A Content-Based Approach for detecting Smishing in Mobile Environment

Sandhya Mishra, Devpriya Soni

Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India

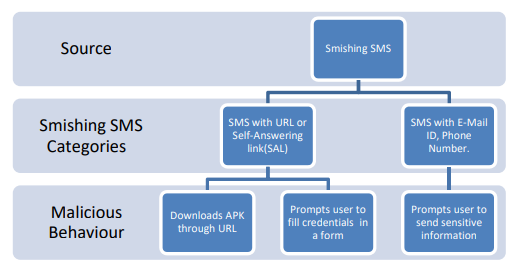
FROM: Elsevier SSRN 2019

Abstract:

The abstract discusses a novel method to detect smishing (SMS phishing) attacks by analyzing SMS content and URL behavior. With the increase in smartphone use and sensitive information storage, mobile devices are vulnerable to phishing attacks. Traditional detection methods, including **SMS feature analysis, blacklisting, and heuristic methods, have limitations**, particularly in reducing false positives. The proposed technique uses machine learning to classify messages based **on malicious keywords, URL inspection for malicious behavior, and checks for APK downloads** and form tags, aiming to differentiate between malicious and non-malicious messages more accurately.

Introduction:

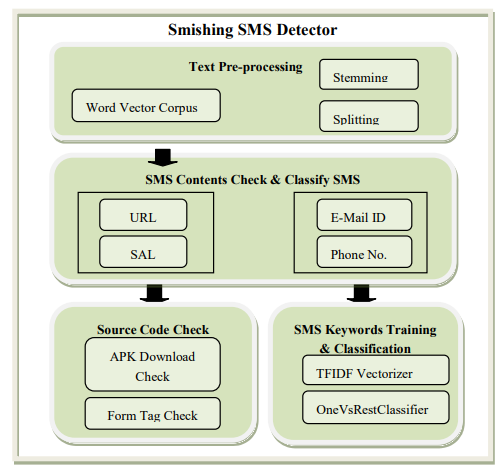
The introduction section of the document emphasizes the growing concern of smishing attacks due to the increased use of smartphones and their storage of sensitive information. It outlines the limitations of existing smishing detection methods, such as SMS feature analysis, blacklisting, and heuristic approaches, which struggle with high false positive rates. The document proposes a novel detection method that leverages machine learning to analyze **SMS content and URL behavior, aiming to more effectively distinguish between malicious and non-malicious messages by inspecting URLs for malicious activity and checking for APK downloads and form tags.**



Proposed approach:

Then, the model processes the SMS based on the contents present in it. SMS is classified using machine learning algorithm on the basis of keywords present in it. It also analyzes the behavior of the URL present in the text message.

Architecture:



Experimental Evaluation:

**SMS Content Analyzer Development:** A Python-based SMS content analyzer was developed to analyze the text content of SMS messages. This analyzer employed text preprocessing techniques such as removing punctuation, converting words to lowercase, tokenizing, stemming, and preparing a word vector corpus.

**Classification Process:** The messages were classified into two parts based on their content. Messages containing URLs were processed separately from those containing phone numbers or email IDs. The classification was based on keywords present in the messages using machine learning algorithms.

**Tfidf Vectorizer and OneVsRestClassifier:** These tools were used to classify messages according to the keywords present. A word frequency matrix generated by the Tfidf Vectorizer helped the OneVsRestClassifier to learn from the data and predict whether a message was smishing or legitimate.

Future Works and Conclusion:

**Integration with the Android platform:** The prototype, currently implemented in Python, is intended to be integrated into the Android operating system, potentially as an app.**Real-time smishing detection:** The envisioned app would be capable of identifying smishing messages as they are received in a user's messaging inbox, with options to automatically discard or save messages based on whether they are flagged as smishing.**Addressing more sophisticated threats:** Future enhancements aim to incorporate additional techniques to counter more intelligent and varied smishing threats.**Focus on preventing personal information leakage:** Subsequent research and development efforts will concentrate on safeguarding against the leakage of personal information and improving the accuracy of smishing detection to reduce false positives​​.