Online Applications Using Strong Authentication with OTP Grid Cards

Bayalagmaa Davaanaym)
Department of Professional
Soyol Erdem University
Ulaanbaatar,48/88,Mongolia
E-mail: bayalag2007@yahoo.com

***Abstract*— Last days several technologies are considered grow-up enough to be a new tool for user authentication in the accessible network system. The One-Time Password (OTP) authentication protocol is an fugacious password that can be used as a multi-factor authentication method when secure authentication is needed an user by a server .**

Focusing on techniques that are used to carry out strong authentication for online application user identities and improve grid card security, this paper aims to obtain a wide range view of strong user authentication by examining its conceptions, implementation approaches, and challenges/additional concerns at the architectural section. It discusses effective solution approaches, overall architecture models, and developments. Authentication system over grid card allows you to change the consideration and define the entropy of a card and its strength. Grid cards also may be set to expire with greater recurrence that requiring the issuance of new cards — to increase security.

Keywords—One time password, grid card authentication

I. INTRODUCTION

Passwords as a means of authentication have long reached their expiry date. Web-based user-authentication systems without compromising usability and ubiquity, when the Internet is accessed mostly through a browser that has limited access to the client environment and hardware devices. The major of typical solution reaches that are used today involve, in more generalized terms, various forms of enhanced shared-secret and multifactor authentication.

Enhanced shared-secret authentication refers to extensions of conventional knowledge-based (single-factor) authentication—for example, additional passwords, site keys, preregistered graphical icons to support mutual authentication, challenge-response, randomized code selections that are based on input patterns, CAPTCHA, and so on.

Multifactor authentication refers to a compound implementation of two or more classes of human-authentication factors: Something known to only the user—Knowledge-based (for example, password, pass phrase, shared secrets, account details and transaction history, PIN, CAPTCHA, and so on).

Something held by only the user—Possession-based (for example, security token, smart card, shared soft tokens, mobile device, and so on).

Something inherent to only the user—Biological or behavior biometric traits (for example, facial recognition, fingerprint, voice recognition, keystroke dynamics, signature, and so on).

In practice, however, there is a wealth of implementations, methods, and permutations of them—all with varying trade-offs in terms of cost, complexity, usability, and security.

It is standard practice to achieve strong authentication by requiring the communicating party to provide two different pieces of authentication of different types: in this case these are the user password (something known) and the one-time password (something possessed).

In Mongolia, online banking and online services are increasing. Online banking (or Internet banking) that allows customers to conduct financial transactions on a secure website. However, with increased convenience, the threats of online banking fraud have also become a greater concern. Customer confidence and loyalty to a bank with online banking services depend greatly on the protection against banking fraud and identity theft.

TABLE I. MONGOLIAN MAJOR ONLINE BANKS PASSWORD COMPARISON

Banks Name	Protection passwords type			
	OTP (HW)	PKI (HW)	Graphical passwords	Password
TDB	*			
KHAN BANK				*
TURIIN BANK			*	*
GOLOMT BANK	*			
HAS BANK	*			

From Table 1, we can see that major Mongolian banks secure their customers with single password authentication.

But Most of the banks are single password authentication is still in use, it by itself is not considered secure enough for online banking in Mongolia.

Goal of this paper that introduce a OTP grid card system using salt passwords and improve an online applications secure in Mongolia. The grid card is functionally equivalent to the electronic tokens commonly used for applications such as online banking.

Chapter 2 of this study explains the grid card authentication related study, and chapter 3 presents a password key creation method through extraction of grid card with OTP. Grid card authentication is strong authentication function, it can create temporary one time password keys. Chapter 4 carries out a simulation adopting the presented one time password key using grid card algorithm, and lastly, draws a conclusion.

II. RELATED WORKS

A. *Grid card authentication*

The multi-factor authentication system requires a password, plus the grid that's often printed on the back of a special card and salt. When a user logs in using their ID and password , they are prompted for a random cell in the grid. The user then enters the correct combination of numbers and letters in that cell and is granted access.

Each grid card is unique and carries a serial number, so every user can be uniquely identified and authenticated. Each time a user is asked to authenticate they are presented with a different challenge requiring them to validate via a different set of grid coordinates. The coordinate request changes for each authentication challenge. In this scenario, the challenge presents the user with coordinates such as B2, F5 and J4. The user refers to their unique grid card to provide the information from the requested cells: 18, H1, X8.

Challenge Generation Algorithms

After enabling grid authentication, Authentication system allows you to choose between two challenge-generation algorithms. Random Challenge algorithm (default) picks cells randomly when creating a challenge. The process for creating a challenge does not depend on previous challenges. Random Challenge algorithm that choose DRBG. Deterministic Random Bit Generators (also known as Pseudo Random Number Generators – PRNGs) take input (a seed) from either the noise source(s) or the conditioning step and produce outputs of random values

Least-Used Cells Challenge

This algorithm uses one or more least-used cells (set in policy) in every challenge. By generating challenges using the least-used cells from a user's grid, it becomes more difficult for an attacker who has previously viewed some successful authentications to correctly respond to the challenge.

B. *One Time Password*

One Time Password (OTP) is a password system where passwords can only be used once, and the user has to be authenticated with a new password key each time. It is a password key creation method that makes it extremely difficult to predict the next password key based on the current password. A new password key is created in its own device constantly after a set period of time and the user has to enter a new password every time he or she uses the system, so it prevents exposure of the user's password due to hacking or the user's mistake. OTP has much stronger security because the user has to enter a newly created password key even if his or password is exposed. Most OTPs' password key creation algorithms are based on one-way functions. For example, S/Key systems (RFC1760) in almost all UNIX OS use such functions. The OTP is standardized by the IETF, and standardized again by verification related companies, and the RSA and OATH are carrying out the most competitive standardizations.

III. CREATION OF PASWORD KEYS USING GRID CARD

Normally when a user requests authentication, even after first contact, certain important services confirm passwords again. However, as explained above, the existing password system has many weaknesses, and a solution for this is one time password mechanism.

The elements of one time password mechanism are a token included in a security/password algorithm or one time password key creating device, a authentication server and a authentication client. Since the one time password mechanism is a program, it is programmed to be random, but the randomness breaks after a certain period of time and passwords become predictable so one time password mechanisms have the disadvantage of having to exchange OTP modules after a certain period of time.

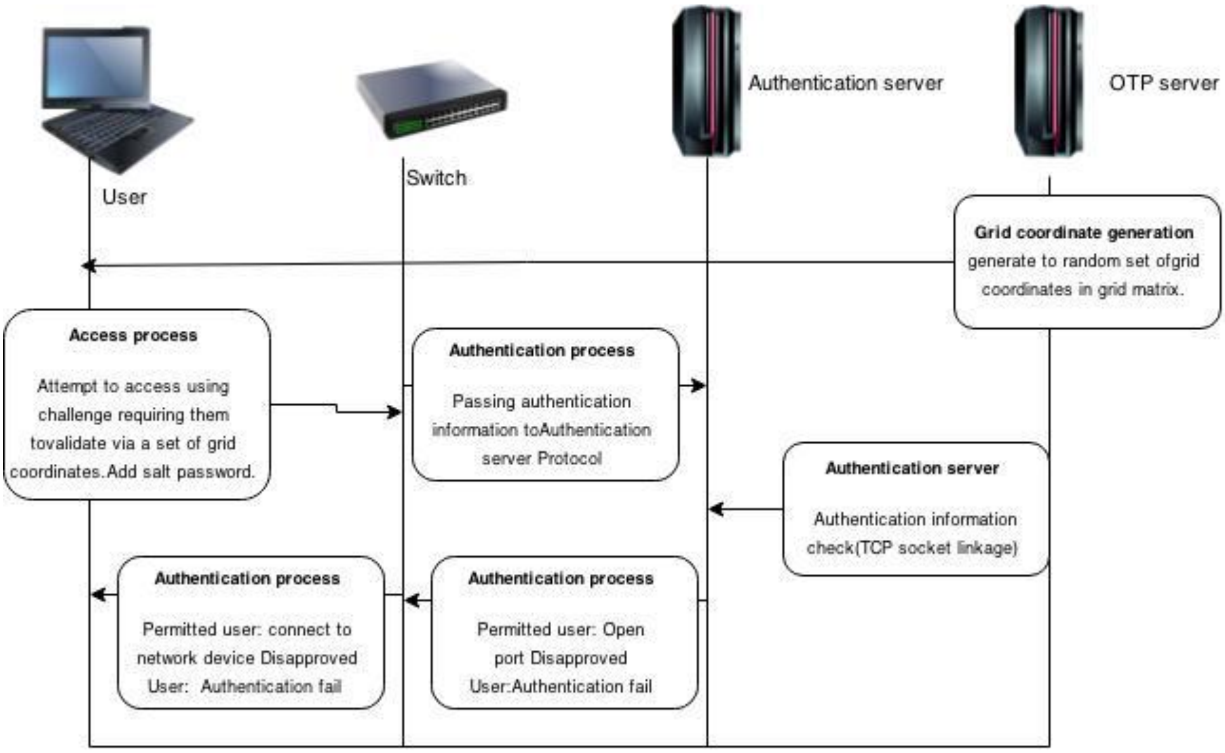
In order to overcome such weaknesses, this study presents a method of creating one time password keys in OTP Clients using grid card characteristics. On characteristics of this study that should be focused on is that the OTP system is not positioned in the OTP Server.

The password key creation process starts with a user logs in using their ID and password send to request to server. Then next process shows the randomly prime number of coordinate challenge selecting and reply to client. The process of creating a combination of permutation using the selected prime number by order, and creation of coordinate challenge using S/Key authentication scheme.

OTP password is a secret key that salt words and information in the corresponding cells from the unique grid card they possess.

This secret key can either be provided by the user, or can be generated by a computer. In case we choose salt is a random string of data used to modify a password hash. Salt can be added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system.

Figure1. Grid card authentication system with salt passwords


User
Switch
Authentication server
OTP server
Grid coordinate generation
generate to random set ofgrid coordinates in grid matrix.
Access process
Attempt to access using challenge requiring them tovalidate via a set of grid coordinates.Add salt password.
Authentication process
Passing authentication information toAuthentication server Protocol
Authentication server
Authentication information check(TCP socket linkage)
Authentication process
Permitted user: connect to network device Disapproved User: Authentication fail
Authentication process
Permitted user: Open port Disapproved User:Authentication fail

IV. SECURITY ANALYSIS

Grid authentication card security is determined by a number of factors. Card size is arguably the most important variable. Increasing the grid size (i.e., number of cells) and format (i.e., contents of the cell) exponentially increases the number of challenge responses available.

Entropy is defined as the uncertainty involved in predicting the value of a random variable. In this case, it refers to the ability to predict the information contained on a grid card — both coordinates and characters.

A larger grid card and additional cell contents increase the uncertainty of predicting the coordinates and characters on the card. In other words, more variables mean less chance of “cracking” the grid.

However, OTP security measures have not proven totally secure. Once grid cards and tokens appeared on the online banking landscape, it was not long before the banks started to see phishing scams targeting OTPs.

Some banks do not limit reloading times it keep reloading until the eavesdropped pattern appears. If the grid card does not have many enough numbers, the card could be reproduced by eavesdropping for several times. And it can be successfully phished by entering all the numbers in grid card. Grid card adopts 8-10 random numbers even easier to phish.

In these cases, phishing e-mails generally tried to trick the banking user by asking him to "authenticate" or "revalidate" his token or grid card by entering a long series of OTPs from the token or the entire contents of the grid card. So we add salt password so without a salt, a successful SQL injection (it is a code injection technique that exploits a security vulnerability in a website’s software to retrieve the database contents to the attacker) attack may yield easily crackable passwords. Because many users re-use passwords for multiple sites, the use of a salt is an important component of overall web application security. The benefit provided by using a salted password is also making a lookup table assisted dictionary attack against the stored values impractical.

Salt also makes brute-force attacks (the technique for checking all possible keys until the correct key is found in a database) for cracking large numbers of passwords much slower. Without salts, an attacker who is cracking many passwords at the same time only needs to hash (the random bit string) each password guess once, and compare it to all the hashes. Using Salt each password will likely have a different bit; so each guess would have to be hashed separately for each Salt, which is much slower since hashing is generally computationally expensive. Simple, easy-to-use authenticator for any industry, region or user population and proven authenticator as part of the software authentication platform . Cost-effective solution that is a fraction of the cost of traditional two-factor options. The coordinate request changes for each authentication challenge.

V. CONCLUSION

Online banking services were introduced by banks in 2002 and the number of service providers reached 9 commercial banks by the end of 2009. As of 2009, Online bank users numbered 3,566, representing 134,100 transactions and 3.3 billion MNT in value.

Conducting financial transactions was made easy with online banking that allows customers to conduct financial transactions on a secure website. However, with increased convenience, the threats of online banking fraud have also become a greater concern. Customer confidence and loyalty to a bank with online banking services depend greatly on the protection against banking fraud and identity theft.

The use of a secure website has become almost universally adopted. Though single password authentication is still in use, it by itself is not considered secure enough for online banking in Mongolia. Basically there are two different security methods in use for Mongolian online banking that is OTP token and Passwords.

Many of the banks in the Mongolia, the task becomes inherently more expensive, especially when customers are not willing to pay for such tokens. A typical hardware token based on a 3-year period costs the bank almost US$ 60-$125 per customer (when fully implemented, cost of hardware device, servers, support, marketing, postage, etc.)

This situation shows how customers depending upon single-factor authentication (a password only) can be easily defeated by trusted insiders or simple passwords cracking.

So this research area, introduces multifactor authentication methods and improves salt passwords with OTP systems based grid cards against fishing method that main disadvantage of OTP grid cards system. It can be strong secure in online systems and online banks.

Further, make a practice with online service companies and destine to more real consequence.

REFERENCES

[1] THE S/KEYTM ONE-TIME PASSWORD SYSTEM"Neil M. Haller,Bellcore http://www.cs.utk.edu/~dunigan/cs594-cns/skey.pdf. (*references*)

[2] The N/R One Time Password System"Vipul Goyal, Ajith Abraham, Sugata Sanyal and Sang Yong Han OSP Global, Mumbai, India.

[3] "One-Time Password Authentication Scheme Using Smart Cards Providing User "YOON Eun-Jun ; YOO Kee-Young, Deparment of computer engineering,Kyunbook National University K. Elissa

[4] http://en.wikipedia.org/wiki/Stream_cipher -incl: RC4, A5/1, A5/2.

[5] "Enhanced Authentication In Online Banking" Gregory D. Williamson GE Money – America's Journal of Economic Crime Management 2006

[6] "Security Analysis of Pseudo-Random Number Generators with Input" Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergnaud, and Daniel Wichs

[7] " Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices"Teddy Mantoro, Andri Zakariya

[8] "How to Make Secure Email Easier To Use" Simson L. Garfinkel Erik Nordlander Robert C. Miller MIT CSAILCambridge, MA {simsong,erikn,rcm}@mit.edu David Margrave Amazon.com Seattle, WA DavidMA@amazon.com Jeffrey I. Schiller MIT Network Services

[9] NIST Special Publication 800-90A "Recommendation for Random Number Generation Using Deterministic Random Bit Generators"Elaine Barker and John Kelsey

[10] A. Emigh. The crimeware landscape: Malware, phishing, identity theft and beyond. Technical report, Anti-Phishing Working Group Technical Report, 2006.

[11] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. Lecture Notes in Computer Science, 2259:1–18, 2001.

[12] I. Goldberg and D. Wagner. Randomness and the netscape browser. Dr. Dobb's Journal of Software Tools, 21(1):66:68–70, 1996.

[13] INTECO. Second wave of the study on information security and e-trust in spanish households. Technical report, INTECO, July 2007.

[14] Andrew Kalafut, Abhinav Acharya, and Minaxi Gupta. A study of malware in peer-to-peer networks. In IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, pages 327–332, New York, NY, USA, 2006. ACM.

[15] Tobias Klein. All your private keys are belong to us, 2006.

[16] Liam OMurchu. Banking in silence. Technical report, Symantec, 2008.

[17] Matthew Pemble. Evolutionary trends in bank customer-targeted malware.Network Security, 2005(10):4–7, October 2005.

[18] Symantec. Internet security threat report. Technical report, Symantec, 2007