Phishing Detection and Trackback Mechanism

by

Isredza Rahmi A Hamid
Bachelor of Information Technology (Honours)
MSc (Information Technology)

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Deakin University

January, 2015

Abstract

Phishing attacks are one of the most prevalent forms of cybercrime worldwide. Cybercriminals use phishing for various illicit activities such as identity theft and fraud as well as installing malware on unsuspecting end user systems to gain access to the victims' systems. Phishing attacks have also been responsible for many sophisticated attacks perpetrated against financial institutions, government agencies, healthcare providers and businesses. In particular, email-born phishing attacks in which the phishers send fake emails pretending to be from a legitimate organization to extract sensitive information such as account numbers, passwords, or other personal information from victims or trick them into downloading malicious software embedded in documents or links have turned out to be a challenging problem. Although there exist many phishing email filtering approaches, email-born attacks continue unabated to plague Internet users and causing considerable economic losses worldwide. This calls for the development of effective countermeasures against email-born phishing attacks in order to safeguard critical infrastructures such as financial institutions. This is especially paramount as email is a critical communication medium for most organizations. Furthermore, with the widespread use of new technologies such as smart phones for emails and various Internet-based activities as well as social networks, phishing emails are more active than ever before and putting the average Internet users and organizations at risk of significant data, brand and financial losses. This thesis addresses phishing attacks problem with emphases on email-born phishing attack detection and prevention. Firstly, a hybrid feature selection approach for use in the detection of email-born phishing attack is developed. The proposed method is based on the combination of content-based and behaviour-based approaches. The hybrid feature selection approach includes various attribute are extracted from structural and behavioural components of the emails. Secondly, a new email-born phishing detection approach that is based on profiling and clustering techniques is developed. The phishing profiling algorithm takes into account various features present in the phishing emails as feature vectors and generate profiles based on clustering predictions. Following, we apply clustering techniques based on modified Two-Step clustering algorithm to generate the optimal number of clusters. Thirdly, a phishing trackback framework in order to find the origin of an attack either it is coming from the single or the collaborative attack is developed. First, the proposed phishing trackback framework grouped the phisher by using a clustering algorithm in email analyser phase. Then, similarity measurement is used in forensic backend to group the phisher into single or collaborative attack. Generally, the phisher may work alone or in groups. Typically, single attacker is hard to detect because they always changing their modus operandi. The proposed trackback framework is a simple solution to trace phisher and easy to implement where it allows automated detection of phishing email. Finally, we carried out extensive experimental analysis of the proposed approaches in order to evaluate their effectiveness in detection of email-born phishing attacks on large datasets. Next, the sensitivity of the proposed approaches to various factors such as the type of features, number of split and misclassification issues are studied. The results of the experiments show that the proposed approaches are highly effective in the detection of email-born phishing attacks as well as in the identification of a group and origin of phisher.

Contents

Chapter 1

Introduction

In recent years, much concern has been paid in securing the network infrastructure subject to various kinds of network-based attack. Phishing is among the active attack launch that can cause financial lost. Phishing is a combination of social engineering and web spoofing technique to lure users into revealing confidential information [1][2]. Phisher used various method involving the web, email and malicious software to steal personal information and account credentials. Hence, the phishing email detection has drawn a lot consideration for many researchers and the installation of malicious detection devices in email servers as a safety measure. However, phishing has become more and more complicated and attack can detour the filter set by anti-phishing techniques. It is strategic importance for information security to trace back the origin of internet attack. A number of trace back methods have been proposed where most of them deal with Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack. However, it is particularly challenging due to the evading techniques that attacker used. In this chapter, we discussed the research motivation and scope, significance, problems, objectives, methodology, contributions and the organization of the thesis.

1.1 Motivations and Scope

Phishing scams have flourished in recent years due to favourable economic and technological conditions. The technical resources needed to execute phishing attacks can be readily acquired through public and private sources. Some technical resources have been streamlined and automated, allowing use by non-technical criminals. This makes phishing both economically and technically viable for a larger population of less sophisticated criminals. A report by the Anti-Phishing Working Group (APWG) found that the number of unique phishing emails reported by consumers rose 20% in the first half of 2012 compared to the same period in 2011 [3]. There was also an increase by 73% in the number of unique phishing websites detected, in the first half of 2012 as compared to 2011. As phishing attacks are serious threats to security and economy worldwide [4], there is a strong need for automated phishing attack detection algorithms. Based on Gartner survey, approximately 109 million U.S adults have received phishing e-mail attacks with an average loss per victim estimated to be $1,244 [5]. These illustrate the essential of new phishing detection approach in this research as phishing is a highly profitable activity for criminals.

Over the year, there has been an increase in the technology, diversity, and sophistication of phishing attacks in response to increased user awareness and countermeasures, in order to maintain profitability. The ability to detect phishing email may help other individual particularly email users and organization in identifying normal email. The efficiency in profiling the attacker may significantly contribute into an accurate decision between normal or malicious email.

The scope of the research will be focusing on solving phishing problem including detection and profiling attackers. We also focus on the trace back mechanism in order to track the attacker. Our aim is to provide a solution with accuracy and efficiency to detect phishing attacks.

1.2 Research Significance

Phishing email detection has drawn a lot consideration for many researchers. Yet, phishing has become more complicated and attacker can detour the filter set anti-phishing techniques. A number of phisher implement new techniques such as by embedding hyperlinks from the original website, encoding or obfuscating website URL or redirecting victims to phishing website using malware to install the malicious software.

Existing classifications of phishing are based on simple features of phishing attacks such as URLs. Many of the currently available tools for combating phishing are based on simple rules, such as a blacklist consisting of reported phishing URLs. These tools are not effective for profiling, even though they may be effective at blocking. Thus, it is an urgent demand to identify phishing behaviour in a computer network to detect phishing email.

The next problem that we are going to tackle is how to profile phishing email. Knowing our enemy is a critical component of computer security. Therefore, identifying and understanding the attacker and the motivations behind phishing activities are just as crucial as the technical skills, techniques, and tools used to uncover them. Phishers normally have their own signatures or techniques. Thus, a phisher's profile can be expected to show a collection of different activities. We aim to develop an attacker profile by looking at the specific signature of the attacker.

We also focused on assessing anomalous behaviour in computer systems that would benefit user agencies and allow them and their clients to maintain secure computer network operation even under attack. Again, this is to ensure the user receives genuine emails from reputable sources. Therefore, a trace back mechanism will aid in determining the source of attacks and enable appropriate action, including possible legal action.

1.3 Research Problems

This thesis deals with phishing email problems which aim to detect the phishing email based on its behaviour. This research also looks at how to profile attackers based on their special traits and identify them by tracking the source of the attack. In particular we address the following three research issues in this thesis:

1. *How to detect phishing email in an efficient manner:* Detection is a vital aspect to fight against phishing. Numbers of anti-phishing solutions have been proposed in order to solve the phishing problem at various levels. However, the number of attacks increased each month showing that the phisher has become more and more complicated, and they can detour the filter set by anti-phishing techniques. Therefore, a new approach for phishing detection is compulsory where hybrid feature selection by combining the content based approach and behavioural approach which cannot be disguised as legitimate behaviour by an attacker is proposed.
2. *How to profile attacker an inaccurate way:* Knowing our enemy is a critical component of computer security. Therefore, identifying and understanding the attacker and the motivations behind these activities are just as crucial as the

technical skills, techniques, and tools used to uncover them. Here, the attacker's profiling for phishing email is presented. There is still an open problem what is the best method that can be used to do the phisher profiling due to lack of research in this area. Our goal is to propose phishing email profiling and filtering algorithm that could improve accuracy the accuracy of phishing detection.

3. *Trackback mechanism:* The phishing trackback mechanism is one of the hardest parts in Information security. Several novel trackback techniques have been proposed to trace the approximate spoofed source of the attack. Each technique has some unique advantages and disadvantages over the others. Most of the trackback effort focusing on the implementation of phoney token to detect the phisher. However, this method unable to capture the attacker unless the phisher interacts with the honeypot. So, utilising the phishing email features and suggests forensic techniques are vital in an attempt to trace the phisher.

1.4 Research Objectives

To achieve the research aim, four main research objectives are identified and need to be fulfilled:

1. To develop the taxonomy of phishing detection that contributes understanding towards current approaches, issues and challenges related to the topic.
2. To develop approaches to detect phishing email based on the hybrid feature selection approach.
3. To propose a phishing email profiling and filtering algorithm that could improve accuracy of phishing detection.

4. To proposed trace back mechanism to trace the attacker back to their origin in order to analyse the strategies.

1.5 Methodology

The proposed work will be carried out based on the experimental computer science method. This method examines the research work to demonstrate two vital concepts: proof-of-concept and proof-of-performance.

To demonstrate the proof-of-concept, some significant steps were performed. First, the research area within phishing detection is critically reviewed to provide the overview that leads to the formulation of valid problem statements. From this review, the research work in is justified. Then, the proposed approach of phishing detection is designed and analytically analysed.

Proof-of-performance is demonstrated by conducting the implementation for the phishing detection algorithm using simulations. In those simulations, various parameters and workloads were used to examine and demonstrate the viability of the proposed solutions compared to the similar baseline solutions. Also, analytical analysis of some proposed algorithms is performed to evaluate the correctness.

1.6 Research Contributions

We detail the thesis contributions as the following:

1. *Phishing email taxonomy.* This thesis presents a taxonomy of Phishing email. It investigates related concepts, describes the design themes and identifies implementation components required. The presented taxonomy is mapped to the

current phishing detection system to demonstrate its accuracy. Also, the mapping assists to perform a gap analysis in this research field.

2. *Phishing detection.* The thesis introduces an approach to detect phishing email. The phishing email is detected based on its behaviour by looking at the attacker sending email pattern. The approach is compared with the other baseline method and proves that its performance is superior to others.
3. *Profiling attacker.* The thesis presented an efficient profiling algorithm to profile the attackers. The proposed algorithm used various types of features to the cluster type of attacker.
4. *Trackback mechanism.* The thesis presents a mechanism to trackback the attacker back to their origin. The trackback mechanism is extremely important to trace the attacker involved in phishing email and analyse strategies deployed by the attacker.

To summarize, the work presented in this thesis is in line with the current trends that detect phishing email without having to build a dedicated. Therefore, it is our thesis to present phishing detection solutions that are scalable and efficient.

1.7 Thesis Organization

The chapters of this thesis are derived from various papers published during the PhD candidature. The remainder of the thesis is organized as the following:

1. *Chapter 2: Phishing Email Taxonomy.* This chapter provides an in-depth analysis and overview of existing phishing email detection approaches, presented within a comprehensive taxonomy.

2. *Chapter 3: Phishing Detection Framework.* This chapter offer overview framework for detecting and trackbacking phisher based on profiling and clustering technique. The framework consists of three phases: phishing detection, phishing profiling and phishing trackback.

3. *Chapter 4: Phishing Detection.* This chapter presents an approach to detect phishing email. This chapter is derived from the following publications:

   1. I.R A Hamid and J. Abawajy. (2011). Hybrid Feature Selection for Phishing Email Detection. The 11th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP-11). Melbourne, Australia. 24-26 October 2011.
   2. I.R A Hamid and J. Abawajy. (2011). Phishing Email Feature Selection Approach. The 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11), Changsha, China, 16-18 November, 2011.
   3. I.R A Hamid, J. Abawajy and T.H Kim. (2013). Using Feature Selection and Classification Scheme for Automating Phishing Email Detection. Studies in Informatics and Control 22 (1), pg 61-70.

4. *Chapter 5: Profiling Attacker.* This chapter presents an algorithm to profile attacker in phishing email based on various types of features. This chapter is derived from the following publication:

   1. I.R A Hamid and J. Abawajy. (2013). Profiling Phishing Email Based on Clustering Approach. The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-12), Melbourne, Australia, 16 July, 2013.

2. I.R A Hamid and J. Abawajy. (2014). An Approach for Profiling Phishing Email Attacks, Computers & Security, 45 (2014), pg 27- 41.

5. *Chapter 6: Trackback Mechanism*. This chapter presents an approach to trackback attacker and group them into a single or collaborative attack.

6. *Chapter 7: Conclusion and Future Directions*. The concluding chapter provides a summary of contributions and a future research challenges.

Chapter 2

Literature Review

In this chapter, a comprehensive literature review of phishing attacks will be discussed. There are various techniques used to detect phishing messages. The chapter includes in-depth analysis on existing approaches, listing the advantages and disadvantages of each approach. A taxonomy that classifies phishing detection into a well-defined category is presented. The taxonomy can be used by researchers to understand the current undertaking of phishing detection, the challenges and expectation in the future.

2.1 Introduction to Phishing

Cybercrime is a growing problem nationally and internationally, as organised crime gangs and continue to consolidate their highly profitable operations in identity theft and fraud. In today's information driven world, cyber criminals are more active than ever before and putting the average computer user and organizations at risk of significant data, brand and financial loss. Recently, one method that is commonly employed is phishing.

Phishing is an illegal deceptive attack in which victims are sent emails that deceit them into providing account numbers, passwords, or other personal information to an attacker. Phisher attracts user into revealing confidential information by using fake emails that usually appear as a reliable entity coming from popular social websites, auction sites, online payment processors or IT administrators such as eBay, PayPal, Suntrust and others. Generally, the email content wants the victim to update their personal information to avoid losing access rights to services provided by the organization. Unfortunately, they lure users to a bogus web site implemented by the attacker.

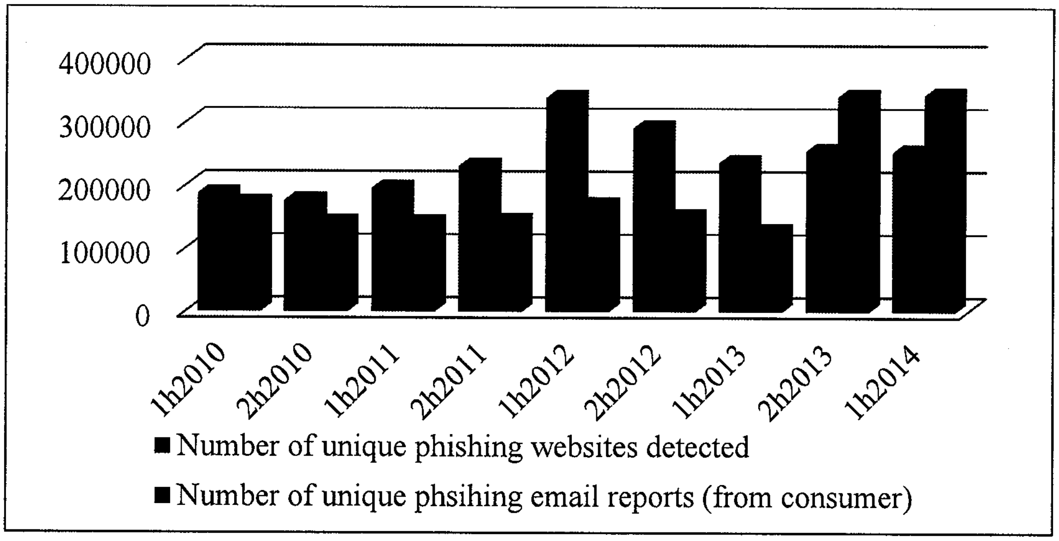


Figure 2.1: Number of phishing website and phishing email from 2010 to 2014

As the Internet playing significant role in business and commerce activities, phisher gain motivation to launch attacks in high return online scams. The graph in Figure 2.1 shows the number of phishing attacks which are collected worldwide between first half of the year 2010 and first half of the year 2014, analysed from the

APWG's (Anti-Phishing Working Group) phishing trend report [6]. The APWG is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The phishing attacks are shown in two ways, email and website phishing. Throughout four years, the number of phishing attacks through email decrease gradually from about 170000 reports to about 120000 reports in the first half of the year 2013. The number of phishing email increased drastically from about 12000 to 34000 attacks.

Phishing website increased dramatically between the first half of the year 2010 and first half of the year 2012 before a slight decrease in the second half of the year 2012. Next, the number of phishing website increased considerably in the first half of the year 2013. In conclusion, even though there is a slight decrease about 47000 phishing website report later in 2012, the phisher become more complicated and they manage to detour the filter set. Thus, the number of email phishing report raises radically to its highest peak in the first half of the year 2014 for about 340000 reports.

The rapid increase in the number of email users and the low cost of distributing emails via the Internet and other electronic communications networks has made marketing and communications with existing customers via email an attractive advertising medium. Therefore, email is frequently used as the medium for unsolicited communication known as phishing. This contributes a big negative impact on consumer confidence about e-commerce because it is a very lucrative business for the phisher. It costs Internet users billions of dollars a year. Survey by Consumer Reports National Research CenterNet shows that phishing attacks are almost as dominant today. The number of U.S. phishing attacks has increased significantly since last year, costing consumers billions in damages, according to the Anti-Phishing Working Group. Table

2.1 shows the U.S national incidence and total damage caused by Internet threat for years 2010 [7].

Table 2.1: Internet threat [7]

Internet threats	Scenario	Total damage	Attack frequency	National incidence
Spam	12 million households received suspicious e-mail.	N/A	Down from last year.	1:3 users had heavy of spam.
Virus	1.8 million households replaced infected personal computer.	$2.7 billion	Up from last year.	1:5 users had a serious virus attack.
Spyware	617,000 replaced slow or impaired personal computer.	$1.2 billion	No change.	1:11 users had a serious spyware problem.
Phishing	28.897 attack in December 2009.	$650 million	No change.	1:167 user lost money

According to a Gartner survey, more than 5 million U.S. consumers lost money due to phishing attacks in 2008. It was a 39.8 percent increase over the number of victims in 2007. Approximately, 3985 U.S online adults have been victimized by phishing attack. The average consumer loss per victim has grown from $220 to $351 per victim in 2008, a 60 percent decrease from the year before [5].

Based on National Consumer Reports survey, in spite of a rash of high-profile data breaches and cyber threats, an alarming 62 percent of U.S. online consumers have done nothing to protect their privacy on the Internet. Therefore, it is not surprising if the number of victims is still on the rise. In 2013, approximately one in seven online consumers was alerted that their personal data had been breached. It was a 56 percent increase from 2012. Moreover, 11.2 million people were projected to fall for e-mail phishing scam which is a 22 percent increase from the year 2013.

2.1.1 Phisher

Phishing is a term used to define various scams that use fraudulent email messages or spoofed website, send by phisher to lure victims into revealing personal information. Phisher on the other hand, is a criminal (person) who used this information to take credential information, steal money from the victim's bank account or hijack victim's computer. They gather any personal data from their targeted victim to advance their criminal activities.

Phishers have used a number of phishing procedures to gain personal information from users. A phishing message may point out that the user had problems with their computers or data and they need to verify their account information in order to ensure they could continue using the services. Others phishing message might suggest situation that a suspicious purchase was made using the user's credit card. They have to make further action by contacting them using the link given in the email if they want to cancel the transaction. There is also phishing message by using email claiming that the user has won the lottery. Then, they should click on to the secure web link provided, enter bank account information and the winning money will be deposited into their account. Another phisher's modus operandi is sending an email claiming to be from the tax company requesting the victim to refund tax money due to an accounting error. They query for the victim banking information to process the reimbursement.

2.1.2 Phishing Attack

As technology becomes more advanced, the phishing techniques being used are also more inventive. Internet users should have knowledge of various types of phishing techniques and be aware of anti-phishing techniques to protect themselves from getting phished. Phishing attacks take advantage of software and security weaknesses on both the client and server sides.

Phishing attacks can be divided into two groups: flash attacks and non-flash attacks. Flash attacks are characterized by a large volume of similar phishing messages sent within a short period of time. Non-flash attack messages are spread over a relatively long time span, but maintain their identifiable similarity. The interaction between phishing message and receiver could happen by following malicious link, filling deceptive forms or replying with useful information which are relevant for the message to succeed. All phishing attacks fit into the same general information flow. The phishing process involves five phases: planning, setup, attack, collection and identity theft or fraud.

2.1.2.1 Planning

Firstly, phishers will determine the targeted company or user to be their victim. Then, they will decide how to get personal information such as password, account number or e-mail addresses from their victim. Generally, mass-mailing and address collection techniques are commonly used for personal information from the victim. These two techniques are best known as spammers.

2.1.2.2 Setup

After phishers have decided which company to spoof and who their victims are, they will prepare for the attack. In the setup phase, the phisher will create techniques for sending the phishing message and collecting the valuable data. Normally, this involves e-mail addresses and a developing a web page.

2.1.2.3 Attack

In attack phase, a malicious payload arrives through three common propagation vectors either by spam email, phony message or establishing a rogue website. Normally, the phishing messages appear to be coming from a trustworthy source. Then, the victim may take action that makes them vulnerable to an information compromise. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan.

2.1.2.4 Collection

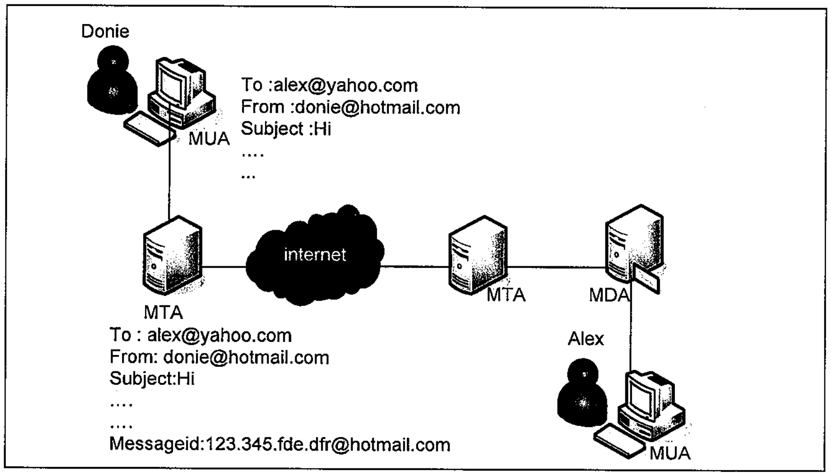
The confidential information is then transmitted from a phishing server to the phisher when it is compromised. Phishers will record every information that is entered by the victims into Web pages or popup windows.

2.1.2.5 Identity Theft and Fraud

Finally, the phishers gathered the confidential information from the victim. This information is used to impersonate the victim and making illegal purchases or otherwise commit fraud. Next, the success and failures of the completed scam are evaluated. This step is important for the phisher if they wish to organize another attack. Then, they have to start the phishing process again.

2.2 Email System Components

A typical email system components consist of three components: Mail Transport Agent (MTA), Mail Delivery Agent (MDA) and Mail User Agent (MUA) as shown in Figure 2.2. MTA handles message transportation and acts as a sorting area and mail carrier. On the other hand, MDA acts as an incoming mail server and MUA is represented as a software program that user used to retrieve email.



To :alex@yahoo.com
From :donie@hotmail.com
Subject :Hi
....
...

To : alex@yahoo.com
From: donie@hotmail.com
Subject:Hi
....
....
Messageid:123.345.fde.dfr@hotmail.com

Figure 2.2: Email system component

Every email sends from sender to receiver will go through the MTA. MTA will act as the post office where all emails are received, sorted and carried out to the receiver. These emails will be stamped with an email header information, including message-ID tag. When an email is sent, the message is routed from sender's server to the recipient's email server through the MTA. MTA handles the message transportation and acts as sorting area and mail carrier. The communication between MTAs are using Simple Mail Transfer Protocol (SMTP) which are logically known as SMTP servers. This server handles all outgoing mail servers from the sender to the recipient. The recipient's MTA then delivers the email to the MDA that acts as an incoming mail server.

MDA is a computer software that in charge of message delivery to the recipient's mailbox until the user accepts it. Within the email system component, local message delivery is accomplished through the message handling process from MTA and storing email into the recipient's mailbox. A user's email is managed by MUA which is an email client such as Mozilla Thunderbird, Microsoft Outlook and Eudora Mail. The email client is only active when a user runs it. Users of the email system need to log-in and run a mail client on the computer that hosts their mailboxes to retrieve the email message.

2.3 Structure of Email

Commonly, an email has two basic parts: i) email header and ii) message body. The header contains information about the sender's address, the recipient address and message route. Most email programs allow full headers to be displayed, but many header fields are not shown by default. After the email header is the body of the message which contains whatever the sender wish to send to the recipient.

A header is a set of lines containing information about the message's setting, such as the sender's address, the recipient's address, or timestamps showing when the message was sent by intermediate servers to the transport agents (MTAs) as depicted in Table 2.2. The header begins with a *from* line and changed each time it passes through an intermediate server. The header also shows the exact path taken by the email and the time taken for each server to process. However, this part of the email header is not visible to most users, but it is a useful indicator in determining phishing email. The message-ID tags found in email headers is a globally unique identification and can be used for mining the email sender behaviour.

Table 2.2: Email's header field

Header tag	**Description**
From	The sender's email address. This can be easily forged and can be the least reliable.
To	The recipient's email address, but may not contain the recipient's address
Date	Show the date when the email was sent by the sender.
Received	Contains information about the intermediate servers and the date when the message was processed. The received tag is the most reliable part to detect forged email. The last "Received" line show where the mail originated.
Reply-To	The email address for return mail.
Subject	The message's subject that sender place as a topic of email content.
Message-ID	A unique identification of the message. This could be forged, but need skill to intrigue recipient.

The body of an email message contains a simple and short piece of the plain text message which is sent from a sender to a recipient. Some of the message body, include signatures or automatically generated text that is inserted by the sender's mailing system. An attachment and any separated files could be part of the email message. In this thesis, we consider to mine different features from the email header and email messages to detect phishing email.

2.4 History of Phishing Detection Approach

Early work in this area focused on recognizing different type of email fraud such as phishing, Nigerian scam and lottery scam based on linguistic structure, terminology, knowledge and system engineering [8]. There have been many approaches to detect and prevent phishing attacks like using multi-tier classifier [9], anti-phishing toolbars [10] and scam website blockers [11]. Further, machine learning approaches based on features such as hyperlink, number of words, subject of emails and others have been proposed in the literature [12][13][14]. This increase in difficulty and depth allowed attackers to always change their modus operandi in order to evade from being detected.

In early 2003, classic phishing attack focused on text-based email [15]. Then, the attacker improvises it by embedding websites, complete with the returned address and logo of targeted company to make the email looks real. In Mid-2004, the attacker employs the use of HTML coding to modify the presence of the victim's address bar by replacing the URL of the phishing site with the company being impersonated [16][17][18] . This is a major breakthrough in phishing attack.

Later, phishers started to insert the message into attached image known as image phishing to bypass usual text-based filtering techniques. Invisible hyperlink or malicious content is often inserted into the attached image to evade from being detected by the anti-phishing tools. Due to this, some work investigates the layout of phishing sites in order to detect the malicious contents [19]–[22].

To date, phisher started to launch sophisticated attack using malicious content or malware where this tool managed to steal victim's personal information such as email address, password or completely take over the victim's computer. The examples of malware are keystroke, logger, spyware, ransomware, shareware, adware, Trojan horses or worms. Some of these malware can be downloaded into the computer by clicking the attachment or hyperlink given in phishing message. Despite these issues, a large amount of work in phishing detection has led to many perceptions. More recent work by [23][24][25][26][27][28] in phishing detection has focused on many approaches, which is discussed in the next section

2.5 Phishing Detection Taxonomy

In the literature there are taxonomies on phishing detection that discussed specifically for mobile devices [29]. Our taxonomy definitely focused on phishing detection, which is very important topic in phishing because it determines the system i) reliability and ii) efficiency. The reliability of the system depends on the detection process accuracy and the efficiency of the system depends on how the detection process is carried out. Our phishing detection taxonomy is divided into two categories which is feature selection and detection approaches as depicted in Figure 2.3.

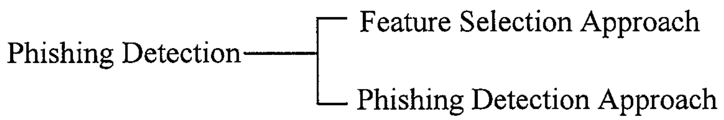


Figure 2.3: Phishing detection taxonomy

2.5.1 Feature Selection Approach

Adequate selection of features may improve accuracy and efficiency of classifier methods. There are two main approaches for feature selection that are wrapper and filter method. Wrapper methods is where the features are selected using the classifier, and filter methods select features is independent of the classifier used. Although the wrapper approach may obtain better performances, it requires greater computational resources. For this reason, currently a new hybrid approach, that combines both filter and wrapper methods has emerged. However, in this thesis, we work on a filter method which focus on detection phishing email based on heuristic based features.

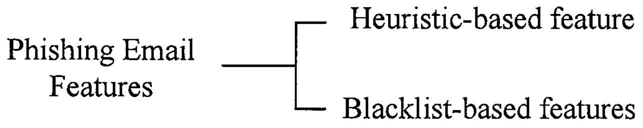


Figure 2.4: Feature selection approach

2.5.1.1 Heuristic-based Features

Anti-phishing tools use heuristic approaches that employ features such as the host name, checking the URL for common spoofing techniques, and checking against previously seen images or for detecting phishing sites. The work of Khonji summarizes the literature's phishing detection features into five subsets based on characteristics of emails: email body features, email headers features, URL features, Javascript features and external features extracted from SpamAssasin datasets [30]. A quite similar feature list is used by Bergholz et al. where they review five basic features: Structural features, Link features, Element features, Spam filter features and Word list features [31]. Toolan et al. [26] grouped the features into five: body-based features, URL-based features, subject-based features, script-based features and sender-based features. They divided the header features into subject-based features and sender-based features and discard external features, SpamAssassin features [27]. Following, features are categorized into more general group: content features, orthographic features and derived features [2].

These representations of email messaging were established to classify sets of features that would be dependable in determining phishing email attack. All features play important roles in order to detect phishing email. Not all collections of feature vectors were used in the testing contributes the most or the least, which leaves opportunity a better combination, may be achievable. Moreover, the increasing number of phishing attacks shows that there is still essential to find features that could increase the phishing detection rate. Based on listed features [2], [30], [31], [27], the phishing email feature can be determined into heuristic-based features: Content-based feature, Header-based feature, URL-based feature, Spam filter feature and Derived Features as shown in Figure 2.5.

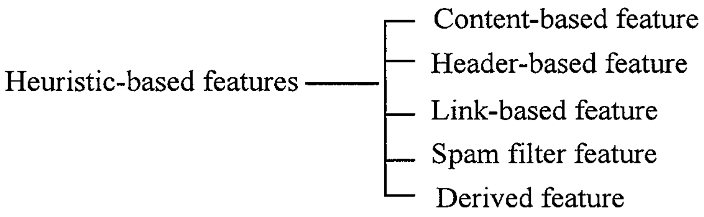


Figure 2.5: Heuristic-based features characteristics

a) Content-based Feature

Content-based features are extracted from the body parts of email messages. These features include data type in binary or continuous data which are listed in Table 2.3.

Table 2.3: Email body features

Features	Data Type
The existence of the words "dear" or "suspension"	Binary
The existence of phrase "verify your account"	Binary
Email content-type such as HTML or multipart	Binary
Contain form	Binary
Total number of characters	Continuous
Total number of function word. Example: account, log, access, minutes, bank, password, credit, recently, click, risk, identity, social, inconvenience, security, information, service, limited, suspended, urgent [14]	Continuous
Existence of unique words	Binary
Richness of body's content	Continuous

b) Header-based Feature

The header-based features listed in Table 2.4 are extracted from email header field. The email header contains information about the sender's address, the recipient address and message route. It shows the exact path taken by the email and the time taken for each server to process.

Table 2.4: Header-based feature

Feature	Data Type
Weather sender and reply-to address are different	Binary
Existence of function word in the subject field (e.g. bank, debit, verify, FW, RE)	Binary
Total number of character in subject field	Numerical
Total number of words in subject field	Numerical
Weather domain sender in not the same as modal domain.	Binary
The richness of email subject	Continuous

REFERENCES

[1] C. Ludl, S. McAllister, E. Kirda, and C. Kruegel, "On the effectiveness of techniques to detect phishing sites," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 4579, Springer Berlin Heidelberg, 2007, pp. 20–39.

[2] L. Ma, B. Ofoghi, P. Watters, and S. Brown, "Detecting phishing emails using hybrid features," in *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC '09. Symposia and Workshops on*, 2009, pp. 493–497.

[3] "APWG phishing attack trends reports," *Anti-Phishing Working Group*, 2012. [Online]. Available: http://http//www.antiphishing.org/resources/apwg-reports/.

[4] J. Abawajy and A. Kelarev, "A multi-tier ensemble construction of classifiers for phishing email detection and filtering," in *Cyberspace Safety and Security*, 2012, vol. 7672, pp. 48–56.

[5] C. STAMFORD, "Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008," *Gartner Survey*, 2009. [Online]. Available: http://www.gartner.com/newsroom/id/936913.

[6] "APWG phishing attack trends reports," *Anti-Phishing Working Group*, 2014. [Online]. Available: http://http//www.antiphishing.org/resources/apwg-reports/.

[7] "State of the Net 2010," *Consumer Reports National Research Center*, 2010.

[8] K. Kerremans, Y. Tang, R. Temmerman, and G. Zhao, "Towards ontology-based e-mail fraud detection," in *Conference on Artificial intelligence*, 2005, pp. 106–111.

[9] M. R. Islam, J. Abawajy, and M. Warren, "Multi-tier phishing email classification with an impact of classifier rescheduling," in *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN)*, 2009, pp. 789–793.

[10] "CallingID toolbar." [Online]. Available: http://www.callingid.com/.

[11] "SpoofGuard." [Online]. Available: http://crypto.stanford.edu/SpoofGuard/.

[12] J. James, L. Sandhya, and C. Thomas, "Detection of phishing URLs using machine learning techniques," in *International Conference on Control Communication and Computing (ICCC)*, 2013, pp. 304–309.

[13] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," in *Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit*, 2007, pp. 60–69.