IJCSN International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014
ISSN (Online) : 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

Ameliorate Security by Fifth Factor Authentication

[1] Siva Srinivasa Rao Mothukuri

[1] Information Technology, RVR & JC, Acharya Nagarjuna University
Guntur, Andhra Pradesh, India

Abstract - In modern world, data storage is a major part of assets. Security is only way to protect data assets from thefts. Increase in the technology not only ameliorates the security measures but also meliorates data thefts. To have more security, organizations are concentrating on a place area i.e., data centers, so that no other unauthorized person can enter into security zone. This paper concentrates on how to restrict the access to people in a particular period with having multiple security gateways. As we know there are 4 factors of authentication (password, smart card, biometrics, GPS), In this paper, we discuss another level to add up security in narrowing down to particular time.

Keywords - *Biometrics, GPS, Smart Cards, RFID.*

1. Introduction

Now-a-days, with respect to data, security is considered as a critical aspect. Let us consider a real time example. When valuable items like gold and platinum are left in open area, there is no security for those items. Moreover, there is no proof to find who own those items. In case of data, loss is counted at high rate, since there is no standard proof to pose the ownership. This is due to having incomplete proof that shows the data is owned by someone else. So, in today's world, there is a single point where one can assess the data. To be more secure, we need to follow a set of authentication methods. Out of all types of authentication, four factor authentications hold positive feedback where security is mandatory.

However, four factor authentications also have some vulnerability. If a person enters restricted area at particular time say at 3:00 am and tries to hack systems with any user access then having these many levels of security has no use. Here comes the next level of security, if we take time as a factor of authentication then this could possibly have good effect for securing the data like sending an email to necessary people.

2. History (Four factors of authentication)

Four factor authentication is a methodology of having series of different authentications over a single or multiple secured data units.

2.1. First Factor (Object, you can remember)

This is a common authentication method used by many users in the world. Pass phrase, a set of letters, is used for authenticating users.

Example: password, 1234567890, P@ssw0rd, G6y$*g#SQ

However, the drawback is key-loggers records every keystroke and pass to attacker.

2.2. Second Factor (Object, you possess)

In this method, a special authorized object say, some type of card, is given to users. Authentication can be done in different ways. One such method is RFID where all the details are preloaded into database. Whenever person swipes the card, he/she will get access to particular restricted area for performing their job.

Example: Smart Card, SIM card.

2.3. Third Factor (In-build, what you have)

This method, most often deals with the security authentications a man possesses uniquely like, fingerprints, iris, face. These features differ from person to person. In addition, no one else can gain access other than authorized person. This is an added advantage.

Example: Fingerprint, Iris, Facial passwords.

2.4. Fourth Factor (Place, you access)

To delineate, this method is used rarely only for specific purposes like military zones. This gives security by taking security coordinates through GPS and location of ISP servers from where the person is accessing the account. Likewise, this method gives most security when attacker is outside restricted area by not allowing him to access the data.

Example: Military Zones.

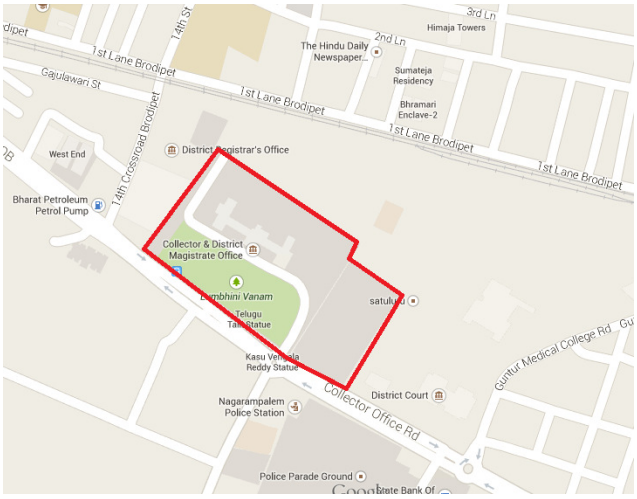

Figure 1: Illustrating region of accessible area

Above figure shows the radius of accessible area through which we can access data and authenticated. Nonetheless, if attacker is working in the military zone, then he can gain access to all the servers. Having four security authentications can be useless.

3. Time Authentication Criteria

Now, this is the time to discuss the actual area if four authentications got compromised with the attacks. Considering time as authentication criteria, there are two ways for inducing security.

3.1 Unusual Activity

Attacker can have a good opportunity to attack the system only when there are no people around him observing in person. No attacker tries to make him visible to world, to be fortunate; person tries to attack at unusual time. For example, if a person working hours are between 9:00 AM to 6:00 PM. He will attack the system after 6:00PM since he has access to all the systems. It becomes very easy to penetrate into system.

Here comes our security measure by adding time as a factor of authentication. If a person log's to one's system then authentication protocols sends a series of alarms to higher authorities and security experts. They can remotely seal off access to servers or slowdown the process which makes him to be caught with evidence.

3.2 Furthermore Than General Time Activity

But the above stated method alone can't solve the problem. If attacker is smart enough, then he can accomplish his task within few hours. Organizations face difficult problem with these kind of attackers. This is where, second method comes into picture. This method will logs user activity time. For instance; if a person accesses his account for 4 hours daily, but when he uses his account more than 6 hours a particular day, then he needs to be suspected. Even though this seems to be ridicules i.e., suspecting every person who work at more than usual time period; we can't compromise on the security, as data is most important and valuable. Alarm will be raised for security team showing the list of activities that are performed in-between. Combining above two methods, narrows down the access levels to the data and restricts for only certain time period. Even though, if a person needs to work in unusual hours, he can work just by the approval from the supervisor.

4. Implementation

The implementation of these levels of security depends on integrity of the data. For having better security we use hashing techniques to prevent data to be shown as plain text even to employees who work.

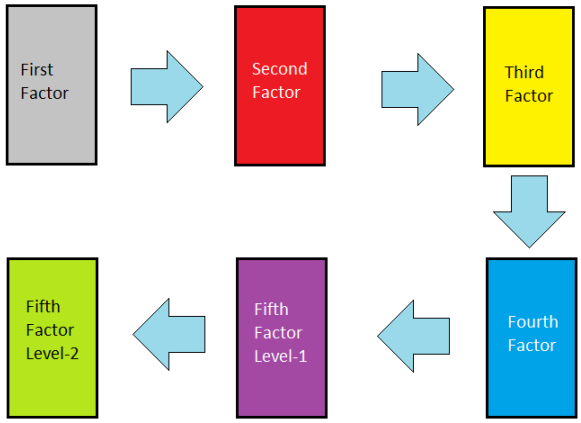

Figure 2: shows levels involved in authentication.

4.1. Algorithm for First Factor Authentication

Algorithm :: First_Factor
Preconditions :: User must be already registered
Input :: String from user
Output :: Access to Second Level of Authentication

Function First_Factor
Start:
Show User interface area to accept set of letters meeting specific precondition
Add security hashing techniques (MD5, SHA512)

```
        Check with the user details present already in the database.
        If valid authorization
                Grant access to Second factor authentication
        Else
                Deny access, count number of attempts.
                If count is greater than specific limit
                        Raise alarm as security incident
                Endif
        Endif
End
```

4.2. Algorithm for Second Factor Authentication

```
Algorithm :: Second_Factor
Preconditions :: User must be already registered & must pass First level of security.
Input :: Acceptable smartcard
Output :: Access to Third Level of Authentication

Function Second_Factor
Start:
        Place smart card in contact with the smartcard reader (RFID Tags, NFC)
        Add security hashing techniques (MD5, SHA512)
        Check with the user details present already in the database.
        If valid authorization
                Grant access to Third factor authentication
        Else
                Deny access, count number of attempts.
                If count is greater than specific limit
                        Raise alarm as security incident
                Endif
        Endif
End
```

4.3. Algorithm for Third Factor Authentication

```
Algorithm: Third_Factor
Preconditions :: User must be already registered & must pass Second level of security
Input :: Acceptable biometrics (Face, Iris, Fingerprint)
Output :: Access to Fourth Level of Authentication

Function Fourth_Factor
Start:
        Accept biometrics of a person through reader
        Add security hashing techniques (MD5, SHA512)
        Check with the user details present already in the database.
        If valid authorization
                Grant access to Fourth factor authentication
        Else
                Deny access, count number of attempts.
                If count is greater than specific limit
                        Raise alarm as security incident
                Endif
        Endif
End
```

4.4. Algorithm for Fourth Factor Authentication

```
Algorithm :: Fourth_Factor
Preconditions :: User must be already registered & must pass level 3 authentication.
Input :: User must be at acceptable region
Output :: Access to Fifth Level of Authentication

Function Fourth_Factor
Start:
        User must grant access to GPS Device for tracking location.
        Input co-ordinates from GPS.
        Add security hashing techniques (MD5, SHA512)
        Check with the user location details.
        If valid authorization
                Grant access to Fifth factor authentication
        Else
                Deny access, count number of attempts.
                If count is greater than specific limit
                        Raise alarm as security incident
                Endif
        Endif
End
```

4.5. Algorithm for Fifth Factor Authentication

4.5.1. Algorithm for Unusual activity

```
Algorithm :: Fifth_Factor_level_1
Preconditions :: User must be already registered & must pass level 4 authentication & All times must be in sync
Input :: User must be at acceptable time period
Output :: Access for Fifth Factor level-2.

Function Fifth_Factor_level_1
Start:
        Access time period from eclectic sources
                .1 RTC
                .2 Sever time
                .3 Client time
        Check for sync of time
        If No
                Raise alarm to administrative unit for right settings.
                Deny access to the users.
        Else
        Add security hashing techniques (MD5, SHA512)
        Check all times with respective to working hours
        If valid authorization
                Grant access to Fifth factor level-2 authorization
        Else
                Deny access
                Raise alarm as security incident
                Report to higher authorities and request access
                If access granted
                        Invoke assess to Fifth factor level-2 authentication
                Else
                        Deny the access
                        If user retries
                                Deny the access and process it as unauthorized access with locking user account
                        Endif
                Endif
        Endif
End
```

4.5.2. Algorithm for Furthermore than general activity time.

Algorithm :: Fifth_Factor_level_2
Preconditions :: User must be already registered & must pass level 5_1 authentication.
Input :: User must be at acceptable time.
Output :: Access to Data.

```
Function Fifth_Factor_level_2
Start:
        Record every activities and time period duration for every
user.
        Add security hashing techniques (MD5, SHA512)
        If authenticated user enters into unusual time period
                Monitor all activities along with the time
period.
                If User crosses daily activity time period
                        Send notification to higher
authorities
                                If still this continues more than
                                                grace period
                                        Raise alarm, request for
                                                extension of access
                                If valid authorization
                                        Grant access to Data.
                                Else
                                        Deny the access
                                        If user retries
                                                Deny the
                                        access and process it as
                                                unauthorized access
                                        with locking user account
                                        Endif
                                Endif
                                Endif
                                Endif
                Endif
        Endif
End
```

4. Conclusion

We can't regret just simply loosing data due to lack of security. Having a single level of authentication is not that simple to protect confidential data. To have furthermore security, this paper amplifies the levels of security by adding one more level i.e. fifth level. As of now these levels of security is only important to high level classified areas where data loss is considerable to degrade national and economical pride of a country. At this point, fifth factor authentication is more important and plays a good role in understanding and remotely shutting down the access to users who tries to attack.

References

[1] Eldefrawy, M.H.,Alghathbar, K. ; Khan, M.K. "OTP-Based Two-Factor Authentication Using Mobile Phones", "Information Technology: New Generations (ITNG), 2011 Eighth International Conference", IEEE

[2] Jing-Chiou Liou,Bhashyam, S., "A feasible and cost effective two-factor authentication for online transactions", "Software Engineering and Data Mining (SEDM), 2010 2nd International Conference", IEEE

[3] Xinyi Huang, Yang Xiang ; Chonka, A. ; Jianying Zhou ; Deng, R.H; "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems", "Parallel and Distributed Systems, IEEE Transactions on (Volume:22 , Issue: 8) Biometrics Compendium, IEEE", IEEE

[4] Mathew, H.M. Raj, S.B.E. ; Gundapu, P.S.J. ; Angeline, S.J.F; "An improved three-factor authentication scheme using smart card with biometric privacy protection, "Electronics Computer Technology (ICECT)", 2011 3rd International Conference on (Volume:3)", IEEE

[5] Sanghoon Jeon; Four-factor verification methodology for entity authentication assurance, "Information Science and Applications (ICISA), 2011 International Conference", IEEE

Siva Srinivasa Rao Mothukuri born in Guntur, in the year 1991. Acquired bachelor's degree from Acharya Nagarjuna University in 2012, also Certified in Ethical Hacking. Worked as Assistant Professor in R.V.R & J.C College of Engineering. Currently working as ASE in Tata Consultancy Services (TCS).