ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Risk Based Multilevel and Multifactor Authentication using Device Registration and Dynamic QR code based OTP Generation

Deepak R. Thorat[1], Sheetal S. Sonawane[2]

PG Student, Department of Computer Engineering, Pune Institute of Computer Technology, Pune, India[1]

Associate Professor, Department of Computer Engineering, Pune Institute of Computer Technology, Pune, India [2]

Abstract: Online and Enterprise resources typically required authentication before user allow to access the sensitive applications and information. Sensitive information generally contains user personal information, transactions, confidential data, etc. Traditional user authentication system used user identifier, Password, Personal Identification Number (PIN), Token code etc. These Systems can't fulfil the current requirement of the user authentication. So that most of the system used multilevel and multifactor authentication mechanism to allow authorized user to get access the sensitive application and information. Recently such multilevel and multifactor security is provided using Risk Based Authentication (RBA) mechanism. The RBA provides access based on Enforcement policy and access decision based on the risk score. Due to which RBA mechanism provides a more secure way to access the sensitive application and information by the user. In this paper, we will propose RBA mechanism based on User's machine specific authentication information and Dynamic Quick Response (QR) code based One Time Password generation for User step Up Authentication.

Keywords: Security, Access Control, Authorization, Risk Based Authentication, One Time Password

I. INTRODUCTION

Current technological revolution leads sensitive application and information security. This mainly includes Banking, Financial, and Enterprise applications. To access such sensitive applications and information, System should not only authenticate the user, but based on the user role and responsibilities authorization has to be done. Such authorization has been done using the multilevel and multi-credential or multifactor authentication [5]. Many times multilevel System provided the highest level of security using multifactor System. Such combination of these two system forms Risk Based Authentication mechanism [1, 2, 3, 6].There have been lots of Systems proposed towards the Risk Based Authentication mechanism. This includes Mouse and Keystroke dynamics [11, 13], Location Based RBA, User Biometrics [4, 13], secrete Question and Answering, etc. In Mouse and Keystroke dynamics based System [11, 13], User needs to follow some specific mouse pattern and enter a static line of words using the keyboard. Such system used user history of mouse and keyboard handling. Users handling vary leads to system fails to authenticate the authorized user. Location based RBA System track user location information based on IP address, GPS, etc. Every time it is not possible to user location exactly. Sometimes users don't want to track location due to privacy. The user Biometric [4, 13] based system required additional device such as Thumb scanner, retina scanner, etc. This leads to extra cost to the user. Secrete question and answering based RBA system fails due to it is associated with user attributes and history. Validation of the user for higher level in RBA System is using User identifiers, Password and PIN.

In the traditional user Identifier can be used to authenticate the user which is easy to trace and spoof. Similarly User Password may be identified using user history, browser cookies, etc. Most of the system assigns a PIN to the user that used to authenticate the user. Basically the PIN is four to eight digit numbers which are used to authenticate the user. Many times this PIN is used as alone or with the other above explained System. When a user registers with any System, System generates the PIN and transfer or displays it to the user. If the PIN is static, user needs to remember the PIN. In such case if the user forgot the PIN, then authorized user can't access the system. The many times PIN can be generated using mathematical function and properties [8, 9, 10] such as Logarithmic, Hash function, etc. Many times users used the same PIN for more than one System, in such case PIN may be stolen by Malicious Parties. Many times users need to provide other information to receive the dynamically generated PIN. In such System, System generates new PIN or token automatically based on user information stored on server side and send it to the user with out of band network [12].

In This paper, Risk Based Multilevel and Multifactor Authentication using Device Registration and Dynamic QR code based OTP Generation System is proposed. It is based on multilevel authentication System with multi-credential values for validation of users. Next paper is organized as follows; Section II defines the mathematical model of the proposed System. Section III defines the proposed idea of the System and Section IV defines the Results and Analysis of the System. Section V defines Conclusion with future enhancement.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

II. RELEVANT MATHEMATICS

Consider S be the System that describes a method to perform user device registration, validation and Dynamic QR code generation. System S consists of two subsystems S1 and S2 respectively, which is given below.it.

A. Device Validation

Below model describes the User device validation. The system assigns the weight to the each user machine specific attributes. When a user registers his device, System stores all machine specific attributes. In future when the user access the System, System calculates the Aggregate weight using the defining attributes. Based on Aggregate weight and Configured weight, System validates the user using calculated Risk as shown in System S_1.

S_1 = {I, O, F, Su, Fa}
Where
I: Input to the system S_1.
O: Output of the system S_1.
F: Set of Functions.
Su: Success of system S_1.
F: Failure of system S_1.

INPUT:
I = {An, Cn, $\boldsymbol{\phi}$}.
An = {a_1, a_2, a_3….a_n}, set of Attribute list.
Cn = {c_1, c_2, c_3….c_n}, set of configured weight for each Attribute.
$\boldsymbol{\phi}$ = Threshold value.

OUTPUT:
O = {Aggregated Weight, Risk score (R)}

FUNCTIONS
F is a set of functions where.
F = {F_1, F_2, F_3}
F_1 is the function to calculate Aggregate Weight
F_1= set of Aggregate Weight to each attribute
F_2 is a function to calculate the Risk Score
F_2: I->R $1 - \frac{\sum Aggregated \quad weig\,ht}{\sum Configured \quad weig\,ht}$

F_3 is a function to validate the user

SUCCESS: $0 \leq R \leq 1$

FAILURE: $0 > R > 1$

In the above System, if $R \leqslant \boldsymbol{\phi}$ user accesses the Sensitive information and application otherwise System validates the user using another mechanism.

B. One Time Password based on Dynamic QR code

System S_2 validates the user in next level using the Time based OTP value which is generated using the dynamic QR code.

S_2= {I, TOTP, F, Su, Fa}
Where
I: Input to the system S_2.
O: Output of the system S_2.
F: Set of functions.
Su: Success of system S_2.
F: Failure of system S_2.
INPUT:
I is the input set such that
I= {URL, SS, T}
SS= {S_1, S_2,…….Sn | Random Number}
URL= User assigns Uniform Resource Locator
T= Throttling Pointer= Largest Number of Attempts
OUTPUT:
O= {QR, OTP}
QR= Dynamically Generated QR code
OTP= Time Based One Time Password
FUNCTIONS:
F is a set of functions where.
F = {F_1, F_2, F_3}
F_1 is a function to generate Dynamic QR code value
F_1: I–>QR
F_2 is a Function to Encryption (EQR) and Decryption (DQR) of QR code
EQR (·): QR → Image
DQR (·): Image → QR
F_3 is a Function to generate Dynamic One Time Password
F_3: StringToNum {truncate ($\gamma \oplus$ QR)}
Where γ is Synchronization Counter

γ = DQR (EQR (OTP)) $\oplus$QR receiver derived random number generate
SUCCESS: OTP generated

FAILURE: Authenticator gives an Error

III. PROPOSED SYSTEM

Every organization defines certain policy to access the sensitive application and information. The main aim of these policies is to authorize user should access the sensitive application and information. There are different mechanisms to implement these policies. RBA is the one of the mechanism to implement these policies so that authorized user should access the critical application. Below System explains in details of RBA using the Device registration and One Time Password generation using the dynamic QR code.Many times users preferred to access sensitive application and information using the user own device. In that case we proposed user's own Device registration and validation mechanism. FIG 1 shows the Architecture diagram of the proposed System. As shown in the FIG 1 whenever user send request to access System, Webserver passed it to the Access Manager for user validation. Access Manger validates the user based on the user specific information stored on the database.

User Specific Information contains user details, user Machine Specific Information. Access Manager decides the user Authentication level to base on the way the user logged in. As an example System assign a lower Authentication level to the user whom login through social networking site than System portal Authentication. Similarly Device Registration has the higher Authentication level than the System portal Authentication.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

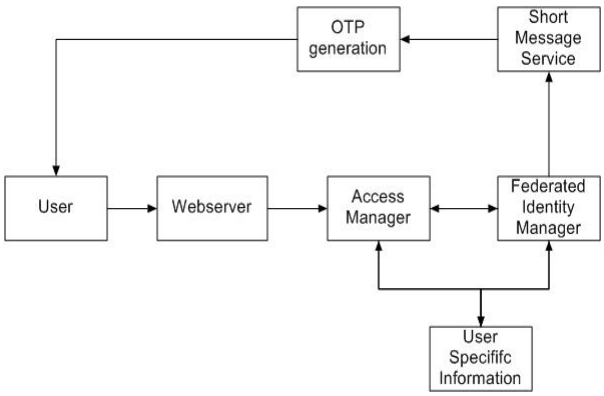

Fig. 1 A simple Architecture Diagram

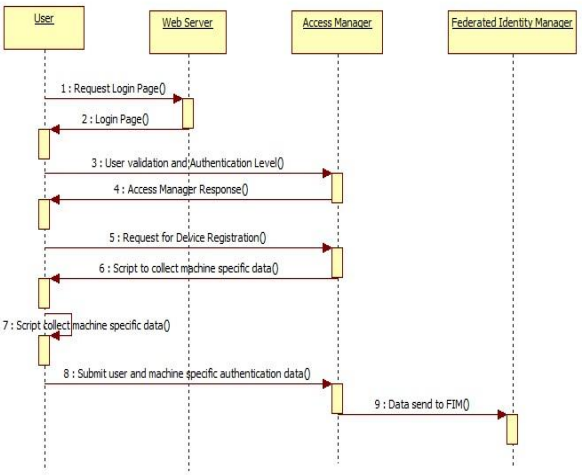

Fig. 2 sequence of events showing User Device Registration

Federated Identity Manager comes into to picture whenever user tries to access the sensitive application and information with the less than required Authentication level defined by the System. In that case validation has to be done using the Federated Identity Manager. A detail of the System is explained as below.

FIG 2 is a diagram showing a sequence of events for logging on a user for the first time to the System. When a user logs into the system, Web Server sends user request to Access Manager which should ask to register device or not? If the user provides the consent to register the device, Access manager sends the scripts using Web Server to the client machine and collects the user Machine Specific Information. Machine Specific Information may include the machine MAC address, IP Address, Browser information, Browser language, user agent, cookies details, screen resolution etc.

This information stored on the server side to validate the user in next logging based on his device properties. In such case Risk Score calculated based on Exact Match, Network or Location Match and Behavioural Match of the System. Some of the attributes of the device have never changed such as the MAC address of the system. In such case if the MAC address of the device exactly matches with the stored MAC address then no need for further validation of user.

In Location matches System needs to compute the location of login session is in the allowed range of the known Location. In the Behavioural match, System needs to compute the risk score based on behaviour of user in last history.

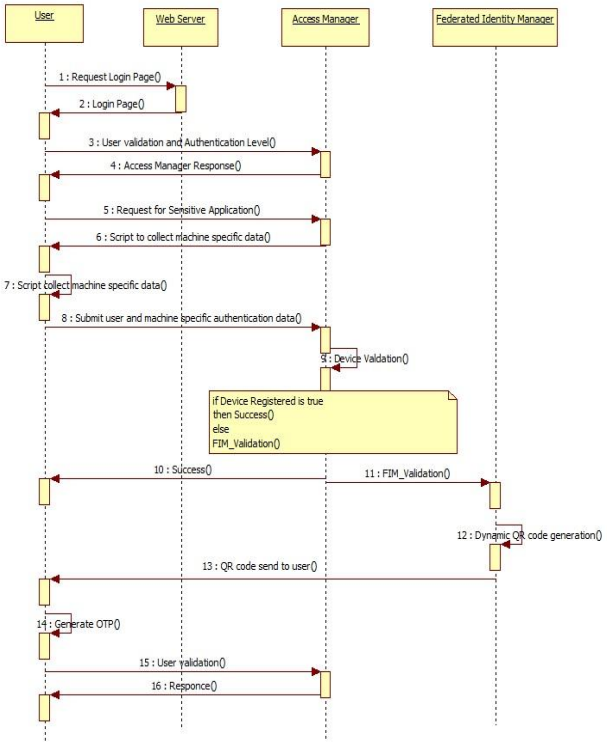

Fig. 3 sequence of events showing Device Validation and QR code generation

In such case cookies characteristics used to validate the user identity. The main aim of the collection of the user machine specific authentication information is even hacker obtained the user credentials for System login and try to access the sensitive application and information, the hacker's machine has different attribute value than the authorized user machine. It results to hacker, whom trying to impersonate the user should not get access the sensitive applications and information.

Validation of the user in next consecutive login is as shown in FIG 3. When next time user tries to access the sensitive application or information, Access manager sends script to access user machine specific information. This information is used to calculate the risk score that used to validate the user. Risk scores calculated using the formula $1 - \frac{\sum Aggregated\ \ weig\ ht}{\sum Configured\ \ weig\ ht}$ If the Risk score is less than the value provided by the System i.e. $\boldsymbol{\phi}$, user gets access to the sensitive application otherwise System used multilevel authentication mechanism based on dynamic Quick Response code.

In multilevel authentication mechanism, further validation of the user has been done using the Federated Identity Manager. The Federated Identity Manager is responsible for the generation of Quick Response Code based on the user attributes. Each user is associated with the QR code which is updated when Access Manager forward request to user validation to the Federated Identity Manager. FIM generate the new QR code and send it to the user using other Out of Band network. QR code, mainly consists two

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

values Uniform Resource Locator (URL) and shared secret between server and client. If the user's shared secretes same for a long time, malicious parties may get access to the sensitive application and information. Therefore Federated Identity Manager generates dynamic QR code every time when user tries to access sensitive application and information using other than his own device. QR code, mainly consists of two attributes manly URL and Shared Secrete (SS).

URL assigns to each user is unique till user is registered with the System. So we randomly change the SS value for user so that the dynamic QR code generated every time in case of user try to access the sensitive application and information using unregistered device. SS value generated using a random number generator algorithm. We will use the Pseudo Random Number generator algorithm to generate the random number with good randomness properties. As the System generate new QR code every time when user tries to access the critical application through other devices. There has needed to send this QR code to the user through the Out of Band Network. We proposed the Short Message Service to transfer the QR code to the User.

Authorization System needs to send the dynamic QR code through the Email server or Messaging system to the user. As we use the Out of Band network [13] to transfer the Dynamic QR code, our System becomes more secure to handle the shared secrets between the user and server. In next step user needs to generate the time based DOTP value by using this QR code and synchronization counter.

One Time Password generator mainly used synchronization counter value and QR code as a shared secret between the user and Authorization system. Dynamic OTP generation takes place in three steps. In first step 20 bytes Massage Authentication code generate by using a HAMAC-SHA-1 function which hashed the QR code and synchronization counter. In next steps Message Authentication code truncated into the 8 byte values.

In next step string to a number convertor function used to generate OTP value. A Function to calculate Dynamic OTP value is shown as DOTP= StringToNum (Truncate (HMAC-SHA1 (γ, QR))). This OTP value used to get access to the sensitive application and information.

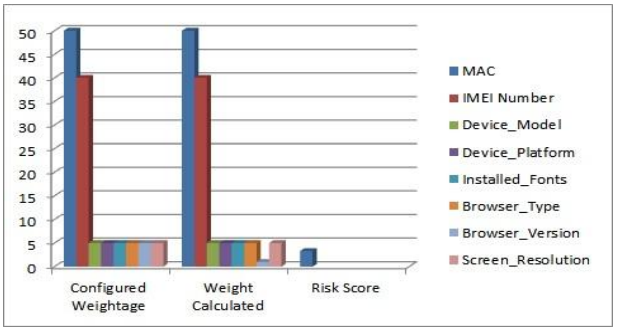

Fig. 4 Graph showing calculated Risk score with device registration

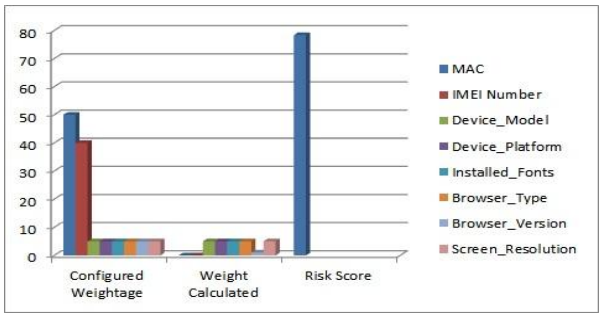

Fig. 5 Graph showing calculated Risk score without device registration

IV. RESULTS AND ANALYSIS

The experimental result of the calculated risk score for device registration and without registration give in FIG 4 and 5. It shows that based on configured weight of each device property risk score of the system changes. The MAC address of the device and IMEI address of the device has assign more configured weight because, it is difficult to change these values by the user. Whenever a user registers his device, system stores the user's device properties. These details used to validate the user authentication when a next time user tries to access sensitive information and application. As shown in FIG 4, risk score value is low due to the exact matching between attribute properties of the device. So the user gets access to the critical application. Similarly FIG 5 shows that the user device attributes does not match with persistent attributes that stored when device registered first time. Due to which the risk score is high and system can't provide access to the user.

V. CONCLUSION

As per the discussion in the last few sections sensitive application and information security becomes the key aspect for every organization. The main aim of the every organization is only authorized user should get access to the sensitive application and information so that minimize the fraud of the transactions, applications. So that in this paper, we proposed the User Specific Authentication information and Dynamic Quick Response code based Authentication System. A user tries to access sensitive information where a simple user ID and password authentication is not sufficient. In such case we propose the user device registration and a fingerprint mechanism to validate the user. Most of the time Users require to access from remote locations that are not trusted and user used other than his own devices such as mobile devices and notebooks. In such case to validate the user, we proposed dynamic QR code based One Time Password generation mechanism. Due to the use of the above two mechanisms we improve security during authentication and authorization of the application. Risk-based access improves the user experience by limiting secondary authentication mechanisms. As we use the Dynamic QR code for validation of users, makes difficult for malicious parties to access the sensitive application and information. It is also immune to different network attacks.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

REFERENCES

[1] Diep N. N., S. Lee, Y.-K. Lee, H.J. Lee, "Contextual Risk-based Access Control", *Security and Management*, pp. 406-412, 2007.

[2] Enokido, T.; Takizawa, M., "Purpose-Based Information Flow Control for Cyber Engineering", IEEE Transactions on Industrial Electronics,Vol. 58, No.6, pp.2216-22225, June 2011.

[3] Bardram, J.E., Kjær, R.E., Pedersen, M.Ø.: Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing. In: Dey, A.K., Schmidt, A., McCarthy, J.F. (eds.) UbiComp 2003. LNCS, vol. 2864, pp. 107–123. Springer, Heidelberg (2003).

[4] H. M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp. 958-961, 2000.

[5] Jae-Jung Kim and Seng-Phil Hong, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[6] Hayashi, E., Das, S., Amini, S., Hong, J., Oakley, I.: CASA: context-aware scalable au-thentication. In: Proceedings of the Ninth Symposium on Usable Privacy and Security, pp. 1–10. ACM, Newcastle (2013)

[7] Kuan-Chieh Liao; Wei-Hsun Lee; Min-Hsuan Sung; Ting-Ching Lin" A One-Time Password Scheme with QR-Code Based on Mobile Phone "INC, IMS and IDC, 2009. NCM '09, Page(s): 2069-2071.

[8] Leslie Lamport, Password Authentiction with insecure communicaton, Communication of the ACM, v.24 n. 11p.770772, Nov. 1981.

[9] M'Raihi D, Bellare M, Hoornaert F, Naccache D, Ranen O (2005) HOTP: An HMAC-Based One-time Password Algorithm. The Internet Society, Network Working Group. RFC4226. Dec. 2005.

[10] M'Raihi D, Machani S, Pei M, Rydell J (2010) TOTP: Time-based One-time Password Algorithm draft-mraihi-totp-timebased-o5.txt. The Internet Society, Network Working Group, April, 2010.

[11] Monrose, F., Rubin, A., "Authentication Via Keystroke Dynamics", In Proc. of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 01-04, 1997, pp. 48-56, 1997.

[12] Ronald Kainda , Ivan Flechais , A. W. Roscoe, Usability and security of out-of-band channels in secure device pairing protocols, Proceedings of the 5th Symposium on Usable Privacy and Security, July 15-17, 2009, Mountain View, California.

[13] Traore I, Woungang I, Obaidat MS, Nakkabi Y, Lai I (2012) Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments. In Proc. of the 4th IEEE Intl. Conference on Digital Home (ICDH 2012), Guangzhou, China, pp.138–145,Nov.Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.