LITERATURE SURVEY

1. Title: Large-Scale Automatic Classification of Phishing

Author: Colin Whittaker, Brian Ryner, Marria Nazif

Phishing websites, fraudulent sites that impersonate a trusted third party to gain access to private data, continue to cost Internet users over a billion dollars each year. We describe the design and performance characteristics of a scalable machine learning classifier we developed to detect phishing websites. We use this classifier to maintain Google's phishing blacklist automatically. Our classifier analyzes millions of pages a day, examining the URL and the contents of a page to determine whether or not a page is phishing. Unlike previous work in this field, we train the classifier on a noisy dataset consisting of millions of samples from previously collected live classification data. Despite the noise in the training data, our classifier learns a robust model for identifying phishing pages which correctly classifies more than 90% of phishing pages several weeks after training concludes.

2. Title: RUS Boost: Improving Classification Performance when Training is Skewed.

Author: Chris Seiffert, Taghi M. Khoshgoftaar, Jason Van Hulse, Amri Napolitano.

Constructing classification models using skewed training data can be a challenging task. We present RUS Boost, a new algorithm for alleviating the problem of class imbalance. RUS Boost combines data sampling and boosting, providing a simple and efficient method for improving classification performance when training data is imbalanced. In addition to performing favourably when compared to SMOTE Boost (another hybrid sampling/boosting algorithm), RUS Boost is computationally less expensive than SMOTE Boost and results in significantly shorter model training times. This combination of simplicity, speed and performance

makes RUS Boost an excellent technique for learning from imbalanced data.

3. Title: Application of Machine Learning Algorithm Intrusion detect dataset within misuse detection context.

Author: Maheshkumar Sabhnani, Gursel Serpen

A small subset of machine learning algorithms, mostly inductive learning based applied to the KDD 1999 Cup intrusion detection dataset resulted in dismal performance for user-to-root and remote-to-local attack categories as reported in the recent literature. The uncertainty to explore if other machine learning algorithms can demonstrate better performance compared to the ones already employed constitutes the motivation for the study reported herein. Specifically, exploration of if certain algorithms perform better for certain attack classes and consequently, if a multi-expert classifier design can deliver desired performance measure is of high interest. This paper evaluates performance of a comprehensive set of pattern recognition and machine learning algorithms on four attack categories as found in the KDD 1999 Cup intrusion detection dataset. Results of simulation study implemented to that effect indicated that certain classification algorithms perform better for certain attack.

4. Title: Learning Fast Classifiers for Image Spam

Author: Mark Dredze, Reuven Gevaryahu, Ari Elias-Bachrach

Recently, spammers have proliferated “image spam”, emails which contain the text of the spam message in a human readable image instead of the message body, making detection by conventional content filters difficult. New techniques are needed to filter these messages. Our goal is to automatically classify an image directly as being spam or ham. We present features that focus on simple properties of the image, making classification as fast as possible. Our evaluation shows that accurately classify spam images in excess of 90% and up to 99% on real world data. Furthermore, we introduce a new feature selection algorithm that selects features for classification based on their speed as well as predictive power. This technique produces san accurate system that runs in a tiny fraction of the time. Finally, we introduce Justin Time (JIT) feature extraction, which creates features at classification time as needed by the

classifier. We demonstrate JIT extraction using a JIT decision that further increases system speed. This paper makes image spam classification practical by providing both high accuracy features and a method to learn fast classifiers.

5. Title: Using Syntactic Features for Phishing Detection

Author: Gilchan Park, Julia M. Taylor

This paper reports on the comparison of the subject and object of verbs in their usage between phishing emails and legitimate emails. The purpose of this research is to explore whether the syntactic structures and subjects and objects of verbs can be distinguishable features for phishing detection. To achieve the objective, we have conducted two series of experiments: the syntactic similarity for sentences, and the subject and object of verb comparison. The results of the experiments indicated that both features can be used for some verbs, but more work has to be done for others.

6. Title: Detecting Phishing Emails the Natural Language Way

Author: Rakesh Verma, Narasimha Shashidhar, and Nabil Hossain

Phishing causes billions of dollars in damage every year and poses a serious threat to the Internet economy. Email is still the most commonly used medium to launch phishing attacks. In this paper, we present a comprehensive natural language-based scheme to detect phishing emails using features that are invariant and fundamentally characterize phishing. Our scheme utilizes all the *information* present in an email, namely, the header, the links and the text in the body. Although it is obvious that a phishing email is designed to elicit an action from the intended victim, none of the existing detection schemes use this fact to identify phishing emails. Our detection protocol is designed specifically to distinguish between "actionable" and "informational" emails. To this end, we incorporate natural language techniques in phishing detection. We also utilize contextual information, when available, to detect phishing: we study the problem of phishing detection within the contextual confines of the user's email box and demonstrate that context plays an important role in

detection. To the best of our knowledge, this is the first scheme that utilizes natural language techniques and contextual information to detect phishing. We show that our scheme out performs existing phishing detection schemes. Finally, our protocol detects phishing at the email level rather than detecting masqueraded websites. This is crucial to prevent the victim from clicking any harmful links in the email. Our implementation called Phish Net-NLP, operates between a user's mail transfer agent (MTA) and mail user agent (MUA) and process search arriving email for phishing attacks even before reaching the inbox.

7. Title: iTrustPage: A User-Assisted Anti-Phishing Tool

Author: Troy Ronda, Stefan Saroiu, Alec Wolman

Despite the many solutions proposed by industry and the research community to address phishing attacks, this problem continues to cause enormous damage. Because of our inability to deter phishing attacks, the research community needs to develop new approaches to anti-phishing solutions. Most of today's anti-phishing technologies focus on automatically detecting and preventing phishing attacks. While automation makes anti phishing tools user-friendly, automation also makes them suffer from false positives, false negatives, and various practical hurdles. As a result, attackers often find simple ways to escape automatic detection. This paper presents iTrust Page – an anti-phishing tool that doesnot rely completely on automation to detect phishing. Instead, iTrust Page relies on user input and external repositories of information to prevent users from filling out phishing Web forms. With iTrust Page, users help to decide whether or not a Web page is legitimate. Because iTrust Page is user-assisted, iTrust Page avoids the false positives and the false negatives associated with automatic phishing detection. We implemented iTrust Page as a downloadable extension to FireFox. After being featured on the Mozilla website for FireFox extensions, iTrust Page was downloaded by more than 5,000 users in a two-week period. We present an analysis of our tool's effectiveness and ease of use based on our examination of usage logs collected from the 2,050 users who used iTrust Page for more than two weeks. Based on these logs, we find that iTrust Page disrupts users on fewer than 2% of the pages they visit, and the number of disruptions decreases over time.

8. Title: Phishing Environments, Techniques, and Countermeasures:

Author: Ahmed Aleroud, Lina Zhou

Phishing has become an increasing threat in online space, largely driven by the evolving web, mobile, and social networking technologies. Previous phishing taxonomies have mainly focused on the underlying mechanisms of phishing but ignored the emerging attacking techniques, targeted environments, and countermeasures for mitigating new phishing types. This survey investigates phishing attacks and anti-phishing techniques developed not only in traditional environments such as e-mails and websites, but also in new environments such as mobile and social networking sites. Taking an integrated view of phishing, we propose a taxonomy that involves attacking techniques, countermeasures, targeted environments and communication media. The taxonomy will not only provide guidance for the design of effective techniques for phishing detection and prevention in various types of environments, but also facilitate practitioners in evaluating and selecting tools, methods, and features for handling specific types of phishing problem.

9. Title: Phishing Detection: A Literature Survey

Author: Mahmoud Khonji, Youssef Iraqi

This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber-attacks are spread via mechanisms that exploit weaknesses found in end users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defence, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

10. Title: Presented types of phishing attacks in mobile devices

Author: Belal Amro

This survey presents types of phishing attacks in mobile devices and different mitigation techniques and anti-phishing techniques. Also they provided important steps to protect against phishing in mobile systems. The paper highlighted that current anti-phishing techniques have some shortcomings which makes them less efficient in detecting phishing attacks.