ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

REVIEW OF PASSWORD PROTECTING MECHANISM

Ms.K.Banu priya[†] and Dr.P.Venkateswari[††]

[†]M.E. (CSE) Second Year, Erode Sengunthar Engineering College, Erode,Tamilnadu,India
[††]Head of Department, Erode Sengunthar Engineering College, Erode, Tamilnadu,India

ABSTRACT

In the online communication, the password has an important role to secure user personal details. These passwords are taken to be secure and it must be retain personally. The third person may take a password without knowledge of original user and they may do any fraudulent activities on the victim's account. The passwords can be stolen by using any one of the attack mechanism such as Phishing attack, Password Stealing Program Attack and etc… The user may use personal details in online environment. These personal details must be secured. There are many types of mechanisms are available to secure the password and user's data. This paper makes a survey about such types of protection mechanism and makes awareness to the people.

Keywords:- Phishing Attack, Password Stealing Program Attack, Shoulder-Surfing Attack

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

ATTACKING MECHANISM

In the **Phishing Attack** [1][2], the aggressor attains the user information, by acting as a responsible person.

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 trust 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 cybercafe, 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 very strong and it would be changed frequently and it should be easily memorable by the user. It was the basic repurement to choose the password.

One time password mechanism, virtual keypad, graphical password and biometric based authentications are suggested as a redimidal measure to overcome the above mentioned attacks.

LITERATURE SURVEY

In this review makes the attention to the user for protecting their account (i.e. password). Here password protecting mechanisms and authentication mechanisms are reviewed. In this section is survey about the papers that are written by various authors with their better outcome of knowledge.

LOGIN INTO INTERNET CAFE WITHOUT WORRYING ABOUT KEYLOGGER

The roaming user may use the internet cafe for browsing. In that system the key logger program may be installed on that system. The author [7] of the system defines the security against key logger program. In this mechanism, the user types a password with an extra character. The software stores all the keys typed on the keyboard. If we type the extra characters then the aggressor got confuses to obtain the password.

For example, the user password is "trustme", when 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 know which 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 system is to secure the password from the Key Logger software. The disadvantage of this system is Shoulder-Surfing Attack is possible.

GRAPHICAL USER AUTHENTICATION

The graphical password schemes are better than the character passwords. The author of the system [14] 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.

AUTHENTICATE THE USER WITHOUT IDENTITIES

In this paper [5], the user didn't 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 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.

AUTHENTICATION IN SOCIAL NETWORK

Now-a-days the usage of the Online Social Networks (OSN) [17] is increased. In that OSN, the user begin contacts without meet each other. It may cause vulnerability against security. Here the attacking mechanism is known as Impersonation Attack.

The aggressor creates an account using another personal details and make 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.

ONE TIME PASSWORD

The one time password [11] is valid for one time login and it protect the password against replay attack. The password is based on three approaches that are 1.Time Synchronization 2.Depend on the previous password and 3.Depend on the Challenge. The advantage is, it is a dynamic password.

VIRTUAL PASSWORD MECHANISM

Another secure mechanism is virtual password mechanism [14][15][16]. 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.

PASSWORD – BASED AUTHENTICATION IN TLS

A strong password-based authentication used in TLS. It uses the Third-party group Diffie-Hellman protocol [4]. 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 ciphersuites 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.

SPINS

In sensor networks, security is a central issue; the researchers are only focus on sensor network feasible and usage of sensor networks. SPINS[13] is a security protocols 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.

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.

SiB

Seeing is Believing (SiB) use the camera phones for human-verifiable authentication. The cameras are attached with the system for authentication. As camera-equipped mobile phones rapidly approach ubiquity, a platform for secure human verifiable electronic communication becomes available.

Today's mobile phones increasingly have Internet access and come equipped with cameras, high-quality displays, and short-range Bluetooth wireless radios. They are powerful enough to perform public key cryptographic operations in fewer than one second. This constitutes a unique and powerful platform for security applications that can be deployed quickly and easily to millions of users.

Recent improvements in the image quality and processing power attainable on camera-phones have enabled the development of effective barcode-reading software. In SiB, one device uses its camera to take a snapshot of a barcode encoding cryptographic material. This barcode can contain a commitment to the creating device's public key material, or an array of barcodes can be used to send key material directly. Barcodes can be pre-configured and printed on labels attached to devices, or they can be generated on-demand and shown on a device's display.

Using camera-equipped mobile phones to recognize bar codes. Several projects exist that seek to allow camera-equipped mobile phones to interact with physical objects through the use of 2D barcodes.

The concepts of SiB can be applied in different ways to devices with different capabilities, each equipped with either a camera and display, a camera only, a display only, or neither. In some cases, these device configurations impose some limitations on the strength of the achievable security properties.

The Trusted Computing Group (TCG) specifies a Trusted Platform Module (TPM) that can be used to enhance the security of many computing platforms. The TPM is a chip connected to a computer's processor, with no other I/O capabilities.

One challenge in designing systems which incorporate a TPM is how a user can communicate securely with the TPM, since the user only has a keyboard and display to communicate with the TPM, with untrusted operating system software in between.

The advantages of this mechanisms are provides better security against unauthorized attack and barcodes are unique for each user. The disadvantages of this mechanism are extra device charges are high and limited authentications only allowed.

SELF-ENCRYPTION PROTOCOL

A self-encryption authentication protocol[8] is developed for teleconference service. The main advantage of this mechanism is to identity anonymity, one-time Pseudonym Identity (PID) renewal and location intractability**.** Identity anonymity is achieved by concealing the real identity of a mobile conferee in a prearranged PID. One-time PID Renewal mechanism, in which the mobile conferee's PID is frequently updated and it was communicated with the network centre. This mechanism introduced to offer location intractability.

A mobile conference is a synchronous communication, in which the remote users are connected at the central node. The central node is known as Network Center (NC). A simple authentication protocol uses **Secret Splitting**.

Secret Splitting is a type of information-hidden technique, in which a message is divided into several components. The original message can be reconstructed if and only if the number of components gathered is equal or greater than the preset threshold.

The self-encryption authentication protocol decomposes the original identity into PID and random number. The PID is used for transmission and the random number was only known by the NC. In addition, to prevent the mobility of a particular mobile conferee from being traced, the PID is renewed frequently using proposed One-time PID Renewal mechanism. The conversation privacy is also guaranteed when participants join or leave the on-going teleconference meeting by properly renewing and re-distributing the conference session key.

The advantages of this mechanism are Provide better security in teleconference service security and secret splitting is used to hide information. The disadvantages of this mechanism is Man- in-middle attack is possible.

SANC

SANC: Source Authentication Network Coding [6] is for providing advantage of network code and probable transactions with the widely accepted throughput benefits, particularly in multicast

scenarios. Network coding has shown higher throughput than conventional multicast theoretically and experimentally. In this mechanism, the authentication information is implant with the network coding Global Encoding Vector (GEV). This is achieved by using mapping function that provides structure for global encoding vector for receiver side authentication. The differences between the source packet and the destination packets are used for security analysis.

This SANC mechanism mainly focus the following,

- It influence network coding packet mixing, beside by homomorphic encryption, to authenticate source nodes.
- It proposes a scheme for enclosing the information into the network coding GEV using a simple authentication mapping function with least collision on the decoding probability.

It shows the efficiency and effectiveness of the proposed scheme by carrying out exhaustive simulations of this approach.

Homomorphic encryption is one type of encryption where the arithmetic operations that takes place on cipher text is reflected on the plain text. This mechanism has the following properties,

- **Addition Property:** The summation of two cipher text is equivalent to the encryption of their addition, that is,

$$E(A) + E(B) = E(A + B).$$

- **Multiplication by Scalar Property:** The multiplication of a cipher text by a scalar value is equivalent to the encryption of the text multiplied by a scalar value, that is,

$$\alpha E(A) = E(\alpha A).$$

This mechanism is suitable only in small networks. For large networks it has a problem known as finite field wrapping problem. This problem is attributed to the fact that elements from a finite field reach their maximum value after a certain number of hops and, hence, tend to wrap around. It is the scalability challenge in SANC mechanism.

The advantages of this mechanism are, provides secure transaction in multicast environment and Homomorphic encryption is used for encryption method. The main limitation is to protect the bit pattern, in the GEV, throughout the packet mixing process at intermediate nodes. Bit pattern is used in mapping function. The mapping functions are very complex. Privacy protection is not taken care by SANC.

These reviewed mechanisms are describing the difficulties available in online environment to secure the user information. The authentication mechanisms are used to allow particular user with acceptable identity.

CONCLUSION

The survey of this paper makes knowledge about the password stealing activities and protection mechanism available on the online network communication. The protection of the password is the important activity in online system. It avoids vulnerability activities and anonymity loss of the individual user. In future we try to implement new mechanism from this survey that makes better 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] [Online].Available: http://en.wikipedia.org/wiki/shoulder surfing
[5] 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.
[6] Choi.T and Acharya.H.B, "Is That You?Authentication in a Network without Identities" ,Int.J.Security Netw., vol. 6, no. 4,pp.181-190, 2011.
[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] Jiang.Y, Lin.C and Shen.X, "A self-encryption authentication protocol for teleconference services ", Int.J.Security Netw., vol. 4, no.3-4,pp.198-205,2006.
[10] Koetter.R and Medard.M, "An Algebraic Approach to Network Coding, IEEE/ACM Transactions on Networking", vol. 11, no. 5, pp. 782- 795, Oct. 2003.
[11] McCune.J.M, Perrig. A and Reiter. M.K, "Seeing-Is-Believing:Using Camera Phones for Human-Verifiable Authentication", Int.J.Security Netw., vol. 4,nos. 1-2,pp.43-56, 2009.
[12] *One-Time Password* [Online]. Available:http://en.wikipedia.org/wiki/One-time−password.
[13] [Online].Available: http://obr.typepad.com/financial innovations/2005/11/ing−direct−adds.html
[14] 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.
[15] 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.
[16] Yang Xiao, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky, " Differentiated Virtual Passwords, Secret LittleFunctions, and Codebooks for Protecting Users From Password Theft" in *Proc. IEEE ICC*,Feb 2012.
[17] Y. Xiao, C.-C. Li, M. Lei, and S. V. Vrbsky, "Secret little functions andcodebook for protecting users from password theft," in *Proc. IEEE ICC*,May 2008, pp. 1525–1529.M. Lei, Y. Xiao, S. V. Vrbsky, and C.-C. Li, "Virtual password using random linear functions for on-line services, ATMs, and pervasive computing," *Comput. Commun. J. Elsevier*, vol. 31, no. 18, pp. 4367–4375, Dec. 2008.
[18] X. Zhao, L. Li, and G. Xue, "Authenticating strangers in online social networks," *Int. J. Security Netw.*, vol. 6, no. 4, pp. 237–238, 2011.