APDs: Framework for Surveillance of Phishing words in Instant Messaging Systems Using Data Mining and Ontology


Abstract — Instant Messaging Systems (IMS) generically cannot detect many deceptive phishing attacks; hence they are vulnerable for cyber frauds. To overcome, we propose an Active-Phishing Detection System (APDs), developed using Data Mining (Rule-based) and Ontology. APDs monitor the user’s psychology and predict type of the detected phishing activity with an alert to achieve zero-minute phishing attacks.

I. INTRODUCTION

The APDs, dynamically predicts any potential deceptive phishing attacks, when instant messages are exchanged between users of an IMS. Currently, IMS lacks a stronger mechanism to deal with phishing at content-level. Few researchers proposed various methods to detect phishing attacks [1] [2]. But, lack the Rule-based method without Ontology [5], and trapping the users into deceptive phishing attacks [3]. The emails of Google are categorized into Primary, Social, Updates, and Forums, ignoring the issues of phishing attacks. Recently, leaked news of PRISM-NSA as one of the largest surveillance programs monitoring the Networks exploiting against cyber international law.

II. PROPOSED ACTIVE-PHISHING DETECTION SYSTEM

The operational Framework of APDs is shown in Fig. 1. The APDs algorithm initiates the steps to capture the phishing words that are exchanged between the users and then stores them into database for identifying phishing words using pre-defined phishing rules of Table I. The APD algorithm is shown in Fig. 2. In APDs, the Monitoring system program identifies the culprit details of Phisher and report to the victim client. Steps of algorithm are illustrated as follows:

1. In this step, the phishing words are identified by using GSHL and Tree Alignment Algorithms as discussed in [4]. These messages are stored in Text database (TDB), where unnecessary words are filtered using Ontology Based Information Extraction technique (OBIE) (stemming, N-gram technique, ignore words) [6] [7].
2. The frequently recurring words are extracted from the TDB dynamically using Association rule mining technique [8] and SSPWDB (pre-defined rules) guided with Ontology database (ODB), later these words are pushed to TPDB. The metadata is a gist of information related to instant messages.
3. Once the Phishing words are detected, the message is considered as suspicious, as given in Table I (rule 1). The KDB maintains the detected stem words along with the domain (i.e. type of Phishing activity).
4. Profile details are traced from EDB, which are provided during the creation of an email id, with the aid of Relational Wrapper Algorithm [9].
5. The email- id through which the phishing words are sent is tracked using metadata, and the victim is alerted.
Table I. Pre-defined Phishing rules

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Phishing words / scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Financial gain</td>
<td>Account no, bankers, credit card details, dob, name initials, fav mobile</td>
</tr>
<tr>
<td>2 Fame and notoriety</td>
<td>Password, aliases, hobbies, fav game, designation, prof_goal, strengths</td>
</tr>
<tr>
<td>3 Identity access</td>
<td>Kids name, pets name, fav food, fav teacher, middle name, fav team, school name, pen name, pet name, alias</td>
</tr>
<tr>
<td>4 Deceitful elicitation</td>
<td>Phony email, phony txtmsg, screen name, pet-name, phony url, multiple email acc, manage details, phony social networks</td>
</tr>
<tr>
<td>5 Acc_creation tips</td>
<td>Emp id, all caps, special characters, alpha-numeric, common pwd</td>
</tr>
<tr>
<td>6 URL related</td>
<td>Suspicious page URL or link contains- or @, contains more than 5 dots, false login page, host-name portion is an IP address, organization’s name (e.g. Ebay) in a URL path but not in the domain name, page is not accessible, inconsistencies are found in a image &amp; non-image URL’s domain</td>
</tr>
</tbody>
</table>

Phishing Rule 2 (Threshold value) Check the Threshold value for the stem words using OBIE Framework

<table>
<thead>
<tr>
<th>Phishing Rule 3 (multi lingual &amp; undetected words)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilingual and undetected words to be checked and updated automatically</td>
</tr>
</tbody>
</table>

The given Text Input (TDB) is converted to pure textual format by the preprocessor component using NLP tools. The information extraction techniques filter unnecessary words from unstructured text. The stem words that are found and stored in TPDB, are guided by ontology internally by the Ontology Generator component using TreeAlignment algorithm. During this process it makes use of semantic lexicon (WordNet) and Error detection and Correction, for stem words that are extracted and builds a Tree with empty root node initially. The input given from pre-defined phishing rules (SSPWDB) to Ontology Editor is again mapped with the Ontology Generator by identifying the exact Domain for the empty root node. Finally the root word(s) along with stem words are stored in knowledge database (KDB). The experimental results obtained for predicting the type of phishing activity detected from IMS are shown in Fig. 4, that shows Taxonomic Structure of words mapped from Text Pattern Database (TPDB) with pre-defined phishing axioms (SSPWDB). The experimental results obtained for predicting the type of phishing activity detected from IMS using OBIE framework of Fig. 3, is shown in Fig. 4.

IV. ISSUES AND CHALLENGES

1. Deceptive phishing messages are sent in any format other than textual (Images, Audio, Video), then they are not detected as shown in Fig. 5.
2. Rules lack multilingual support for deceptive phishing detection.
3. Issue with the interpretation of a message written in multiple languages.

REFERENCES


Fig. 3. Proposed OBIE Framework to detect phishing words from Instant Messaging Systems (IMS).

Fig. 4. Shows Taxonomic Structure of words mapped from Text Pattern Database (TPDB) with pre-defined axioms (Set of Suspicious Phishing Words Data Base (SSPWDB))