**An Analysis of Trends in Vulnerabilities of the NVD Database**

Matthew Eltze

**Abstract**

**General Terms**

**Keywords**

**1.) Introduction**

The NVD database is a repository of security vulnerabilities run by the United States government.

The CVSS scoring guideline is a free and open standard for accessing vulnerabilities. Due to its flexible design it can be used to grade vulnerabilities across many platforms both hardware and software based.

While the guidelines are managed by Forum of Incident Response and Security Teams (FIRST) the scores are created by product vendors, vulnerability bulletin analysts, and other security professionals who are more familiar with a specific vulnerability.

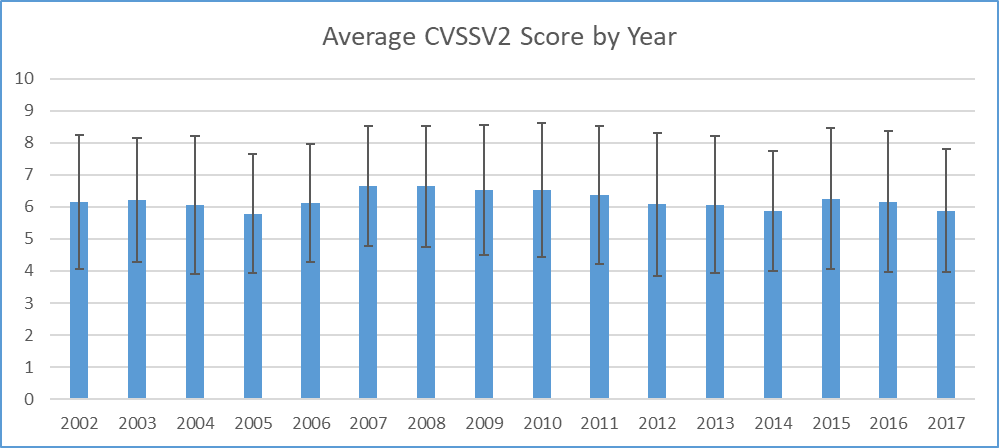
CVSSv2 was chosen due to its backwards compatibility with earlier years in the NVD database.

**2.) Related Works**

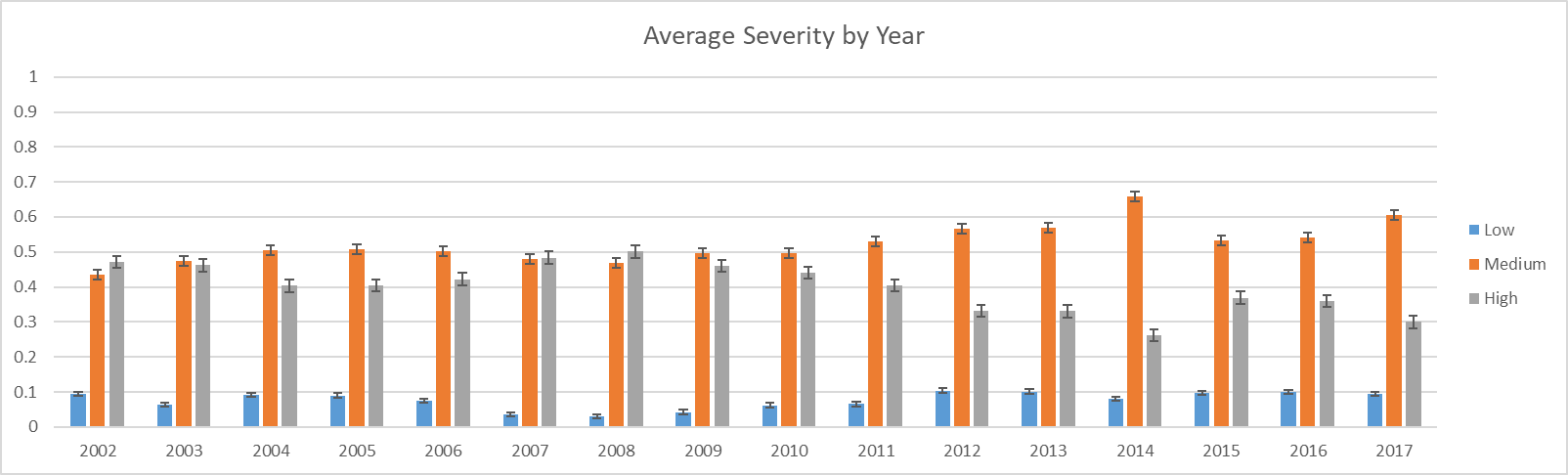
The paper, how different and why

More years, and over time linear regression/predictions

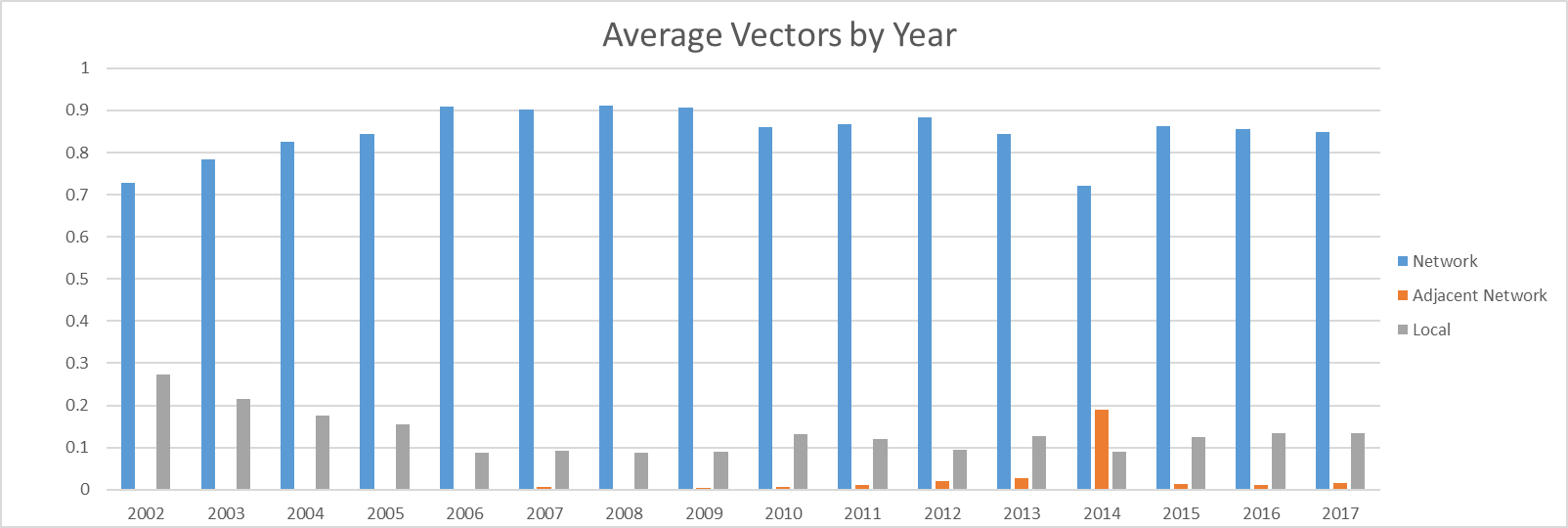
**3.) Common Trends**

****

The score of a CVE generated by a function based on how impactful and exploitable the vulnerability is. The average vulnerability score has remained largely consistent over time. The buffer bars of the graph represent the standard deviation of this metric. The standard deviation is also largely consistent over time.

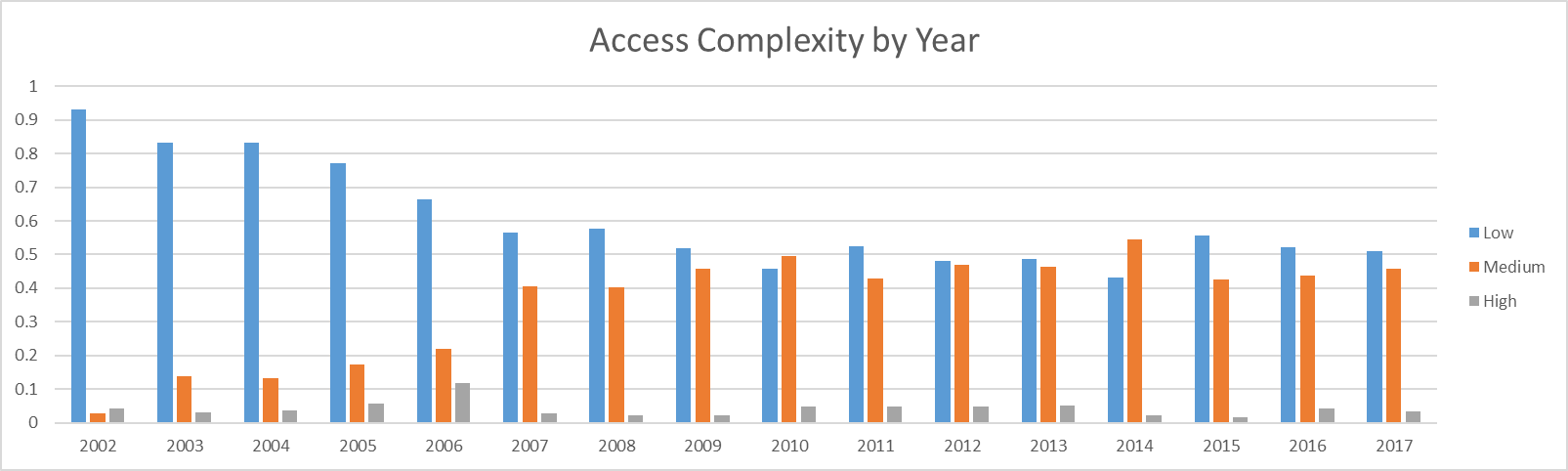


Severity level provides a qualitative ranking for the CVSSv2 scores. Low is 0.0-3.9, Medium is 4.0-6.9, and High is 7.0-10.0. We can see that the share of vulnerabilities classified as Medium has increased over time. The share of Low severity CVEs decrease through the 2004 to 2008 but rebounded and has been fairly stable at around 10% of CVEs.



Vector is a metric that shows how the Vulnerability can be exploited. Local-based attacks are the least severe attacks, in which the attacker must already have access to the machine, either physically or via a local shell account. Adjacent Network exploits allow for attacks via broadcast or collision domain. An example of this would be via Bluetooth or local ethernet. Network based attacks do not require the attacker to have access to anything locally. Vulnerabilities in this class as “remotely-exploitable” and therefore the most severe.

The proportion of attack Vectors has largely stayed the same since 2006, apart from adjacent network exploits which have grown. There is an outlier in 2014 which can be attributed to a large number of a specific exploit in mobile applications with improper cryptography (CWE-310). In specific Android applications which didn’t verify X.509 certificates from SSL servers, which allows man-in-the-middle attacks.

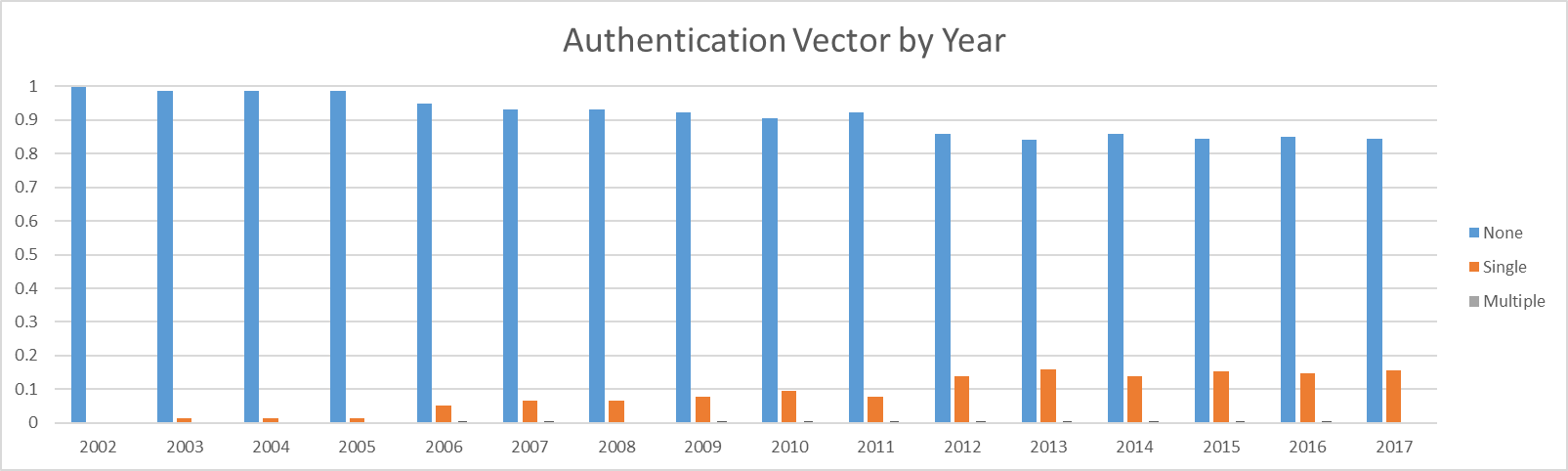


Access complexity is a measure of how easy it is to exploit the vulnerability. To be a High complexity exploit there must be specialized conditions in place already. For example, the attack must already have elevated privileges, or the attacked system have an uncommon configuration.

Medium complexity exploits include things such as phishing which require the user to fall for the exploit. Some information about the system is required or some setup, and therefore isn’t a general exploit.

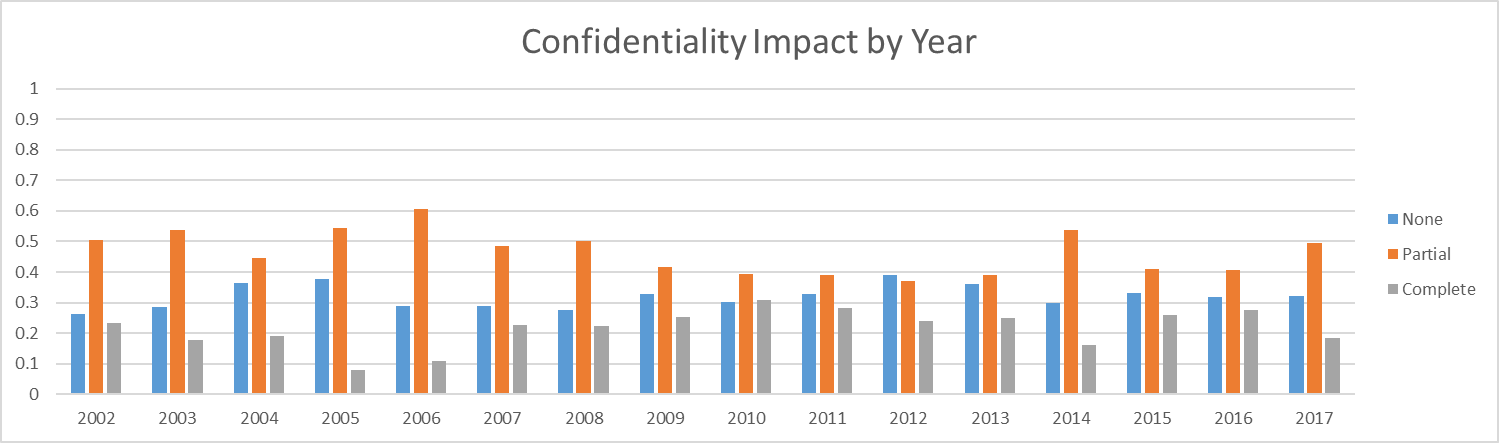
Low complexity exploits are general exploits or require minimal information about the system.

The number of low complexities exploits consistently decreased until 2007, where all three categories have stayed largely consistent.

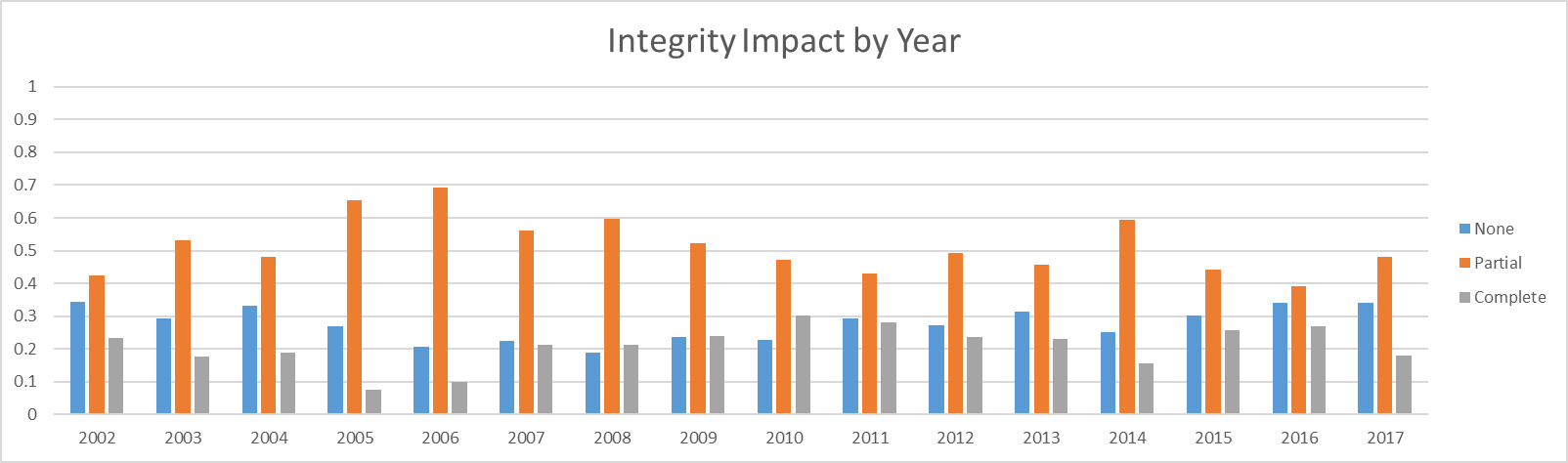


Authentication vector is a measure of how many times the attacker is required to input credentials before making the attack. This metric doesn’t gauge the strength of the authentication, just the number of times it is required.

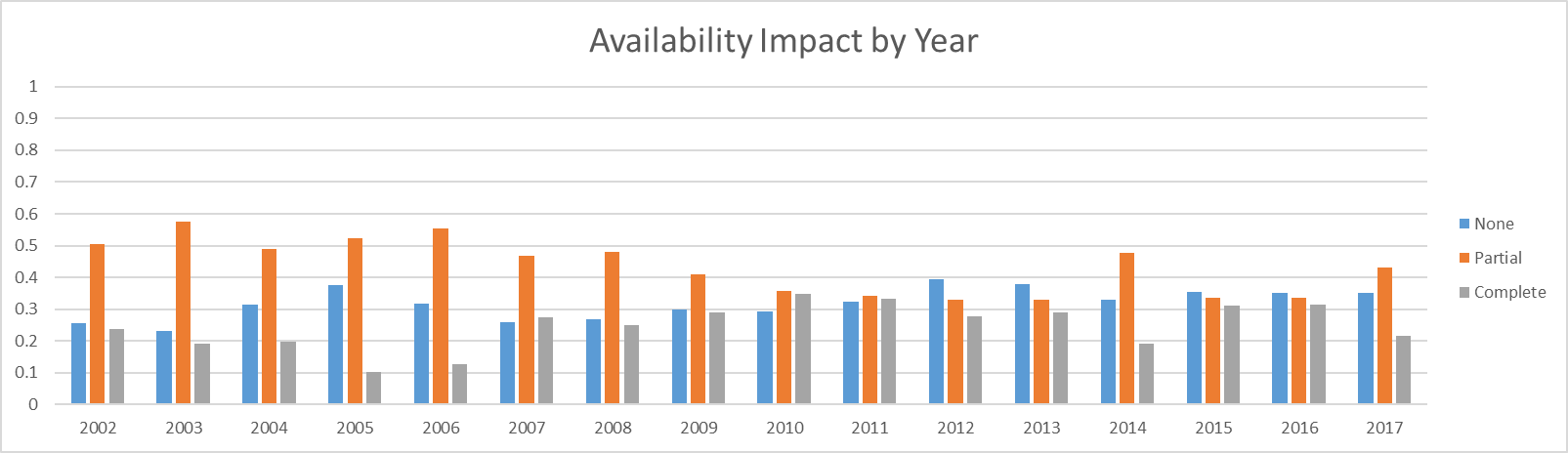
There has been a growth in single authentication attacks. We were unable to identify the cause of this growth.



This metric measures how much data is disclosed to the attackers. There is considerable variability in this metric throughout the years. There was a downward trend in partial confidentiality exploits until 2014 where it rebounded. This is in part due to the same outlier found in the access vector. However, we see a similar growth in 2017.



Integrity Impact is a measure of how much of the exploited machine’s data is potentially subject to having been modified or damage. A complete system integrity loss would have the potentiality that all the files on the machine are subject to having been modified. A partial system integrity loss either means the attacker has no control over what is modified, but can make some modification, or the scope of what can be modified isn’t complete.



Availability Impact is a measure of how accessible the system under attack is during/after the attack. A partial score means that the system is accessible but has reduced performance or interruptions. A complete score means that full denial of service has occurred, and the system is unavailable.

**4.) Trends of the Most Severe Vulnerabilities**

4 CWE’s have been selected: CWE-20 Improper Input Validation, CWE-89 Improper Neutralization of Special Elements used in SQL commands, CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer, and CWE-264 Permissions, Privileges, and Access Controls.

Include 77, 78, 94,74

Command Injection

OS Command Injections

Code Injection

Injection

**Works Cited**

https://www.first.org/cvss/v2/guide

1. Copy as Microsoft object into powerpoint
2. Print to pdf
3. Export as jpeg > quality high to max