ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Study and Analysis of Ant phishing Schemes in Cryptography

Rubeena Jabi, Deepty Dubey, Dr. Punyaban Patel

M.Tech scholar, Dept of Computer Science & Engg..CSIT, Durg (C.G.), India

Associate Professor, Dept of Computer Science & Engg. CSIT, Durg (C.G.), India

Professor, Dept of Computer Science & Engg., CSIT, Durg (C.G.), India

ABSTRACT: Phishing attack is a kind of attack in which a fake web page or website poses itself as a legal one to gain the personal information of user. In Phishing attack, a phisher makes a fake website which exactly looks like an original website. For a user it's ID (user ID) and password is very sensitive information so phisher tries to gain this information in illegal way. They try to access user's personal information through the fake website or web page so it is called phishing attack and phishers use this information for fraud. This paper reviews some anti phishing techniques which are used to detect, predict and prevent the phishing attacks.

KEYWORDS: Phishing, Anti phishing, Visual Cryptography, Authentication.

I. INTRODUCTION

Phishing attacks are popular now days. There are numerous e-banking and e-commerce websites which are used today to fund transactions online. For online transactions security is most important aspect and to provide security various techniques are used.

Phishing is method of attack that is completed by an individual person referred to as a Phishers, and they attack personal data of a user. Various ways are mentioned in this paper to avoid Phishing. For example: Phishers sends the email to the victim "Due to some technical fault SBI database is crashed and urgently need your account related information". The user clicks on the link contained in the email and visits the fake website that exactly looks like a original website. When users enters its personal info like user ID, password and submit this info then it is passed towards the anonymous database which is accessible to Phisher.Four major steps which are involved in a Phishing attack are:

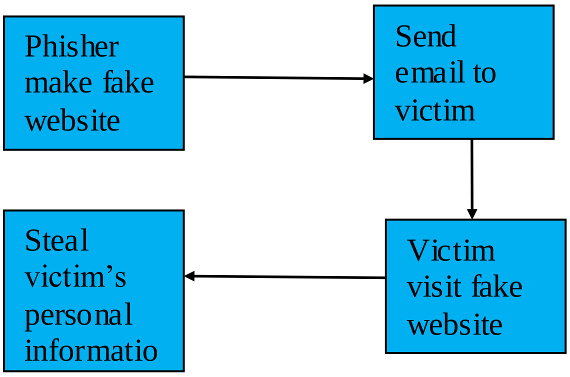
Phisher make fake website
Send email to victim
Victim visit fake website
Steal victim's personal informatio

Figure 1: Phishing attack process

1. A faux web site is made by phishers which is the exact copy of the original web site.

DOI: 10.15680/IJIRCCE.2015. 0311214

2. A link of the phishing website is sent by the phishers via email to their victim.
3. Phishers victim visit web site by the faux link.
4. Phishers steals the private info of users, once users enter their info on fake web site.[3]

Anti phishing approach is detecting and preventing the phishing computer. An anti phishing program tries to verify phishing content contained in computing machine or email. It is sometimes integrated with web browsers. Anti phishing practicality might also be enclosed as an inbuilt capability of some application program. [1]

II .CLASSIFICATION OF PHISHING ATTACKS

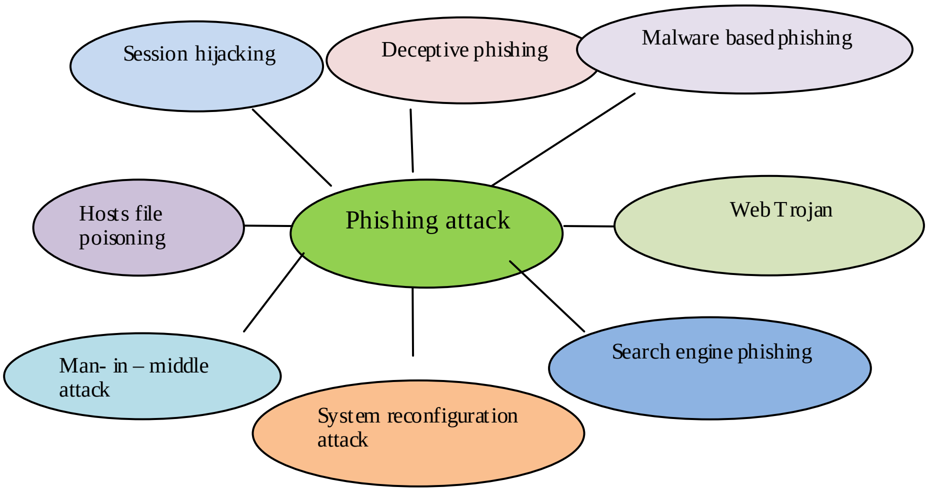

Figure 2: Types of Phishing attack

Deceptive phishing: Bulk emails containing a message are sent to the victim by a phisher. Users are influenced to click on a link and visit the online web site where they enter their personal information which is utilized by attackers for illegal activities.

Malware based phishing: It could be a executable program that contains some kind of malicious script or code running on user's machine which is normally introduced as legal email attachment. Once installed these programs may send information to other parties unknown to the user.

Session hijacking In this kind of phishing attack the activities of users are clearly monitored until a user logged in a faux account.

Web Trojans: In this information of the user is collected through a popup acting as a legitimate profitable deal and the the user is influenced to enter their personal information. Internet Trojans are invisible to user. User's credentials are collected by internet Trojans and transmitted to the phishers.

Hosts file poisoning: Hosts file is an method for resolving names to IP addresses in absence of DNS Services. Hosts file is present by default in every windows system which is used for overriding DNS name resolution. The attacker generally drops a script on users desktop and modifies or poisons the hosts file.Whenever the IP address is accessed by user then he/she is directed to website of attackers choice.

Man –in-the- middle phishing: It's onerous to notice than several alternative varieties of phishing. In these attack hackers sit between the user and additionally the online website or the system. They record the data being entered by the user however the user dealings don't seem to be affected and also the user remains unaware. Later, they sell or use the data which can be master card details, checking account details.

Search engine phishing: Phishers develop e-commerce computing machine with attractive offers. Later these sites are linked completely to different search engines. Once user look for services. These sites fool by various scams like false banking sites that provide lower credit prices or higher interest rates than various banks users by influencing them to enter their info .[2]

III. RELATED WORK

In [4] containing the steps of visual cryptography during which two phases are carried out. First is registration part and second is login part. In registration part the secret key is asked from the user for the secure web site . The server enters the key and user enters the key, then by the each key string organized in a list and image captcha is generated and divided it into two shares using visual cryptography. One key kept with user and another kept with the server. In login part user enter that share of image captcha rather than secret. Once the user's share mix with server's share then original image captcha is revealed. Through the revealed image captcha user decides its phishing website or not. If reveal image captcha is same with the generated captcha of registration part, thus it isn't phishing web site but if it isn't matched then its phishing site. Matched captcha is utilized to log in into web site. It provides authentication between user and server.

In [5] there are RSA rule is utilized for the key writing and secret writing of user id and password. For the authentication user choose a picture and by visual cryptography, it divides that image into shares of 2, one share unbroken with user and another share unbroken with the trusted server, these all process is done in registration phase. In login phase, user uses that image share as a password. In login phase enter user id, select image share and enter public key. The user id, image share is encrypted using the public key and sent to the server, where its is decrypted by using public key or private key. Now server's share and user's share stacked along, an the original image is shown which is then sent to the user's browser. A user use that image captcha for login to verify whether the website is phishing website or not. In this approach used RSA algorithm is employed which has an issue of factoring of large whole number.

In [6] the approach is divided into three sections which are - registration phase, login phase and share recovery phase. In registration phase contain the same process as we discussed previously that the user enter the key and image captcha is displayed. It is divided into 2 shares, one kept with the user and another kept with the server .The share that is kept with the user is used by the user at the time of login. In the login section user browses the share that is kept with his/her. The share sent to server, which is stacked with the server’s share to show the original image captcha and to show the text which is then entered for the login into the web site. Once user lost his share then share recovery part is employed. If the user looses his/her own share then a new request is made for the generation of new share .For latest share sever uses share formula (t, ∞). Server generates a fresh new share on user’s request, then it's downloaded by the user to continue the login process.

In [7] suggests a specific approach that guards the links sent through email. Is is due to fact that the emails that are infected are not previously verifed . This email containing the link of spoofed internet site and this internet site is created by the phishers to realize the info of victim. The spoofed websites are exactly look like a legal website or original website. In this implementation hackers send email to the user and these email link is send to the communication that collect all the data which is then sent to the analyzer which contains the code that analysis the link. Analyser checks the link with the DB containing URLs.Black list DB contains all the links that are blacklisted and white list contains legal links. Analyzer sends result to the logger that stores the connected info and alerts the user. The algorithm provides the distinction between visual link and actual link. This paper compared implemented algorithm and SHA algorithm. The approach provides 94% security than the SHA algorithm that provides 90% security for preventing and detecting phishing attack.

In [8] study has been conducted for two types of phishing namely website and phone based phishing. The phishing web site that precisely appears like a certified web site but for the user it's troublesome to spot the malicious website. If the user looks closely to those sites it can be observed that the pc address of every legal and phishing site are different on the basis of containing domain name where they use IP address in place of domain name and using http .Style id is poor and having spelling mistakes etc.The web site normally sends a link with email to their victim that contain a message like your e-banking account is in danger owing to hacking therefore please login on the given link of website and check the balance, once user enter their identification(user ID, password)it hacked by phishers. In phone phishing experiment the telephonic conversation is used to gain the financial and personal information of the user for the purpose of financial fraud. This paper also includes the characteristic and indicators of phishing website. A mathematical and neural network based model is used that contain the unreal neurons cluster. In this paper the details archived for a phishing wesite are send to the pre-processor that convert it into a format that is understood by a machine. The result of pre-processor the rules that are generated using neural network. . The neural network is trained with the result data. An appropriate weight is also assigned to neural network. If the weights are matching with archived info in DB then the online web site is classified as a phishing web site.

In [9] a model is used that uses rule based approach using Genetic Algorithm., Genetic Algorithm is used for the generation of a rule set that if matched to the rule set in DB (database), the rule set is kept and reported as a link of phishing web site In this system if sent hyperlink matches to the rule, then the website owner is alerted and is informed to action to prevent phishing attack. Genetic algorithm is like computational model that include selection and evolution principles. In genetic algorithm a problem is represented by chromosomes and problem attributes indicating the chromosome position that are encoded like a numbers, bits, characters. During evolution stage the chromosomes set are known as population. Chromosomes fitness is calculated by the function of evaluation. There are mutation and crossover employed in evolution. To generate child offspring. The iteration stops if the criterion of optimisation is met. During this paper genetic formula is employed to generate a rule that offers the distinction between the faux web site and original web site. In this the historical data is collected. The historical data contains fake and original URLs for the testing of preventing and detecting phishing system. For anti-phishing this dataset is utilized. The dataset is analysed for fitness and its results fed to the genetic algorithm. The execution of algorithm is performed and it generated rule sets are stored in database which are then used of prevention and detection of phishing websites.

In [10] the method of data exchange between the server of phishing website and phishers victim is justified in which the phishing website server asks the victim to submit the data and on submission the phishers will grab the information. Once user or victim queries the information to the phishing website server for retrieving information then no data is provided by the phishing website server. In this method phishing is prevented using code word technique.. It contains two phases namely sign-in phase and sign-up phase. In sign-in phase user can register by visiting original website, then after filling of registration form a user ID, password is created. By the code generation technique a novel code is generated by web site (organization) that is saved with the detail of user. The generated code is also sent to user. This code should be remembered by user. In sign -up phase through the email user will get the link of website then user go through that link, fills their user id and any 2 digits as a unique code. If the digit is correct then complete code is displayed by the server on the screen of user if the code matches the code that was generated at the time of registration then the user can be certain that the page is not a phishing page. The code is a combination of user ID character, password character number (it must be of 5 characters) and date and month (it should be greater than or equal to ten, but if it's less than in date & month's sum add 10). In the sign-up phase user will enter any random code in page and if user code is correct then the server will provide complete correct code on user’s screen. This verifies the site is legal.

IV.CONCLUSION

There are some techniques that stop, predict and notice the phishing attack. Phishing attacks have become one of the most talked-about problems as a result of on-line dealings . In some papers authentication is provided to prevent phishing and various algorithms like RSA, Genetic algorithm and Link guard algorithm used to provide the solution for stopping the continuously increasing phishing attacks. So there are several techniques are created that gives the answer for the avoidance of phishing attack.

REFERENCES

1. https://en.m.wikipedia-org/wiki/anti-phishing_software.
2. http://googleweblight.com/?lite_url=http://www.innovateus.net/science/what-are-different-types-phishing-attacks&ei=kz2jtzfh&lc=en-IN&s=1&m=864&ts=1446986267&sig=APONPFlp4Szgua3R6sDB_vANxSvfxUT5MA.
3. Gaurav, Madhuresh Mishra, Anurag Jain "Anti-Phishing Technique: A Review", International journal of engineering research and application, ISSN:2248-9622, vol. 2, Issue 2, Mar-Apr 2012.
4. Divya James and Mintu philip, "A Novel Anti Phishing Framework Based On Visual Cryptography", International journal of distributed and parallel system Vol.3, No.1, January 2012.
5. Sayali Vaidya, Shreya Zarkar, Prof. Achal N. Bharambe, Arifa Tadvi, Tanashree Chavan, " Anti-Phishing Structure Based On Visual Cryptography and RSA algorithm" , International Journal of Engineering Trends and Technology, Volume 20 Number 4 -Fenb 2015.
6. Mangala S Wale, Anita Jadhav, Bharati Kale, Ankita Gupta,"Anti Phishing using (t, n) Visual Cryptography Scheme For Commerce Bank ", International Journal of Emerging Research in Management & Technology, ISSN:2278-9359, Vol-4, Issue 2, February 2015.
7. A. Sarannia, U.R.Padma, "Prevention Model For Phishing Attack In Web Application Using Linkguard Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Issue 1, March 2014.
8. A. Martin, Na.Ba.Anutthamaa, M.Sathyavathy, Marie Manjari Saint Francois, Dr. Prasanna Venkatesan, "A Framework for Predicting Phishing Website Using Neural Network", International Journal of Computer Science Issue, Vol. 8, Issue 2, March 2011.
9. V.Shreeram, M.Suban, P.Shanthi, K.Manjula, "Anti-Phishing Detection of Phishing Attack Using Genetic Algorithm", January 2010.
10. Madhuresh Mishra, Gaurav, Anurag Jain, "A Preventive Anti-Phishing Technique using Code Word", International Journal of Computer Science and Informational Technologies, Vol. 3, 2012.

BIOGRAPHY

Rubeena Jabi, female obtained the B.E. degree in Computer Science & Engineering from Chhattisgarh Institute of Technology, Rajnandgaon, Chhattisgarh, India in 2014. Currently she is pursuing MTech from Chhatrapati Shivaji Institute of Technology, Durg, and Chhattisgarh, India. Her current research interests are in Cryptography and Anti Phishing Techniques etc.

Mrs .Deepty Dubey, female obtained the B.E. degree in Computer Science & Engineering from Shri Shankaracharya College of Engineering & Technology, Bhilai, Chhattisgarh, India, in 2005, the MTech.degree in Computer Science & Engineering, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India., in 2010. She is currently an Associate Professor in Chhatrapati Shivaji Institute of Technology, Durg, and Chhattisgarh, India. Her current research interests are in Cryptography and Cloud Computing.

Dr Punyaban Patel, male, is working as a Professor in the Department of Computer Sc. & Engineering, Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India, since 22nd March 2014 to till date. He obtained Bachelor degree in Electrical Engineering in 1996, Master of Engineering (Computer Sc & Engineering) degree in 1999 and Ph.D (Computer Science) in November 2014. He has been working as a convener, co-convener and session chair of many national & international conferences and workshops. He has been working as a reviewer & editorial board member of many national & international conferences and journals. His specializations are image processing, wireless sensor networks and network security, software engineering, cloud computing.