RESEARCH ARTICLE OPEN ACCESS

A Survey and Scheme for Securing Web Application Using Physical Token

Krutika Dhavale[1], Priyanka Kalase[2], Archana Dashpute[3], Nikita Kharat[4],
K V Kokil (Scientist)[5] , Shanthiguru[6]
1(Department of Computer Engineering, Pune/D.Y.Patil College Of Engineering Akurdi)
2(Department of Computer Engineering, Pune/D.Y.Patil College Of Engineering Akurdi)
3(Department of Computer Engineering, Pune/D.Y.Patil College Of Engineering Akurdi)
4(Department of Computer Engineering, Pune/D.Y.Patil College Of Engineering Akurdi)
5(Armament Research and Development Establishment/DRDO,pune)
6(Department of Computer Engineering, Pune/Professor at D.Y.Patil College Of Engineering Akurdi)

Abstract:

Securely accessing and storing data is a major concern in organisations which have critical data. Access to that data is given according to the role. If someone has the credentials of a particular user then the security is compromised, the hacker can access the data of the user from anywhere without the knowledge of user. Two factor authentication is one way which provides security to the users. In the proposed system, a web application is secured using two factor authentication including physical token .The user cannot proceed unless both the credentials hold true. Role based access control plays an important role and also helps in maintaining secrecy of data. This system also encrypts the data that is entered by the user during the session and as per the requirement, displays that data in decrypted format. We utilize the security provided by https, and U2F.

Keywords —**Two factor authentication, integrity, cryptography, external key, confidentiality, hardware root of trust, non-repudiation, and authentication.**

I. Introduction

We have important confidential data which can be accessed through web based technologies on various platforms and devices where the need of security is paramount. In the proposed system a web application is created which stores the data in encrypted format and displays it in decrypted format according to the requirement of the user. This application will only be accessible to the user when the external key is connected. Two-factor authentication is a type of multi-factor authentication. Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. This mechanism is used in this system as follows: The first factor will be the user's credentials based on what user 'knows' and second factor is the hardware token or external key. If both the factors are successfully verified only then the user can proceed. This enhances the security of the system. If the external key is ejected in between the session, access will be denied.

II. Basic concepts - In the context of our survey, we understand and use the terms in following way

- Two factor authentication

Two factor authentications are also known as 2FA.It is a two-step verification process. It provides an extra layer of security. For example, 2FA can include a process where not only user identity and knowledge of a shared secret is required but also possession of a physical token. Thus username and password is the first factor and physical token is the second factor. As these two factors are used for authentication it is known as two factor authentication.

- Role based access

Role based access is the process of providing access to the privileged resource based on the role associated with the user identity. E.g. Organizational role may be an important access control parameter for accessing resources. Access is the ability of a user to perform particular task. For e.g. create, view or modify a piece of data. Roles are assigned according to job competency, authority, or responsibility within an organisation.

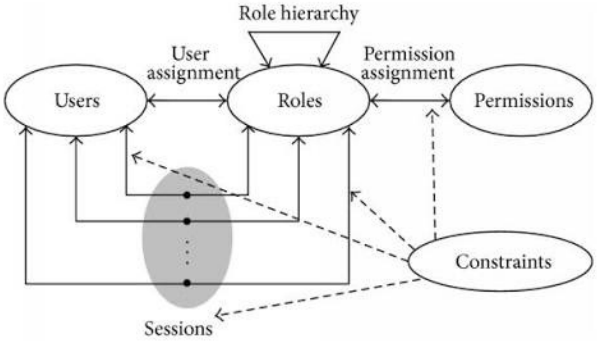

Figure: Role based access

- Cryptography

It is the process of converting plain text into cipher text. It is method of storing and retrieving data in specific form. Only the intended user can read and process the data. It is the way to hide information in storage and transmit. Cryptography not only protects the data but also can be used for user authentication. Cryptography is associated with scrambling ordinary plain text into cipher text which is known as encryption and then back again into plain text which is known as decryption. Cryptography concerns with following objectives:

- Confidentiality-Information is understood only to the intended user.
- Integrity- Information cannot be modified.
- Non-repudiation-Once the sender sends the data he cannot deny his intentions in transmission of data.
- Authentication-Sender and receiver can confirm each other.

Following techniques are used in cryptography:

- Symmetric key cryptography- Sender and receiver shares the single key. Sender uses this key to encrypt the data and send this encrypted data to the receiver. On the other hand receiver uses the same key and receives the data.
- Asymmetric key cryptography- In this technique two keys are used public key and private key. Public key is freely distributed and private is kept secret. Public key is used for encryption while private key is used for decryption.

III. Literature Survey And Observations About Usage In Proposed System

Chi Po Cheong et al. [1] introduces a new secure token for the improvement of existing web security standards. As messages are transferred over the internet security is the main concern. The existing web service security standard only protects the message. Authors have proposed a sender location authentication. If user of a particular organisation is granted with some rights then according to the standards he should be able to access the web services from anywhere irrespective of the location. A secure token scheme is proposed which will monitor and control the location of the consumer who wishes to access the service. The location is authenticated first so that the load on system resources is reduced by blocking the false users. This secure token provides two features first is authentication of service consumer location and second is permitted domain list which is used to reject the soap message from an unknown domain. Our Observations: As the location is used as first factor it requires continuous monitoring of the service consumer location which is a drawback. The concept of physical token is utilized in our proposed system for the indicated advantages.

Paras Babu Tiwari et al. [2] propose single sign-on feature implemented by combining the concept of one time password (OTP) with single sign-on. The

OTP is a mechanism that prohibits the unauthorized access of protected resource like user account. The OTP approach entails the user to use different password for each login and it is widely used for two factor authentication. In this paper approach of implementing SSO, the OTP is used to establish the communication among the applications. Our Observations: In this paper md5 algorithm is used to generate one time password but this algorithm has been broken. The concept of one time password is utilized in our proposed system for the indicated advantages.

Paul Crocker et al. [3] describe two factor encryption architecture for cloud storage that incorporates the use of hardware token. YubiKey USB cryptographic token is used as the external two-factor module which enables use of two factor encryption and authentication mechanism to ensure privacy of data. The YubiKey USB token is used as authentication and not as part of encryption process. One time password is generated by token which is used together with the user's credentials. The files are then encrypted using custom key derived from passphrase and key stored in YubiKey token. Here they have proposed a two-factor key derivation scheme using a hardware token and present a proof of concept that enables this approach in a cloud storage scenario, assuring end-to-end encryption and therefore, the privacy of the user's data. Our Observations: In this paper the data is stored on cloud and in our proposed system we are creating a web application for the same utilizing the advantages of Yubikey token and OTP.

Jongho Moon et al. [4] proposes a biometric based user authentication scheme which makes use of smart card. Here user authentication scheme is based on fuzzy extractor. In the proposed scheme biometric based fuzzy extractor, which converts biometric information into random strings is described. The scheme consists of four phases: - login, authentication, key - agreement and password changing phase. Two factors for authentication in this scheme are user credentials that are identity and password and biometrics. The proposed scheme can resist outsider attack, insider attack, impersonating attack, offline password guessing attack. It also provides perfect - forward secrecy. Our Observation:In this approach biometric is used as factor of authentication, but biometric systems are not 100% accurate. They have two types of errors: false reject error which rejects authorized person trying to access system and false accept error which accepts person who is not in fact who he/she claims to be. Besides that biometric readers are not suitable for mobility over Internet.

Jongho Moon et al.[4]use biometric as on of the factor for authentication. Biometric system cannot be reset and this is a drawback. In our proposed system we are making use of physical token instead biometric to avoid the above problems.

Chi Po Cheong et al.[1] use location as first factor it requires continuous monitoring of service consumer location to overcome this problem we are not using location as an authentication parameter rather we are using credentials of the user.

IV. PROPOSED SYSTEM

We have proposed a system in which the concept of physical token with one time password is utilized to secure a web application using two factor authentication.The two factors used are: a combination of username & password and the OTP generated by hardware/physical cryptographic token.

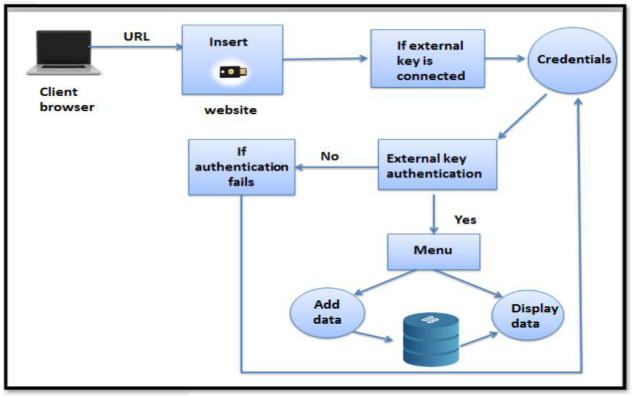

Figure:Proposed system

The two factors are used for verification and authentication of the user. Two factor authentication scheme ensures security and prevents unauthorized access to private data of user. The user cannot proceed further unless both the factors are true. If any one of the factor fails, the user is denied access to application.

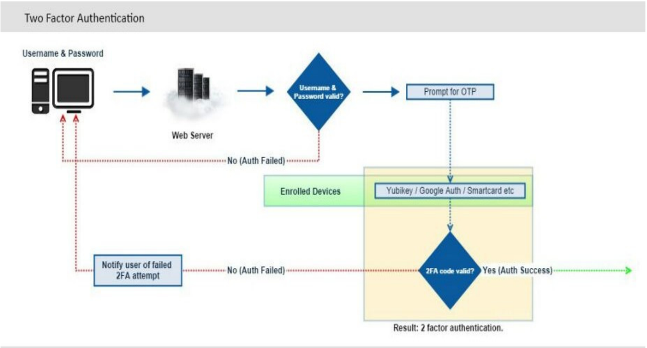
Two Factor Authentication
Username & Password
Web Server
Username & Password valid?
Prompt for OTP
No (Auth Failed)
Enrolled Devices
Yubikey / Google Auth / Smartcard etc
Notify user of failed 2FA attempt
No (Auth Failed)
2FA code valid?
Yes (Auth Success)
Result: 2 factor authentication.

Figure: Two factor authentication system

Proposed system makes use of https protocol which creates a secure channel over an insecure network. It ensures protection from eavesdroppers and man-in the middle attacks. At the authentication stage, an OTP is generated by this token and used together with the user's credentials in order to obtain access the system.

We intend to use a physical token with an open standard like U2F. [8] *U2F is an open authentication standard that enables keychain devices, mobile phones and other devices to securely access any number of web-based services — instantly and with no drivers or client software needed.*

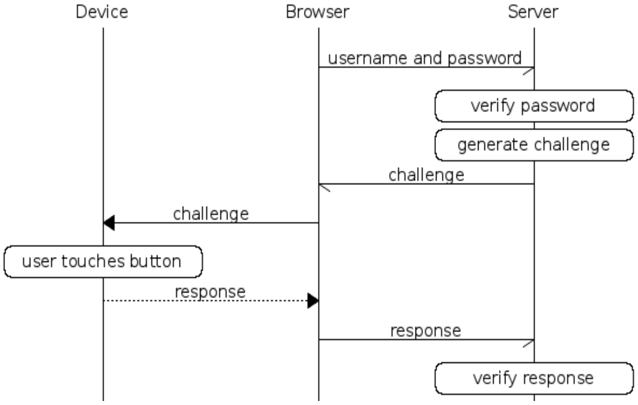

Figure:U2F Process Flow

After the successful authentication of user, the user can manage his/her account and can perform various functionalities provided in the application like store data, retrieve data and modify data. While the user logs into the application an access token is issued. Every issued access token is valid for a few minutes, a time span that we believe to be able to accommodate a normal usage session. Every time this token expires, user is forced to re-enter his/her credentials so that a new access token can be issued.

The system allows user to store data in encrypted format and as required retrieve it back in decrypted format. The system provides role based access control which plays an important role. The access to data is provided only to authorized and privileged users. In this way it also helps in maintaining secrecy of data.

Thus our proposed system tries to address the issues of information security like authentication, access control, role based authorization, data encryption and communication channel secrecy for simple web applications with advantage of simplicity of implementation and user mobility. Usage of a physical token assures information security provided by hardware root of trust. This root of trust is mobile and does not require a network connection and mobile network unlike SMS based OTP.

We intend to implement a solution demonstrating the working of the architecture that we are proposing. The detailed system architecture of used protocols will evolve in the next publication in line after this paper.

V. CONCLUSIONS

This survey describes the work done in two factor authentication and also throws light on our proposed system. Our system will be using two factor authentication so that only the authorized person who has the credentials will be permitted access to the web application. As we are using username and password together with physical token it is harder for the intruders to gain access and steal the user's personal data or identity. It also provides security of data as the data entered will be stored in encrypted format and will only be displayed to the authorized user after successful login.Combining the existing protocols like https and techniques like hardware root of trust in terms of Yubico or equivalent physical token.

VI. REFERENCES

[1] Chi Po Cheong, Chris Chatwin, Rupert Young, "A new secure token for enhancing web service security". 978-1-4244-8728-8/11/$26.00 ©2011 IEEE.

[2] Paras Babu Tiwari, Shashidhar Ram Joshi, Ph.D." Single Sign-on with One Time Password".2009 IEEE

[3]Paul Crocker, Pedro Querido. "Two factor encryption in cloud storage providers using hardware token".2015 IEEE.

[4] Jongho Moon, Jiye Kim,Donghoon Lee,Dongho Won,"Security enhancement of robust anonymous two factor authenticated key exchange scheme for mobile client-server environment".2016 IEEE

[5] Edna Elizabeth.N, S.Nivetha."Design of two factor authentication ticketing for transit application".2016 IEEE

[6] Joseph K. Liu, Man Ho Au , Xinyi Huang, Rongxing Lu, Jin Li. "Fine-grained Two-factor Access Control for Web-based Cloud Computing Services"

[7] https://www.yubico.com/

[8] https://developers.yubico.com/U2F/

[9] Prof (Dr.) Mohd Hussain, Md Nadeem Ahmed. "Privacy Preserving Web based Transaction using E-Smart Cards and Image Authentication"