Rule-Based Framework for Detection of Smishing Messages in Mobile Environment

Ankit Kumar Jain, BB Gupta

6th International Conference on Smart Computing and Communications ICSCC 2018

FROM: Elsevier.com

Abstract:

The abstract of the paper outlines a rule-based framework for detecting smishing messages in mobile environments. It emphasizes the increasing prevalence of smishing attacks and the need for effective detection methods. The study proposes a novel approach using a rule-based data mining classification technique. This technique involves identifying specific characteristics of smishing messages, which are then used to filter out such malicious content. The framework demonstrates effectiveness in detecting these threats, contributing significantly to mobile security.

Introduction:

The introduction of the paper discusses the rising concern of smishing (SMS phishing) in mobile communications. It highlights the vulnerability of mobile devices to security threats and emphasizes the need for effective detection systems. The section introduces the concept of smishing, outlining how attackers exploit SMS to deceive users into revealing sensitive information. The authors argue for the development of robust mechanisms to counter these threats, setting the stage for their proposed rule-based detection framework. This introduction essentially sets the context for the paper, underlining the significance of addressing mobile security challenges like smishing.

Proposed approach:

The proposed rule-based approach in the paper for detecting smishing messages involves a data mining classification method. This method employs nine specific rules, each designed to identify characteristics typical of smishing texts. These rules are based on the common features observed in smishing attacks, such as the use of URLs, phone numbers, and certain keywords. The approach includes algorithms like Decision Tree, RIPPER, and PRISM to effectively classify and filter SMS messages. Additionally, the method incorporates text normalization to adapt to the informal and varied nature of SMS language, improving the accuracy of detection. This framework provides an efficient and reliable way to identify and mitigate smishing threats in mobile environments.

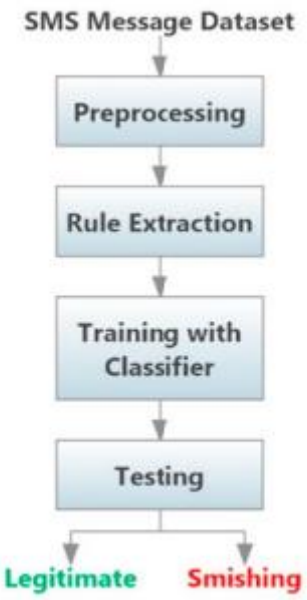
Process steps:

- **SMS Input:** The framework begins with the receipt of an SMS message that needs to be evaluated.
- **Text Normalization:** This step involves processing the SMS text to normalize its format. Given the informal nature of SMS language, this step ensures that the text is in a suitable form for analysis.

- **Application of Classification Rules:** The core of the framework lies here. Nine specific rules are applied to the normalized text. These rules are designed based on common characteristics observed in smishing attacks.

- **Rule Examples:**
    - Presence of URLs or shortened links.
    - Inclusion of phone numbers.
    - Urgent or alarming language prompting immediate action.
    - Requests for sensitive personal information.
    - Use of promotional or enticing language.
    - Classification Process: Using algorithms like Decision Tree, RIPPER, and PRISM, the SMS is analyzed under these rules to classify it.

- **Categorization into 'Smishing' or 'Legitimate':** Based on the analysis, each SMS is categorized as either a smishing message or a legitimate one.
- **Effective Detection:** The framework is designed to efficiently identify smishing messages, thereby protecting users from potential phishing attacks via SMS.
- **High True Negative Rate:** The proposed system is shown to have a high true negative rate, meaning it effectively identifies non-smishing messages correctly, reducing false positives.
- **Zero-hour Attack Detection:** The framework is also capable of detecting new, previously unseen smishing attacks (zero hour attacks).



Experimental Evaluation:

Dataset: The authors utilized a dataset comprising both smishing and legitimate SMS messages. This dataset was essential for training and testing the classification models.

Preprocessing and Normalization: Before applying the classification rules, the SMS messages underwent preprocessing and normalization to standardize the text, making it suitable for analysis.

Application of Rules: The nine specific rules identified for smishing detection were applied to the dataset. These rules were based on common characteristics of smishing messages, such as the presence of URLs, phone numbers, and certain keywords.

Classification Algorithms: The paper details the use of several rule-based classification algorithms, including Decision Tree, RIPPER, and PRISM, to evaluate the effectiveness of the proposed framework.

Performance Metrics: The evaluation focused on various performance metrics, such as accuracy, precision, recall, and the true negative rate. These metrics provided a quantitative measure of the framework's effectiveness in distinguishing between smishing and legitimate messages.