International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 01 | Apr-2015 www.irjet.net p-ISSN: 2395-0072

CONTENT BASED APPROACH FOR DETECTION OF PHISHING SITES

Anjali Gupta[1], Juili Joshi[2], Khyati Thakker[3], Chitra bhole[4]

K.J. Somaiya Institute of Engineering & Information Technology, Mumbai, India

ABSTRACT: ***Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. In this paper, we present the design, implementation, and evaluation of content-based approach to detecting phishing web sites. We also discuss the design and evaluation of several heuristics we developed to reduce false positives. Our experiments show that CANTINA is good at detecting phishing sites, correctly labeling approximately 95% of phishing sites. We are going to implement Revelation of Masquerade Attacks: A Content-Based Approach to Detecting Phishing Web Sites using PHP & MYSQL.Our system will crawl the original site of bank and it will retrieve all URL's, location of bank's server and whois information. If user get any email with phishing attack link. Then our system will take that url as input and crawl the link, retrieve all url's and system will compare these url's with original banks url database, try to find url's are similar or not. Then system will find location of Phishing link URL and compare location with original banks location. After that system will find out Whois information of URL.System will analyze the information and show the results to the user.***

KEYWORDS-*Phishing,CATINA,url,phished website.*

1.INTRODUCTION

The main purpose that banks have been serving since their inception is keeping our money safe for us. While keeping our money safe, they also let us earn a certain amount of interest on the money deposited with them. Traditional banks have been doing this, and internet banks continue the same function. The only difference is in the way the transactions are made. We all know about internet banking and most of us use it quite often as well, but few of us actually understand about the history of internet banking and how it all came out. Knowing the history of internet banking can be incredibly useful, especially since it will allow us to have more respect for the little things that we take for granted.

In today's world, computers play an incredibly large role in the way the world exists in general, and the majority of tasks could actually not be completed if not for the use of computers. Although there are certainly some areas and jobs that cannot yet be completed solely by computers and which thus still require actual manpower, for the most part, computers have helped to make life significantly easier, productive, and more convenient for us all.

Internet banking has been around for quite a few years now, but has really only become prominent over the past year or so in particular. Interne banking offers an array of different advantages to the user, including account balances and history including year-to-date information, the ability to transfer money from one account to another and to payees for bill payments, check history, reorders, and stop payments, check credit card balances and statements, complete online loan applications, secure interactive messaging with staff, and much more.

Internet banking basically allows you to be able to do everything that you can in your regular banking institution, only with the benefit that you can do it all right from the convenience of your own home. Not only is this great because you can be comfortable and have peace of mind knowing that you can keep track yourself of all your banking issues, but as well it allows for more ease because you never have to worry about rushing out and making it to the bank.

The word "phishing" comes from the analogy that Internet scammers are using fake email to steal for Passwords and personal financial data from the sea of Internet users.[16] Phishing is the creation of email messages and web Pages in such a way that the replicas of existing web sites to fool users and instruct them to submit their personal or financial details into fraudsters fake pages. Pharming is a technique to redirect users from real websites to the fraudulent websites by using malware/spyware, typically DNS hijacking. Pharming uses modifications in the

© 2015, IRJET.NET- All Rights Reserved

name resolution [2]system, so as when a user clicks a financial institution web page, it actually goes to the spoofed website. Phishing attack carried out from phone is also known as Vishing attack. During the last five years phishing has been growing rapidly, with an estimate citation of approximately 8 million daily phishing attempts all over the world.

The word 'Phishing' initially emerged in 1990s. The early hackers often use 'ph' to replace 'f' to produce new words in the hacker's community, since they usually hack by phones. Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to visit a faked Web site by sending them faked e-mails (or instant messages), and stealthily get victim's personal information such as user name, password, and national security ID, etc. These information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). The frequently used attack method is to send e-mails to potential victims, which seemed to be sent by banks, online organizations, or ISPs.[20] In these e-mails, they will make up one causes, e.g. the password of your credit card had been miss entered for many times, or they are providing upgrading services, to allure you visit their Web site to conform or modify your account number and password through the hyperlink provided in the e-mail. You will then be linked to a counterfeited Web site after clicking those links. The style, the functions performed, sometimes even the URL of these faked Web sites This work was supported by the National Natural Science Foundation of China (NSFC) under contract No. 60503049 are similar to the real Web site. It's very difficult for you to know that you are actually visiting a malicious site. If you input the account number and password, the attackers then successfully collect the information at the server side, and is able to perform their next step actions with that information (e.g., withdraw money out from your account). Phishing itself is not a new concept, but it's increasingly used by phishers to steal user information and perform business crime in recent years. Within one to two years, the number of phishing attacks increased dramatically. According to Gartner Inc., for the 12 months ending April 2004, "there were 1.8 million phishing attack victims, and the fraud incurred by phishing victims totaled $1.2 billion" [6]. According to the statistics provided by the Anti-Phishing Working Group (APWG) [2], in March 2006, the total number of unique phishing reports submitted to the APWG was 18,480; and the top three phishing site hosting countries are, the United States (35.13%), China (11.93%), and the Republic of Korea (8.85%). The infamous phishing attacks happened in China in recent years include the events to counterfeit the Bank of China (real Web site www.bank-ofchina. com, counterfeited Web site www.bank-off-china.com), the Industrial and Commercial Bank of China (real Web site www.icbc.com.cn, faked web site www.1cbc.com.cn), the Agricultural Bank of China (real webs ite www.95599.com, faked Web site www.965555.com), etc. Phishing Techniques Link manipulation Most methods of phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization.[3]Misspelled URLs or the use of sub domains are common tricks used by phishers. In the URl, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of the your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the < A > tags) suggests a reliable destination, when the link actually goes to the phisher's site.[4] The following http://en.wikipedia.org/wiki/Genuine, appears to take you to an article entitled "Genuine"; clicking on it will in fact take you to the article entitled "Deception". In the lower left hand corner of most browsers you can preview and verify where the link is going to take you. In the section 2,we discussed about the related work like Reasons of people being victim of phishing attacks, Making People Aware of Phishing Attacks, Anti-Phishing User Interfaces, automated detection of phishing, features of Catina. In section 3,overview of earlier work is presented. Section4, give problem of statement. Implementation design of our system is presented in section 5 as well as a brief description of evaluation of heuristics(content, url ,ip address, whois) is described in section 6. And hence we conclude in a nutshell.

2. RELATED WORK

Generally speaking, past work in anti-phishing falls into four categories: studies to understand why people fall for phishing attacks, methods for training people not to fall for phishing attacks, user interfaces for helping people make better decisions about trusting email and websites, and

© 2015, IRJET.NET- All Rights Reserved

automated tools to detect phishing. Our work on CANTINA contributes a new approach to the development of automated phishing detection tools.

2.1 Reasons of people being victim of phishing attacks

A number of studies have examined the reasons that people fall for phishing attacks. For example, Downs et al have described the Carnegie Mellon Anti-phishing and Network Analysis Tool Copyright is held by the International World Wide Web Conference results of an interview and role-playing study aimed at understanding why people fall for phishing emails and what cues they look for to avoid such attacks [10]. In a different study, Dhamija et al. showed that a large number of people cannot
differentiate between legitimate and phishing web sites, even when they are made aware that their ability to identify phishing attacks is being tested [9]. Finally, Wu et al. studied three simulated anti- phishing toolbars to determine how effective they
were at preventing users from visiting web sites the toolbars had determined to be fraudulent [3]. They found that many study participants ignored the toolbar security indicators and instead used the site's content to decide whether or not it was a scam. Next, sub-point is about making people aware of phishing attacks.

2.2 Making People Aware of Phishing Attacks

Anti-phishing education has focused on online training materials, testing, and situated learning. Online training materials have been published by government organizations [3, 4], non-profits [3]
and businesses [1, 8]. These materials explain what phishing is and provide tips to prevent users from falling for phishing attacks.

Testing is used to demonstrate how susceptible people are to phishing attacks and educate them on how to avoid them. For example, Mail Frontier [26] has a web site containing screenshots
of potential phishing emails. Users are scored based on how well they can identify which emails are legitimate and which are not.

A third approach uses situated learning, where users are sent phishing emails to test users vulnerability of falling for attacks.

At the end of the study, users are given materials that inform them about phishing attacks. This approach has been used in studies conducted by Indiana University in training students [20], West Point in instructing cadets [5, 2] and a New York State Office in educating employees [13]. The New York study showed an improvement in the participants' behavior in identifying phishing over those who were given a pamphlet containing the information on how to combat phishing. In previous work, we developed an email-based approach to train people how to identify and avoid phishing attacks, demonstrating that the existing practice of sending security notices is ineffective, while a story-based approach using a comic strip format was surprisingly effective in teaching people about phishing [22].Below subsection is about anti-phishing user interfaces.

2.3 Anti-Phishing User Interfaces

Other research has focused on the development of better user interfaces for anti-phishing tools. Some work looks at helping users determine if they are interacting with a trusted site. For example, Ye et al. [9] and Dhamija and Tygar [18] have developed prototype user interfaces showing "trusted paths" that help users verify that their browser has made a secure connection to a trusted site. Herzberg and Gbara have developed Trust Bar, a browser add-on that uses logos and warnings to help users distinguish trusted and untrusted web sites [21].Other work has looked at how to facilitate logins, eliminating the need for end-users to identify whether a site is legitimate or not.
For example, PwdHash [23] transparently converts a user's password into a domain-specific password by sending only a oneway hash of the password and domain-name. Thus, even if a user falls for a phishing site, the phishers would not see the correct password. The Lucent Personal Web Assistant [7] and Password Multiplier [25] used similar approaches to protect people. PassPet [14] is a browser extension that makes it easier to login to known web sites, simply by pressing a single button. PassPet requires people to memorize only one password, and like PwdHash, generates a unique password for each site.

Web Wallet is web browser extension designed to prevent users from sending personal data to the fake page [38]. Web Wallet prevents people from typing personal information directly into a web site, instead requiring them

© 2015, IRJET.NET- All Rights Reserved

to type a special keystroke to log into Web Wallet and then select their intended web site.

Our work in this paper is orthogonal to this previous work, in that our algorithms could be used in conjunction with better user interfaces to provide a more effective solution. As Wu and Miller demonstrated, an anti-phishing toolbar could identify all fraudulent web sites without any false positives, but if it has usability problems, users might still fall victim to fraud [17].Overview of automated detection of phishing is given in next description.

2.4 Automated Detection of Phishing

Anti-phishing services are now provided by Internet service providers, built into mail servers and clients, built into web browsers, and available as web browser toolbars (e.g., [4, 5, 2,8, 9, 2]). However, these services and tools do not effectively protect against all phishing attacks, as attackers and tool developers are engaged in a continuous arms race [6]. Anti-phishing tools use two major methods for detecting phishing sites. The first is to use heuristics to judge whether a page has phishing characteristics. For example, some heuristics used by the SpoofGuard [24] toolbar include checking the host name, checking the URL for common spoofing techniques, and checking against previously seen images. The second method is to use a blacklist that lists reported phishing URLs. For example, Cloudmark [19] relies on user ratings to maintain their blacklist. Some toolbars, such as Netcraft [9], seem to use a combination of heuristics plus a blacklist with URLs that are verified by paid employees. Both methods have pros and cons. For example, heuristics can detect phishing attacks as soon as they are launched, without the need to wait for blacklists to be updated. However, attackers may be able to design their attacks to avoid heuristic detection. In addition, heuristic approaches often produce false positives (incorrectly labeling a legitimate site as phishing). Blacklists may have a higher level of accuracy, but generally require human intervention and verification, which may consume a great deal of resources. At a recent Anti-Phishing Working Group meeting, it was reported that phishers are starting to use one-time URLs, which direct someone to a phishing site the first time the URL is used, but direct people to the legitimate site afterwards. This and other new phishing tactics significantly complicate the process of compiling a blacklist, and can reduce blacklists' effectiveness.Our work with CANTINA focuses on developing and evaluating a new heuristic based on TF-IDF, a popular information retrieval algorithm. CANTINA not only makes use of surface level characteristics (as is done by other toolbars), but also analyzes the text-based content of a page itself.
Section 2.5 gives idea about features of content based approach.

2.5 Features of Content Based Approach:

CANTINA is a content-based approach to detect phishing websites, based on the term frequency–inverse document frequency (TF-IDF) information retrieval algorithm.[15].CANTINA examines the content of the page to determine whether the site is phished website or not. CANTINA included eight features in their proposed model.

The features are described as follows:

a) *Age of Domain:* This heuristic is used to check whether the age of the domain name is greater than 12 months or not. Initially the phishing site's lifespan is 4.5 days but now the heuristic does not account for phishing sites based on existing web sites where criminals have broken into the web server, nor does it account for phishing sites hosted on otherwise legitimate domains, for example in space provided by an ISP for personal homepages [6].

b)*Suspicious URL:* In this heuristic check whether the page's URL contains the symbol '@' or '-', because '@' symbol in the URL indicates that the string in its left side can be discarded and consider only right part 59 of the string after the symbol. An '-'symbol is rarely used in the legitimate sites.

c) *Suspicious Links:* This heuristic checks whether the links in the page satisfies the above condition or not. If it satisfies the condition then it is marked as suspicious link.[7]

d) *IP Address:* It will check whether the given URL contains IP address as its domain or not.
Below is a brief description of Earlier Work.

© 2015, IRJET.NET- All Rights Reserved

3. EARLIER WORK

Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. [15]To respond to this threat, software vendors and companies have released a variety of anti-phishing toolbars. For example, eBay offers a free toolbar that can positively identify eBay-owned sites. However, when conducted an evaluation of ten anti-phishing tools for a previous study, found that only one tool could consistently detect more than 60% of phishing web sites without a high rate of false positives. Thus, there is a strong need for better automated detection algorithms.

Disadvantages of Earlier Work

1. Only one tool could consistently detect more than 60% of phishing web sites without a high rate of false positives.

2. There is not use better automated detection algorithms.
Section 4,provide various formulation of phishing problem and survey phishing tactics.

4. PROBLEM STATEMENT

In this, consider various formulations of the phishing problem and survey phishing tactics, both those in use today and those likely to appear in the near future and also consider the aspects of user behavior typically exploited by phishing attacks. [19]Phishing has becoming a serious network security problem, causing finical lose of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally, phishing has made e-commerce distrusted and less attractive to normal consumers.

Attacks

A typical phishing attack begins with an email to the victim, supposedly from a reputable institution, but actually from the phisher. The text of the message commonly warns the user that a problem exists with the user's account that must immediately be corrected. [18,12,11,10]The victim is led to a spoofed website designed to resemble the institution's official website. At this point, the phishing site may launch a passive or an active attack. In a passive attack, the web page prompts the victim to enter account information (e.g., username and password) and may also request other personal details, such as the victim's Social Security number, bank account numbers, ATMPINs, etc. All of this information is relayed to the phisher, who can then use it to plunder the user's accounts. In an active attack, the phisher may act as a man-in-the-middle attacker, actively relaying information from the legitimate site to the user and back.[20]

While early phishing emails typically employed plain text and grammatically incorrect English, current attacks demonstrate increased sophistication. Phishing emails and websites often employ the same visual elements as their legitimate counterparts. As a result, spoofed sites and legitimate sites are virtually indistinguishable to users. Phishers also exploit a number of DNS tricks to further obscure the nature of the attack. The spoofed site may use a domain name like www.ebay.com.kr, which very closely resembles eBay's actual domain, but instead points to a site in Korea. Some attacks use obscure URL conventions to craft domain names like www.ebay.com@192.168.0.5, while others exploit bugs in the browser's Unicode URL parsing and display code to conceal the site's true domain name. Implementation Design is given in next section.

5. IMPLEMENTATION DESIGN

We are going to implement CANTINA: A Content-Based Approach to Detecting Phishing Web Sites using PHP & MYSQL. It is an implementation of a project our system will crawl the original site of bank and it will retrieve all URL's, location of bank's server and whois information[22]. If user get any email with phishing attack link. Then our system will take that url as input and crawl the link, retrieve all url's and system will compare these url's with original banks url database, try to find url's are similar or not. Then system will find location of Phishing link URL[13] and compare location with original banks location. After that system will find out Whois information of URL. System will analyze the information and show the results to the user.

© 2015, IRJET.NET- All Rights Reserved

Table 1. Heuristics used to reduce false positives. Note that we added TF-IDF-Final as a "heuristic" to determine the proper weight to assign to it.

Heuristic	Suspected Phishing?
Age of Domain	<= 12 months
Known Images	Page contains any known logos and not on a domain owned by logo owner
Suspicious URL	URL contains @ or -
Suspicious Links	Link on page contains @ or -
IP Address	URL contains IP address
Dots in URL	>= 5 dots in URL
Forms	Page contains a text entry field
TF-IDF-Final	TF-IDF-Final suspects phishing

Module

- Crawling
- Parsing
- Server info
- Data Collection
- Data Processing
- Locating phishing server
- Analyzing Details
- Results

Crawler

A Web crawler is one type of software agent. In general, it starts with a list of URLs to visit, called the seeds. As the crawler visits these [22]URLs, it identifies all the hyperlinks in the page and adds them to the list of URLs to visit, called the crawl frontier. URLs from the frontier are recursively visited according to a set of policies.

WHOIS

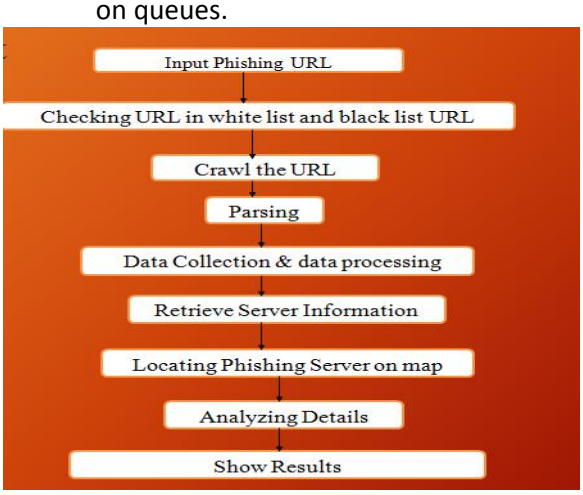
WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The Whois protocol is documented in RFC 3912[18].

Locating Phishing Server

- URL is nothing but IP Address.
- Using IP address our system will locate phishing server.

Advantages

- User can easily find out phishing attacks.
- System will add one more layer into online transaction.
- User can get real Bank site information.
- Reduce/prevent financial loss from phishing attacks
- Create a banking system that is easily accessible by customers from The comfort of their homes, offices etc .
- Reduce the time wasted in going to banks to stay on queues.

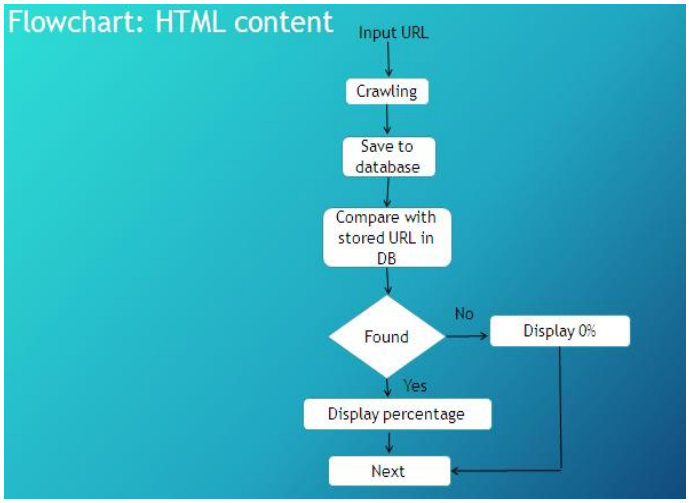


How our system will be evaluated is described briefly in next section i.e 6.

6. EVALUATION

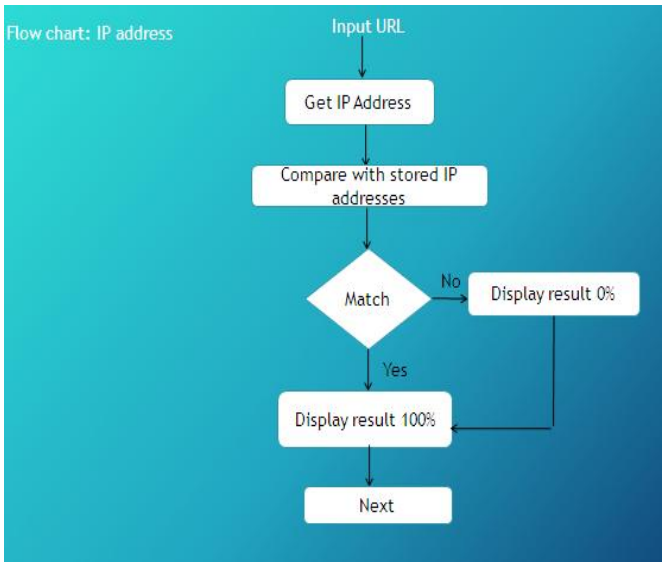
Evaluation of our system is as follows:
Experiment 1 – Evaluation of HTML Contents

© 2015, IRJET.NET- All Rights Reserved



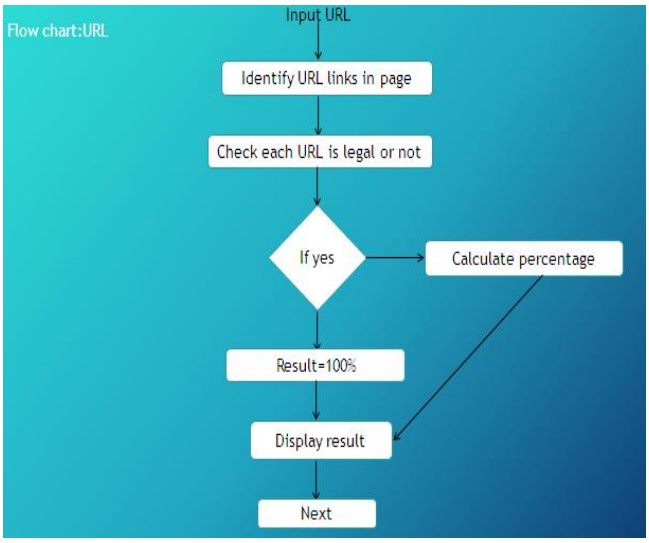
In this, user will input the url and our system will crawl the page, Save to the database. After saving of the crawled page it is compared with stored url in the database and appropriately takes the decision. If crawled page is matched entirely with the original page which is stored in the database then display the appropriate result of the matched page with appropriate matched percentage of the contents. Now, next Heuristic will be calculated which is the IP address.

Experiment *2* – Evaluation on basis of IP Address



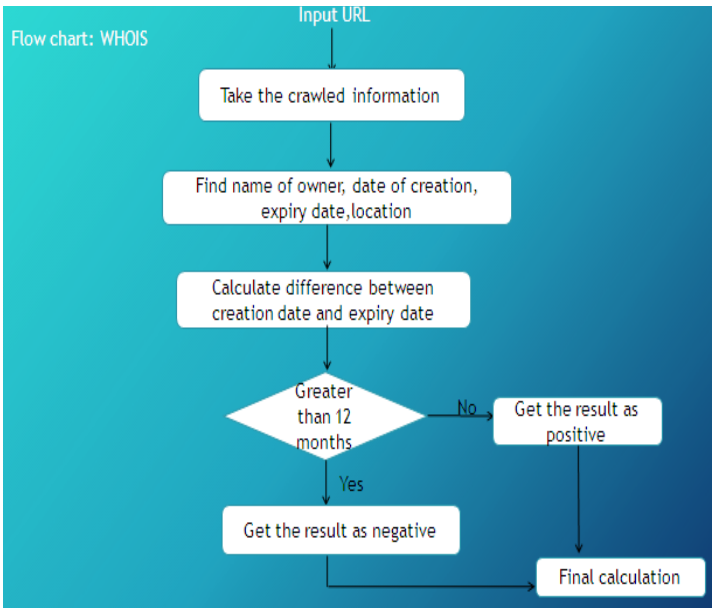
In this heuristic, system will take the URL from the user, get the IP address and compare this ip address with the stored original ip address of the URL from the database and output the amount of matched IP address in the terms of percentage.

Experiment 3 – Evaluation on basis of URL



In URL heuristic, take input of URL from user and then identify url direction of links in page. Check each direction of this url is legal or not. If legal, then calculate respective percentage of matched direction of url else show 0% output.

Experiment 4 – Evaluate WHOIS

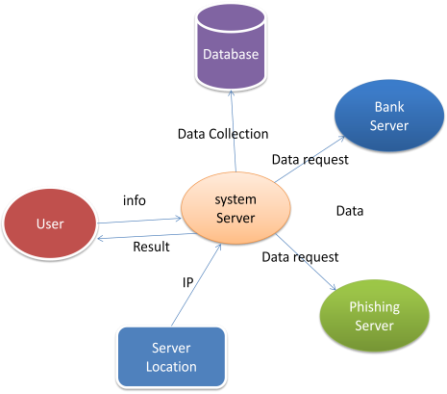


© 2015, IRJET.NET- All Rights Reserved

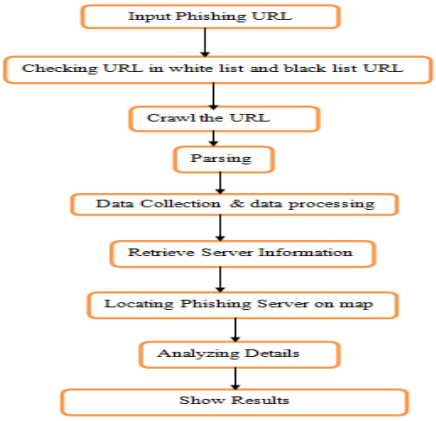
WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.[21] The protocol stores and delivers database content in a human-readable format. WHOIS heuristic give information about name of owner of site, date of creation of site, expiry date of site ,location as well as it calculate the difference between date of creation and date of expiry .If this difference is greater than 12 months then it is a legal site or else if age of domain is below 12 months then it is a phished website.

7. IMPLEMENTATION:

The system DFD of level 1 is shown in the figure.



The working of the system is represented in the flowchart given below:



8. SCREENSHOTS OF OUR SYSTEM:

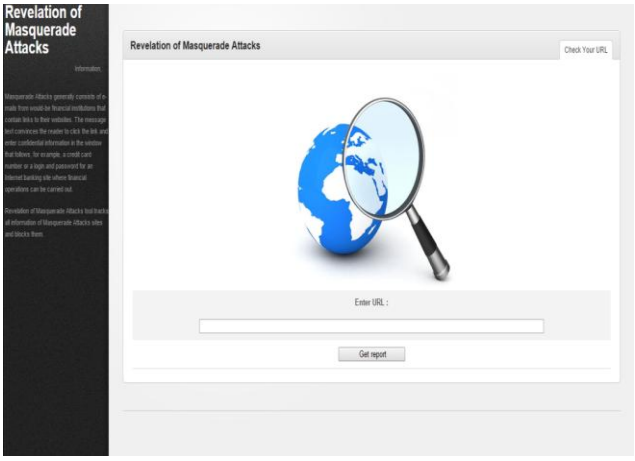


Fig :Input url to check for phishing

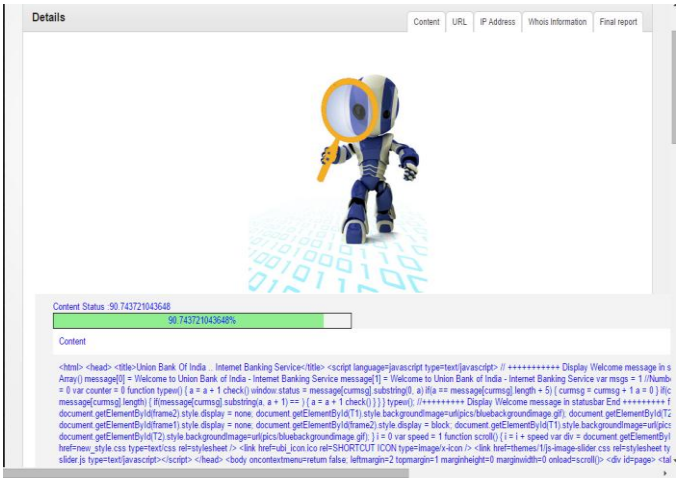


Fig : HTML contents of Crawled page.

© 2015, IRJET.NET- All Rights Reserved

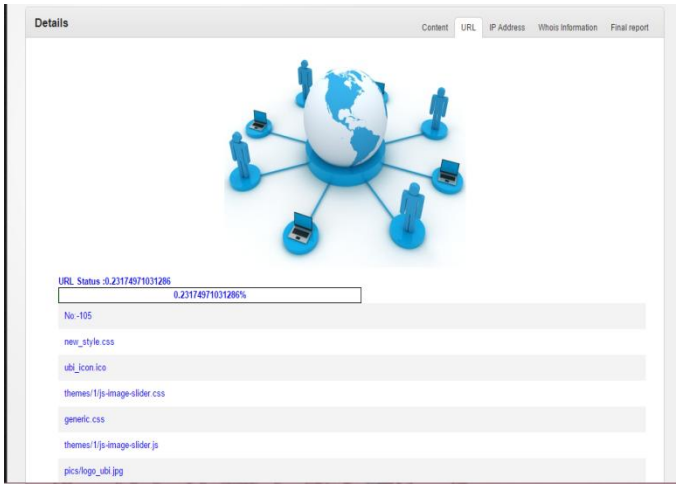


Fig :URL of crawled page.

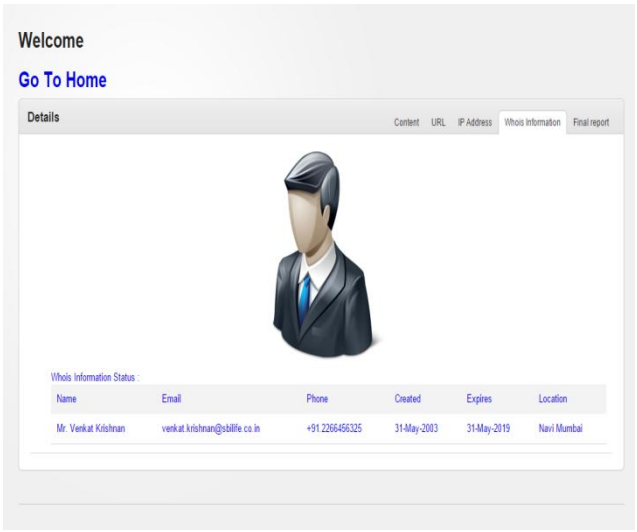


Fig :Whois Information of crawled Page

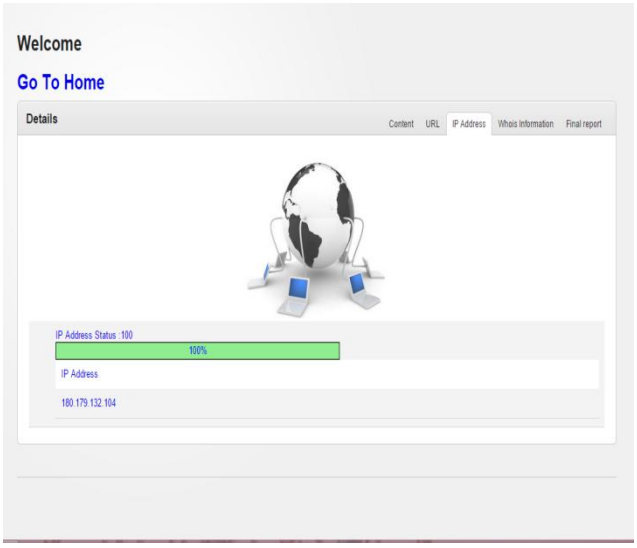


Fig :IP Address of crawled Page

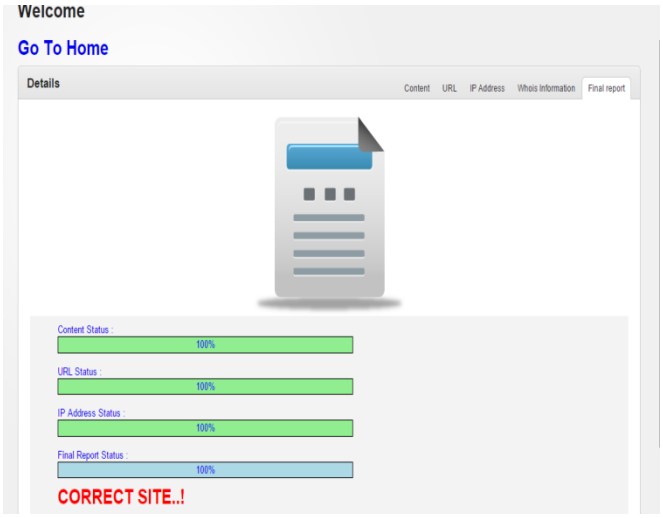


Fig: Final result of our System.

9. CONCLUSION & FUTURE MODIFICATION

In this paper, we presented the design and evaluation of CANTINA, a novel content-based approach for detecting phishing web sites.[8]CANTINA takes Robust Hyperlinks, an idea for overcoming page not found problems using the well-known Term Frequency / Inverse Document Frequency (TF-IDF) algorithm, and applies it to anti-phishing. We

© 2015, IRJET.NET- All Rights Reserved

described our implementation of CANTINA, and discussed some simple heuristics that can be applied to reduce false positives. We also presented an evaluation of CANTINA, [24]showing that the pure TF-IDF approach can catch about 97% phishing sites with about 6% false positives, and after combining some simple heuristics we are able to catch about 90% of phishing sites with only 1% false positives. In future work, we plan on refining[16] CANTINA in preparation for wider-scale deployment and evaluation. We also plan on developing and evaluating better user interfaces. Even if an anti-phishing toolbar is highly accurate, users might still fall victim to fraud if users do not understand what the toolbar is trying to communicate.

1. We will increase the capacity of database.
2. We will add more parameters to detect phishing attack more accurately.

REFERENCES

[1] M. Weiser, "The Computer for the 21st Century," Scientific American, vol. 265, no. 3, pp. 94-104, September 1991.

[2] D. J. Goodman, "The wireless Internet: promise and challenges," Computer, vol. 33, no. 7, pp. 36-41, July 2000.

[3] S. Saha, M. Jamtgaard, and J. Villasenor, "Bringing the wireless Internet to mobile devices," Computer, vol. 34, no. 6, pp. 54-58, June 2001.

[4] P. Pace, G. Aloi, and A. Palmacci, "A Multi-Technology Location- Aware Wireless System for Interactive Fruition of Multimedia Contents," IEEE Transactions on Consumer Electronics, vol. 55, No. 2, pp. 342-250, MAY 2009.

[5] F. O. Akgul, and K. Pahlavan, "Location Awareness for Everyday Smart Computing," Proceedings of the 16th International Conference on Telecommunications, pp. 2-7, Marrakech, Morocco, May 2009.

[6] S. Hartwig, M. Luck, J. Aaltonen, R. Serafat, and W. Theimer, "Mobile multimedia - challenges and opportunities," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 1167-1178, November 2000.

[7] D.L. Lee, W.-C. Lee, J. Xu, and B. Zheng, "Data Management in location-dependent information services," IEEE Pervasive Computing, vol. 1, no. 3, pp. 65-72, July-Sept. 2002.

[8] P. Bellavista, A. Kupper, and S. Helal, "Location-based services: back to the Future," IEEE Pervasive Computing, vol. 7, issue 2, pp. 85-89, April-June 2008.

[9] Kumaraguru, P., Y.W. Rhee, A. Acquisti, L. Cranor, and J. Hong. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In Proceedings of CHI2007.

[10] Mail Frontier, Phishing IQ. Visited: Nov 20, 2006.

[11] McMillan, R., Gartner: Consumers to lose $2.8 billion to phishers in 2006, NetworkWorld, 2006.

[11] Microsoft, Consumer Awareness Page on Phishing. Visited:Nov 20, 2006.

[12] Netcraft, Netcraft Anti-Phishing Toolbar. Visited: Nov 20,2006.

[13] New York State Office of Cyber Security & Critical Infrastructure Coordination. 2005. Gone Phishing… A Briefing on the Anti-Phishing Exercise Initiative for New York State Government. aggregate Exercise Results for public release.

[14] Panahy, A., Google Parser, The Code Project - C# Programming. Visited: Nov 20, 2006. http://www.codeproject.com/csharp/googleparser.asp

[15] Phelps, T.A. and R. Wilensky, Robust Hyperlinks and Locations, D-Lib Magazine, vol. 6(7/8), 2000. http://www.dlib.org/dlib/july00/wilensky/07wilensky.html

[16] PhishTank. Visited: Nov 20, 2006. http://www.phishtank.com/

[17] PhishTank, Statistics about Phishing Activity and PhishTank Usage. Visited: Nov 20, 2006.

© 2015, IRJET.NET- All Rights Reserved

http://www.phishtank.com/stats/2006/10/

[18] Salton, G. and M.J. McGill, Introduction to Modern Information Retrieval. New York, NY: McGraw-Hill, 1986.

[19] Stanford Applied Crypto Group, PwdHash. Visited: Nov 20, 2006. http://crypto.stanford.edu/PwdHash

[20] Wu, M., R. Miller, and S. Garfinkel. Do Security Toolbars Actually Prevent Phishing Attacks? In Proceedings of ACM Conference on Human Factors in Computing Systems

[21] Wu, M., R.C. Miller, and G. Little. Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. In Proceedings of The Second Symposium on Usable Privacy and Security (SOUPS 2006). pp. 102-113 2006.

[22] Ye, Z., S. Smith, and D. Anthony, Trusted paths for browsers. ACM Transactions on Information and System Security 2005. **8**(2): p. 153-186.

[23] Yee, K.-P. and K. Sitaker. Passpet: Convenient Password Management and Phishing Protection. In Proceedings of The Second Symposium on Usable Privacy and Security (SOUPS 2006). pp. 32-43 2006.

[24] Zolnikov, P., Extending Explorer with Band Objects using.NET and Windows Forms, The Code Project - C# Programming. Visited: Nov 20, 2006.

© 2015, IRJET.NET- All Rights Reserved