Token Based Authentication using Mobile Phone

Parekh Tanvi
SIMS, Indore
tanvi.parekh@sims-indore.com

Gawshinde Sonal
SSSIST, Indore
sonal209@yahoo.co.in

Sharma Mayank Kumar
IET-DAVV, Indore
leomayank @yahoo.com

Abstract: Digital identity is the key representation of user and getting most crucial subject for information security. The password based authentication is weak solution and no longer adequate. User select static password which is easy to guess and remember, relevant information or common for all authentication process. This simplicity makes weak authentication scheme; as so far, static passwords are known as easiest target for attackers. Further, Security Token based runtime interaction could extend the strength of authentication control. Security tokens can be used for strong authentication but inconvenient for user and costly for the service providers. To avoid the user inconvenient and extra cost mobile phone is an emerging alternative. These papers comprise the study of various digital identification schemes and give motivation to integrate mobile token. In order to establish standard for mobile token, work starts with the review of current schemes and explores the security architecture for strong authentication with mobile token. Password algorithm is derived to generate dynamic password for token authentication. Thereafter explore various authentication mechanisms to implement mobile token on different prospective. At the end, it describes the various test cases and evolutionary result of various attacks on suggested schemes.

Keywords: Authentication, Dynamic Password, Mobile Token

I. INTRODUCTION

The enrichment of Internet, business solutions, online services, government portals, social networking sites, information portals are replacing the traditional way of working and the communication. Authentication helps to establish proof of identity. These are the way to prove that, the user, trying to access the account is authentic. [1] Most of the solutions comprise personal details, operational credits, certified information or services, which requisite digital identification for making proof of authenticity. Today, three universally recognized philosophy are used for digital identification: what we know (i.e. password), what we have (i.e. Tokens and cards) and universal identity (i.e. Biometric characteristics). In order to extend authentication strength and make work more flexible and strong, recent work has been done on the field of virtual identification approach (i.e. virtual token). These virtual tokens not only help to reduce extra cost but also overcome the problem of remembrance and keeping the token. [5]

Static passwords are known as one of the easier target for attackers; further biometric readers are very costly and not feasible for web applications. Security tokens are great way to make strong authentication and ascertain runtime interaction to increase identification strength. The resistance behind security token is, cost, server synchronization and worry to carry multiple tokens for multiple solutions. In advance, we assume that every user has mobile phone. Accordingly, to address the strong authentication and replace security token, mobile phones could be great solution. These solutions make cheaper and flexible strong authentication for user as well as for the service provider and reduces worry of carrying extra hardware for identification only.

In this paper we have used mobile phone as security token and proposed an authentication model for strong digital identification. To increase randomness paper demonstrates a Password algorithm to calculate dynamic password for digital identification. Paper also includes various mechanisms to implement mobile token. Work reveals that, the system consists a sms gateway or GSM modem to send dynamic password via SMS and verify to check digital identification.

II. BACKGROUND

The concept of security is not only important but mandatory to the success of digital solution. There is no clear definition for strong authentication. Strong authentication is an approach to extend security level and try to achieve security requirement. [5] Security is not only meant for buying, exchanging or selling products or services but also important to maintain decency of information and system. It is also important to establish network and communication between PCs, servers, application and mobiles phones. Identification and authorization is the key requirement of security[8]. Currently, solutions rely on "static password" to establish trust and verify user authenticity [1] User chooses password, which is easy to guess and remember, relevant information or common for all authentication process. Sometime user derive password from what they have in there mind. Strong password (i.e. @my$sit13*) is tiresome to remember and demands hard time to handle it. People like to store passwords into diary or take common password for all; these are susceptible for password leek. Weak authentication scheme may cause to exploit access level vulnerability and liable for information leek. Furthermore, Attack methods are generally unique to the targeted application or system, and common techniques can be used. Attacker have multiple option to steel passwords like spoofing, surfing, eavesdropping, brute forcing , predicting, profile study and many more. These study conclude that, work demand an interactive security process which should be variant in each identification.

Token based authentication is the mechanism, which requires hardware interaction of user for completion of authentication process. Usually this hardware consist software usage to generate password and synchronized with server application. When user demand to give digital identification it uses the password displayed on token. Security token used time stamp to integrate variation on password and password changes with time. Security token uses 3 digit of timestamp, as so far dynamic password would exist for 10 minutes. This is known as one time password, no longer to use. Limited time and

978-0-7695-4437-3/11 $26.00 © 2011 IEEE
DOI 10.1109/CSNT.2011.24

complex algorithm create cumbersomeness for the attackers and unauthorized user should not be able to predict the next password in the sequence. Security tokens are commercial security devices and various security tokens on different algorithms exist in the market. Security token algorithm uses seed value and timestamp. Seed value increases complexity and help to generate pseudorandom number. It also consist time stamp synchronized with server time to introduce variation in password sequence. At the time of configuration security factors has to be configured on application server also. These paradigms give connectionless model to generate dynamic password and create strong authentication [1].

Nevertheless, security tokens extend the authentication strength but relatively its high cost and central authentication server for deployment increases installation cost. The study of security token paradigm conclude that hardware authentication token cost vary from $10 to $50. [7] Further there reader cost is very high and can't be easily affordable. Consider the case study of Bank of America, they begun to provide security token to its 14 million customers for digital identification. [9][10] Where minimum investment cost for security token was $140 million when they use cheapest security token. These make the worry about to look out another security option for strong authentication. Further, The National bank of Dubai made compulsory for commercial customers and optional for personal customers to obtain tokens. [9] Another key aspects of security token is, not only used by banking industry but also used in ERP system for employee login and digital verification (i.e. Merrill lynch) [9][11]. From the recent study, work states that use of security token can be very costly for organization. Million of users require million of token and service provider has to bear this cost. Furthermore they have to arrange training program to use and maintain customer support. Another major problem is to always carry security token. If a user has multiple accounts in multiple organizations, user has to carry and maintain multiple securities token. The major inconvenience for user is to carry multiple token for multiple applications. In case of stolen and lost who will bear the token cost it is also another management issue. [9][10][11]

These paper addresses the mobile phone as emerging alternative of security token to not only reduce cost but also give generalize solution to replace and deploy the mobile phone instead security tokens. Work also address that this is not only made for web application or ERP system but it can also use to establish identification in WLAN or PLAN using Bluetooth or Wi-Fi.

III. AUTHENTICATION ARCHITECTURE

In Figure 1 the general overview of strong authentication using mobile phones is shown. It consists of the following elements:

1. User is the key element; wants to get access of application and connect with application or node with any network technology.
2. Password algorithm is the proposed algorithm design to generate dynamic password for each digital identification process.
3. The GSM server or SMS gateway help to generate SMS to send dynamic password to the user.
4. Visitor password register (VPR) is a temporary register used to store username and dynamic password for current session.

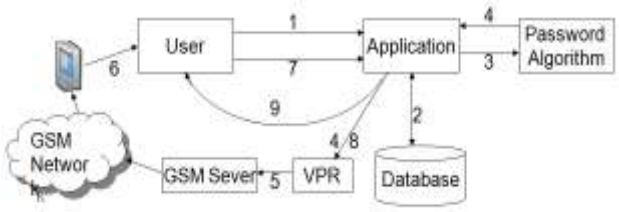

Figure 1, Security architecture for strong authentication

Through this paper we address the overview of token based strong authentication. The sequence of events during the strong authentication is as follow:

1. The user makes a URL request and sends its general identity (i.e. user id & static password) to the application server.
2. Application server will look out user's existence from database and find its authorization.
3. Thereafter, it sends password request & static password to the password algorithm to generate dynamic password for particular user. By taking seed value, timestamp, date and static password, algorithm generates a 24 bit (8digit) dynamic password for digital identification.
4. Now application will store this dynamic password into VPR.
5. Thereafter server send dynamic password to the user via GSM modem/SMS gateway.
6. Afterwords, user retrieves the dynamic password from mobile phone.
7. Then it gives identification request with user name and dynamic password.
8. Now, server verifies the given password with stored one form VPR.
9. After getting positive verification, access would be granted

Because, algorithm is taking time as key element, it would change password after 60 seconds. This is the very small time duration to retrieve and supply digital identification. Another aspect is, on verification time system has to once again calculate password, which increase the server overhead. To overcome these problem servers maintain VPR known as visitor password register. This register is a temporary register who maintain the individual password to particular user. Permanent entry of password may create vulnerability for replay attack. Session time out helps to update VPR after every minute and reduce this vulnerability. After every 1 minute system automatically deletes prior expired dynamic password. [11] This 3 minute session time is derived from practical experience of SMS delivery, reading and filling the dynamic password.

IV. MECHANISM FOR TOKEN AUTHENTICATION

In this paper we proposed general authentication architecture for mobile phone authentication. Strong authentication requisites mechanisms to implement mobile token as security token. These are an attempt to overcome cost and effort for strong authentication with security token services. The proposed system can implement following mechanism.

SMS Based Dynamic Password:

In this approach user send user id and 4 digit static passwords to the server to retrieve dynamic password. Server verifies the request as of user details and forwards it to password algorithm for generation of dynamic password. By helping static password, password algorithm generates a unique dynamic password for individual user. Thereafter, system stores it to VPR with user id for current session and sends it to user via SMS. Now, user has to submit this dynamic password with user id to gain application access. System verify requested password with stored one and redirect to main application access. Because VPR store dynamic password for verification, may be vulnerable for replay attack. To overcome it, we purposed a session time but VPR is updating in every instance of minute, we decide to make session time for every entry. The VPR session time out is 3 minutes and on every minute system run updating service which deletes the outdated value from VPR. In simple words, complete life of dynamic password is 3 minutes.

SIM Based Authentication:

It is a scheme where both dynamic password request and response done through SMS. This proposed mechanism use IMSI number, which are unique to each mobile phone and use to identify the device. IMSI number is stored into SIM card inserted into mobile phone. This number is also stored into server database with user details

In order to gain application access, user sends 4 digit static passwords with registered SIM to the application server via SMS. Thereafter, server detect its IMSI number and retrieve static password from contain. Now, server detects the existence of IMSI number in user details and forwards the static password to password algorithm. Thereafter, password algorithm return 24 bits dynamic password to application server, which store into VPR and send it to requested SIM via SMS. Now, user gives user id and dynamic password and gain application access.

Second approach is more secure and authentic then first one because here we verify the requested SIM identification along with static password. But this mechanism also increases the implementation cost and complexity because application server also has to detect IMSI number and read the requested number.

In order to be able to understand the sequence of multiple events into both mechanisms we develop a general sequence diagram shown in figure 2.

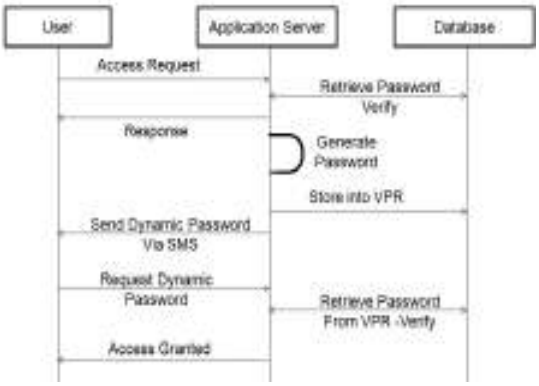

Figure 2, Strong Authentication using Mobile phone

V. PASSWORD ALGORITHM

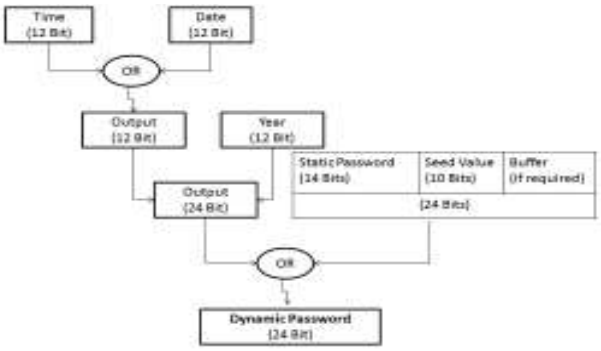

Figure 3, Password Algorithm

In order to secure the system, dynamic password should be hard to guess, retrieve and untraceable. Therefore, we proposed a strong password algorithm to generate dynamic password. This not only help to generate password but also able to introduce variation into two consecutive outcomes. In the proposed algorithm, following factors has been chosen to generate 24 bit dynamic password.

Static password: This is 4 digit (max. 14 Bits) predefined values, help to generate outcome for each individual request.

Date & month: Makes the outcome unique for the particular date of the year.

Year: Makes the outcome unique for the year.

Seed value: To introduce randomness in the outcome sequence through server and making hard to guess for attackers.

Buffer: Fill 0 before the start bit (if required) would help to make complete string of 24 bits.

The following steps would be used to generate execute the proposed algorithm.

Step 1: System will retrieve server current date (dd: mm) and time (hr: mm) and perform OR operation to generate 12 bit outcome.

Step 2: System will concatenate this 12 bit outcome with current year (12 bit) and make 24 bit string.

Step 3: Thereafter, System will use static password value to make password for individual user. System will concatenate this 14 bit value with 10 bit seed (pseudorandom number) and develop 24 bit string.

Step4: If the string size is less than 24 bit, buffer bit would be added to frame 24 bit string.

Step 5: Now, System would again perform OR operation on the above 24 bit outcomes and generate 8 digits (24 bit) dynamic password. In these proposed password algorithm we chose time, date and year to make unique value for the particular instance of year. 4 digit Static passwords would help to generate a unique string for each individual request. Because Time and date is known by everyone, Seed value would help to introduce randomness for each outcome. Due to this entire factor generated password would be very unique and very hard to trace and predict.

VI. EXPERIMENTAL RESULTS

This section presents experimental results from a prototype implementation of proposed mechanism. Table 1 show the comparative result of security token and mobile phones on different parameters. An employee system was implemented using java. SMS gateway was hired for sending the dynamic

password to the user. Each SMS cost conclude into form of 03 paisa/ sms. The smslib API was used to include SMS service with the application. Mysql 5.0 was used to develop VPR and user database. The complete application was deployed into Linux based web server and tested with 1400 employee database. More than 8000 times user request was sending on different time and date of weak and finds that each time; generated password was different due to different time and date. Furthermore 3 minute session time increase the security level and creates unwieldiness for session hijacking and replay attack. To check the repetition of the password as prototype model for password algorithm was made and generate more than 1000 dynamic password. A static password array was created to consist more than 1000 passwords. Prototype model generates more than 1000 dynamic password with uniqueness.

The study of raw output during model execution, we observed that, seed value introduces great randomness, when different user has same static password and they request on same time on same date.

Further, this evaluation addresses the comparative result between security token and mobile phones. This comparison made through the evaluation of proposed model and mechanism and analysis and study of security token and mobile phones. Parameters are the major security properties addressed from this paper.

Parameter	**Security Token**	**Mobile Phone**
Extra Cost	$10 to $50 / token	Not Applicable
Power life	Non Chargeable Battery required	Chargeable Battery required
Security	Single Level Approach	Multilevel approach
Hardware Identification	Infeasible	Feasible
Server Synchronization	Mandatory	Not Mandatory
Multi Application use	Infeasible	Feasible
Eavesdropping	Infeasible	Feasible
Brute force Attack	Rarely Possible	Rarely Possible
Man in middle attack	Infeasible	Very complex
Session Hijacking	Rarely Feasible	Rarely Feasible

Table 1 Comparison of two factor Authentication

VII. CONCLUSION

Security is the mandatory key element to get success of any digital solution. Authentication is the way to prove that; the user, trying to access the account is authentic? This paper explores the possibilities to use of mobile phone instead of security tokens for strong authentication. Static password is no longer secure and easily vulnerable for attackers. Security token can be easily extending the authentication strength but extra cost, single use and server synchronization become most shortcoming issues. Further, hardware token is given to each user for the respective account which increases the number of carried tokens and the cost. For the manufacturing and maintaining them, has become a burden on both the client and organization. As we know that most of the people do carry mobile phone, work proposed authentication architecture to replace security token with mobile phones and to introduce the dynamic interaction on demand. To generate dynamic password and to increase the randomness in the sequence, we proposed a password algorithm generate 24 bit (8 digits) dynamic password for each request. Proposed mechanism gives the standard to implement mobile phone for two factor authentication. Both mechanism uses GSM gateway to send dynamic password via SMS. No doubt, it also includes the small cost which is affordable for the strong authentication.

Future development includes more flexible and strong mechanism without embedding hardware (i.e. Virtual token). Further proposed approach can also be extendible for Bluetooth, WI-Fi, WLAN, and WPAN for two factor authentication with dynamic password generation approach.

REFERENCES

1. Fadi Aloul, Syed Zahidi, Wassim El-Hajj *"Two Factor Authentication Using Mobile Phones"* proceeding of 978-1-4244-3806-8/0 IEEE Conference in 2009.
2. SIMSON L. GARFINKEL *"Email-Based Identification and Authentication: An Alternative to PKI?"* published by The IEEE Computer Society proceeding 1540-7993/03 in 2003.
3. Ghassan Kbar "*Wireless Network Token-Based Fast Authentication"* published in proceeding of 17th International Conference on Telecommunication 978-1-4244-5247-7/09 in 2010.
4. Sharma M.K., Gawshinde S., Parekh T., "Values of Authentication in E-Business" published in proceeding of 1st International Conference in 2011.
5. Do van Thanh, Ivar Jorstad, Tore Jenvik *"Strong Authentication with mobile phone as token"* Proceeding of 978-1-4244-5113-5/09 IEEE Conference in 2009.
6. Haidong Xia, Jos´e Brustoloni "*Virtual Prepaid Tokens for Wi-Fi Hotspot Access*" Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) 0742-1303-in 2004.
7. Hristo Bojinov, Dan Boneh *"Mobile Token-Based Authentication on a Budget" in Proceeding ACM 978-1-4503-0649-2 in 2010.*
8. L. E. Sebola and W.T. Penzhorn *"A Secure Mobile Commerce System for the Vending of Prepaid Electricity Tokens".*
9. D. Ilett, "*US Bank Gives Two-Factor Authentication to Millions of Customers*" 2005.
10. A. Herzberg, "*Payments and Banking with Mobile Personal Device*" Communications of the ACM, 46(5), 53-58, May 2003.
11. "*RSA Security Selected by National Bank of Abu Dhabi to ProtectvOnline Banking Customers*" 2005 Available at http:// www.rsa.com/press reease.aspx: id=6092.