Transaction Security Control in Banking System By Using Syfer Lock

San Ohnmar Kyaw
University of Computer Studies (Meiktila)
sanohnmarkyaw83@gmail.com

Abstract

Numerous reports with respect to online extortion in assortments media make distrust for leading exchanges on the web, particularly through an open system, for example, the Internet, which offers no security at all. Web based banking-which offers the financial types of assistance through web changed the business exchange of banks radically, additionally diminishing the expense and improving the straightforwardness for the client. On the web/Internet banking administrations comprise of data enquiry warnings and installment move. The issue with Internet-Banking application is that they send information legitimately to client in plain content structure, trading off with security. Accordingly, innovation for security is fundamental to help secure web based business on the Internet. This system presents the online banking security control by using Token Less Two Factors Authentication (TFA) / Syfer-Lock's Authentication Solution. TFA is used for the secure confirmation code for the editing of the user critical information such as password, username, pin and so on.

Keywords: *Internet-Banking, Token Less Two Factors Authentication (TFA), Syfer Lock's Authentication Solution*

1. Introduction

Today Security Risks are of extraordinary concerns. Numerous organizations are compactable with ensuring their classified data and exchanges with a secret phrase. A basic secret key security might be powerful for ensuring noncritical information. Be that as it may, remembering passwords, managerial issues and secret key hacking devices render a secret word just validation approach deficient for securing private data.

Confirmation is the demonstration of setting up or affirming something (or somebody) as genuine, that cases made by or about the subject are valid. This may include affirming the character of an individual, following the sources of an antique, or guaranteeing that a PC program is a confided in one. There have been various techniques proposed for making verification system increasingly secure.

There are various ways by which the protected passwords can be hacked, for example, Hashing, Guessing, Default Passwords, etc. For the most part, a secret word containing both capitalized and lowercase characters, numbers and unique characters as well; is a solid secret key and can never be speculated. Yet at the same time isn't a lot of secure method for confirmation. One approach to fortify the validation strategy is by including elements, for example, tokens, computerized endorsements and biometrics. The most widely recognized type of multifaceted confirmation is two-factor verification utilizing a token or keen card as the second type of ID.

2. Related Work

Another technique is smartcards [6], which likewise bolster individual access forms similarly as equipment tokens. The upsides of smartcards are the numerous utilization of the card for building access and for putting away various endorsements in a single spot. The drawback is the arrangement of the smartcards and furthermore the conveyance and security of the endorsements that live on them. Similarly an authentication has an opportunity to live and this is the greatest issue with testament the executives where chairmen need to supplant or repudiate a declaration. Notwithstanding the sending of the smartcard so ancillaries are required likewise as the client's terminal needs to have a smartcard per user, which is frequently not coordinated. This implies proper equipment or programming must be introduced. This typically brings about an expanded requirement for worker support as they need to figure out how to utilize the smartcards and the related equipment and programming. Another hindrance is that smartcards can't be utilized with portable terminals, as a unique perusing gadget isn't incorporated and can't be introduced or associated because of the thin plan of versatile terminals when all is said in done.

This financial framework [5] presents cash move exchange from bank to bank framework to give credible, respectability benefits by utilizing ElGamal open key computerized mark and SHA-512 hash work calculation. The security of ElGamal signature calculation depends on registering discrete logarithm over a limited enormous prime. The security of SHA-512 is enormous size of condensation yield. In the event that two hash esteems are equivalent, the substance of ticket message isn't changed after marked and show pass message of cash move is effective. If not, the substance of ticket message is changed after marked. Favorable circumstances: From the perspective on assaults on ElGamal advanced mark conspire, the security of the framework lays on the supposition of discrete logarithm and they are hard to figure for the assailants. SHA 512 hashing gives the framework to accomplish validation for clients and guarantee the respectability of the exchange message (ticket). Weaknesses: ElGamal has the drawback that the figure content is twice the length of the plaintext.

3. Background Theory

Authentication is the demonstration of demonstrating an attestation, for example, the character of a PC framework client. Interestingly with recognizable proof, the demonstration of showing someone or something character, verification is the way toward checking that personality. It may include approving individual personality records, checking the legitimacy of a site with an advanced declaration, [1] deciding the age of a relic via cell based dating, or guaranteeing that an item or archive isn't fake. Confirmation is pertinent to numerous fields. In craftsmanship, collectibles and human studies, a typical issue is checking that a given antique was created by someone in particular or in a specific spot or time of history. In software engineering, confirming a client's personality is frequently required to permit access to secret information or frameworks [2].

3.1. Two-factor Authentication

The advancement of IT safety efforts - particularly for verification forms - has seen security authorities move towards joining a few components with one another. This classification likewise incorporates two-factor verification (shortened as 2FA). In this methodology, in any event two of three potential components are required to plainly distinguish a client [3]:

- Something known uniquely to the client (for example PIN);
- A unmistakable thing that the client alone has (for example a token as a USB stick) and additionally
- Something that is indivisible from and extraordinary to the client, for example, a unique finger impression.

A typical case of verification utilizing the two-factor technique is getting cash from a money machine: to finish the exchange effectively, the client needs his own bank card just as his PIN. Access to the record is can't if both of these two segments is missing or if the PIN isn't entered accurately.

This twofold assurance diminishes the danger of crooks quickly having the option to abuse taken access information to capture another person's record. In numerous 2FA arrangements, something in the client's ownership is joined with a grouping of numbers for one-time use, for example a one-time password (OTP). This OTP is either created by a thing in the client's ownership, for example, a security token, or a solid server produces the OTP and sends it as a second factor to the gadget/token. A case of one such exchange strategy is an instant message sent to the client's cell phone. As another number is created each time, OTPs are far less inclined to be captured than static or basic passwords, which can likewise be seized by methods for phishing, keylogging or replay assaults.

3.1.1. Access by Hardware Token

The ordinary technique utilized in a 2FA arrangement is equipment token. A token can, for instance, be a USB stick or a key coxcomb. A showcase frequently demonstrates the blend of numbers to be entered by the client so as to sign in. The OTP produced by the token is then utilized together with close to home login subtleties to obviously recognize the client.

3.1.2. Advantages and Disadvantages of Tokens

This type of token can be utilized at whenever and anyplace for client verification. Moreover, the client isn't dependent on any extra equipment or the need to introduce programs. The drawbacks of this strategy are not withstanding, chiefly concern token taking care of, security and expenses. For instance, it is important to dispense a token to a particular client. This causes the IT office a ton of distribution work to send: the more representatives who get a token, the more individual setups are required.

Extra expenses are caused because of the constrained existence of the gadgets (around three to four years) and through misfortune or burglary. In the event that representatives are based everywhere throughout the world, costs are likewise brought about in sending the gadgets to them. There is additionally the angle that the client is dependent on the token in light of the fact that the client needs to take it with them consistently to confirm. In the event that the token is lost or overlooked, get to is unimaginable. After some time, the representative could think that its an irritation to consistently need to take the token with him "in the event of some unforeseen issue". A security issue exists and is featured as the client doesn't generally convey a token with them, so when it isn't with the client, where right? This powerlessness is a significant security issue and stressed as clients may have various tokens to convey.

3.2. Token Less Authentication

Token Less Authentication is a product token: a kind of two-factor verify security gadget that might be utilized to approve the utilization of PC administrations. Programming tokens are put away on a universally useful electronic gadget, for example, a work station, PC or cell phone.
Focal points of Token Less Authentication:

- No need to convey any additional equipment or gadget.
- It is more secure to use than a client ID or secret phrase and can coincide with both

Drawbacks of Token Less Authentication:

- Requires some measure of client preparing
- Deployment needs a controlled domain

3.3. Token Less Two-Factor Authentication

A trustworthy option in contrast to equipment tokens are token less arrangements. Token less arrangements are not depend on exclusive equipment yet rather utilize existing equipment that is as of now in the hands of clients. They play out the entirety of the security capacities that equipment tokens offer, and sometimes improve security, yet are not dependent on costly, single-use, equipment innovation. The intensity of token less is particularly solid when the gadget being used is a PC which is utilizing unbound correspondence arrange.

Focal points of Token Less Two-Factor Authentication: Cost investment funds: there is no requirement for extra equipment tokens, which must be bought, designed, kept up and consistently supplanted whenever lost or taken. It works with all the most recent cell phones, cell phones, PCs, tablets, Microsoft PCs and Apple Macs. Adaptable code transmission alternatives(for instance by content, email, delicate token or voice call). The client has the decision and is in charge, taking a great deal of the strain off the IT office, as it just needs to characterize the general conditions, for example, the particular time for occasional password refreshes and such like. There is no requirement for customized setup, in contrast to the case with tokens, so this additionally decreases the remaining task at hand [4, 7].

4. Syfer Lock's Software-based Authentication

Uber patterns, for example, the rise of distributed computing, server and work area virtualization, the expansion of portable innovations and bring-your-own-gadget, the expansion in representatives requiring remote access, and the expanded utilization of long range informal communication in the workplace have made new vulnerabilities and dangers for organizations. Clients hope to get to data from for all intents and purposes anyplace through the Internet and cell phones, for example, advanced mobile phones and tablets, and that implies it is more enthusiastically than at any other time for IT and security administrators to ensure an association's data resources. Probably the best concern with respect to security is unauthenticated access to frameworks and data. Given the multiplication of representatives working remotely and the utilization of cell phones, and the potential danger that speaks to for corporate systems, verification has become a higher need for undertakings. Username and static secret phrase alone don't give satisfactory security. Furthermore, in certain businesses, for example, medicinal services and money related administrations, the development or advancement of administrative necessities are constraining significantly progressively rigid requirements for solid validation [7].

Syfer Lock's product based confirmation arrangements give token-less one time passwords (OTPs), offering a straightforward, progressively secure approach to get to data while utilizing existing passwords and secret word framework. Syfer Lock's adaptable, versatile arrangements empower ventures to cost-adequately address two-factor and multifaceted validation over a scope of utilization cases and with a scope of stages. Syfer Lock is advertise approved with a developing client list and various honors from autonomous research firms and industry productions. Syfer Lock was named a 2013 Emerging Technology Vendor by CRN Magazine. Progressively, ventures are going to Syfer Lock and its boss programming based confirmation answers for reinforce security, take out equipment tokens and to decrease Total Cost of Ownership (TCO).

4.1. Objective of the Proposed System

The objectives of the system are:

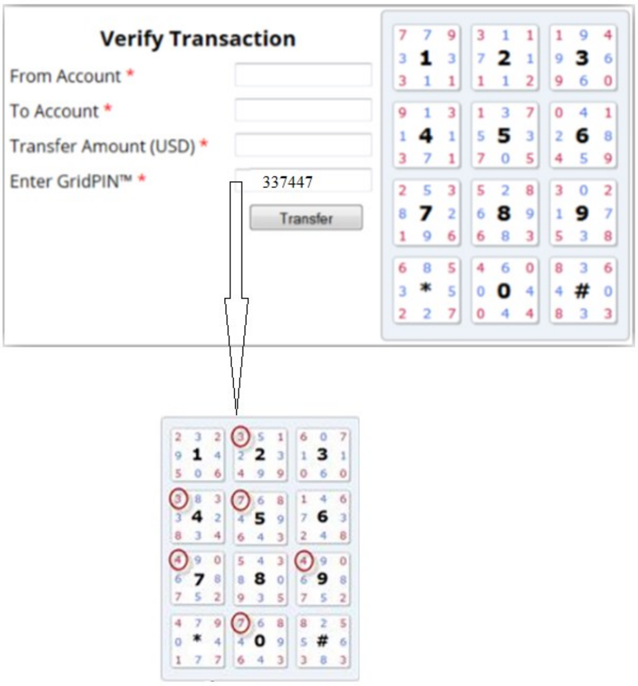
- To provide next generation Token-less passwords for secure access to computers, networks and the Internet.
- To convert static passwords/PINs into secure dynamic token-less password.
- To study superior software-based authentication solutions to strengthen security, eliminate hardware tokens and to reduce Total Cost of Ownership (TCO).
- To develop a secure token-less 2FA internet banking system.

4.2. Example Operation of Token-less 2FA Solutions Work

At sign in, a lattice (as demonstrated as follows) of cells is appeared, every cell containing:

- A static number or image in the inside, and
- Random numbers in the corners that change with every confirmation.

Client inputs the numbers comparing to their preselected corner position instead of related static secret phrase/PIN characters as their one-time secret word/PIN (OTP). For instance, with a static PIN of "245790" and a preselected corner of "upper left", the client would include a Grid PIN of "337447" for this sign in endeavor as appeared in figure 1.



Verify Transaction

From Account *

To Account *

Transfer Amount (USD) *

Enter GridPIN™ * 337447

Transfer

Figure 1: Example Operation of Syfer Lock

Upon each invigorate or potentially new sign in, the corner numbers haphazardly change, making another OTP. These single cells with number in the corners that change with each sign in are the establishment for Syfer Lock's licensed programming based networks that are utilized to change over static passwords/PINs into secure one-time passwords/PINs (OTPs).

4.3. Pseudo Code for Syfer Lock

```
Let   SP = Static Grid Pin Number;    //245790
        RP = Respective corner Dynamic Grid Pin of User Selected Static Grid Pin; // top left
BEGIN
     Step1: Generate Random numbers in the corners of grids;
     Step 2:   RP ← Accept related dynamic pin of user's SP; // 337447(i.e. preselected corner position in place of associated SP/static password)
     If(RP = = Dynamic Grid Pin of User's SP)
                         // (337447 = = 337447)
     {
            Grand the user requested operation;
     }
     Else
     {
          Message " Entering Random Grid Pin
            does not belong to the Random Grid Pin of
          User preselected SP";
          GOTO: Step1;
     }
     End If
END
```

4.4. Benefits of Syfer Lock's 2FA (High Security Control of Syfer Lock)

Syfer Lock's unique methodology covers the verification range giving two-factor validation using licensed programming based lattices to change over static passwords/PINs into secure one-time passwords/PINs (OTPs) at each sign in without the requirement for any extra equipment, tokens or customer side programming. Syfer Lock tends to the shortcomings of the conventional one time secret key (OTP) without the requirement for any extra equipment. Syfer Lock wipes out a scope of assaults.

Syfer Lock's, programming based verification arrangements give cutting edge one-time passwords/PINs (OTPs) for secure access to PCs, systems and the Internet. Syfer Lock has designed an improved validation strategy and framework utilizing token-less OTPs that gives clients a straightforward, increasingly secure approach to get to data utilizing their current passwords. Syfer Lock conveys unrivaled adaptability through a scope of answers for address different and developing validation needs. Zero impression viewpoint gives gadget less, once secret key/PIN age with no extra customer side equipment or programming (security control calculation). Syfer Lock's philosophy additionally permits the making of a layered way to deal with current confirmation forms: remain solitary, or utilized related to different variables.

4.5. Implementation of the System

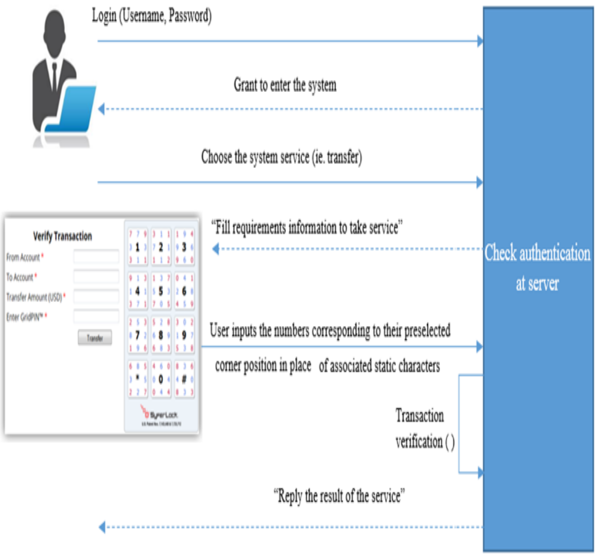

Login (Username, Password)
Grant to enter the system
Choose the system service (ie. transfer)
"Fill requirements information to take service"
Verify Transaction
From Account *
To Account *
Transfer Amount (USD) *
Enter GridPIN™ *
Transfer
SyferLock
User inputs the numbers corresponding to their preselected
corner position in place of associated static characters
Transaction
verification ( )
"Reply the result of the service"
Check authentication
at server

Figure 2: System Overview

The web has assumed a key job in changing how we connect with others and how we work together today. Because of the web, electronic trade has developed, permitting business to all the more adequately associate with their clients and different partnerships inside and outside their enterprises. One industry that is utilizing this new correspondence channel to arrive at its clients is the financial business. The e-banking framework tends to a few developing patterns: client's interest for whenever, anyplace administration, item time-to-showcase objectives and progressively complex back-office joining difficulties. The difficulties that restrict electronic banking are worries of security and protection of data.

This framework makes it simple to incorporate Syfer Lock's protected innovation into exclusively fabricated web applications. The syfer Lock can be utilized to tie down access to applications or for value-based level verification, for example, requiring the client to enter their GridPIN before performing touchy capacities inside an application, for example, cash moves in a financial application as appeared in figure 2.

Pre-defining the user pin at Authentication Server : The first time the user accesses the system (or any time the user changes their password), they will be prompted to select a target corner along with their password. For subsequent log-ins, the user will, using Syfer Lock's one-time password methodology, input the numbers corresponding to their pre-selected corner position in place of associated static password characters as their one-time password. The authentication processes are controlled and evaluated by the authentication server.

4.6. Summary on Syfer Lock's Appliances

Syfer Lock is an inventive supplier of cutting edge verification and security arrangements. Syfer Lock's licensed programming based confirmation and security arrangements empower undertakings and government associations to cost-adequately address solid validation/2 factor verification to make sure about each passage, including PCs, systems, online access and cell phones, over a scope of uses including restrictive systems, distributed computing and cell phones. Syfer Lock's easy to use programming based arrangements convey two-factor and multifaceted confirmation through tokenless one-time passwords or PINs (OTPs) without the requirement for any extra equipment, tokens or customer side programming, furnishing unrivaled security alongside incredibly diminished Total Cost of Ownership (TCO). Syfer Lock's verification arrangements are accessible in big business and cloud releases. Syfer Lock's adaptable approach is anything but difficult to send, is incredibly lightweight and can be sent in a High-Availability (HA) bunch. Progressively, undertakings are going to Syfer Lock and its boss programming based two-factor and multifaceted validation answers for reinforce security, kill equipment tokens and to diminish TCO.
Syfer Lock is advertise approved with a developing client list, serving associations worldwide in various markets including Utilities/Energy, Healthcare, Pharmaceuticals, Financial Services, Banking, Government and Media/Entertainment [7].

Syfer Lock has a worldwide patent portfolio for its software-based two-factor and multi-factor authentication solutions that includes the United States, Canada, Europe, Israel, Australia, China, India, Japan, Korea, Singapore and Taiwan. Syfer Lock has also been the recipient of numerous awards from independent research firms and trade publications including Frost & Sullivan and CRN.

5. Conclusion

Now a days, utilizing static passwords, as it is normally accomplished for getting to the secret information and data is not any more thought to be secure and safe. Thus Two Factor Authentication turns out to be increasingly well known. This framework is a model to show how security in internet banking can be improved and more work is required subsequent to running and propelling assaults on the framework in an ongoing domain. This is a working model that can be created to turn into a significant instrument for banking clients. To expand the security of the framework by being savvy, the structure engineering can be upgraded by recognizing the different kinds of assaults and giving insurance against such assaults.

REFERENCES

[1] E. Valente, 2009, Two-Factor Authentication [Online] http://www.sans.org / reading_room / whitepapers /authentication / twofactor-authentication-choose-one_33093 Federal

[2] Financial Institutions Examination Council (2008). [Online] "Authentication in an Internet Banking Environment" Available.

[3] "Software Tokens Based Two Factor Authentication Scheme", Manav Singhal and Shashikala Tapaswi, International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.

[4] Zachary B. Omariba, Nelson B. Masese, "Security And Privacy Of Electronic Banking", Masinde Muliro University of Science and Technology, International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.

[5] "Online Money Transfer System Using ElGamal Digital Signature Scheme", Sandar Moe, M.C.Sc 2012, University of Computer Studies, Yangon.

[6] "Two-Factor Authentication for Banking",
Building the business case, CRYPTOMATIC
Journal, 2012.

[7] SyferLock Technology Corporation, "Token-less OTP Authentication Solutions", System and Method U.S. and Foreign Patents and Patents Pending. 2015.