Abstract— Nowadays, User authentication has become a tough challenge to all the web services like banking sector, e-commerce sites etc. To facilitate these same requirements, we are going to implement Hi-pass system which is a combination of session password & a random key which is validated with the help of a cell-phone and a web service.

The SHA (Secure Hash Algorithm) is a set of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file.

Previously, SHA-1 was utilized to generate session password. In the proposed system, we are going to implement the system using SHA-2 algorithm. SHA-256 is one of the inheritor hash function to SHA-1, and is one of the strongest hash functions available. SHA-256 generates an almost-unique, fixed size 256-bit (32-byte) hash. The algorithms SHA-256, SHA-384, and SHA-512 are together referred to as SHA-2. Hash is a one way function – it cannot be reversed back. This makes it suitable to maintain security.

Keywords— Session password, SHA, Digital signatures, Authentication, encryption, cryptosystems

I. INTRODUCTION

One of the ancient ways to prove identity or gain access to a resource is passwords. A password is nothing more that consists to be of any secret word or string of character that is used for authentication purpose. A typical computer user may require passwords for many purposes: logging into computer accounts, various web accounts, retrieving the email from servers, retrieving the database, accessing the networks, websites. In websites, in order to maintain privacy to greater extent and provide high level of security we use passwords. People select their username and text passwords when registering accounts on a website. In order to login to the website successfully, users must recall the selected passwords. Password based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-recall passwords (i.e., weak passwords) even if they know the passwords might be unsafe.

Another crucial problem is that users tend to reuse passwords across various websites which causes domino effect; when a hacker compromises one password, they will make use of it to gain access to more websites.

Second, entering passwords into un-trusted computers suffers password thief threat. Passwords are prone to various types of attacks like brute-force attack, password reuse attack, password thieving attack, password guessing attack, etc. In order to reduce the negative influence of human factors in the user authentication procedure, the researchers have investigated a variety of technologies. Since humans are more a dept in remembering graphic based passwords than text passwords, many graphical password mechanisms were designed to address humans password evoke problem. Using password managing tools is an alternative. These tools automatically generate powerful and random passwords for each login, which are not easy to guess and recycle. The advantage is that users only have to remember a master password to access this tool. Despite the assistance of these two technologies-graphical password and password management tool the user authentication system still suffers from some considerable drawbacks. Graphical passwords are still vulnerable to several attacks. Password management tools execute well; but, some users doubt its safety and thus feel insecure to use it.

Authentication mechanisms on the Internet are typically used to give users access to their accounts. The procedure of identifying a person on internet is usually based on a username and password. The requirements for the authentication mechanism are focused by the requirements of the services to which they enable access. As the provider of the service is the party that ultimately makes the decision which authentication mechanism is to be deployed, we will list some common requirements from a service provider’s viewpoint.

The first requirement is availability. Web services should be available from a number of machines that can in general only be expected to have standard available tools, in particular any common web browser. A typical user expects to access his email and any other accounts from any machine he has access to, for example, the user might use any computer when he is on his vacation. To ensure that the authentication mechanisms availability, they also must be moveable or portable among a variety of different computers and devices.
The second decisive factor is **toughness and reliability**, which means that a genuine user should always succeed in logging into his account, it means that the user who has it’s correct username and password must be logged into his/her account within seconds.

The next decisive factor is **user openness**. Internet services hard to provide a good user experience and many of them try to promote the internet usage. For example, giving out the payments easily via Internet banking is much cheaper for the bank than processing paper cheque’s or demand drafts, telephone banking or having the customers to come into the branch to proceed their transactions. Preferably, authentication should be as flawless and as unseen as possible.

Another key requirement from the service provider’s viewpoint is that authentication mechanisms should have **low costs to execute and operate**. These deployment costs go beyond purely technical costs, but also involve the significant costs for customer support calls, in case users are not able to log into their accounts.

In this proposed system, we are developing an authentication protocol named Hi-pass system which makes use of a user’s cellular phone or may be a smart phone and Short Message Service (SMS) to prevent password cracking and password reuse attacks. Using Hi-pass system, users can firmly log into their web accounts thus preventing their passwords from being stolen. The main idea of the Hi-Pass system is to free users from remembering or entering any passwords into conventional computers for authentication. Unlike general user authentication mechanisms, Hi-pass introduces a new gadget, the cellular phone of the user, which is used to generate session passwords and a new communication channel, SMS, which is used to send encrypted messages; Thereby maintaining the security and integrity of the websites.

II. SESSION PASSWORD

A session password is a password that is valid for only one login session. Sessions passwords evade a number of shortcomings that are associated with traditional (static) passwords. The most important limitation that is addressed by session passwords is that similar to the static passwords, they are not susceptible to repeated attacks. This means that a potential intruder who manages to trace a session password that was already used to log into a service or to conduct a transaction will not be able to exploit it, since it will be no longer valid. On the downside, session passwords are difficult to remember. Therefore they require additional technology to work.

Session password production also typically makes use of pseudo or randomness. This is compulsory because otherwise it would be easy to predict future session passwords by observing previous ones.

We are using HMAC (Message Authentication code) to generate the random session passwords. Typically, message authentication codes are used between two parties that share a secret key in order to authenticate information transmitted between these parties. HMAC is a mechanism which is used for message authentication using cryptographic hash functions. HMAC can be used with any cryptographic hash function, for example: MD5, SHA-1,SHA-2 in combination with a secret shared key. The cryptographic power of HMAC depends on the properties of the underlying hash function which is being used in combination with it.

III. LITERATURE SURVEY/RELATED WORK

A number of previous researchers have proposed techniques to protect the user credentials from various attacks in user authentication.

I) **Password Management Strategies For Online Accounts**

   **By Shirley Gaw, Edward W. Felten**

   In 2006, Shirley Gaw and Edward W. Felten has given the extensive use of password authentication in on-line correspondence, payment services, and e-commerce, there is growing worry about identity theft. When people use the same one password across multiple web accounts, they increase their vulnerability; compromising one password can help an invader take over several other web accounts[1] They sometimes fail to realize that personalized passwords such as phone numbers can be cracked given a large enough dictionary and enough tries. They discuss how current systems support poor password practices. They also present potential changes in website authentication systems and password managers.

II) **A Large scale Study of Web Password Habits**

   **By Dinei Florencio And Cormac Herley**

   In 2007, Dinei Florencio And Cormac Herley shows the results of a large scale study of password use and password reuse practices. The study involved a million users over a period of three months. A device on users' machines recorded a variety of password strength/ usage and occurrence metrics. This allows us to measure or estimate quantities such as the average number of passwords and average number of accounts each user has, how many passwords he/she uses per day, how regularly passwords are shared among different sites, and how often they are forgotten.
We get very detailed data on password strength, the types and length of passwords chosen, and how they diverge by site. The data is the large scale study of its kind, and yields plentiful other insights into the role the passwords play in users' online experience.[2]

III) The Domino effect of password reuse by Blake Ives, Kenneth R. Walsh and Helmut Schneider

In 2004, Blake Ives, Kenneth R. Walsh and Helmut Schneider concluded that using the same password to gain access to various web accounts and websites causes domino effect. In domino effect, when a fragile system loses its secret code, some information will be exposed that will support the hackers in infiltrating other systems which may cause loss of huge sensitive data[3]

IV) PassPoints: Design and longitudinal evaluation of a graphical password system By Susan Wiedenbeck, Jim Waters, Jean-amille Birget, Alex Brodksiy and Nasir Memon

In 2005, Susan Wiedenbeck, Jim Waters, Jean-amille Birget, Alex Brodksiy and Nasir Memon introduced the concept of graphical password system called Pass Points which was based on two areas i.e. security and usability.[4] They concluded that Pass Points are more efficient for security. Based on complicated and complex, natural images with hundreds of potential click points, one can be easily obtain large passwords spaces. Another thing is that, they developed a robust discretization which enables that system to cryptographically hash Pass-Points passwords. This strong discretization makes the system secure storage and protected during file back-up. Also it appears from the small sample in their experiment that users did not too often chose points that were within a grid square chosen by another individual.


In 2010, P.C. Van Oorschot, Amirali Salehi-Abari[5], Julie Thorpe introduced and evaluated various methods for purely programmed attacks against Pass Points style graphical passwords. To generate these attacks, they introduced a graph based algorithm to efficiently create dictionaries based on heuristics such as click-order patterns (e.g., 5 points all along a line). Some of their methods combined click-order heuristics with focus of-attention scan-paths generated from a computational model of visual attention, yielding significantly better programmed attacks than previous work.[5]

One resulting computerized attack finds 7-16% of passwords for two representative images using dictionaries of roughly 226 entries (where the full password space is 243). Relaxing click-order patterns considerably increased the attack efficiency with larger dictionaries of approximately 235 entries, allowing attacks that guessed 48-54% of passwords (compared to previous results of 1% and 9% on the same dataset for two images with 235 guesses). The results show that programmed attacks, which are easier to arrange than human-seeded attacks and are more scalable to systems that use multiple images, pose a significant risk to basic PassPoints-style graphical passwords.

VI) Trustworthy and personalized computing on public kiosks by Scott Garriss, Reiner Sailer, Ramón Cáceres, Leendert Van Doorn, Stefan Berger, Xiaolan Zhang

In 2008 Scott Garriss, Ramón Cáceres, Stefan Berger, Reiner Sailer, Leendert Van Doorn and Xiaolan Zhang presented the design of a system in which a user’s mobile device serves as a vehicle for establishing trust in a public computing kiosk by verifying the integrity of all software loaded on that kiosk. Procedure made use of several promising security technologies, namely the Integrity Measurement Architecture, the Trusted Platform Module, and new x86 supports for establishing a vibrant trust.[6] This system maintains data privacy against the need of the kiosk owner to prevent exploitation of the kiosk.

VII) Passpet: Convenient Password Management and phishing protection by KaPing Yee and Kragen Sitaker

KaPing Yee and Kragen Sitaker introduced the thought of Passpet in 2006. Passpet is a system that improves the easiness and security of website login. Passpet system helps users to manage multiple accounts. If user is using single memorized password for multiple accounts then that single password is turned into different passwords for different accounts and for different websites logins.

VIII) A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks By Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin

Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin proposed a user authentication protocol that is used to defend against the password reuse attacks in the year 2012. An attacker can commence several password stealing attacks to grab passwords, such as brute-force attack, password reuse attack, password thieving attack, password guessing attack, etc.
In this paper, the authors have developed a user authentication protocol named oPass which makes use of a user’s cellular phone and short message service to avoid password stealing and password reuse attacks. oPass only requires each website must possess a unique phone number, and leverages a Telecommunication Service Provider (TSP) in order to obtain the appropriate phone numbers of websites and that of the users respectively. The SMS service to support system in establishing a very secure channel for exchange of messages in the registration and recovery phases. Through oPass, users only need to memorize a long-term secret code for login on all webs accounts. [8] Therefore, the main conception of oPass is to free users from having to memorize or enter any passwords into conventional computers for authentication. Unlike common user authentication, oPass involves a new gadget, the cell-phone of the user, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit encrypted messages.

IV. SHA-2 ALGORITHMS

SHA stands for Secure Hash Algorithm and SHA is a collection of NIST-approved cryptographic hash functions. When a message of any length < 2^64 bits (for SHA-1 and SHA-256) or < 2^128 bits (for SHA-384 and SHA-512) is input to an algorithm, the product is an output called a Message Digest. The message digests vary in length from 160 bits to 512 bits, depending on the algorithm. Secure hash algorithms are usually used with other cryptographic algorithms, such as digital signatures and keyed-hash message authentication codes, or for the generation of random numbers (bits).

SHA-2 is one of the four hash functions defined in the Federal Information Processing Standards (FIPS-180-3). All four hash functions were developed by the National Security Agency and issued by NIST in 2002. SHA-2 consists of a family of cryptographic hashing algorithms developed by NIST (National Institute of Standards and Technology) The algorithms SHA-256, SHA-384, and SHA-512 are together referred to as SHA-2.

SHA-256 is an iterated cryptographic hash function with a hash output size of 256 bits, a message block size of 512 bits and using a word size of 32 bits. The algorithms SHA-256, SHA-384, and SHA-512 are together referred to as SHA-2.

SHA-2 was developed to replace the aging SHA-1 hashing algorithm and its weaknesses. In 2005, security flaws were detected in SHA-1, explicitly that a mathematical limitation might exist, indicating that a stronger hash function would be advantageous.

Although SHA-2 bears some resemblance to the SHA-1 algorithm, these attacks have not been productively extended to SHA-2. Since 2008, no collision attacks have been published on SHA-2.

V. CONCLUSION

In this paper, we have surveyed many technologies and in contrast to these technologies, the Hi-pass based authentication scheme proposed here scores very well with relation to all the requirements stated above.

We have proposed a system which consists of a powerful user authentication protocol named Hi-Pass that makes use of the user’s cellular phone and short message service (SMS) to ensure protection against password stealing and password cracking attacks. Hi-Pass system requires a unique phone number that will be possessed by each participating website. In our belief, it is difficult to exploit password reuse attacks from any scheme where the users have to memorize the pass-codes. Largely, the password attacks occur when users are required to type any passwords into public computers. Therefore, keeping this as the main consideration, the main perception of Hi-Pass is to free users from remembering or typing any passwords into conventional computers for authentication. In contrast to the general user authentication mechanisms, Hi-Pass involves a new component, the cell phone of the user, which is used to generate session passwords and a new communication channel, SMS, which is used to broadcast authentication messages.

Moreover, we are using the HMAC which is a Message Authentication Mechanism in combination with the SHA-2 algorithm for secured hashing as SHA-2 is more secure, also it has a larger message digest than SHA-1 algorithm and moreover, SHA-2 has not yet been compromised in any way. Thus, we can build a more robust system which will resist the various attacks thus enhancing and improving the security of the users.

REFERENCES


