A Survey on Password Stealing Attacks and Its Protecting Mechanism

Venkadesh .S[#1], K.Palanivel[*2]

[#]*Department of Computer Science and Engineering, Pondicherry University, Pondicherry-605014, India*

***Abstract*—People enjoy the convenience of on-line services, however on-line environments might bring several risks. In the on-line communication, the password has a crucial role to secure user personal details. These passwords are taken to be secure and it should be retain in person. The third person might take a password without knowledge of original user and they might do any dishonest activities on the victim's account. The passwords are taken by using anyone of the attack mechanism like Phishing attack, password Stealing Program Attack and etc… The user may use personal details in on-line setting. These personal details should be secured. There are many types of mechanisms available to secure the password and user's information. This paper makes a survey concerning such forms of protection mechanisms and brings awareness to the people.**

***Keywords*—Phishing Attack, Password Stealing Program Attack, Shoulder-Surfing Attack, Password Management Practices**

I. INTRODUCTION

Internet is a system where wide ranges of people are getting connected. In that system, the password is the secure key to protect the user's personal details. The user may use the open network for online banking, passport registration. These online transaction or registration needs a personal details such as bank account number, credit card number and personal details of the user. To protect such type personal information from the online attackers, password is used. It was selected by the user with easily memorable and not guessed by others. For better security, the passwords are changed frequently. The password is insecure due to online attacks like Phishing Attack, Password Stealing Program attack and Shoulder-Surfing attack. Such types of attacks become a threat to the on line community. The review of all such attacks are briefed below

II. PASSWORD STEALING ATTACKS

In the Phishing Attack [1][2], the aggressor attains the user information, by acting as a responsible person. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. For example, a phisher can set up a fake website and then send some emails to potential victims to persuade them to access the fake website. This way, the phisher can easily get a clear-text of the victim's password. Phishing attacks have been proven to be very effective.

In the Password Stealing Program Attack, software codes are used to attain the password. The Key Logger Program and Trojan Redirectors are example for password stealing program.

In the Key Logger [3], the software that will be installed on the system and that software records all the activities done on the key board are recorded. Whenever the user trusts the third party system, that software may be installed on the system. This type of software not displayed on the task manager. From the recorded key, the aggressor gets the password within a short time and less effort. The Trojan Redirectors uses to redirect the network into aggressor preferred location.

In Shoulder-Surfing Attack, the camera is fixed to monitor all the activities of the user. For this purpose, the hidden cameras are normally used by the aggressor. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they:

- Fill out a form
- Enter their PIN at an automated teller machine or a POS terminal
- Use a telephone card at a public payphone
- Enter a password at a cyber-cafe, public and university libraries, or airport kiosks
- Enter a code for a rented locker in a public place such as a swimming pool or airport

Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand. The aggressor may use any one of the attacking mechanism for obtaining the password without knowledge of the user.

The aggressor does any fraudulent activities using the password and in banking transaction they may transfer user's amount to their account. It may injure the user's personal life. To avoid password stealing, choose the password as a very strong one, and it should be changed frequently and should be easily memorable by the user. One time password mechanism, virtual keypad, graphical password and biometric based authentications are suggested as a remedial measure to overcome the above mentioned attacks.

III. GOOD PASSWORD MANAGEMENT PRACTICES

Password policies are generally known and often include advice on proper password management [4][5] with the most common including:

- Never share login data for a personal computer account, as such sharing will result in reduced security through accidental or international further sharing of login data.
- Never use identical password for over one account, to reduce the risk of anybody password being compromised.
- Never reveal a password to anyone, together with people that claim to be from customer service or

security, to prevent social engineering tries to steal a password.

- Never write down a password, since written passwords could also be unknowingly unconcealed to others.
- Never communicate a password via email or instant messaging, and only rarely via telephone, as these communication media may be compromised.

Always logout before leaving a computer unattended, that prevents accidental access to sensitive information on one's computer that could lead on to compromise of one's password.

Change passwords whenever there is suspicion they may have been compromised, reducing the risk of exposure of confidential information.

The general goals of password management policies are to maintain the integrity, privacy and efficacy of password-based security system. Among the most critical is the careful selection of a password.

IV. CHOOSING AN APPROPRIATE PASSWORD

By following guidelines for selection of a password, the risk of a password being compromised through guessing or cracking is greatly reduced [4][5]. The level of password strength required depends, in part, on how easy it is for an attacker to submit multiple guesses.

While some systems limit the number of times that a user can enter an incorrect password before a delay is imposed or the account is frozen, other systems allow virtually unlimited login attempts. An attacker can try passwords by guessing commonly used ones based on a user's name and other personal information. Common guidelines for appropriate password selection are:

- Make passwords as long as possible, as longer passwords are harder to guess.
- Use as many different characters, numbers and symbols as possible to create it more durable to guess.
- Do not use common dictionary words, as they are easier to guess than random characters.
- Do not use personal information, because it is definitely guessed.
- Change passwords on a regular basis to minimize the danger of compromised passwords.

While following such guidelines can reduce the chance that a password will be guessed and therefore compromised, a stronger justification for following these practices is to reduce the change that password cracking software will compromise a password.

V. LITERATURE SURVEY

In this survey, it makes the attention to the user for shielding their account (i.e. password). Here password protective mechanisms are reviewed. This section concerns the papers that are written by various authors with their better outcome of knowledge.

A. LOGIN INTO INTERNET CAFE WITHOUT WORRYING ABOUT KEYLOGGER

The roaming user might use the internet cafe for browsing. In that system the key logger program may be installed on the system. The author [8] of the system defines the protection against key logger program. In this mechanism, the user types a password with an additional character. The software stores all the keys typed on the keyboard. If we have a tendency to type the additional characters then the aggressor got confuses to get the password. For instance, the user password is "trustme", once the user enters it on the untrusted system they type correct password on password field and type random characters on the floor. These random characters and passwords are typed in mixed. The key logger didn't recognize that characters are typed on the password field and which are all typed on the floor. The result of keylogger is "fftrtewriuksllat34f3plkutm90ehy" for "trustme" password. The advantage of this technique is to secure the password from the keylogger software. The disadvantage of this technique is that Shoulder-Surfing Attack is possible.

B. GRAPHICAL USER AUTHENTICATION

The graphical password schemes are better than the character passwords. The author of the system [11] explains, this type authentication is complex to hack. It allows Convex Hull Click (CHC) to secure the password. This paper allows a user to select the image from image set. The user may select more number of images that is equal to the number of password characters. The advantage of this system is to protect the password against Shoulder-Surfing Attack. The disadvantage of this system is huge memory is required to store the images and same images are repeated more time.

C. AUTHENTICATE THE USER WITHOUT IDENTITIES

In this paper [6], the user does not have any identity for authentication. Here each user has their address and pseudonyms. The address and the pseudonyms have the three conditions that are 1.Not Necessarily Fixed 2.Unique 3.Approved by a Central Authority. Here the registration table was maintained, in that table, the user update their address every T seconds. The pseudonyms are also updated at the regular interval time.

The central authority is responsible for maintain the registration table. The new address is allocated for new user that is not available on the registration table. It was maintained by the central authority. The advantage of this mechanism is, communications are simple and provide better security without using any identity. The disadvantages of this mechanism are, communication structure cost is high, frequent update mechanism and, message loss and Denial-of-Service attacks are possible.

D. AUTHENTICATION IN SOCIAL NETWORK

Now-a-days the usage of the Online Social Networks (OSN) [7] is increased. In OSN, the user begins contacting without meeting each other. It may cause vulnerability against security. Here the attacking mechanism is known as Impersonation Attack. The aggressor creates an account using another person's details and makes communication with each other. In this mechanism, the public key was generated between the two users and it will be exchanged in secure channel (i.e. mobile channel or direct meeting). These public keys are stored on the third-party; whenever the user makes a

communication they request a key from the third-party. The advantage of this mechanism is secure in OSN because of third-party authority.

E. ONE TIME PASSWORD

The one time password [9] is valid for one time login and it protects the password against replay attack. The password is based on three approaches that are 1.Time Synchronization 2.Depending on the previous password and 3.Depending on the Challenge. The advantage is, it is a dynamic password.

F. VIRTUAL PASSWORD MECHANISM

Another secure mechanism is virtual password mechanism [12]. The virtual password is similar to the one time password it was generated by using the secret little function. The secret little functions are kept as secret and, it uses two input values that are fixed alphanumeric value and random number. The random was displayed by the server system.

In this mechanism, the user name, alphanumeric password, constant value for virtual password creation and secret little function. That are kept as secret on the server. During the login time, the user manually calculates the virtual password using registered information, at the same time the server also calculate password. Both the values are equal then server allows user to access information. The advantage of this mechanism is, it protect the password against Trojan Program Attack, Phishing Attack and Shoulder-Surfing Attack. It is valid at one time. The disadvantage of this mechanism is difficult to remember all the registered values. It needs another storage media to store all the values.

G. PASSWORD–BASED AUTHENTICATION IN TLS

A strong password-based authentication used in TLS [6]. It uses the Third-party group Diffie-Hellman protocol. The open source software is popularly known between users of the computer. The user of the open source software can read, redistribute, and modify the source code for a piece of software, and release new version. The Diffie-Hellman protocol is used for exchanging the key between the two parties. The secure way for the user to identify him is to tie his authentication to the TLS secure channel using some variant of the strong Password-based Authenticated Key Exchange (PAKE) primitive. A PAKE is a key exchange with one or two flows encrypted using the password as a common symmetric key. Instantiations for the encryption primitive were either a password-keyed symmetric cipher or a mask generation function computed as the product of the message with the hash of a password. The simple open key exchange cipher suites named as 3-party group Simple Open Key Exchange (TLS-3SOKE), Since they run between two players (client and server) where the TLS server consists of two parties. This mechanism describes proficient and provably secure cipher suites for password-based authentication in the TLS protocol. It is first attempts at drafting a provably secure PAKE cipher suites for TLS that are believed that they are not violate existing patents.

The advantage of this authentication methods are, Diffie-Hellman protocol is used for exchange the secret key since it make secure transmission. It is symmetric communication mode. It supports open source environment security. The disadvantage of this authentication mechanism is difficult to implement key exchange mechanism. Since Diffie-Hellman protocol is used it is vulnerable to Man in Middle attack.

H. SPINS

In sensor networks, security is a central issue; the researchers only focus on sensor networks, feasible and usage of sensor networks. SPINS[10] is a security protocol for sensor networks. It has two secure building blocks such as SNEP and µTESLA. SNEP protocol provides Data confidentiality, two-party data authentication, and data freshness. Broadcast data authentication is important in sensor networks. µTESLA protocol provides authenticated broadcast for strictly resource-controlled environments. SPINS explores security challenges in sensor networks and design and developing µTESLA and SNEP. Using these building blocks protocol design and develop the authenticated routing protocol. In sensor networks security is impossible because it has some challenges such as imperfect power processing, bandwidth, storage and energy. The main challenge is broadcast authentication. The goal of SPINS is to provide security mechanism for different sensor nodes. It needs the following requirements.

1) REQUIREMENTS OF SPINS

Data confidentiality makes sure sensor readings to nearest network. For protecting the secret data, this mechanism implements secure channels between the base station and communication nodes. In standard network, encryption methods are used to provide data confidentiality.

Data authentication is important for administrative purpose and to avoid the vulnerability access. In two way communication the identity of a source and destination are proved by using authentication mechanism. Basically, symmetric key authentication is used in network communication but while sharing of secret key and MAC may be hacked by unauthorized user. Hence develop a symmetric mechanism, that includes asymmetry with delayed key disclosure and one-way function key chains.

Data integrity is achieved in sensor networks by using data authentication. It is the strongest property and ensures the received data are not get modified.

Data freshness is used to guarantee the data that was transmitted recently without any modification. Two types of freshness are strong and weak. Strong freshness provides a total order on a request-response pair, and allows for delay estimation. It is used for time synchronization. Weak freshness provides partial message ordering, but carries no delay information. It is used in sensor networks.

The SNEP have following advantages,

- It has low communication overhead since it only adds 8 bytes per message.
- Many cryptographic protocols use a counter. Transmitting of the counter value can be avoided by keeping state at both end points.
- SNEP achieves even semantic security, a strong security property which prevents eavesdroppers from inferring the message content from the encrypted message.

- It is considered as a simple and efficient protocol which provides data authentication, replay protection, and weak message freshness.

µTESLA has been developed to solve the following problem,

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for epoch.
- It is expensive to store a one-way key chain in a sensor node. µTESLA restricts the number of authenticated senders.

The advantage of this mechanism is, computation cost of symmetric cryptography is low and Communication costs are low. The disadvantage of this mechanism is availability of memory and Buffering restrictions limit the effective bandwidth of authenticated broadcast.

VI. CONCLUSION

This survey paper gives knowledge regarding the password stealing activities and protection mechanism available on the online network communication. The protection of passwords is a vital activity in an on-line system. It avoids vulnerable activities and anonymity loss of the individual user. In future we attempt to implement a new mechanism from this survey that improves security against all kinds of attack.

REFERENCES

[1] [Online].Available:http://en.wikipedia.org/wiki/Phishing

[2] Anti-Phishing Working Group. [Online]. Available:http://www.antiphishing.org

[3] [Online].Available: http://en.wikipedia.org/wiki/Key${-}$logger

[4] S. Furnell, “An assessment of website password practices,” Computers & Security, 26(7-8), December 2007, pp. 445-451.

[5] Microsoft whitepaper, “Strong passwords: How to create and use them,” 2006, Accessed Jan. 31, 2008,Available at: http://www.microsoft.com/protect/yourself/password/create.mspx.

[6] Abdalla.M, Bresson.E, Chevassut.O, Moller.B and Pointcheval.D,“Strong Password-Based Authentication in TLS using the Three-Party Group Diffie-Hellman Protocol”, Int.J.Security Netw., vol. 2, nos.3-4,pp. 284-296, 2007.

[7] Fathy. A, ElBatt.T and Youssef.M “A Source Authentication Scheme Using Network coding”, Int.J.Security Netw., vol. 6, nos.2-3, pp.123-135, 2011.

[8] Herley.C and Florencio.D, “How to login from an internet café without worrying about keyloggers”, in proc. SOUPS, 2006.

[9] One-Time Password [Online]. Available:http://en.wikipedia.org/wiki/One-time−password.

[10] Perrig.A, Szewczyk.R, Tygar.J.D, Wen.V and Culler D.E,”SPINS: Security Protocols for Sensor Networks”,Wirel.Netw., vol. 6, no. 5, pp. 521-534, 2002.

[11] Widenbeck.S, Waters.J, Sobrado.L, and Birget.J, ”Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme”, in Proc. Working Conf.Adv. Vis.Interfaces.

[12] Yang Xiao, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky, ” Differentiated Virtual Passwords, Secret LittleFunctions, and Codebooks for Protecting Users From Password Theft” Systems Journal, IEEE