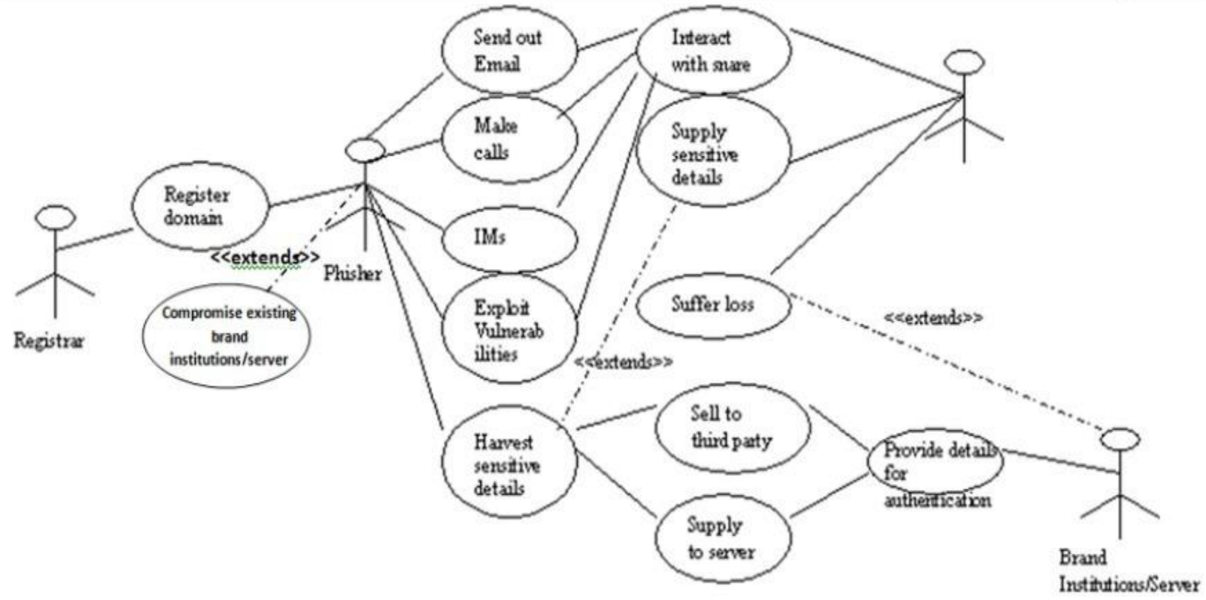
WEB PHISHING DETECTION

The URL of phishing websites may be very similar to real websites to the human eye, but they are different in IP. The content-based detection usually refers to the detection of phishing sites through the pages of elements, such as form information, field names, and resource reference.

Use case:



Related works:

Junaid Rashid et al[1] used machine learning based phishes detection gadget relies upon efficiently on the aspects of accuracy. The most of antiphishers researchers center of attention on optimizing new feature proposals or classification algorithms, where developing proper features analysis and selection techniques is not the important plan. The paper involved phishing-enabled, reaching an effective positive rate of 97% and a false positive rate of 4%. The features are obtained by META tagging, web pages content, URLs, hyperlinks, TF-IDF, and more.

Ping Yi[2] et al used deep learning frameworks to detect web phishing. This paper mainly focuses on applying a deep learning framework to detect phishing websites. This paper first designs two types of features for web phishing: original features and interaction features. A detection model based on Deep Belief Networks (DBN) is then presented. The test using real IP flows from ISP (Internet Service Provider) shows that the detecting model based on DBN can achieve an approximately 90% true positive rate and 0.6% false positive rate.

Jain, A.K. et al [3] described anti-phishing technology that removes 19 features on the buyer's side to determine phishing websites from approved sites using machine learning. They used 2,141 phishing pages as well as the famous Alexa website, some online debit gateways, and some great banking websites.

Chiew[4] et al proposed to use probability minimization standard and Monte Carlo algorithm using a new neural network-based classification technique for detecting phishing net pages. The thirty points were used to categorize the four main areas, especially around the bar-based, anomaly-based, HTML and JavaScript.

Zhang, W., et al[5] extract features towards URL, text, and web content and utilize Extreme Machine Learning (ELM) technology. The first step in this method is to write the text content of the classifier to determine the content of the label text through ELM. In this case, OCR software is used to retrieve the text from the image. It is a second-stage-based hybrid that combines text and other function classifiers.

BROWSERS:

Many phishing sites examined stayed live for at least 48 hours, they monitored all sites for at least two days. Based on Cyren's analysis, Google Chrome and Firefox did the best job detecting and blocking known phishing sites with Chrome blocking 74% of phishing sites within 6 hours and 20 minutes on average.

APPS:

Netcraft Anti-Phishing App For Android

You can access this anti-phishing service in the Google Play store as well as the Amazon Playstore. To protect you from malicious phishing sites, this app uses their enterprise's leading anti-phishing feed.

Email phishing detection:

VirusTotal is a great tool to use to check for viruses that a user's own antivirus software may have missed and also to verify against any false positives. VirusTotal is free to end users for non-commercial use.

Reference:

[1]Junaid Rashid;Toqeer Mahmood;Muhammad Wasif Nisar;Tahira Nazir; (2020). Phishing Detection Using Machine Learning Technique . 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), (), –. doi:10.1109/smart-tech49988.2020.00026

[2] Yi, Ping; Guan, Yuxiang; Zou, Futai; Yao, Yao; Wang, Wei; Zhu, Ting (2018). Web Phishing Detection Using a Deep Learning Framework. Wireless Communications and Mobile Computing, 2018(), 1–9. doi:10.1155/2018/4678746

[3] Jain, A.K. and B.B. Gupta, Towards detection of phishing websites on client-side using machine learning based approach. Telecommunication Systems, 2018. 68(4): p. 687-700.

[4] Chiew, K.L., et al., Utilisation of website logo for phishing detection. Computers & Security, 2015. 54: p. 16-26.

[5] Zhang, W., et al., Two-stage ELM for phishing Web pages detection using hybrid features. World Wide Web, 2017. 20(4): p. 797-813.