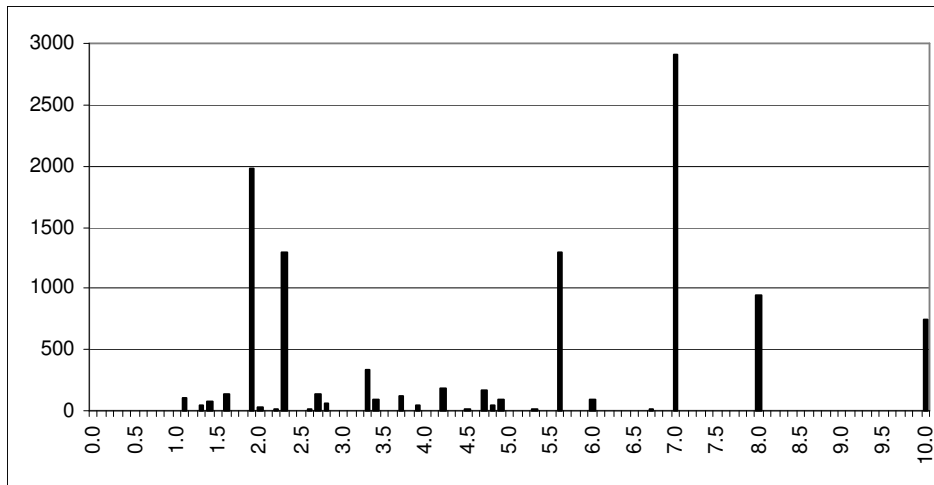
Theoretical distribution of CVSS v1 scores



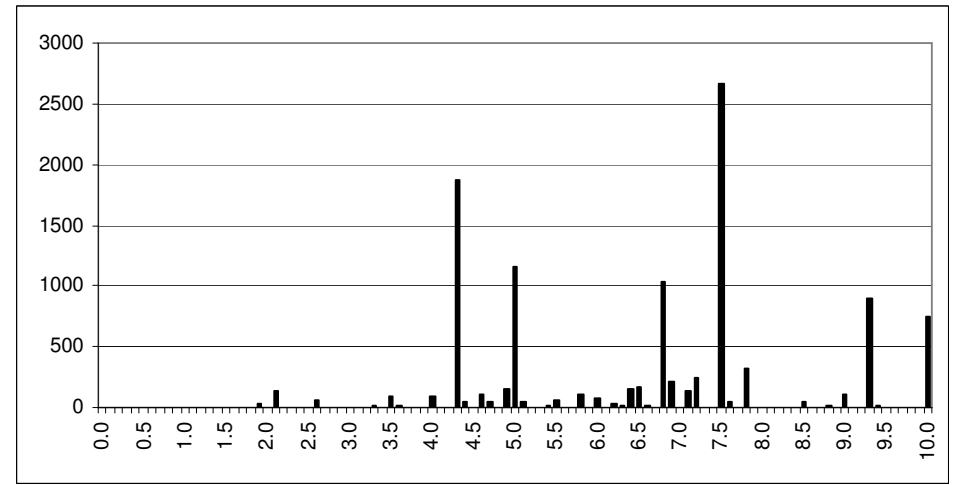
Theoretical distribution of CVSS v2 scores

Goal: v2 should produce generally higher scores than v1

Experimental Score Distribution



Experimental CVSS v1 scores



Experimental CVSS v2 scores

V1 mean was 5.1 and median was 5.6

v2 mean was 6.6 and median was 6.8

Goal: v2 should produce generally higher scores than v1

Score Diversity

- Theoretical Analysis
 - V1 has 66 possible scores out of 101
 - V2 has 75 possible scores out of 101
- Experimental Analysis
 - 35 distinct v1 scores
 - 51 distinct v2 scores

Goal: CVSS v2 should have greater score diversity

Score Diversity

10 most common vectors comprise 77% of all v2 vulnerabilities

Most common v2 vectors in experimental data

Freq	AV	AC	Au	C	I	A	v1	v2
2662 (24.2%)	N	L	N	P	P	P	7.0	7.5
1527 (13.9%)	N	M	N	N	P	N	1.9	4.3
999 (9.1%)	N	M	N	P	P	P	5.6	6.8
896 (8.1%)	N	M	N	C	C	C	8.0	9.3
743 (6.7%)	N	L	N	C	C	C	10.0	10.0
577 (5.2%)	N	L	N	P	N	N	2.3	5.0
443 (4.0%)	N	L	N	N	N	P	2.3	5.0
251 (2.3%)	L	L	N	C	C	C	7.0	7.2
240 (2.2%)	N	L	N	N	N	C	3.3	7.8
217 (2.0%)	L	M	N	C	C	C	5.6	6.9

Most common v1 and v2 scores in experimental data

v1 score	v1 freq	v2 score	v2 freq
7.0	2916 (26.5%)	7.5	2662 (24.2%)
1.9	1979 (18.0%)	4.3	1872 (17.0%)
2.3	1293 (11.7%)	5.0	1153 (10.5%)
5.6	1291 (11.7%)	6.8	1038 (9.4%)
8.0	948 (8.6%)	9.3	896 (8.1%)
10.0	745 (6.8%)	10.0	743 (6.7%)
3.3	331 (3.0%)	7.8	321 (2.9%)
4.2	183 (1.7%)	7.2	251 (2.3%)
4.7	163 (1.5%)	6.9	217 (2.0%)
2.7	140 (1.3%)	6.5	167 (1.5%)

CVSS treats confidentiality, integrity, and availability as equally important which lowers score diversity

Exploitability Characteristics

Frequencies of each value for exploitability metrics

Metric	Value	v1	v2
AccessComplexity	Low	55.7%	55.7%
	Medium	N/A	41.9%
	High	44.3%	2.4%
Authentication	Not required/None	93.3%	93.3%
	Required	6.7%	N/A
	Single	N/A	6.7%
	Multiple	N/A	0.0%
AccessVector	Remote	90.2%	N/A
	Network	N/A	89.9%
	Adjacent Network	N/A	0.3%
	Local	9.8%	9.8%

Red and bolded percentages show v2 metrics that did not have a large impact on the scoring distribution

Impact Characteristics

Frequencies of each value for impact metrics

Metric	Complete	Partial	None
Confidentiality	22.8%	47.4%	29.8%
Integrity	21.9%	57.2%	20.9%
Availability	26.5%	45.5%	28.0%

Could achieve greater score diversity by adding more granularity to partial

Severity Rankings

- V1 to v2 shift caused percent of vulnerabilities ranked by NVD as medium or high to jump from 59% to 96%
- Effects payment card industry security

NVD severity rankings for experimental data

Rank	v1 freq	v2 freq
Low	4490 (41%)	393 (4%)
Medium	1912 (17%)	5388 (49%)
High	4610 (42%)	5231 (47%)

Conclusions

- v2 met its design goals
 - v2 has higher scores than v1
 - v2 has greater score diversity than v1
 - The more granular metrics for exploitability increased complexity of scoring and added very little to scoring diversity
- Further change to CVSS could negatively effect use and impact