Preventing Phishing Attacks Using Anti-Phishing Prevention Technique

[1]Gladston Chelliah.A, [2]Aruna.S
[1]M.Tech Student, [2]Assistant Professor
[1,2]Dept of Software Engineering, SRM University, Kattankulathur, Chennai, India-603203
[1]a.gladston@gmail.com, [2]aruna.s@ktr.srmuniv.ac.in

***Abstract*— Phishing attack is a major attack in online banking which is carried through web spoofing, in this paper proposed an Anti-Phishing Prevention Technique namely APPT. which is based on the concept of preventing phishing attacks by using combination of one time random password and encrypted token for user machine identification. The method starts by retrieving the password by SMS or by alternate emails. During login the end user request for the password to the server, in that request it contain of encrypted token. If the end user is valid the password with encrypted token will be send through SMS or EMAIL. By using the login id and OTP password user can access the website. For generating encrypted token, x.509certificate2 uses IP address to generate and it's been encrypted by RSA algorithm.**

***Keywords* - Phishing attacks, Anti phishing, SMS, OTP, Authentication, X.509Certificate2, Encryption, IP and APPT.**

I. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, or denial of a network. Network security involves the authorization of access to data in a network, which is controlled by the network administrators. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.Phishing is a type of attack in which cyber criminals tricks the victims to steal their personal and financial data which has become an organized criminal activity. It mostly uses spoofed e-mail messages that come from legitimate source. Trojans, malware and other malicious software are also used for phishing attacks. The SMTP protocol does not validate or authenticate the sender of the email and therefore anyone can claim to be a valid sender such as from banks, credit card companies and other agencies.

II. TYPES OF PHISHING ATTACKS

Phishing attacks are not limited to spoofed emails only; it includes search engines, man-in-middle, malware, Trojans, instant messaging, social networking sites and etc. Below are some major categories of phishing.

Clone Phishing

It is a type of an attack where a legitimate previously delivered email containing an attachment o-r link has had its content and recipient address taken and used to create a cloned email. This attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. This may claim to be a re-send of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Spear Phishing

It is a technique where specific victim is targeted. The information about the victim is known prior to the attack and the email is sent from the source known by the victim. Due to the nature of the trust on receiving email, this kind of attack has high probability to be successful. An example would be receiving an email from friend, colleague or financial institutions which prompt victim to provide the credentials.

Web Spoofing

Web Spoofing is a security attack that allows an adversary to observe and modify all web pages sent to the user machine, and observe all information entered into forms by the user. Web Spoofing works on both of the major browsers and is not prevented by secure connection. The attacker can observe and modify all web pages and form submissions, even when the browser's "secure connection" indicator is indicated. The user sees no indication that anything is wrong. Once this information is collected, the attacker can use it to buy things with the victims' credit cards, access their bank accounts, and establish false identities. Website spoofing is a growing phenomenon, and puts consumers at considerable risk for identity theft and credit card fraud. The attack is initiated when the victim visits a malicious Web page, or receives a malicious email message (if the victim uses an HTML-enabled email reader).

E-mail spoofing

Email spoofing is email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a various source. Because core SMTP doesn't provide any authentication, it is easy to impersonate and false

emails. Distributors of spam often use spoofing in an attempt to get recipients to open and possibly even respond to their solicitations. Spoofing are been used legitimately. Classic eg., of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency or a "whistle-blower" who fears retaliation. The focus of this paper is to use the above mentioned information to prevent the attacks using APPT.

III. RELATED WORK

The existing system concept the number of phishing attacks are involved. One of the phishing attacks is the spoofing attack. Customers received e-mail notifications that their accounts had been compromised and were being restricted. Message was a hyperlink to what appeared to be an eBay Web page where they could register. The top of the page looked just like eBay's home page and incorporated all the eBay internal links. To register, the customers were told, they had to provide credit card information, ATM personal identification numbers, Social Security number, mother's maiden name and their date of birth. The problem was, eBay hadn't sent the original e-mail, and the Web page didn't belong to eBay -- it was a prime example of phishing. Phishing (sometimes called carding or brand spoofing) uses e-mail messages that purport to come from legitimate businesses that one might have dealings with -- banks such as Citibank; online organizations such as eBay and PayPal; Internet service providers such as MSN, Yahoo and EarthLink; online retailers such as Best Buy; and insurance agencies. This messages may look quite authentic, corporate logos and formats similar to the ones used for legitimate message. They ask for verification of certain information, such as account numbers and passwords for auditing purposes. And because of these e-mails look so official, up to 20% of unsuspecting recipients may respond to them, identity theft and other fraudulent activity against them.

IV. DRAWBACK

In existing system, only One-time password (OTP) mechanism have been used. These mechanism are used for logging on to a network or service using a unique password which can only be used once at that time. This prevents different forms of identity theft by ensuring that a user name/password combination cannot be used a second time. Malicious person with novice computer skills uses tools which are available freely on the internet to conduct a devastating phishing attack and make them less susceptible. Many solutions have been developed to combat the phishing attacks which include both technical and non-technical target areas. The tendency of phishing is expanding and therefore a novel approach to combat the phishing attacks is proposed which is called the Anti-Phishing Prevention Technique.

V. PROPOSED METHODOLOGY

Proposed system uses a new technique called APPT(Anti-Phishing Prevention Technique) which use the combination of one time random password and encrypted token. This technique, users first enter into the one time password retrieve login website. This one time random password will be given to the user through the E-mail / SMS. The encrypted token is used for the authentication process which is stored in the user machine. This token was generated and stored in the user machine. For generating encrypted token x.509 certificate uses IP address to generate and it's been encrypted by RSA algorithm. Once the user enter into access their websites, the token is decrypted and then verify with the database for identifying whether the website accessed by is correct user or not. It provide the effective solution for preventing the Phishing attack from Webpages.

ONE TIME PASSWORD

One-time passwords can be generated in several ways and each one has different benefits in terms of security, convenience, cost and accuracy. A more convenient way for users is to use an OTP token which is a hardware device capable of generating otp. Some of these devices are PIN protected, offers an additional level of security. The user enters the otp with other identity credentials (typically user name and password) and an authentication server validates the login request.

ENCRYPTED TOKEN

If attacker creates a forged website for getting the one time password, he/she will not be able to cause any damage as the site is only used to retrieve the password on mobile or email which is only accessible to the valid user. In order to mitigate against the Cookie attack, the token (cookie) expires in 15 minutes and the cookie is transmitted over encrypted channel and is also encrypted with X.509Certificate2 certificate. By creating a forged site the attacker mislead the victims to provide credentials (OTP). The user credentials are retrieved by the attacker in order to access the sensitive website. Once attacker tries to access the website with the retrieved user credentials, the valid token (cookie) and other machine identification parameters are checked which are not valid and therefore access is denied. The user credentials are immediately set to expire in order to stop the replay attack. Due to expiry time of token and one time password it will be very difficult to launch a successful attack

HYPERTEXT TRANSFER PROTOCOL SECURE

Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially on the Internet. Technically, not a protocol in and of itself; rather it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. The security of HTTP secure is therefore that of the underlying TLS, It uses long term public and secret keys to exchange a short term session key to encrypt the data flow between client and server. Important property in this context is perfect forward secrecy (PFS), so the short term session key cannot be derived from the long term asymmetric secret key; however, PFS is not widely adopted. To guarantee one is talking to the partner one wants to talk X.509 certificates are used. Its a consequence certificate authorities and a public key infrastructure is necessary to verify the relation between the owner of a certificate and the certificate, as well as to generate and administer the validity of certificates. This can be more beneficial than verifying the

identities via a web of trust disclosures made it more widely known that certificate authorities are a weak point from a security standpoint allowing man-in-the-middle attacks.

ATTACK ON WEBSITE

PKI Encrypt function is used to encrypt the token. The cookie is valid only for 15 minutes and contains user machine IP address and other details. The token stored on user machine is used along with the one time password to authenticate with the primary website. If attacker creates a forged website for getting the one time password, he/she will not be able to cause any damage as the site is only used to retrieve the password on mobile or email which is only accessible to the valid user. In order to mitigate against the Cookie attack, the token (cookie) expires in 15minutes and the cookie is transmitted over encrypted channel and is also encrypted with X509Certificate2 certificate. However, if attacker is able to get the user credentials by forged website, it can provide an opportunity for an attacker to flood the victim with SMSs or with email messages and can create lot of nuisance. To prevent such flooding CAPTCHA is used. A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text, but current computer programs can't.

X.509 CERTIFICATE2

A majority of Internet users, either business or social, currently lack the basic ability, knowledge and willingness to effectively use cryptographic applications in a way that can successfully deter imminent threat. The complexity of this task is one of the weaknesses of public key cryptography. A lack of user friendliness and overall usability thus affects solution efficiency. To deal with such issues, software companies have included a bundle of root certificates, which have been audited for security purposes, into user browsers and operating systems. For the sake of user friendliness and interoperability, all web browsers and operating systems currently contain this audited Trusted Root Store of certificate issuing authorities. Certificates issued by these organizations, or their subordinate authorities, are transparently trusted by relying entities. These certificates are automatically deemed as secure and trustworthy, as opposed to those issued by "unknown" issuers, which a relying party is warned not to trust. This interprets into certificates published by all authorities that have not been included in the root store. This approach attempts to make the provision of system security automatic and transparent, and essentially removes from the end user the decision making process about the trustworthiness of web entities. The X.509 standard was primarily designed to support the X.500 structure, but today cases center the web. Many features are of little or no relevance today. The X.509 specification suffers for being over-functional and underspecified and the normative information is spread across many documents from different standardization bodies. Several profiles are developed to solve this, but it introduces interoperability issues and did not fix the problem.

SYSTEM ARCHITECTURE

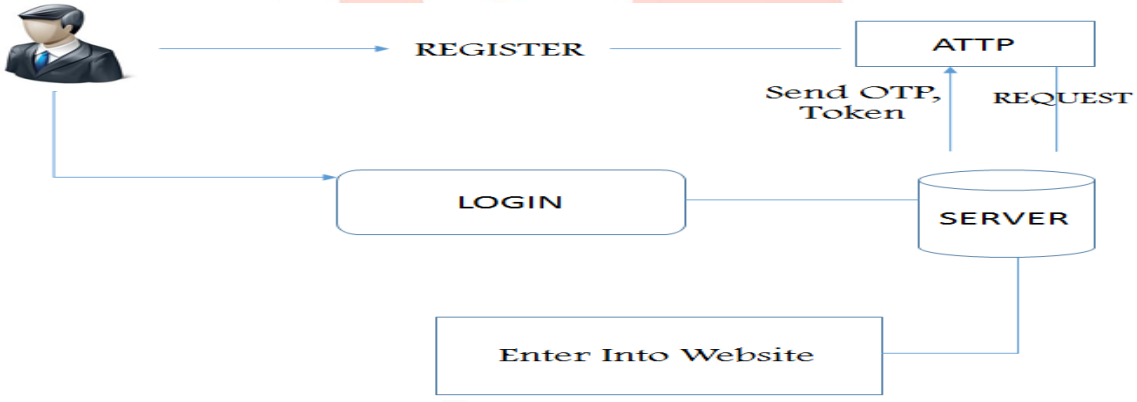

Fig 1

VI. CONCLUSION

To Overcome the problem, proposed a new technique called APPT (Anti-Phishing Prevention Technique) which use the combination of one time random password and encrypted token. In this technique, user first enter into the one time password retrieve login website. This one time random password will be given to the user through the E-mail / SMS. The encrypted token is used for the authentication process which is stored in the user machine. This token was generated and stored in the user machine. For generating encrypted token x509 certificate uses IP address to generate and its been encrypted by RSA algorithm. Once the user enter into access their websites, the token is decrypted and then verify with the database for identifying whether the website accessed by is correct user or not. This provide the effective solution for preventing the Phishing attack from Web Pages.

REFERENCES

[1] Ram Avtar, Bhumica Verma, Ajay Jangra," Data Shield Algorithm (DSA) for Security against Phishing Attacks" ISSN : 2229-6913 Issue Sept 2011, Vol. 4
[2] Mona Ghotaish Alkhozae, Omar Abdullah Batarfi," Phishing Websites Detection based on Phishing Characteristics in the Webpage Source Code" ISSN : OCTOBER 2011
[3] Gaurav, Madhuresh Mishra, Anurag Jain," ANTI-PHISHING TECHNIQUES
[4] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[5] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2372–2379, Jul. 2011.
[6] CSI ONSITE - Phishing techniques, Clone Phishing -Published:March 12, 2012
[7] Clone Phishing - Phishing from Wikipedia, the free encyclopedia, Accessed: 20 February 2013 at 14:42
[8] Cert Carnegie Mellon University, Spoofed Email,March 10, 2012
[9] Princeton University, Department of Computer Science, http://sip.cs.princeton.edu/WebSpoofing Accessed: 09 March 2013
[10] Toni McConnel, Security Sentinel Website Spoofing 101, http://www.iapplianceweb.com/story/oeg20031028s0033 .html Accessed: 09 March 2013