CVSS - Vulnerability Score Prediction
Supervisor(s): David Eyers Veronica Liesaputra

1 What are CVE and CVSS?

The Common Vulnerabilities and Exposures (CVE) program is a dictionary or glossary of vulnerabilities that have been identified for specific code bases, such as software applications or open libraries.[https://nvd.nist.gov/general/cve-process]

2 Motive

2.1 Should we use CVSS?

There have been a few attempts at dethroning CVSS. It does have some shortcomings:

- Vaguerity
- Oversaturation in some scoring bands
- Seemingly arbitrage?/ complexity in the scoring function
- etc...

These being the case, would the cyber sec community use a new standard if one came along? Historically unlikely, especially given the uptake for CVSS 4.0 is so poor.

2.1.1 Why 4.0 is not being used

See if there are any valid reasons why it isn't instead of just inertia

3 Exploration of the Space

NVD is used by majority of studies as primary and sole data source. Reasoning:

- Data is in a nice format
- Largest collection of free CVE and CVSS scores, well maintained and in consistent format

Mitre is another large source. Reasoning:

- Format is more unwieldy
- Large lack of CVSS scores in comparison with NVD

Most other alternatives that were used in the Bayesian study have gone into archive status. There are others however they are either pay to play VulnDB or they have a different focus, i.e searchsploit.

4 Analysis

Analysis is useful in and of itself, knowing the breakdown of each metric, and the confidence there in in relation to a prediciton will be useful. It can show shy the model may be less good at prediction for certain metrics.

4.1 Comparison with previous Bayesian study

The previous analysis used bayesian techniques to compare and contrast different datasets. However, those datasets were hard to attain, even then and were mostly webscraped. Additionally they were using *CVSS 2.0??*, where as we are now up to version 3.1.

5 Results

...

5.1 Key take-aways

Spending time with the dataset, finding its quirks, for example:

- Mitre data only stores the vectors strings, but $\tilde{1}$0 aren't in the expected format.
- Mitre has multiple entries for the same CVE with different scores, containing different parameters. This is generally useful, but awkward when automating a training process.

5.2 Is Mitre still useful to us?

Yes, few possible use cases:

- Use as the test data for the trained models.

This allows the model to be trained on all of NVD, but qureied on Mitre descriptions. This tests two things... Its ability to predict based on unseen data(generalise), and an indirect similarity score. Similarity score, insight into how different experts see the same problem. Clustering? Look into which parts relate to what metric.

Aims