IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 7, July 2015.
www.ijiset.com
ISSN 2348 – 7968

Trends in Web User Security

Radhakrishnan Subramanian
Associate Professor, Saveetha School of Engineering, Saveetha University, Chennai, India
Department of Electronics and Communication (radhakrishnan@saveetha.com)

Abstract - **Security is an important concern in user security. In lieu of threats in and network based environment it becomes essential for the applications to become more and more secured and in this paper we consider several authentication techniques.**

Keywords - Authentication, OTP, 2FA, Mutual Authentication, Partial Authentication, Dual Authentication.

I) INTRODUCTION

With the exploding popularity and necessity of Web based applications being made available through multiple channels viz...Internet Browsers, Mobile application based and Intranet Browser based, it is becoming imperative to ensure the utmost security mechanisms for user data through appropriate user security control and credentials validation. At the same time, while ensuring the appropriate protection, users should not be overloaded with many steps / authentication factors, which could lessen the user experience as well potentially may lead to compromise of security as users; in practical scenarios, such multiple/ complex authentication requirements end-up forcing the users to note down those details into any of their own repositories, instead of remembering in memory and thus defeating the whole intent of security.

In the current technological access advancement via multiple channels and day-to-day raising cyber threats through wide range of hacking, traditional authentication mechanism of login username and with any tough complex logon password is insufficient and proven to be much vulnerable. As Researchers and Technology experts, we are in the juncture of striking right balance between enhancing and tightening the security authentication mechanism on one-side, and on other side ensuring users experience/ ease of use without paving way for compromising on security. This paper outlines few modern and enhanced techniques to provide better user security for the web based applications.

II) MODERN AUTHENTICATION TECHNIQUES

There are variety of simple and improved authentication but though yet powerful techniques available in the industry. Below are some of the key techniques to outline:

- Dual Authentication
- Mutual Authentication
- Partial Authentication
- Adaptive Authentication
- One-Time-Password Authentication
- Two-Factor Authentication (2FA)

Each of these techniques can be used independently, but combination of two or more can provide much enhanced security levels. Vital deciding factors on the level of security, thus the number of authentication aspects required are as below:

1) Risk associated / Value of losing the asset / entity being protected
2) Cost of providing the security for the entire life-cycle of the application
3) Ease-of-login / User experience

III) DUAL AUTHENTICATION

Dual authentication is the simplest enhanced security that can be provided, on top of the usual logon password. In this technique, the user has to enter the typical logon user name, logon password and then one more password which is can the secondary password / authentication. This secondary password can be static personal confidential information pertaining to individual user like date of birth, place of birth, driving license number OR it can be another user defined static password. Earlier approach is preferred as it's not going to burden user to remember one more password, as it's normally the personal related data known to that individual user.

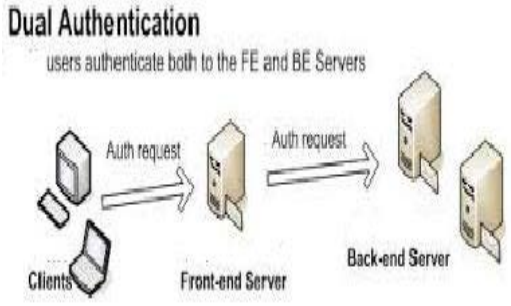

Figure 1 - Dual authentication scenario

ISSN 2348 – 7968

There are many banks and financial websites following this simple method.

IV) MUTUAL AUTHENTICATION

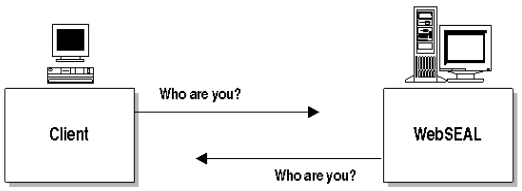

Figure 2 - Mutual authentication scenario

This technical is especially useful to counter-act the phishing attacks by giving hacker URL instead of the actual intended URL. In many situations the hackers / phishers will create their own site which will mimic exactly the actual site and thus user may end-up sharing their confidential information like user-name, password and any other critical details unknowingly.
To avoid such situation, the actual intended URLs / websites can display an image / text that is pre-selected and pre-stored by that individual user when the valid username is entered. Post to that display of pre-stored detail, user can validate and if satisfied then user can enter the password. This way, the user is confident and sure that appropriate website is accessed. In the case of phishing attacks, the pre-stored text / image will not be displayed and user can stop the log process at that stage without entering the password.

V) PARTIAL AUTHENTICATION

With the Partial authentication methodology, user is asked to enter the logon username fully and then only a portion of the logon password (i.e. partial as well varying randomly for every logon. This technique is also called Variable authentication mechanism and combats the Man-In-the Browser (MiTB)/ Man-in-the-Middle (MiTM) attacks effectively.

During first time logon user would be asked to enter partial digits, say 1st, 4th, 6th, 7th and 11th digits of the password. Thus user has to enter the below digits only

1st digit	4th	6th	7th	11th
P	s	0	r	&

3rd digit	4th	6th	8th	10th	11th
s	s	0	d	5	&

While seeking the partial password, digits sought can be displayed as scrambled digits / images with variety of random alignments (similar to Captcha), so that hackers cannot read / catch the digits easily and construct the partial passwords punched, thus increasing the security level better.

VI) ADAPTIVE AUTHENTICATION

Adaptive authentication is much evolved and one of the costly techniques. This technique is used in conjunction to the traditional logon username / password OR with other techniques. This method involves studying and storing the user behavior / patterns over a period, which is also termed as analyzed behavior; post to that, then perform subsequently authentications based on the variance in the user behavior against the analyzed behavior and then update the stored user behavior incrementally with the current authentication as well. This technique is being adopted by financial and various niche industries when underlying data needs strong protection.
In this adaptive authentication, following are the high-level steps that happen:

Step 1 - Profiling: Several user-specific behaviors are captured and stored starting from the first successful logon attempt. This happens behind the scenes seamlessly when every time the user logs in. Essentially we are profiling the individual logon attempt and thus the user eventually. Few usual aspects that are captured as below:

- IP address from where user accesses the application on normal basis
- Type of network request being accessed (home/ enterprise/ cyber café / DMZ, etc...)
- Time of the day usually accessed
- Channel being used like Browser based / Mobile app
- Number of times login/logout in a day
- Login / Password change frequency, incorrect logon attempt

The factors analyzed and captured depend on the individual business needs. More the factors better the security level.

Step 2 - Assess: When next time the user logs in, then user behavior is validated against all the prior stored patterns. If any are different, then appropriate corrective / preventive actions are taken as per the business logic. Typical actions could include one or more of the following –

ISSN 2348 – 7968

- Asking additional user-specific authentication information like the last performed transaction amount / last accessed date
- Randomly requesting the user to enter static confidential personal information like registered mobile number / communication postal pin code/ driving license number. These parameters should have been maintained at the time of account/ user creation.
- Seeking the secondary password (if one available by design)
- Sending a unique one-time key to other secured media of the user like email / mobile and asking to enter that value into the login page.

Step 3 - Decide: Allow the user to logon / access the data / resource if Step 2 is successful. If not deny the access and alert the individual user over a phone call / email.

Step 4 –Profile Enhancement: Update the user-behavior based on the Step 2 and Step 3 for future reference.

VII) ONE-TIME-PASSWORD (OTP) AUTHENTICATION

OTP is becoming much prevalent now, as many of us may be familiar in Banking/ Credit card related transactions. Beauty of OTP is users don't need to remember one more authentication parameter as its generated by System randomly when the particular action/event happens and it is unique to that instance/ action. Thus it's one of the more robust, secured and ease-to-use mechanism.

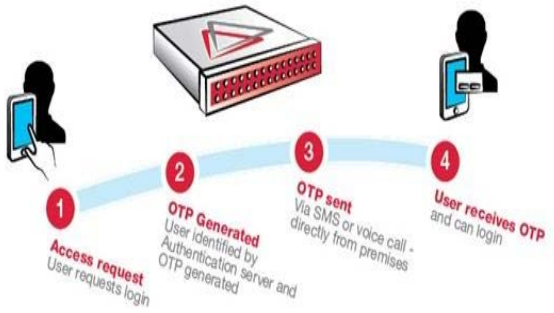

Figure 3: OTP mechanism scenario

In the OTP mechanism, when user is entering the required identification details, say login username/ credit card details appropriately, then system will generate &send the unique password, which is termed as OTP (One-Time-Password), to the registered alternate media like mobile device or e-mail. Then user has to enter the received OTP into the login page, which will be authenticatedsubsequently in the back-end and user logon/ action will be allowed if the OTP matches, else access will be denied. There are few key characteristics of the OTP as listed below:

- OTP should be random for every logon / event transaction; due to the random nature, the OTP is expected to be unique typically.
- Must be auto-generated by back-end system and sent to the registered alternate media (like mobile/ email / another website) just-in-time.
- Has to be time-bound (e.g.: valid for 15 minutes from the time of creation)
- If once used, should be marked expired in the back-end. Even if that attempted logon / action is not successful for whatever reason, the OTP should be expired after one-time use.
- OTP, like any other password, should not be normally visible/ accessible for the back-end system administrators and not stored/ logged as normal readable text; must be stored in encrypted format.

VIII) TWO FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) is much powerful and secured mode of authentication, and has been in use for quite a while in various forms and facets and still evolving. Due to the complexity and secureness involved, the overall cost of this authentication is typically highest when compared to any other mechanism. This security technique tackles and secures users from variety of cyber and hackers threats, including the man-in-the-middle, static password stealers and much more complex cybercrime methods.

In the 2FA mechanism, we need to have the logon username, a standard fixed password as well a variable dynamic password which acts as the second factor of authentication, from which the name Two-factor authentication is derived. This mechanism either follows Time-synchronized one-time passwords or Mathematical-algorithm-based ones. The second factor is created by the back-end system or by another mechanism and verified ultimately by the back-end system. Primary characteristic of the second factor is – it should be random & unique and changing periodically, in other words not predictable by any human user. Thus the strength of authentication is higher.

Much famous 2FA mechanism are RSA authentication tokens from EMC2 Company's RSA division, Thales Security System's SafeSignAuthenticationSystem (SSAS), Entrust Company's IdentityGuard MiniToken.

Figure 4: Two Factor Authentication methodology

ISSN 2348 – 7968

The second factor authentication is usually generated / issued in a separate device called Token. Variety of physical tokens that exist in market include:

- Standalone / Disconnected Tokens: Most common type token. This token device doesn't have any physical / logical connection with the back-end system/ computer. These are typically time-synchronized and sync is set before the token is manufactured and distributed to end- user. RSA tokens are classic example for this category of token devices.
- Smart Card Tokens: This is using the Smart card technology and relatively cheaper. This is used in the Debit/ Credit cards as we might have noticed.
- Mobile Device based Tokens: User's Mobile device can have a software that simulates the token/ receive the second factor authentication from external system. This mechanism is becoming more common as its ease for user, secured and cheaper, as no need to provide an additional token device.

IX) CONCLUSION

Security is an essential system entity to protect and provide appropriate access to the users and provides great privacy if used with right mix of complex techniques and ease-of- use for the end-users. More secured and ease-of-use biological based authentication like face-reader, eyes sensors, and finger print readers may become more predominant in the future web-based-application authentication world thus making things safer, easier and secured.

X) REFERENCES

1) Insecure Trends in Web Technologies, A A Review of Insecure Implementations, Chandrakanth Narreddy White paper
2) An Overview of Different Authentication Methods and Protocols, Authentication Methods, University of OSLO
3) Secure Web Authentication by Multifactor Password a New Approach, Shinde Swapnil K. Patil Yogesh N. Godase Avinash P
4) International Journal of Software and Web Sciences (IJSWS)
5) How to Secure Your Website, IT SECURITY CENTER (ISEC)

Radhakrishnan Subramanian completed Masters in Digital Electronics and Communication Systems from Mysore University in the year 1991. He has worked in ISRO in the area of Satellite Communication. Subsequently he worked in the software industry. For the past six years he is into academics. He works for Saveetha University now. He is pursuing research in the area of Satellite LTE. His interest includes Communication, Embedded Systems and Telecom protocols.