ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

Highly Secured Single Entity User Password Mechanism For Multiple Websites

Ms.K.Prathipa[1], Mr. S. Prakadeswaran[2], Dr. T. Senthil Prakash[3]

[1] PG Scholar, Shree Venkateshwara Hi-Tech Engg College, Gobi, Tamilnadu , India
[2] Assistant Professor, Shree Venkateshwara Hi-Tech Engg College, Gobi, Tamilnadu , India
[3] Professor and Head, Shree Venkateshwara Hi-Tech Engg College, Gobi, Tamilnadu , India
(Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamilnadu, India)

ABSTRACT

The growing demand of users to work with various websites in pursuit of knowledge lead and growing needs to obtain enormous information from various websites has caused our work to extend to Highly Secured Single Entity User Password Mechanism for Multiple Websites. In the existing work, every user is provided with the password authentication in order to login to the sites as and where required by the user to various web sites. Subsequently, for the convenience of user and higher levels of security various websites provide efficient authentication mechanism with current password scenario. Despite extensive research in the past decade, the problem of developing secured single entity user password mechanism for multiple websites remain unsolved. In this paper, we propose to tackle this problem using an approach different from all past solutions. For ease performance of all users, highly secured single entity user password mechanism is presented with. A single entity password mechanism is generated which in turn link towards all of other sites as requested by the user. In order to generate master password mechanism hashing technique is introduced. Password security is introduced in our work to increase the password security with the technique cryptography with MD5 algorithm. Our mechanism has a number of appealing features. Case study and preliminary experiment results conducted in Java proves to be a viable approach using single entity password with multiple sites by user. The performance of Single Entity Password Mechanism is evaluated with multiple sites in terms of the time required to generate master password, response time for login validity and the password length constraints.

1.1 INTRODUCTION

Internet is the most integral part of our daily lives and the people who manages their work with internet like bank transaction, online shopping, share marketing is also constantly growing. The websites which provide these services should be an authenticated one they should allow the user to create their own username and password with a reliable service. Qualified people can access their account by password authentication. A technique such as Secure Socket Layer (SSL) is used for a secure transaction purpose. But some websites offers a poor

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

authentication service which leads to password attacks.

A remote password authentication scheme is used to authenticate the legitimacy of the remote user over an insecure channel. In such a scheme, the password is often regarded as a secret shared between the authentication server (AS) and the user, and serves to authenticate the identity of the individual login. Through knowledge of the password, the remote user can create a valid login message to the authentication server. Authentication Server checks the validity of the login message to provide the access right.

The username or password paradigm is the commonly used authentication mechanism in security applications. Alternative authentication factors, including tokens and biometrics, require purchasing additional hardware, which is often considered too expensive for an application. However, passwords are low-entropy secrets, and subject to dictionary attacks. Hence, they must be protected during transmission. The use of passwords has intrinsic weaknesses. It is a well-known problem that human-user-chosen passwords are inherently weak since most users choose short and easy to remember passwords.

A hash function is any algorithm or subroutine that maps large data sets of variable length called keys. To smaller data sets of a fixed length. For example, a person name could be hashed a single integer and that integer can then serve as an index to an array . The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes. A hash function that assigns unique indices to strings, even if inconsistent between runs, is still a perfectly valid hash.

1.2 LITERATURE SURVEY

Conventional work has resulted in conclusion that traditional passwords are highly insecure. The work [5] reexamines the problem of password selection through the exploration of password selection mechanisms with novel interface designs. At present most password selection mechanisms (PSMs) are not designed according to basic Human Computer Interactive HCI principles. The work [5] proposes the solution for building strong password selection through the exploration of PSMs with novel interface designs

Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over insecure networks. It is more frequently required in various areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems. In this work [4] proposes the result of the survey through all currently available password-authentication-related schemes and classify accordingly on the basis of certain crucial criteria. Most of the existing schemes are vulnerable to various attacks and fail to serve all the purposes an ideal password authentication scheme should. In this work [4] various password authentication schemes are compared in various situations the different types of attacks are also presented. A remote password authentication scheme

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

based on cross product is proposed in this work [2]. In this scheme any authorized user can independently choose his own password using the card initialization phase. With the help of password and smart card mechanism, he can henceforth log into the system successfully. According to the results and discussions obtained intruders cannot obtain any secret information from the public information or transmitted messages and impersonate another authenticated user.

Due to the increased usage of computer and networks on a large scale nowadays, user authentication is extremely important. For achieving privacy and security password authentication is the most popular method in such open environments. Subsequently with the use of smart cards, the proposed work [3] can easily verity user's credentiality over insecure channels and the authenticated users does not necessarily have to be a known person in the network. The proposed work [3] has the ability to bear replaying attack, tampering and eavesdropping on the communication links. Unlike [1] it is not necessary to change user's password periodically to perform authentication processes synchronously in between the smart card and the node.

A technique of user password authentication is explained in this work [1] which is said to be secured even if an intruder can get into access to the systems data and can easily tamper with or eavesdrop on the communication between the user and the system. The method flows in such a way that a secure one-way encryption function is performed with the help of microcomputer in the user's node.

1.3 PROPOSED

1.3.1 Objective

The proposed system works on secured enhanced password authentication scheme. This scheme prevents the attacks effectively and masquerade attack and replay attack. The proposed work is resistant to password guessing attack. In this system mutual authentication is achieved. The proposed scheme is shown to be highly secured by way of making it suitable for distributed user password utility.

1.3.2 User credentials and web site information

A person holding a credential is usually given documentation or secret knowledge which can either be a password or key as proof of the credential. Sometimes this proof is held by a third, trusted party. While in some cases a credential may be as simple as a paper membership card, in other cases, such as diplomacy it may involve presentation of letters directly from the issuer of the credential detailing its faith in the person representing them in a negotiation or meeting.

Counterfeiting of credentials is a constant and serious problem, irrespective of the type of credential. A great deal of effort goes into finding methods to reduce or prevent counterfeiting. In general, the greater the perceived value of the credential, the greater the problem with

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

counterfeiting and the greater the lengths to which the issuer of the credential must go to prevent fraud.

The user information is recorded. Credentiality of the user is verified for further processing. In this phase listing of user interested websites are performed. The website in turn use forms authentication. Subsequently the user logs on to the website by visiting its corresponding login page for further entering their credentials. Credentials are then compared against the user store. On processing of validity the user is granted with a forms confirming with the authentication ticket. The security token indicates identity and authenticity of the visitor. In the similar manner user setting of separate logins are maintained for different websites. The user details are association to interested sites. Further it enhances the enabling of user interested sites for operations.

1.3.3 Master Password Generation

In order to provide login authentication initially the user enters a master user name and master password. The user defined alpha numeric password is converted into binary strings. The passwords that are created in a random manner are highly secured and extremely difficult to guess with. A random password generator is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using simple sources of randomness such as dice or coins, or they can be generated using a computer. A password generator can be part of a password manager. When a password policy enforces complex rules, it can be easier to use a password generator based on that set of rules than to manually create passwords.

The obtained binary string is recorded and is correspondingly linked to respective user credential. The binary password generated is made into single entity constrains. A binary code is a way of representing text or computer processor instructions by the use of the binary number system's two-binary digits 0 and 1. This is accomplished by assigning a bit string to each particular symbol or instruction. For example, a binary string of eight binary digits can represent any of 256 possible values and can therefore correspond to a variety of different symbols, letters or instructions. In computing and telecommunication, binary codes are used for any of a variety of methods of encoding data, such as character strings, into bit strings. The methods may be fixed-width or variable-width. In a fixed-width binary code, each letter, digit, or other character, is represented by a bit string of the same length; that bit string, interpreted as a binary number, is usually displayed in code tables in octal, decimal or hexadecimal notation. There are many character sets and many character encodings for them. In this module script password generation functionality is introduced. It Generate a random password with the ability to include special characters and password restrictions.

1.3.4 Password Hashing

The password hashing method send a hash value derived from the user's password, and the site domain name. The Pass word Hash captures all user

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

input to a password field and sends hash to the remote site, whereas domain is derived from the domain name of the remote site. Hash automatically generates strong passwords from a master password. The Hash is implemented using a Pseudo Random Function keyed by the password. As the hash output is tailored to meet server password requirements hashed password is handled normally at the server with no server modifications required. Password Hash transparently converts a user's password into a domain-specific password. Hash function invokes the single entity binary password and fed as input to the hash function. Hash function generate associated hash key for the master password. Given same master password and parameter hashing provides the same result. Master and generated passwords are not transmitted to the server. Every user binary password is converted in to respective hash key.The user activates this hashing by choosing passwords that start with a special prefix or by pressing a special password key (F2). Password Hash automatically replaces the contents of these password fields with a one-way hash of the pair (password, domain-name). The site only sees a domain-specific hash of the password, as opposed to the password itself.

Hash function used is public and can be computed on any machine which enables users to login to their web accounts from any machine in the world. Hashing is done using a Pseudo Random Function (PRF). In turn strong passwords are automatically generated. The same master key produces different passwords at many sites. It automatically upgrades the master key without updating all sites at once. It supports different length passwords. It supports special requirements, such as digit and punctuation characters.

1.3.5 Message Digest for Hash Linked web sites

Initially the website name and its login password are provided by the user whose authenticity is verified. It extracts the user interested website's name and login password's. Message Digest algorithm is applied for the user credentials to the extracted website info. The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. An MD5 hash is typically expressed as a 32-digit hexadecimal number. MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact.

MD5 was widely used to store passwords. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks and the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with a 64-bit little ending integer representing the length of the original message, in bits.

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C* and *D*. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The digested message is fed into

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

the hash function. Subsequently multiple hash key are generated for different user interested website. User master hash key is linked to his website hash key on message digestion. MD5 algorithm makes sure that no one gets Master Password from generated password. Automatic checking of hash keying is done with user master password which enables user to easily handle and multiple websites with high security.

1.4 Conclusion

In this paper, we present a highly secured Single Entity User Password Mechanism for Multiple Websites. We have surveyed all currently available password authentication schemes and analyzed how they work using the tool Java. Our work defined the security mechanisms making it suitable for distributed user password utility and all of the goals an ideal password authentication scheme satisfy and achieve. Our proposed work is conducted using the algorithms "Password Hashing" and "User Sites Message Digest Algorithm". The proposed single entity user password mechanism proves to be full proof and is resistant to password guessing attack and hence mutual authentication is achieved. Experiments are conducted and a performance analysis show that our proposed work single entity user password mechanism out performs the existing work based on smart card model.

REFERENCES

[1] Lamport, "Password authentication with insecure communication," Computers & Security..Hwang M.S and L.-H. Li, "A new remote user authentication scheme using smart cards," Consumer Electronics, IEEE Transaction.

[2] Sun, "An efficient remote use authentication scheme using smart cards," Consumer Electronics, IEEE Transaction.

[3] Chien, J.-K. Jan, and Y.-M. Tseng, "An efficient and practical solution to remote authentication: Smart card," Computers & Security.

[4] Ku and S.-M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," Consumer Electronics, IEEE Transaction.

[5] Yoon, E.-K. Ryu, and K.-Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," Consumer Electronics, IEEE Transaction.

AUTHOR INDEX:

Ms. K.Prathipa, PG Scholar, received the B.tech degree from Anna University, Chennai, India in 2012 and worked as lecturer in Sri Ramanathan Engineering College from 2012-2015 and Currently persuing her M.E CSE degree in Shree Venkateshwara Hi-Tech Engg College, Gobi, Tamilnadu , India. Her research interests include Web technology, Network Security, Software Engineering.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

Mr.S.Prakadeswaran, received the Bachelor of Engineering in Anna University, Chennai, Tamilnadu in 2008. He received the Master of Engineering in A na University, Chennai, Tamilnadu in 2013. He has the experience in Teaching of 7+Years. He is currently working as Assistant professor in Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamilnadu. His research interest includes Wireless Networks and Pervasive computing. He has published several papers in 9 International Journals.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E(CSE) degree from Vinayaka Mission's University, Salem, India in 2007 and M.Phil.,MCA.,B.Sc(CS) degrees from Bharathiyar University, Coimbatore India, in 2000,2003 and 2006 respectively, all in Computer Science and Engineering. He is a Member in ISTE New Delhi, India, IAENG, Hong Kong.. IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 11+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17 International Journals, 43 International and National Conferences.