Group 1: National Vulnerability Database 18-9-2017

Xander Bouwman ***Paul van der Knaap***

Daan van der Valk ***Dereck Bridie***

Gouri Calamur Viravalli

The National Vulnerability Database (NVD) is the repository used by the National Institute of Standards and Technology (NIST), which is the US government agency responsible for cybersecurity. This project makes use of the NVD's Common Vulnerabilities and Exposure (CVE) list of the year 2016, as this is the most recent yearly set with complete data.

1. What security issue does the data speak to?

The data reports vulnerabilities in software that could potentially lead to incidents, with a corresponding severity that indicates the required action to be taken by system administrators, or the security decision makers and the primary audience for this data. According to TU Delft's framework which provides four security metrics – namely controls, vulnerabilities, incidents, and prevented losses – the NVD falls squarely under the category of vulnerabilities.

The data is presumably gathered with a bias towards the US, as NIST is responsible for systems in the US only. However, since many software vendors are based in the US this may be seen as generally representative of vulnerabilities worldwide.

2. What would be the ideal metrics for security decision makers?

Metrics on vulnerabilities can be used in a variety of contexts. To get an idea of the ideal metrics for security decision makers, it is important to understand the responsibilities and goals of those decision makers. Decisions on cyber security must be made in business, political, and governmental organisations. For each of these groups a brief description of choices is described below.

Metrics should provide information on the following issues:

- From the security perspective, which controls to invest in? Where should resources be allocated?
- How do departments perform security-wise? Do they perform better or worse than before?
- What vulnerabilities will have the most impact in the future? What software or hardware bugs to particularly look out for during development of IT artifacts?
- From the regulatory perspective: for which technologies would new legislation be useful?

Business

In business, IT Management in general is responsible for IT vision and strategy, allocation of technical resources and internal IT policy. General IT Management, led by the Chief Technology Officer, decides which IT infrastructures, services and products to buy externally, and which IT artifacts to develop internally. For cost-benefit analyses of external IT products and services, vulnerability data could help decide which products and services to buy. For internal IT projects, vulnerability data could indicate points of attention during development to avoid certain flaws.
Cyber Security Management in particular, led by the Chief (Information) Security Officer, is responsible for the enterprise's assets protection, and the corresponding vision and strategy. The key performance indicators are all about vulnerabilities and other aspects of risk (like treat and impact). Metrics should assist in allocating resources for security by establishing the security strategy, assessing the security performance, and prioritizing issues.

Politics

Politicians use metrics as inspiration, and justification, for (planned) policy and regulations. Vulnerability-related metrics may inspire politicians to take action against IT service or product categories when its vulnerability levels, or its impacts, are considered undesirable for society. As legislative powers are struggling to keep track of technological developments, predictive analyses of vulnerabilities can help politicians to look forward to security-related issues.

Governments

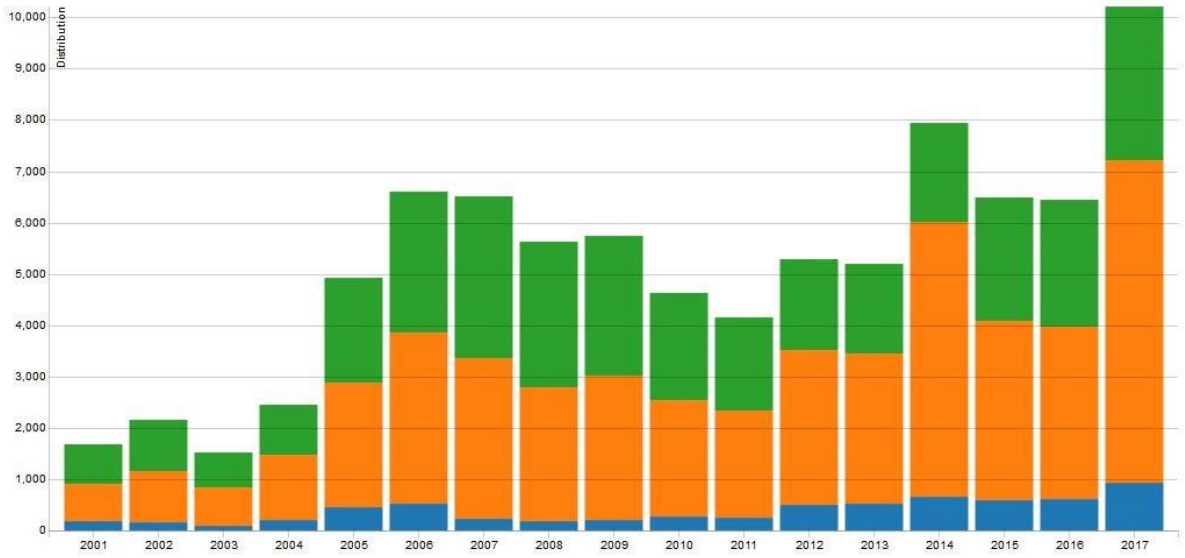
Some governmental organisations interact particularly much with cyber security issues, like the police when handling cybercrime complaints. For example, the Data Protection Authority (Dutch: Autoriteit Persoonsgegevens) may use vulnerability metrics in relationship to data breaches. This can be used to form regulations, or target inspections on certain IT vendors or organisations using certain IT products or services.

The Dutch National Cybersecurity Center (NCSC) is part of the Ministry of Security and Justice, and has similar responsibilities to our data provider NIST. The NCSC does not provide vulnerability data, but instead provides actionable security recommendations to decision makers in business. Each recommendation includes an indication of the probability of an incident occurring, and the severity of damage that it may do. These metrics are similar to respectively the exploitability and the impact fields fields in the NIST CVE data.

In addition to policy and regulations, IT management in governments faces the same challenges as in the business world -- limited resources needs to be spend efficiently for both regular IT operations and its security.

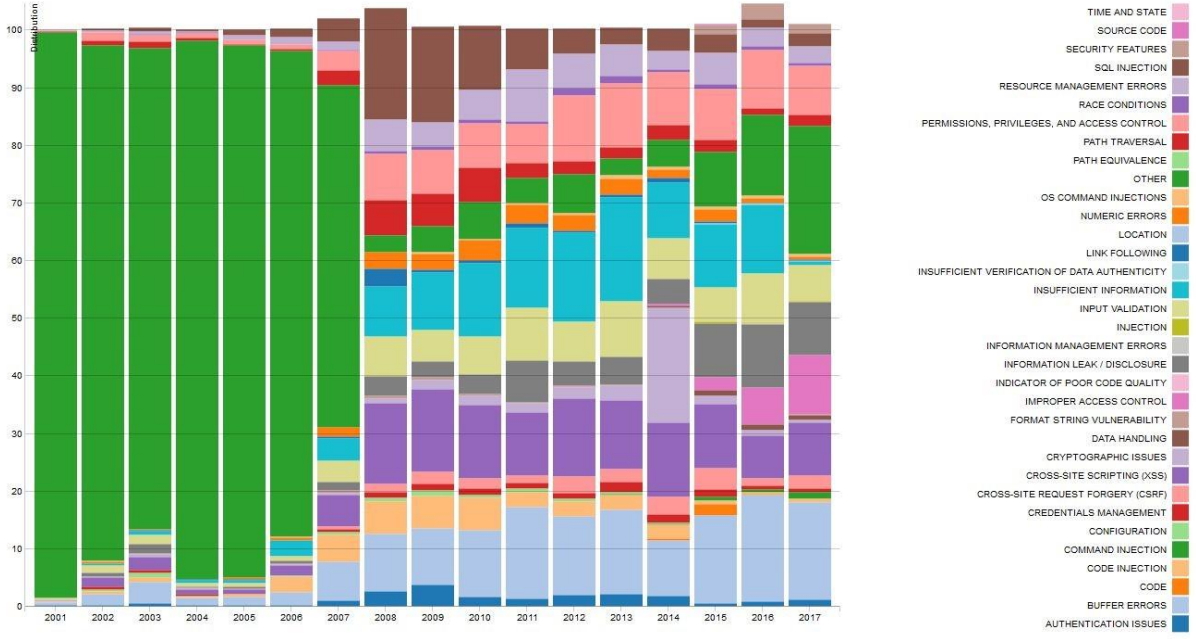
3. What are the metrics that exist in practice?

- Common Vulnerability Scoring System (CVSS) is a metric that was introduced in 2007, and captures data from the NVD to produce an indication of the severity of a vulnerability in terms of a numerical score or a qualitative representation.



CVSS Severity Distribution Over Time

Source: [NIST]



Relative Vulnerability Type Totals By Year

Source: [NIST]

- In 2010, the Center for Internet Security (CIS) has also established metrics in the form of six business functions namely Incident Management, Vulnerability Management, Patch Management, Configuration Management, Change Management and Application Security.
- The Cybersecurity Framework developed by NIST in 2014 presented five functions as a part of the framework's core - identification, protection, detection, response, and recovery.

4. A definition of the metrics you can design from the dataset

CIA Impact: this metric keeps a check on the confidentiality, availability and integrity levels that are required in a system. The higher the value of the metric, the higher the loss will be after a successful breach from an attacker.

Exploitability score: This metric is calculated mathematically using three base metrics. The first is the access vector which indicates the physical layer that the attacker has access to in order to exploit a vulnerability. The second is access complexity which describes the ease/difficulty in exploiting the said vulnerability, and the third base metric is authentication, which indicates how many times the attacker should authenticate a target to exploit it. These three base metrics are calculated as small positive real numbers, and 20 times the product of these 3 metrics gives the exploitability score. The higher the score, the higher the risk of a vulnerability getting exploited.

Base score: The base score metric is a function of both impact and exploitability metric scores. It is used mainly to determine the overall severity of the vulnerability. It is calculated as the integer closest to ((0.6 * impact) + (0.4 * exploitability) - 1.5) * f(impact)) where f(impact) takes value 0 if impact is 0, and 1.176 otherwise.

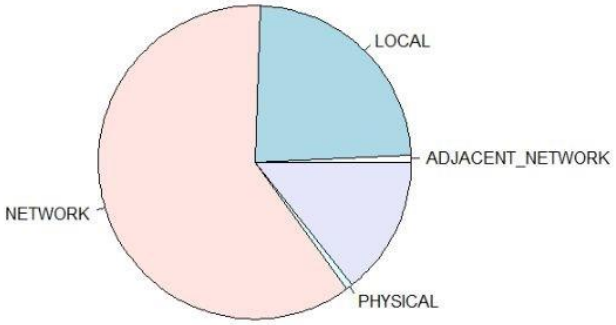
Attack Vector pie chart: The attack vector pie chart will show a distribution and the relative size of all the vector of attacks. This will help in determining the resources to spend on different attack vectors.

User Interaction pie chart: By knowing what percentage of all cases require a form of user interaction it is easier to determine how better and proper training could perhaps mitigate these risks. In addition it is interesting to seek a correlation between the threats which require user interaction, and the severity of the vulnerability.

5. An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).

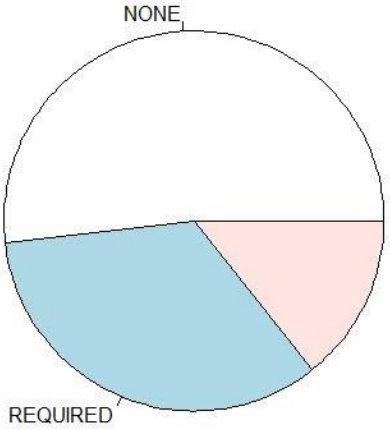
Attack Vector Pie Chart

A pie chart of the attack vector shows that the largest amount of attacks are vulnerabilities which can be exploited remotely over the network.



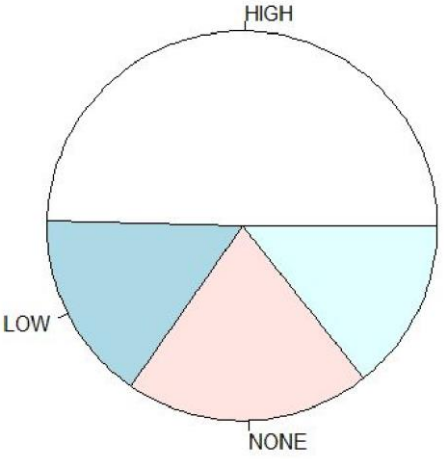
User Interaction Required

The pie chart of the required user interaction shows that, if the unknown cases are excluded, 39% of the threats require a form of user interaction to be exploited.



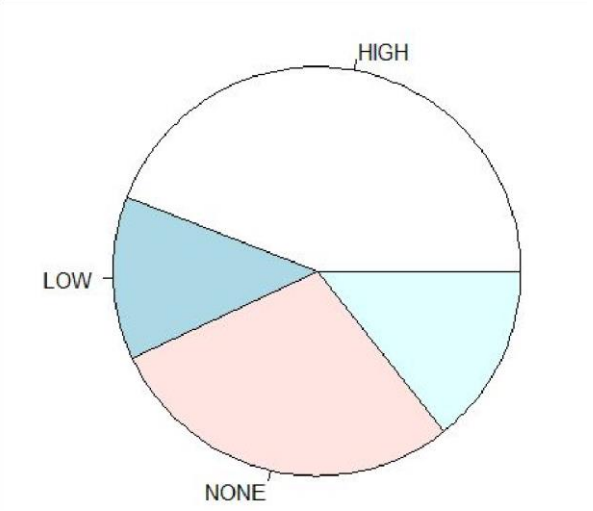
Confidentiality impact

This pie chart shows the relative impact on confidentiality this vulnerability exposes.



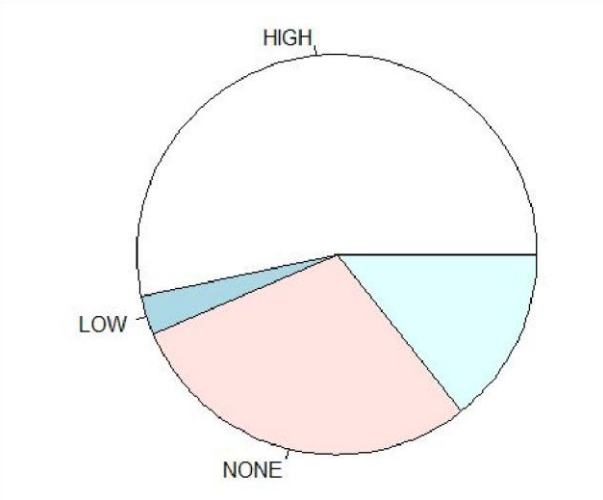
Integrity impact

This pie chart shows the relative impact on integrity this vulnerability exposes.



Availability impact

This pie chart shows the relative impact on availability this vulnerability exposes.



These metrics may be combined to gain further insights. For example, the distribution of severity of impact could be given for each attack vector.

Additionally, a scoring system similar to the CVVS could be designed that outputs a score indicating the security level for a given threat environment. The threat environment could be customized by a decision maker, for example by setting business priorities for CIA-assets and then having these reflected in the score in order to gain insight into where to allocate resources.