A New Conditional Key based Authentication for Secure Shopping

Dr. A.V. Senthil Kumar [1], J. Thiyagarajan[2]
Head and Associate Professor, Department of Computer Applications, Hindusthan College of arts and Science, Coimbatore, Tamil Nadu, India[1]
PG Student, Department of Computer Applications, Hindusthan College of arts and Science, Coimbatore, Tamil Nadu, India[2]

Abstract – This project initiates the study of two specific security threats on online shopping based password authentication in shopping sites. SMS-based password authentication is one of the most commonly used security mechanisms to determine the identity of a remote client, who must hold a valid phone number and the corresponding password to carry out a successful authentication with the server. The authentication is usually integrated with a key establishment protocol and yields SMS-based password-authenticated key agreement. The project creates a new authentication scheme with conditional key verification. In shopping sites, user needs to enter their account details for the transaction, but the information can be stealing by the adversaries. In this case the proposed system provides a new authentication scheme against those password and information stealing attacks. The system uses SMS based authentication, here the user need not enter their sensitive and personal information in unknown host.

Index Terms – Key, Authentication, Secure Shopping, SMS.

1. INTRODUCTION

Remote authentication is of great importance to protect a networked server against malicious remote users in shopping sites. Most early schemes are solely based on password authentication. To strengthen security, SMS-based password authentication has become one of the most common authentication mechanisms. A SMS-based password authentication scheme involves a server and a user, and typically consists of three phases. The first phase is called the registration phase, where the users issues a unique mobile number to the server. The details contain the personal information about the user, which will be used later for the authentication. In this phase, an initial password for the user is also determined (chosen by the user or by the server). Once the registration phase is completed, the user is able to access the server in the log-in phase, which can be carried out as many times as needed.

Since exist of the internet society the human life is divided in real world and virtual world. Large number of the people spends their life in virtual world and many people have misused the internet society [1]. Cyber-crime and cyber-attacks increase exponentially nowadays. To prevent the people and their data from those kinds of attacks, ethical rules have to be taken for virtual world according to real life. Additionally new security actions are required to protect private life in virtual world. This chapter introduces a survey of cyber-attacks and its detection. Cyber-attacks are actions that attempt to bypass security mechanisms of computer systems. Cyber-attack detection has been defined as "the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges.

Eavesdropping Attacks [2]: An attacker taps the information that goes on the wire and uses it for future purpose. It is a kind of replay attack. It may be network eavesdropping or offline eavesdropping. MITM is a kind of eavesdropping attack.

Countermeasure: The message can be encrypted using standard encryption `techniques such as AES 128 bit or RC4 stream cipher. SSL helps to provide the encrypted communication channel. Further Central Authentication Service (CAS), a single sign-on protocol can be used along with SSL. Network eavesdropping can be avoided by using very strong authentication protocols such as Kerberos as it never transmits the password across the network.

Man-in-the-Middle Attack: MITM is a kind of eavesdropper attack. An attacker comes in between two hosts, i.e. customer and the website (bank or shopping), and all the communication between them goes only through the attacker. So he impersonates both the parties to one another and may copy, alter or delete a portion of the data traffic between them i.e. attack on mutual authentication. MITM may be used to simply monitor the data and may not be reused also. It may be a passive attack or active attack.

Countermeasure: Brute Force Attack and MITM can be solved by SSL. Using SSL, the traffic is encrypted so it can't be tampered or modified by MITM or brute force attack [3]. There are ways to fake connections (primarily by proxy servers) so that the user believes they have an SSL connection to a site but they may be navigated to a non-SSL site. The actual SSL connection will be from the proxy server to the website and not from the user to the website. The ultimate result is that

the proxy may be able to read user's information. Moreover, the parties at both ends can be authenticated mutually to prevent MITM attacks. This mutual trust can be obtained by a certification authority. HMAC (Hashed message authentication code) can be used. If there is any alteration in the data by the attacker, then the computation of HMAC on receiving end may fail.

Replay Attacks: An attacker copies the message, data, user credentials or key information transmitted between two hosts and then uses it for a nefarious purpose [4]. Replay attack is a specific category of MITM attack. This attack is absolutely intentional. Masquerading or impersonation is a type of attack in which the attacker impersonates a user. Whereas in replay attack, the attacker just sends the same data packet to some user assuming to have the same effect. For e.g. when the user says "no" for a file deletion, the attacker captures it and modifies it as "yes". In fact, replay attack is a specific type of masquerading attack. Thus, replay attack can be used to impersonate a user or entity. Also, sometimes, replay attack may not relate to impersonation at all. Like password, even a cookie can be replayed. The attacker may capture the cookie sent to the user and replay it for gaining unauthorized access with false identities.

Countermeasure: Timestamp can be utilized along with security tokens. OTP can be applied. The nonce can be generated. SSL helps to eliminate replay attacks and is essential in case of cookie replay attack. Hence both the parties exchange some random number and use it for all encrypted transactions between them. By setting the cookie timeout value for a short period, the replay attack can be prevented as it gives only a short time for the attacker to play.

Phishing Attacks: The phishing is a type of an attack in which the attacker impersonates the website, email or phone call for nefarious purpose. It is an intentional theft of user credentials [5]. Phishing attacks are usually attempted to steal credit card information, email, password, or any other sensitive information. The attacker creates a website similar to the original website, such as banking website. DNS cache poisoning enables the user to navigate to the attacker's fake website automatically.

Countermeasure: Digital certificates can be used to avoid phishing attacks. Unsolicited emails should not be attended such as emails from banks requesting for username and password. When an URL is misspelled, it may lead to a phishing attack. Click the unknown hyperlinks in the emails also leads to a phishing attack. The email attachments should not be downloaded unless it is from reliable sources. The padlock icon in the URL bar can be clicked to verify the identity of the website. The HTTPS protocol must be used in the URL instead of normal HTTP.

Brute Force Attacks: It is generally difficult to protect against brute force attack. Hence, brute force attack attempts on a huge number of key combinations on trial-and-error basis [6]. Unlike dictionary attack, it targets even on unknown combinations. Passwords can be broken up easily when the key size is small. Brute Force attack consumes time considerably when the key size is large and the password chosen is strong. A computer program or ready-made software is commonly used for implementing brute force attack. The computer configuration must be high to perform a brute force attack much faster and efficiently. It starts from the single digit password to the multiple character password and tries out all the keys available on a keyboard.

Countermeasure: Brute force attack does not work for online services. Because when multiple attempts from a particular IP address is tracked, that particular IP will be blocked by the administrator or that account that is used by an attacker may be blocked. Tarpitting is another techniques used for reducing the speed of an attacker. It creates a delay in authenticating which helps to reduce the number of attacks per minute. This method will exhaust the server resources. Instead, honeypot mechanism can be implemented when the number of consecutive login attempts was failed. Today, most of the online websites, especially banking and financial websites deploy CAPTCHA (Completely Automated Public Turing test) mechanism for avoiding brute force attacks [7]. CAPTCHA is a computer program which generates images randomly and invites the user to enter the same in the given textbox. Based on the input given, it determines the user is a human being or streaming bot. Human beings have the ability to read and understand any distorted text, whereas computers cannot read or understand.

Dictionary Attack: A dictionary attack is an attack attempted on authentication data by trying all the possible words in a dictionary. Dictionary attack attempts only to a targeted list of weak passwords or attempts on a limited number of key combinations that has a high possibility of getting succeed [8]. Hence the dictionary attack is always faster than brute-force attack. A dictionary attack is easy when the password chosen is short, weak or common and it becomes very complicated and does not give result when any special characters are included as passwords. Dictionary attack is the first choice of the attacker before trying the brute-force attack. Some examples of software used for dictionary attack are Metasploit, Passcape, Brutus, Cain & Abel, etc.

Countermeasure: Dictionary attack can be avoided by selecting a strong password. A strong password is the one created with the combination of alphabets both uppercase and lower case, numbers, and special characters. It must not be a word in a dictionary. Broadly speaking, the plaintext or encrypted passwords are not used on the database system. Because compromising a key would open the door for the

hacker to see the entire password in a database. Hence, password can be hashed combined with a salt value and then it can be stored on a database.

Insider Attack: The Insider attack is a type of malicious attack attempted intentionally within an organization [9]. The employees of the organization bestowed with more power and knowledge about the environment initiates such an attack. The system administrators or network managers steal the authentication data or exchange keys.

Countermeasure: Intrusion Detection System (IDS) helps to mitigate such attacks. Access control mechanism, monitoring and logging must be strictly maintained.

Keylogger Attack: Keylogger is a computer program or software that captures the keystrokes of the user for stealing his password. Keylogger need not be software always. It can be a hardware device also [10]. Aside from stealing passwords, it can be used for enterprise security, parental control, etc.

Countermeasure: The keylogger attack can be avoided by using the virtual keyboard in which the position of characters will change randomly. OTP (one-time password) can be used to avoid keylogger attacks. For Instance, when Gmail account is configured with two-step authentication, OTP sent to the mobile is required to login. OTP can be obtained in special devices such as SafeNet eToken NG-OTP, RSA SecurID tokens. Antilogger such as Zemana, sandboxie, keyscrambler can be used to avoid keylogger attacks.

2. PROBLEM DEFINITION

Information accessing and sharing is an important functionality in the online applications. In online applications, users often select weak passwords and reuse the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, she /he will exploit it to gain access to more websites. Second, typing passwords, account numbers and account pin numbers into untrusted computers suffers password and account thief threat. An adversary can launch several password stealing attacks to snatch passwords, users account numbers and pin numbers, such as phishing, key loggers and malware. Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. An adversary compromises one password; Humans are not experts in memorizing text strings. Easy-to-remember passwords, Even if they know the passwords might be unsafe Adversary can launch several password stealing attacks to snatch passwords.

Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. Several existing techniques used smart card based data authentication. But the problem in smart card based authentication need some hardware support. However, password-based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. This attack is referred to as the password reuse attack. Despite the assistance of these two technologies—graphical password and password management tool—the user authentication system still suffers from some considerable drawbacks such as Hacking possibilities are high in unknown machines, An adversary compromises one password, Even if they know the passwords might be unsafe, Adversary can launch several password stealing attacks to snatch passwords.

3. PROPOSE SYSTEM

We design a user authentication protocol named SAP (SMS based Authentication Protocol) which leverages a user's Mobile phone and short message service (SMS) to thwart password stealing and password reuse attacks in the shopping website. SAP only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through SAP, users need not trust the unknown computers and no need to remember a long-term password for login on all websites. After evaluating the SAP prototype, we believe SAP is efficient and affordable compared with the conventional web authentication mechanisms. This conditional key is used to generate a chain of one-time passwords for further logins on the target server. The user name is the only information input to the browser. Next, the user get the SAP program on her system and they will get a SMS the user should enter their password; the program will generate a one-time password and send a login SMS securely to the user. The login SMS is encrypted by the using SHA2. the advantages of the proposed system such as it act as an Anti-malware(e.g., key logger) shield, it protects from Phishing, the application provides Secure Registration and Recovery in the online shopping application and finally it prevents Password Reuse and avoids Weak Passwords.

Process involved in the proposed system:

Registration Phase:

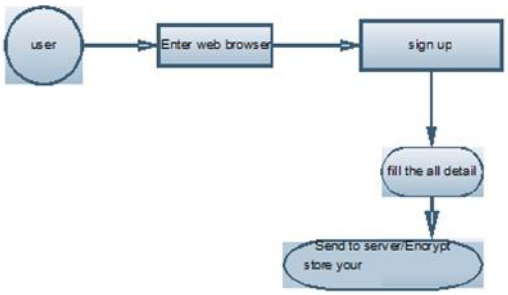

Fig 1.0 Registration process

The aim of this phase is to allow a user and a server to negotiate a conditional key to authenticate succeeding logins for this user. The user begins by opening the SAP program and performs the authentication process.

Login phase:

After registration the use should login with their userid. This shopping application does not need the password filed in the unknown system. After login phase the server process will begins. The server extracts the phone number and creates an encrypted password and send to the user mobile via SMS.

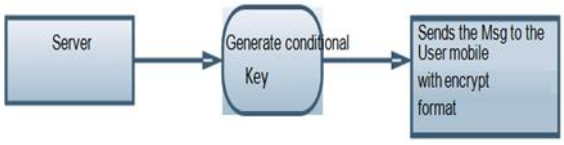

Fig 2.0 Login process

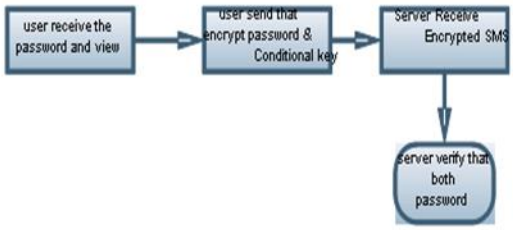

Fig 3.0 Key generation process

Server verification:

Server can decrypt and verify the authenticity of the login SMS and then obtain with the shared key. Server also compares the source of received SMS. Through a un trusted browser the systm will get the session timings. The user uses their mobile phone to produce a one-time password, eand deliver necessary information encrypted with to server via an SMS message.

Fig 4.0 server verification process

Accessing service:

User enter the browser and Register to server then server through sms on long term password with encrypt to mobile then user receive the sms and send to server .then server verify both password ,if correct the password open the view all detail ,else if not match that password means you won't allow the site inside.

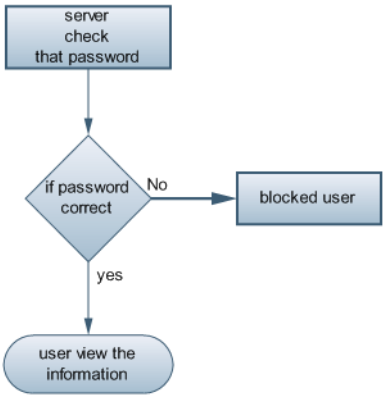

Fig 5.0 password verification process

SMS Channel

SMS is a text-based communication service of telecommunication systems. The proposed scheme uses SMS channel to construct a secure user authentication mechanism against the key misuse and stealing attacks in the distributed networks. Due to several benefits of Short Message Service, the proposed system chose SMS channel because of its security and reliable benefits. Compared with TCP/IP network, the SMS network is a closed platform; hence, it increases the difficulty of internal attacks, e.g., tampering and manipulating attacks. Therefore, SMS is an out-of-band channel that protects the exchange of messages between users and servers. Unlike conventional authentication protocols, users securely transfer sensitive messages to servers without relying on untrusted KAC s. SAP resists password stealing attacks since it is based on SMS channels.

4. IMPLEMENTATION

The thesis has used C#.Net for developing the front end of this software and SQL Server for the back end. The reason for using C#.Net is its flexibility. This can add or remove any features without editing the whole code. This separated the standalone functions like user name matching and password matching in separate functions which are reused again and again. For the back end this needed a freely distributed and powerful database so SQL Server was a good choice. Whole of the games will be stored in the database.

Encrypted password:

The one-time encrypted hash key in SAP is generated by a secure one-way hash function. With a given input, the set of encrypted passwords is established by a hash chain through multiple hashing.

This helps to avoid the password reuse attacks in the data retrieval function on cloud storage. The next one-time encrypted has key is obtained by performing hashes Hence, the general formula and its steps is given as follows:

Steps:

1. The passwords is produced by performing N hashes on the input C
    a. $\delta = Hn - 1(c)$
    b. Where δ is the hash key which is derived from the input C.
2. Repeat the step 1.a until the value of 1 became i.
3. Return the hash key H.

Note that function is a hash which is irreversible in general cryptographic assumption. In practice, is realized by SHA-256 in proposed system. Therefore, the bit length of is 256.

In the *registration* phase, a user starts the program to register the new account on the website to utilize the shopping. Unlike traditional registration process the server requests for the user's unique id and phone number, instead of password. The program sets the user name and password for authentication. This secret key is used to generate a chain of one-time passwords for decryption key creation on the web server. Then, the program automatically sends a registration Email message to the client after completing the registration procedure.

5. CONCLUSION

This proposed a user authentication protocol named SAP which leverages cell phones and SMS to thwart password stealing and password reuse attacks. We assume that each website possesses a unique phone number. We also assume that a telecommunication service provider participates in the registration and recovery phases. The design principle of SAP is to eliminate the negative influence of human factors as much as possible. Through SAP, each user only needs to remember a long-term password which has been used to protect her cellphone. Users are free from typing any passwords into untrusted computers for login on all websites. Compared with previous schemes, SAP is the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously. The reason is that SAP adopts the one-time password approach to ensure independence between each login. To make SAP fully functional, password recovery is also considered and supported when users lose their cellphones. They can recover our SAP system with reissued SIM cards and long-term passwords.

FUTURE WORK:

The shopping sites are very useful and attractive environment for data accessing in term of providing required services in a very cost effective way to their clients. Still the distributed authentication system affects by the un trusted host access and several network attacks. The user need to send conditional key via a un trusted hosts every time. To overcome the above issue and enhancing security and privacy practices in web systems, the proposed security system has been proposed with a new innovative functions and mechanisms.

In the proposed scheme, a new user authentication scheme with conditional key verification which leverages cellphones and SMS to stop key stealing and key misuse attacks. The current proposal presenting a valuable SHA 2 based encryption and authentication framework for data security on the shopping website.

REFERENCES

[1] Liang, Yingbin, and H. Vincent Poor. "Information theoretic security."*Foundations and Trends in Communications and Information Theory* 5.4–5 (2009): 355-580.

[2] Canali, Davide, and Davide Balzarotti. "Behind the scenes of online attacks: an analysis of exploitation behaviors on the web." *20th Annual Network & Distributed System Security Symposium (NDSS 2013)*. 2013.

[3] Bascle, Jeff P., et al. "System and method for reducing the vulnerability of a computer network to virus threats." U.S. Patent No. 7,571,483. 4 Aug. 2009.

[4] Kirda, Engin, et al. "Behavior-based Spyware Detection." *Usenix Security*. Vol. 6. 2006.

[5] Ramzan, Zulfikar. "Phishing attacks and countermeasures." *Handbook of Information and Communication Security*. Springer Berlin Heidelberg, 2010. 433-448.

[6] Dai, Shuaifu, et al. "A framework to eliminate backdoors from response-computable authentication." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

[7] Cho, Jung-Sik, Sang-Soo Yeo, and Sung Kwon Kim. "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value." *Computer Communications* 34.3 (2011): 391-397.

[8] Von Ahn, Luis, et al. "CAPTCHA: Using hard AI problems for security."*International Conference on the Theory and Applications of Cryptographic Techniques*. Springer Berlin Heidelberg, 2003.

[9] Li, Xu, et al. "Securing smart grid: cyber attacks, countermeasures, and challenges." *IEEE Communications Magazine* 50.8 (2012): 38-45.

[10] Syverson, Paul. "A taxonomy of replay attacks [cryptographic protocols]."*Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*. IEEE, 1994.