Analyzing Trends in Vulnerability Classes across CVSS Metrics

Anshu Tripathi
Department of Information Technology
Mahakal Institute of Technology
Ujjain, India

Umesh Kumar Singh
Institute of Computer Science
Vikram University
Ujjain, India

ABSTRACT
Rising vulnerability statistics demands multidimensional trend analysis for efficient threat mitigation. Understanding trends aids in early detection of problems and also in planning defense mechanisms. In this regard, this paper presents fine-grained trend analysis on classified vulnerability data provided by NVD, across six CVSS base metrics. Such analysis of vulnerability data according to their type, CIA impact, access vector and access complexity helpful in identifying most critical class of vulnerability relative to system environment and improve risk mitigation process.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
Vulnerability, Trend analysis, CVSS metrics, CWE, NVD

1. INTRODUCTION
The presence of vulnerabilities is root cause of security attacks. Detection and remediation of vulnerabilities is therefore crucial to ensure security and reliability. The number of vulnerabilities identified has greatly increased in last few years, at rate of 5,000 new vulnerabilities in a year [1]. The number of new vulnerabilities listed in National Vulnerability Database was 1677 in 2001, 2156 in 2002, 5733 in 2009 and 4639 in 2010 [2]. In view of such a large growing population of vulnerabilities, it is necessary to convert such large amount of data into actionable information. But the major issue is that how can such large amount of vulnerability data can be converted into actionable information? One possible solution is to find that, are there some patterns in evolution of vulnerabilities? If yes then do some type of vulnerabilities are more common and which type of vulnerabilities are more severe? Understanding vulnerability evolution is important in order to improve system security. For this, it is necessary to analyze current state and trends. By trend analysis, we can get a sense of where we are today and what will be important in near future. Trend analysis can be understood as a search for patterns over time in order to identify ways in which they change or develop, veer in new directions or shift [3]. Besides assessing past and present, trend analysis also helpful in anticipating future. Prioritizing efforts are often crucial in any resource-constrained and time critical task such as detection and prevention of vulnerabilities, a classification of vulnerabilities into different types might assist in directing the time and resource to most critical ones [4]. Proper classification also helpful in trend analysis in order to study evolution of vulnerabilities and protecting the system proactively [5]. In light of these views, this work focus on trend analysis of vulnerabilities on properly classified data. This paper performs a fine-grained trend analysis of vulnerabilities with the objective to analyze how the number of vulnerabilities varies over time in different severity levels and in different severity measuring factors. Further, it analyzes similar trends for different vulnerability classes and investigates which classes follow general trends and which classes shift from general trends and in which direction. It will be helpful in ranking vulnerability classes as per system security policies. For example some classes may affect confidentiality more as compared to availability. So system administrator can take decisions as per requirement of the system. This trend analysis will be helpful in understanding basic impact characteristics of vulnerability classes and thus in dealing with similar vulnerabilities tactfully. This trend analysis may assist security administrator in finding right combination of vulnerability prevention mechanism and designing proper security policies.

The paper is organized as follows. Section II gives the related work. Section III presents overall vulnerability trends and observations. Section IV presents vulnerability trends on classified data and comparison with overall trends. Finally section V is conclusion of the paper and some future works also shown.

2. RELATED WORK
In this work, we have used National vulnerability database (NVD) [2] to analyze vulnerability trends over the years. NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). NVD provides fine-grained search capabilities for all known vulnerabilities and is continuously updated to provide data for automated vulnerability management, security measurement and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. It records vulnerabilities since 1999, total 46176 vulnerabilities listed under CVE names [6]. NVD is using CWE [7] as a classification mechanism; each individual CWE represents a single vulnerability type. Common Weakness Enumeration (CWE) defines a standardized description of software weaknesses designed to provide a common language for describing software security weaknesses. CWE provides developers and analysts a standard definition of terms for investigating security problems in architecture, design and code. CWE also helps system administrators compare tools that attempt to find security weaknesses. All individual CWEs are held within a hierarchical structure that allows for multiple levels of abstraction. NVD uses CWEs from different levels of the hierarchical structure, by providing a cross section of the overall CWE structure. This cross section of CWEs allows analysts to score CVEs at both a fine and coarse granularity, which is necessary due to the varying levels of specificity

possessed by different CVEs. There are total 23 vulnerability types in NVD classification scheme, which are based on taxonomic features vulnerability cause and vulnerability impact. Vulnerability categories are: Authentication Issues, Credentials Management, Permissions, Privileges, and Access Control, Buffer Errors, Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS), Cryptographic Issues, Path Traversal, Code Injection, Format String Vulnerability, Configuration, Information Leak/Disclosure, Input Validation, Numeric Errors, OS Command Injections , Race Conditions, Resource Management Errors, SQL Injection, Link Following, Other, Not in CWE, Insufficient Information, Design Error. Last four are non CWE categories. NVD supports extensive searching under various categories, published date range, last modified date range and under different CVSS base metric parameter values. Vulnerability severity scores provided by NVD are CVSS scores. CVSS (Common Vulnerability Scoring System) [8] is a tool to quantify the severity and risk of a vulnerability to an information asset in a computing environment. It was designed by NIST (National Institute of Standard and Technology) and a team of industry partners. CVSS metrics for vulnerabilities are divided into three groups: Base metrics measure the intrinsic and fundamental characteristics of vulnerabilities that do not change over time or in different environments. Temporal metrics measure those attributes of vulnerabilities that change over time but do not change among user environments. Environmental metrics measure those vulnerability characteristics that are relevant and unique to a particular user's environment. There are six base metrics that capture the most fundamental features of vulnerability: Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact and Availability Impact (AC). The scoring process first calculates the base metrics according to the base equation, which delivers a score ranging from 0 to 10, and creates a vector. Optionally, the base score can be refined by assigning values to the temporal and environmental metrics. NVD provides qualitative vulnerability rankings as Low, Medium and High severity based on CVSS base score values. NVD adopted version 2.0 of CVSS in June 2007, and most of the vulnerabilities prior to this date were scored using version 1.0 guidelines and subsequently converted to an approximated version 2.0 score.

Some studies exist in literature related to vulnerability trend analysis [1, 4, 9]. In [1] vulnerability severity trends are presented based on NVD data in year range 2001 to 2008. Further, a view on vulnerability population distribution among categories based on CWE in year 2008 presented and related implications also given. [9] is a follow-up of [1] to measure progress in vulnerability trends. In [9] besides severity levels, trends related to access vector and access complexity are also presented for ten years. These two studies are very short and basic and don't provide detailed analysis. In [4] trend analysis of vulnerabilities in five software artifacts has been done by aggregating information from publicly available resources, such as ICAT, Bugtraq and CVE. This analysis suggests that discovery of a vulnerability may influence discovery of more vulnerabilities of same type. Further, it suggests developing a retrospective metric by measuring vulnerability occurrences and predictions based on it. Tim Shimeall et. al. [3] proposes a framework to conduct information security trend analysis using incident reports to CERT. Framework offers a common ground to resolve issues involved in performing the trend analysis and an example analysis process also presented. It is always appropriate to revisit trends as suggested in [9]. Keeping this objective in mind this work provides in depth vulnerability trend analysis on categorized vulnerability data of last ten years across CVSS base metric vectors in following sections.

3. COMMON TRENDS

In this section vulnerability trends in last ten years on unclassified data are presented. Vulnerability information collected in June 2011. Statistics present data for year 2011 of around six months. We started with year wise appearance of vulnerabilities then distribution of vulnerabilities in three severity levels analyzed. Afterward distributions of vulnerabilities with respect to CVSS base metric group are analyzed. The base metric group captures the characteristics of vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability.

3.1 Appearance of Vulnerabilities

Figure 1 presents yearly trend in discovery of vulnerabilities. Number of new vulnerabilities reported is rising every year and highest in year 2006. After 2006 there is decline and number of new vulnerabilities reported in year 2010 is 29% less than in year 2006. In year 2011 based on six month observation we can see trend is going downward giving a positive sign.

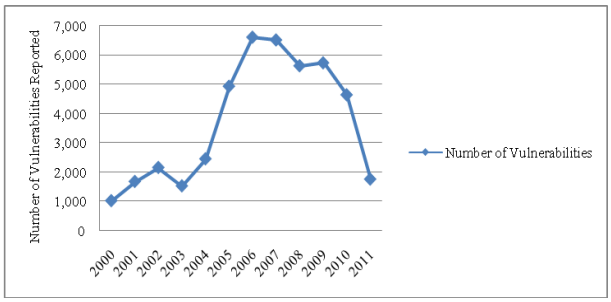

Fig 1: Number of new vulnerabilities reported

3.2 Severity Level

NVD ranks vulnerabilities by assigning one out of three severity levels, low, medium and high. These three severity levels have a mapping on the numeric CVSS scores in ranges: 0.0-3.9, 4.0-6.9 and 7.0-10.0 for low, medium and high respectively. Figure 2 presents trends in distribution of vulnerabilities among three severity levels. Number of low severity vulnerabilities is very less as compared to high and medium severity vulnerabilities. In aggregate analysis high severity vulnerabilities are 45.56%, medium severity vulnerabilities are 48.14% and low severity vulnerabilities are 6.28% of total population. Percentage of low severity vulnerabilities varies between 3.27% in year 2008 to 11.33% in year 2001. As compared to this medium severity vulnerability percentage range is 42.58% in year 2001 to 51.98% in year 2004. High severity vulnerability percentage varies between 39.53% in year 2004 to 50.41% in year 2008. These trends indicate that the proportion at each severity level has changed relatively little in last ten years with slight rise in percentage of medium severity vulnerabilities.

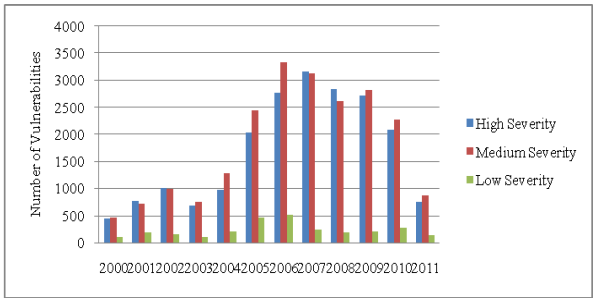

Fig 2: Distribution of vulnerabilities by severity levels

3.3 Access Vector

Access vector metric reflects how vulnerability can be exploited. Possible values for this metric can be local, adjacent network and network. Local access means attacker require physical access to the system or a local account. Adjacent network access means attacker requires access either to broadcast domain or collision domain of vulnerable software. Network access means attacker can exploit vulnerability remotely. Figure 3 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Access Vector. In aggregate analysis 87% vulnerabilities are remotely exploitable, 13% requires local access and population belonging to adjacent network metric is very low 0.30%. In year wise analysis remotely exploitable vulnerabilities range between 71% in year 2001 to 91% in year 2009, vulnerabilities that require local access range between 8% in year 2009 to 29% in year 2001. Vulnerabilities that require adjacent network access for exploitation are very low always below 1%. These trends clearly indicate that access vector metric value is high for majority of vulnerabilities and suggests to do network hardening to thwart attacks.

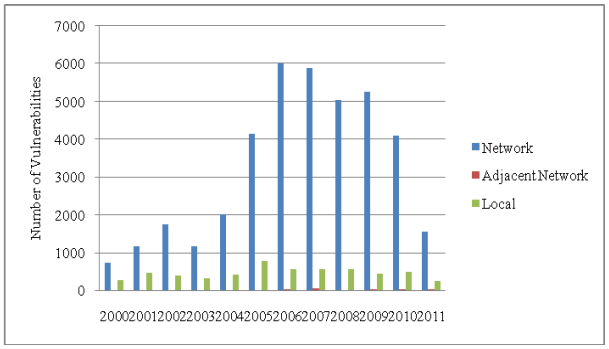

Fig 3: Distribution of vulnerabilities by Access Vector

3.4 Access Complexity

Access complexity measures the complexity of the attack require to exploit the vulnerability after gaining access to system. Possible values for this metric can be low, medium and high. Low complexity means one that involves no specialized conditions, such as a default configuration, or an attack can be conducted manually and requires little skill. Medium complexity means that access conditions are somewhat specialized, such as involving no default configuration or requires specific system knowledge. High complexity involves specialized access conditions such as elevated privileges required, rarely seen configuration and chances of detection also high. Figure 4 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Access Complexity. In aggregate analysis 63% vulnerabilities are easily exploitable, 30% are of medium access complexity and only 5% requires specialized conditions for exploitation. In year wise trends low access complexity vulnerabilities range between 95% in year 2001 to 43% in year 2010, vulnerabilities that require medium access complexity range between 0.20% in year 2000 to 50% in year 2010. Vulnerabilities that require high access complexity for exploitation are very low, range between 2% in year 2008 to 12% in year 2006. In initial years most of the vulnerabilities were of low access complexity but now percentage of low access complexity is decreasing and percentage of medium access complexity is increasing proportionately. While percentage of high access complexity is low always below 6% with an exception of 12% in year 2006. These trends warn us that even not so skilled attackers have favorable chances to exploit the vulnerabilities.

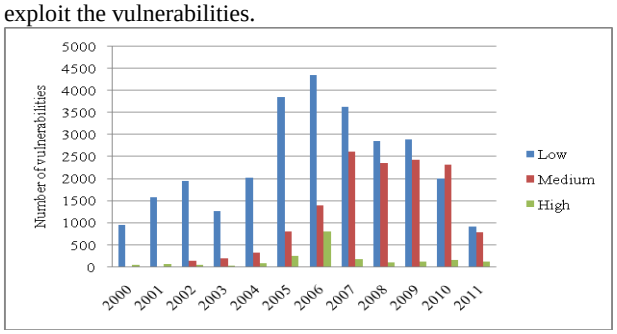

Fig 4: Distribution of vulnerabilities by Access Complexity

3.5 Authentication

Authentication measures number of times an attacker requires authenticating after gaining access on the target system in order to exploit the vulnerability. Possible values for this metric can be none, single and multiple. Multiple authentication means attacker authenticate two or more times. Figure 5 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Authentication. In aggregate analysis 94.79% vulnerabilities require no authentication, 5.17% require single authentication and multiple authentication population is negligible. Up to year 2005, around 99% of vulnerabilities can be exploited once attacker gains access to the system, no further authentication needed. After year 2005 also this percentage is above 91. So these trends clearly indicate that for a successful attack, an attacker just requires to gain access to the system that is also possible remotely and with not so specialized skill set.

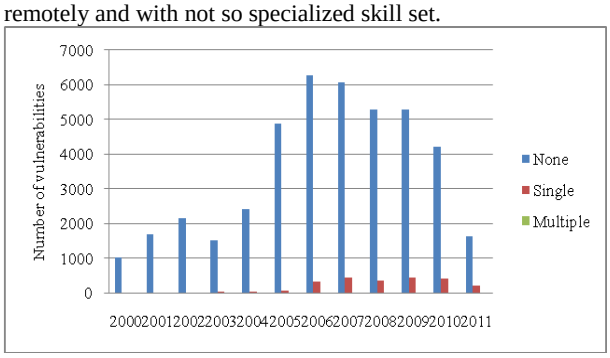

Fig 5: Distribution of vulnerabilities by Authentication

3.6 Confidentiality Impact

This metric measures the impact on confidentiality that is controlling access and disclosure of information to unauthorized persons. Possible values for this metric can be none, partial and complete. Complete refers to total information disclosure, partial refers to considerable

information disclosure and none refers no impact on confidentiality of system. Figure 6 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Confidentiality impact. In aggregate analysis 20% vulnerabilities result in no impact, 30% vulnerabilities impact completely and 50% vulnerabilities impact partially, confidentiality of system on exploitation. In year wise trends percentage population of vulnerabilities with partial impact is always highest ranging from 40% in year 2010 to 61% in year 2006. Then vulnerabilities with no impact in the range 26% in year 2001 to 37% in year 2004. Vulnerabilities that result in complete disclosure are in range 10% in year 2006 to 30% in year 2010. These trends reveal that in last five years vulnerabilities with complete impact are rising, year 2007 shown maximum increase more than double from 10% in year 2006 to 22%.

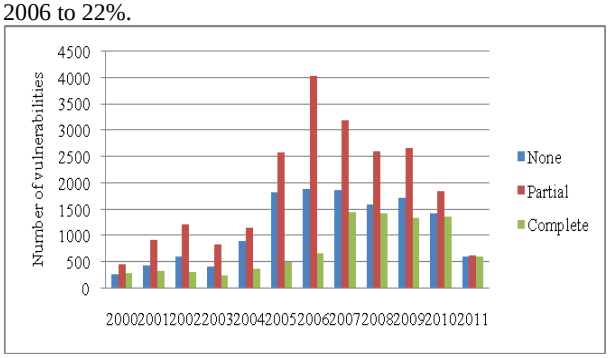

Fig 6: Distribution of vulnerabilities by Confidentiality Impact

3.7 Integrity Impact

This metric measures the impact on trustworthiness and veracity of information. Possible values for this metric can be none, partial and complete. Complete refers to compromise of entire system, partial refers to attacker can modify some information but scope of affect is limited and none refers no impact on integrity of system. Figure 7 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Integrity impact. In aggregate analysis 25% vulnerabilities result in no impact, 19% vulnerabilities impact completely and 56% vulnerabilities impact partially, integrity of system on exploitation. In year wise trends percentage population of vulnerabilities with partial impact is always highest ranging from 32% in year 2000 to 70% in year 2006. Then vulnerabilities with no impact in the range 19% in year 2008 to 40% in year 2000. Vulnerabilities that result in complete compromise are in range 9% in year 2006 to 29% in year 2010. These trends reveal that in last five years vulnerabilities with complete impact are rising, year 2007 shown maximum increase more than double from 9% in year 2006 to 21%.

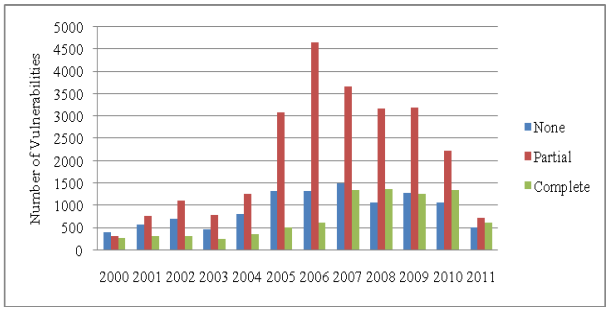

Fig 7: Distribution of vulnerabilities by Integrity Impact

3.8 Availability Impact

This metric measures the impact on accessibility of information resources. Possible values for this metric can be none, partial and complete. Complete refers to total shutdown of affected resource; partial refers to reduced performance or interruptions in availability of resource and none refers no impact on availability of resource. Figure 8 presents trends in distribution of vulnerabilities with respect to CVSS base metric, Availability impact. In aggregate analysis 29% vulnerabilities result in no impact, 23% vulnerabilities impact completely and 48% vulnerabilities impact partially, availability of system on exploitation. In year wise trends percentage population of vulnerabilities with partial impact is always highest ranging from 36% in year 2010 to 57% in year 2003.Then vulnerabilities with no impact in the range 25% in year 2001 to 37% in year 2005. Vulnerabilities that result in complete compromise are in range 12% in year 2006 to 33% in year 2010. These trends reveal that in last five years vulnerabilities with complete impact are rising, year 2007 shown maximum increase more than double from 12% in year 2006 to 27%.

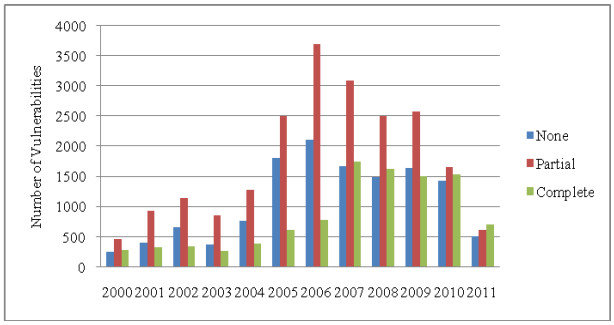

Fig 8: Distribution of vulnerabilities by Availability Impact

4. TRENDS IN VULNERABILITY CLASSES

With the aim of gaining insight into level of affect caused by different vulnerability classes on various security measuring factors, in this section trend analysis done on classified vulnerability data across six base metric vectors of CVSS framework. Classification scheme is same as adopted by NVD which classify vulnerability data in 23 classes based on CWE.

4.1 Population Distribution in Classes

Figure 9 presents distribution of vulnerability population across 23 vulnerability classes. Ten most populated vulnerability classes are SQL Injection (13.04%), XSS (12.56%), Buffer Errors (11.68%), Insufficient Information (10.42%), PPA (7.52%), Input Validation (6.92%), Code Injection (5.96%), Path Traversal (5.36%), Resource Management (5.04%) and Information Leak/Disclosure (3.23%). In all these top ten vulnerability categories contribute 81.72% of total vulnerability population. Not in CWE class contains only 9 vulnerabilities, so it is dropped from further analysis.

4.2 Severity Level

Figure 10 presents distribution of vulnerability population in vulnerability classes across three severity ranking levels: high, medium and low. SQL injection besides being most populated vulnerability class has 85.75% of vulnerabilities of high

severity. Buffer errors being on third place in population percentage has 75.95% vulnerabilities of high severity. In contrast to these two classes, XSS ranked at second position in population percentage includes 91.69% of vulnerabilities of medium severity and just 0.07% of high severity. Code injection and Insufficient information includes 66% and 51.54% of high severity vulnerabilities respectively. Vulnerability class SQL injection and Buffer errors pose high threat to system security in view of population and severity level. In majority of classes number of medium severity vulnerabilities is higher than high severity vulnerabilities. Low severity vulnerabilities are with lowest percentage in all classes.

4.3 Access Vector

Figure 11 presents distribution of vulnerability population in vulnerability classes with respect to access vector values: network, adjacent network and local. Most of the vulnerability classes follow trends similar to common trends that is remotely exploitable vulnerabilities includes maximum population above 70% and adjacent network includes negligible number of vulnerabilities. Vulnerability percentages with local access are also low below 20% in maximum classes. Link following and Race condition are only two classes having high percentage of locally exploitable vulnerabilities.

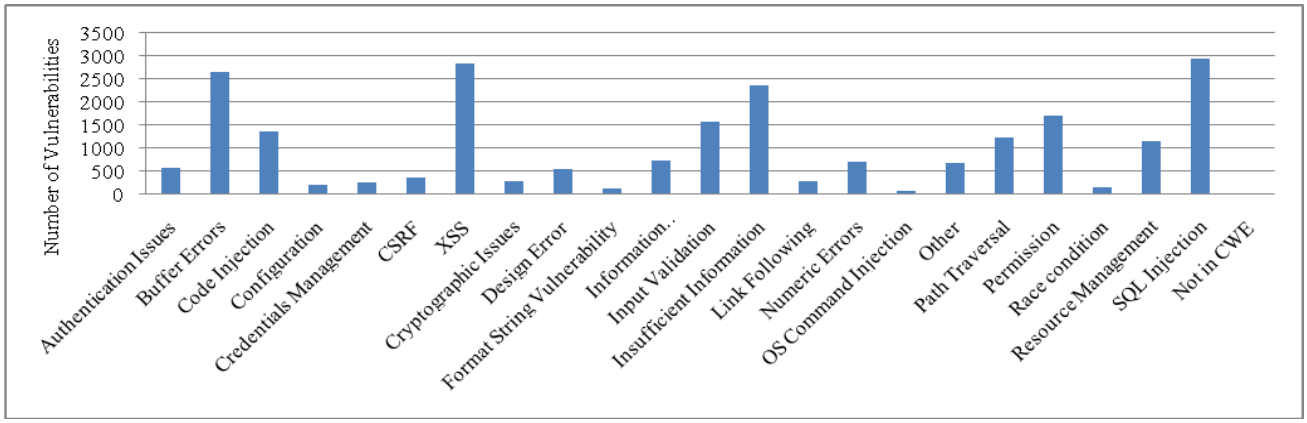

Fig 9: Distribution of vulnerability population in Classes

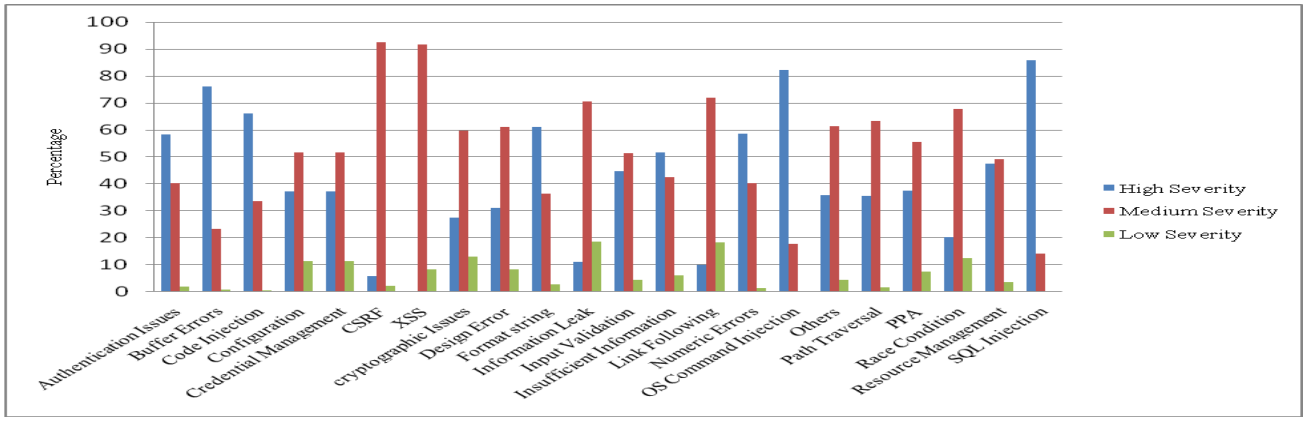

Fig 10: Distribution of vulnerabilities by severity level across classes

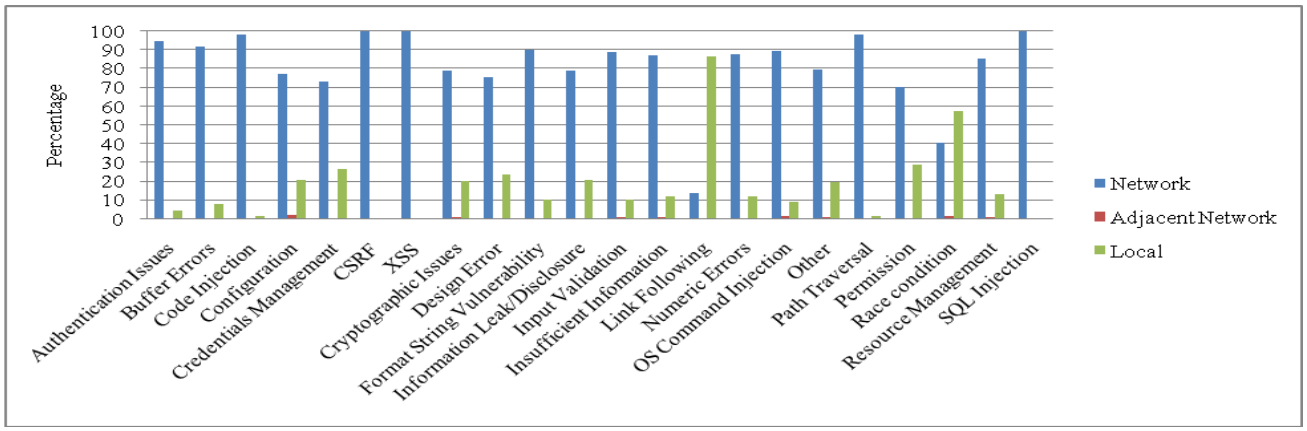

Fig 11: Distribution of vulnerabilities by Access Vector across classes

4.4 Access Complexity

Figure 12 presents distribution of vulnerability population in vulnerability classes with respect to access complexity metric values: low, medium and high. Access complexity is low for 50% of vulnerability population in most of the classes. Population percentage for medium access complexity is also around 50%. High access complexity is below 5% in majority of classes. These trends indicate that even not so skilled attackers can exploit the vulnerability belonging to any class.

4.5 Authentication

Figure 13 presents distribution of vulnerability population in vulnerability classes with respect to access complexity metric values: low, medium and high. Access complexity is low for 50% of vulnerability population in most of the classes. Population percentage for medium access complexity is also around 50%. High access complexity is below 5% in majority of classes. These trends indicate that even not so skilled attackers can exploit the vulnerability belonging to any class.

4.6 Confidentiality Impact

Figure 14 presents distribution of vulnerability population in vulnerability classes with respect to Confidentiality Impact metric values: none, partial and complete. Buffer errors, Link following, Numeric errors, OS command injections are the classes that includes around 50% of vulnerabilities that have complete impact on confidentiality of system. In rest of the classes around 60% vulnerabilities have partial impact on confidentiality of system. Only XSS is an exception in which more than 99% vulnerabilities have no impact on confidentiality.

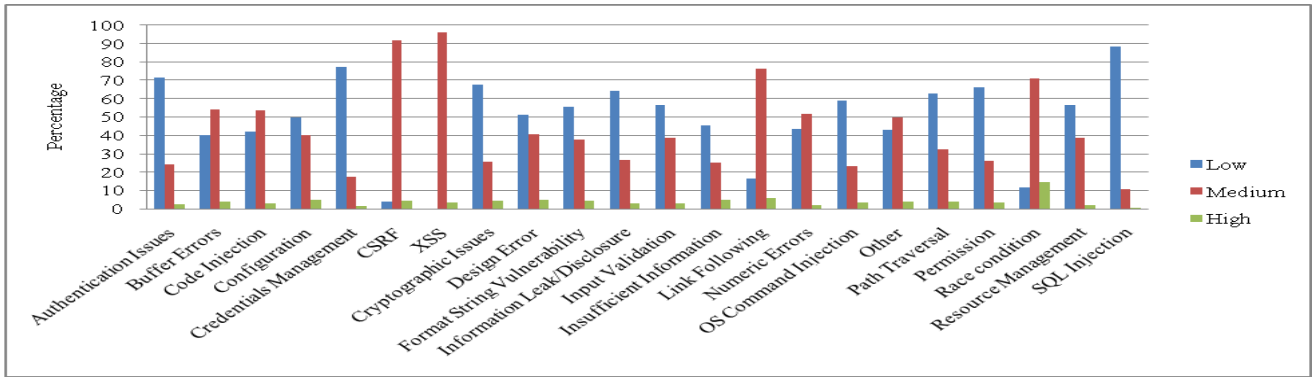

Fig 12: Distribution of vulnerabilities by Access Complexity across classes

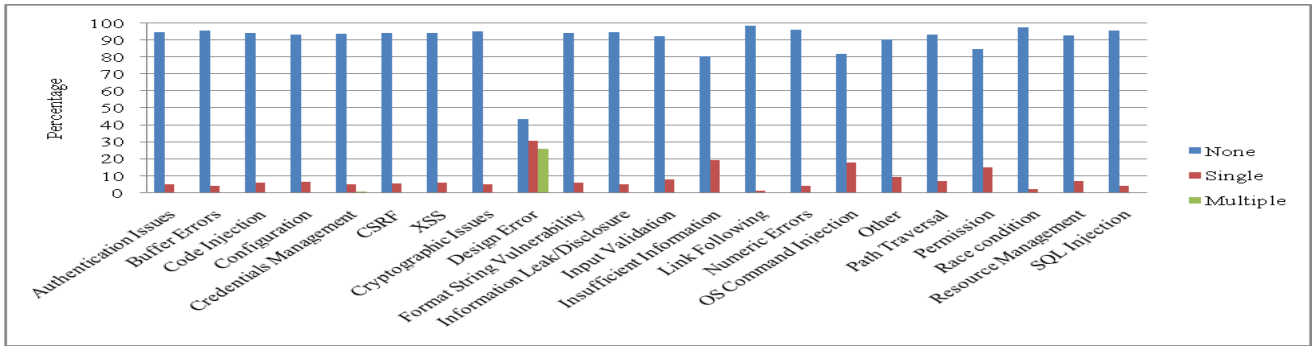

Fig 13: Distribution of vulnerabilities by Authentication across classes

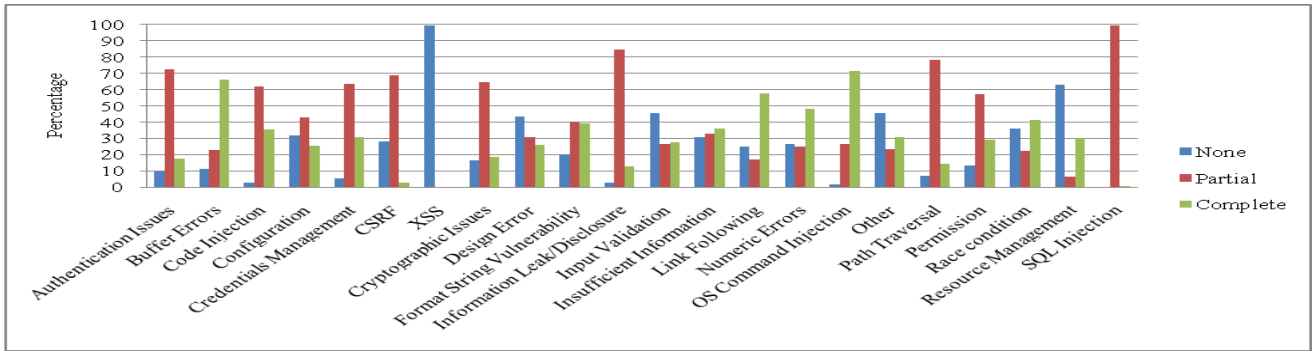

Fig 14: Distribution of vulnerabilities by Confidentiality Impact across classes

4.7 Integrity Impact

Figure 15 presents distribution of vulnerability population in vulnerability classes with respect to Integrity Impact metric values: none, partial and complete. Similar to confidentiality impact, Buffer errors, Link following, Numeric errors, OS command injections are the classes that includes around 50% of vulnerabilities that have complete impact on integrity of

system. In CSRF, XSS and SQL injection classes more than 95% of vulnerabilities have partial impact on integrity of system. In Authentication issues, Code injection and Path traversal classes around 60% of vulnerabilities have partial impact on integrity of system.

4.8 Availability Impact

Figure 16 presents distribution of vulnerability population in vulnerability classes with respect to Availability Impact metric values: none, partial and complete. Vulnerability classes' show diverse trends in case of availability impact. In XSS and Information leak/disclosure classes more than 90% of vulnerabilities have no impact on availability of system resources. In SQL injection class more than 99% of vulnerabilities have partial impact on availability of system resources. More importantly in classes Buffer errors, Insufficient information, Link following, Numeric errors, OS command injection, Race condition, Resource management more than 50% of vulnerability population affect availability of system resources completely.

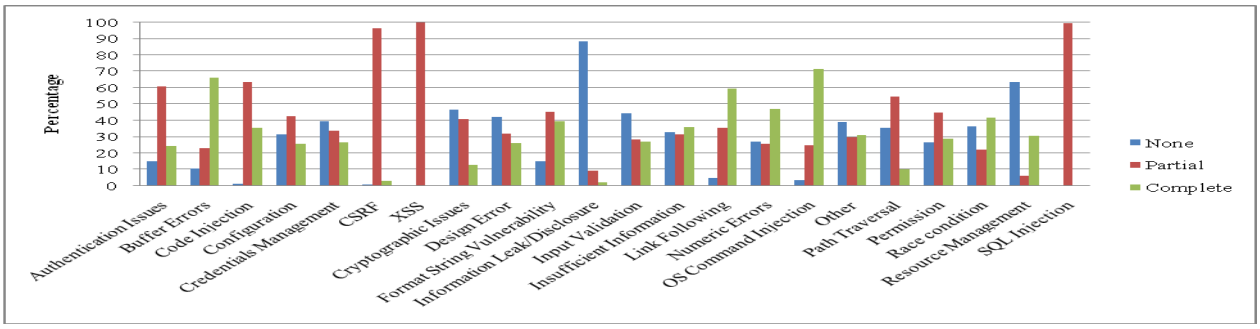

Fig 15: Distribution of vulnerabilities by Integrity Impact across classes

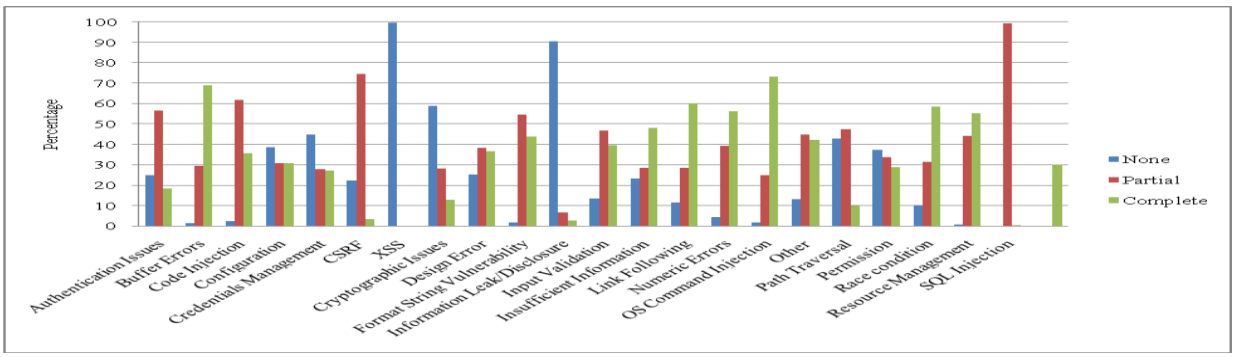

Fig 16: Distribution of vulnerabilities by Availability Impact across classes

5. CONCLUSION AND FUTURE WORK

In this paper, we have analyzed vulnerability trends in last ten years across all six CVSS base metrics using data from NVD. Initially trends for unclassified vulnerability data are presented, followed by trends on classified vulnerability data. Impact characteristics of different vulnerability classes are identified that will help security administrator in taking fast decisions relative to system environment. For example if a vulnerability belongs to class XSS and if confidentiality is a major concern than that vulnerability is relatively of low priority because in XSS as most of the vulnerabilities have no impact on confidentiality. Similarly relative priority of different vulnerability classes can be decided depending on trend analysis presented in this work. Based on presented trend analysis security metrics can be developed in future which aids in security measurement and management.

6. ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers who provided helpful feedback on our manuscript.

7. REFERENCES

[1] R. Kuhn, H. Rossman and S. Liu, "Introducing Insecure IT", IT Professional, Jan/Feb 2009, pp. 24-26.

[2] NHS and NIST, National Vulnerability Database (NVD), automating vulnerability management, security Measurement, and compliance checking, http://nvd.nist.gov/scap.cfm , (Accessed on 15-06-2011).

[3] Tim Shimeall and Phil Williams, "Models of Information Security Trend Analysis", Available at http://www.cert.org/archive/pdf/info-security.pdf.

[4] R. Gopalakrishna, E. Spafford and J. Vitek, "A Trend Analysis of Vulnerabilities", CERIAS TR 2005-06, 2005.

[5] Tripathi, A. Singh, U.K., "Taxonomic Analysis of Classification Schemes in Vulnerability Databases" (Communicated)

[6] Common Vulnerabilities and Exposures. [Online]. Available:http://cve.mitre.org (Accessed on 15-06-2011)

[7] Common Weakness Enumeration. [Online]. Available: http://cwe.mitre.org (Accessed on 15-06-2011)

[8] Zhongqiang Chen, Yuan Zhang, Zhongrong Chen, "A Categorization Framework for Commom Vulnerabilities and Exposures." In the computer Journal Advance Access published online on May 7, 2009, http://comjnl.oxfordjournals.org,doilO.1093/comjnl/bxp040

[9] R. Kuhn and Chris Johnson, "Vulnerability Trends: Measuring Progress", IT Professional, 2010, pp. 51-53.