Paper Title:
A Twitter-based Software Vulnerability Alert Framework using Natural Language Processing
Paper Link:
https://ieeexplore.ieee.org/document/10192794

1 Summary

1.1 Motivation

The paper addresses the necessity of robust safety precautions and addresses the increasing frequency of cyberattacks. It presents a strategy that uses Twitter and Natural Language Processing (NLP) to identify security vulnerability occurrences and send out timely alerts.

1.2 Contribution

Through the use of Twitter data, the tool described in the research helps to promote proactive cybersecurity. The objective is to utilize the abundance of publicly accessible data on Twitter to detect and notify establishments about possible security flaws in their software programs.

1.3 Methodology

Using NLP techniques, the methodology gathers tweets from the security community on Twitter and uses them to calculate ratings based on system specs, polarity, and vulnerability keywords. The proposed system utilizes Twitter API, Python, YAKE!, BeautifulSoup4, and Jira.

1.4 Conclusion

The paper wraps up by summarizing the key contributions, which include the creative method for locating tweets with security-related content, creating alerts for notifications, and offering thorough evaluations of the literature. It also addresses and eliminates some limitations identified in existing works.

2 Limitations

2.1 First Limitation

The current restrictions are as follows: there are no user feedback channels; patches and security upgrades are not applied; notifications may be manipulated through compromised accounts; and keyword extraction techniques are only used infrequently.

2.2 Second Limitation

Another notable constraint pertains to the limited investigation of keyword extraction methods within the domain, which may indicate a potential gap in the suggested framework's comprehensiveness.

3 Synthesis

The concepts presented in this paper have important implications for reality. The suggested methodology takes advantage of Twitter's abundance of information to provide a proactive approach to cybersecurity. Additional data sources can be added to the framework in the future, and notifications for software updates and patches can be sent out.