Browser-Side Countermeasures for Deceptive Phishing Attack

Soumya. T1 & Thilakavathi. P2

1 ME CSE, 2 Assistant Professor CSE
1,2 Sasurie Academy Of Engineering

Abstract: Phishing is a form of online identity theft. Phishers use social engineering to steal victims' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails to lure unsuspecting victims into counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. This is called a deceptive phishing attack. In this paper, a thorough overview of a deceptive phishing attack and its countermeasure techniques, which is called anti-phishing, is presented.

I. INTRODUCTION

Phishing, a term coined in 1996, is a form of online identity theft [1]. Phishing was originally used to describe theft of AOL passwords and corresponding accounts. However, over the decade the definition of phishing has expanded. Phishers today use attack vectors such as email, Trojan horse key loggers and man-in-the-middle attacks to trick the victims. Phishing attack includes deceptive attack, in which Phishers use spoofed e-mails to deceive unsuspecting victim to disclose confidential information; malware attack, in which malwares, such as Trojan horse key loggers and spyware, causes data compromises; and DNS-based attack, in which the lookup of host names is altered to send victims to a fraudulent server. A deceptive phishing attack today typically employs generalized “lures.” For example, a phisher disguising himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient.

II. LITERATURE REVIEW

It has been shown that most phishing sites are created by means of a vulnerable web server being re-purposed by a phisher to host a counterfeit website without the knowledge of the server's owner. In this paper, we examine common vulnerabilities which allow these phishing sites to be created and suggest a method for identifying common attack methods, as well as, help inform webmasters and their hosting companies in ways that help them to defend their servers. Our method involves applying a Longest Common Substring algorithm to known phishing URLs, and investigating the results of that string to identify common vulnerabilities, exploits, and attack tools which may be prevalent among those who hack servers for phishing.

III. PROBLEM STATEMENT

A Data mining Approach for Secure Chat in IM is the essential step in growing cyberspace. From the casual consumer using social media, to online merchants growing their business, to physicians supporting their patients { every sector of our society is increasingly dependent upon technology and networked systems. Without sufficient awareness of the risks in cyberspace, however, behavioural decisions and unseen threats can negatively impact the security of the global cyberspace infrastructure and can cause physical damage in the real world. In Instant Messenger, it allow a real time text based and voice based communication over the internet. It provide ancient and immediate communication between the chat mates. But the real fact that there may be phishing persons are there in the cyber space and acting as a trust worthy to us, they can steal our personal information's, bank account details, and other sensitive information's through questionnaires. At present we have deceptive phishing detection system. But the drawback of this system is that it require a N days of transaction in between the chat mate to identify the phishing person. The Main drawback of this system is that user needs to share some sensitive information with his chat mate and there is no method to trace the short cut words.

IV. PROPOSED SYSTEM

The thesis work entitled 'A Data Mining Approach for Secure chat In IM" propose a new algorithm named 'SecureChat Algorithm" that used to detect
misleading phishing attack in Instant Messenger. The proposed work have 4 modules.
1. Collect the raw data.
2. Extract the Transaction data from raw data.
3. Extract frequent patterns from transaction data and store at pattern database(PDB)(Apply Apriory Algorithm)
4. Extract the Phishing words.

IV. CONCLUSION

A data mining approach for SecureChat in IM is implemented. We develop a SecureChat algorithm based on Apriory algorithm is implemented in this work. The experimental results for this work shows that this one is the most suitable algorithm in instant messenger to identify the misleading phishing attacks and it help to identify phishing thefts and other harmful persons in cyber space. And help the sensational and secret data of user became secure. The future for this approach is look green. The future work of this SecureChat include we can add video instant messages in this. Similarly the challenges include are the voice consist of numbers and fractional numbers are the challenging one. Similarly the number consist of double works like 22(two two) and roman words and other symbols are challenges.

V. REFERENCES