An Alternative Approach in Generation and Possession of Backup Codes in Multi-Factor Authentication Scheme

Darren Pradeep D'Mello[1]

Submitted in June 2014; Accepted in March, 2015

Abstract - The paper describes the need for modification in the methods of generation and possession of backup codes in multifactor authentication schemes. The proposed system eliminates the need for storing/printing the printable backup codes. Here one-time verification code is displayed at the time of authentication. Which, the user has to modify by placing the pseudo key- digit from the pool of digits, at the pseudo key-position rendering authentication. This technique eliminates the risk of exhaustion of backup codes when all codes that were previously generated are used. Backup codes are only valuable to someone who had stolen the password.

Index Terms – Backup-codes, Multi factor authentication, OTVC, Pseudo Key-digit, Pseudo Key-position

1. 0 INTRODUCTION

Multi-factor authentication, MFA, There are several approaches in authentication schemes, M-FA is such a one which requires two or more of the three authentication factors [1]: a *knowledge* factor (KF - "something the person *knows*"), a *possession* factor (PF - "something the person *has*"), and an *inherence* factor (IF - "something the person is").

$$MFA = (KF \wedge PF) \vee (PF \wedge IF) \vee (KF \wedge IF) \quad (1)$$

Two-factor authentication 2FA, T-FA (or multi-factor authentication) is often misunderstood with "strong authentication". However, both are fundamentally different processes. Composite solutions from two or more of the three categories of factors will result into a True multifactor authentication [2].

KFs are the most common form of authentication widely used. In this form, the user or a person proves the knowledge of a secret to authenticate him. Secret in KF involves password or passphrase or PIN or pattern. In PFs security of the system relies on the physical protection of the PF itself and integrity of the authenticator, for example Mobiles, One-time pads, USB tokens etc. IFs determine the user is with the help of biometrics like fingerprint, voice, iris, face, DNA etc.

Proponents say that, In a T-FA, the incidence of online identity theft, and other online fraud, could drastically reduce because the victim's password would no longer be enough to access to the victims info by the hackers. [3]

In 2FA and MFA, PF is verified by One-Time Verification Code (OTVC). OTVC can also be referred as OTP based on the context of how the application being developed. In this paper, OTPs and OTVCs are used interchangeably. Text messaging (SMS) is a common technology used for delivering One-Time Password (OTPs) to the user. Since SMS is a universal correspondence station, being straightforwardly accessible in about every versatile handset, to any portable or landline phone, content informing has an incredible potential to achieve all buyers at a low aggregate expense. However, the cost of SMS for every OTVC may be unbearable to some users. In spite of threats from hackers, the mobile phone operator also contribute to form as a part of the trust chain[4]. Moreover, several mobile phone operators has to be trusted if a user is in roaming network, which may prone to mount a 'man-in-the-middle' attack.

As an illustration, as of late Google has begun offering check codes to versatile and landline telephones for all Google accounts. The user receives the OTVC either as a SMS or as an automated phone call using text-to-speech conversion. In case, if the users registered phone(s) are inaccessible, then the user can even use one of a set of (up to 10) previously generated one-time backup code (BC) as a second authorization factor instead of dynamically generated OTVC, after signing in [5] with their account password. The BCs are advised to be printed and held in a wallet which too imposes a security threat, when a hacker comes into possession.

2.0 EXISTING SYSTEM

OTVC Codes are uniquely crafted for an account when the users need them. Typically, OTVC generation algorithms use pseudo-randomness or randomness; they vary greatly in their generation and methods of delivering them. Codes are sent to user via text message, proprietary tokens etc. as discussed in the introduction. The system functions well until phone service is available. What if a person is travelling in a flight? Today, major email/web service providers allow users to print a set of BCs at the time of registration, to authenticate[6] them when phone is not available or lost. What if all the codes are exhausted? The user has to rely on "Authenticator" apps. There could be several reasons for its unavailability.

[1]*Department of Statistics & Computer Science, KVAFSU/College of Fisheries, Mangalore, Karnataka 575 002, India*
E-mail:darren@cofmangalore.org

3.0 PROPOSED SYSTEM

The proposed system eliminates the need for printing BCs while phone is out of reach. Unlike the existing system, set of BCs are not generated prior and given to the user for their possession, instead OTVC is displayed at the time of authentication. The user has to modify the OTVC code by placing a Pseudo Key-Digit (PK_d) from the pool of digits (L) at Pseudo Key-Position (PK_p) that are displayed during authentication.

The PK_d is derived from the PF; PK_p is derived from KF; both at the time of registration (when phone was available) ensuring a part of MFA scheme. This approach uses KF and derived PF at the time of authentication, PF is derived when phone is available.

4.0 SYSTEM IMPLEMENTATION

The system implementation requires modification in BC generation at the server and its transfer mechanism. Since scalability is a major concern, the entire process does not alter the mode of delivering OTPs when phone is available. Implementation changes are required only when phone is not available with the user.

Conventional OTVPs are generated using Time-based One-time Password Algorithm or Mathematical algorithms [7] and sent to the user via voice/SMS when phone is available, soon after the user's credentials (username and password) are verified. Here, this new approach requires no modification. Its effective use involves the following stages, which are illustrated below,

4.1 Registration Phase

Occurs when phone is available: The Single Sign-On (SSO) [8] credentials are accepted, the user is then presented (as an option or mandatory) of MFA scheme. If the system mandates, then he has to register his mobile number and provide recovery options available under the web service. The server verifies the mobile number immediately by sending an Initial Verification Code (IVC),

The user then enters IVC into registration page to verify the possession of his phone.

PK_p & PK_d registration: Now the user is requested to choose a PK_p, which he has to pick from the position values (L_p).

$$L_p = \{ k \mid 1 \le k \le f(x) \} \quad (2)$$

$$f(x)=\text{DIGITS(OTVC)}+1 \quad (3)$$

The DIGITS function in Eq. (3) returns the number of digits, its value is implementation dependent. OTVC composed of digits from Time-synchronized or Mathematical algorithm. Some web service providers use 8 digits as a standard size for a backup code. To avoid key logging, implementations using AJAX with drag drop functionality is preferred.

Now the server sends a single digit number to the user's verified mobile. The single digit number is a PK_d, Possible values are 0,1,2…..9.

$$L_d = \{ 0,1,2,3,4,5,6,7,8,9\} \quad (4)$$

Which the user has to place it into PK_p to get him authenticated. This step, verifies the user's PF.

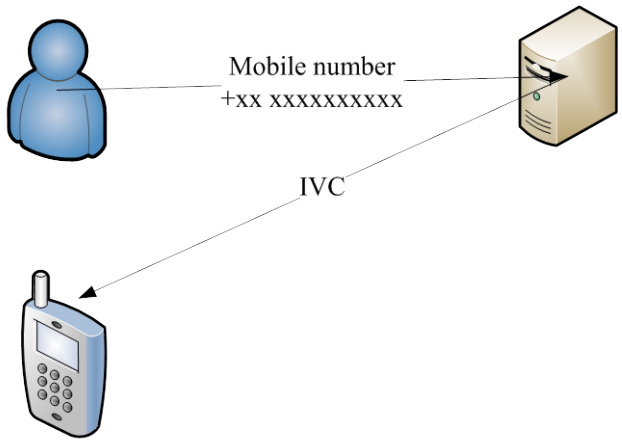

Figure 1: Registration phase

On verification, the user is taken to next step of registration.

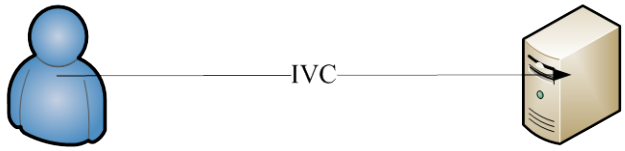

Figure 2: IVC confirmation

4.2 Utilization Phase

When phone is not available: User signs in by providing SSO credentials, and the user is directed to 2-step verification. Since the user has no phone service, he chooses alternate method of verification. Now the utilization phase is exercised as below. The user must now use the knowledge of PK_p and PK_d to complete the sign in.

Consider the example; the user gets OTVC in webpage after SSO as 46889513. This is a one-time code and by no means can the user expect to get the same at next sign in. A set of digits L_d is also presented as individual images[9] appearing as connected. Now the user has to place the PK_d at PK_p. The PK_p=k=4 and PK_d=7. Let us assume that the user's response will be PK_{ud} at position PK_{up}.

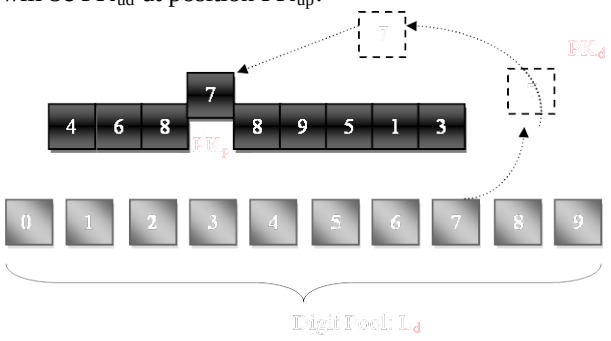

Figure 3: Process of placing PK_d at position PK_p by the user

On supplying PK_{ud} and PK_{up} the response is submitted, the integrity of the key-digit and key-position are verified to that of the user's registration and he is authenticated (if $PK_{ud} = PK_d$ and $PK_{up} = PK_p$). The utilization phase too is implemented using AJAX with drag drop functionality. PK_d and PK_p are stored at server at the time of registration.

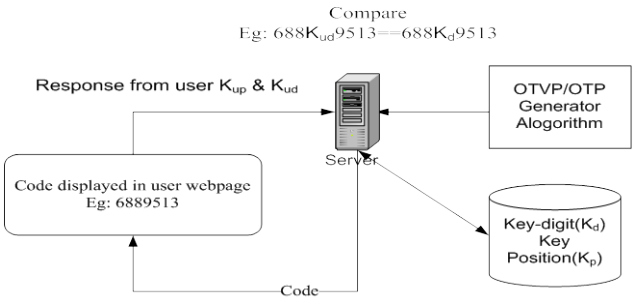

Figure 4: Block diagram of verification process

Any mismatch in key values i.e. if $PK_{ud} \neq PK_d$ or $PK_{up} \neq PK_p$ must prevent the user from signing in further. An invalid attempt limit may also be imposed. The user then has to recover using alternate options as configured by the Web service provider. At the server level, this can be summarized as show in fig 4.

The user must also be presented a choice for changing PK_d and PK_p soon after using them each time, when phone or voice service are available, however the aspiration is to reduce this repetitive overload.

5.0 FEASIBILITY EVALUATION

- It can be observed that, the existing overhead of generating a set of printable BCs at once and storing those in database at the server as well as printing by the user is not required. The cost is reduced.
- The later technique eliminates security risk associated at the user level of losing a printed sheet of BCs.
- Exhaustion of BCs never exists.
- The permutation and combinations of getting the right digit at right position is extremely high, Risk factor is minimum. CAPTCHA [10] may be used to prevent bots.
- Remembering PK_d and PK_p by the user is more effective than possession of a set backup codes.
- Overhead of downloading drag drop AJAX image (digit) is more than text, so workaround is required in minimizing the load.
- One-time passwords are vulnerable to social engineering attacks in which phishers steal OTPs by tricking customers into providing one or more OTPs that they used in the past [11].

6.0 FUTURE ENHANCEMENTS

Increasing the OTVC size or using an alternate alphanumeric algorithm will also enhance the technique.

7.0 CONCLUSION

In this paper, an alternative approach in generation and possession of backup codes in Multi-factor authentication scheme is discussed; although this mechanism cannot completely ensure the proper use of the system[12], it will surely reinforce the existing authentication scheme ensuring service availability to end user even while he is travelling eliminating the need of phone service or a set of backup codes.

REFERENCES

[1]. Wikipedia, Multi-factor authentication, 17 August 2013, http://en.wikipedia.org/wiki/2_factor_authentication

[2]. Federal Financial Institutions Examination Council, "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment", August 15, 2006

[3]. Two-Factor Authentication using Tivoli Access Manager WebSEAL, 06 Oct 2005, http://www.ibm.com/developerworks/tivoli/library/t-webseal

[4]. A. Chaudhary, V. N. Tiwari and A. Kumar, Analysis of Fuzzy Logic Based Intrusion Detection Systems in Mobile Ad Hoc Networks, *BVICAM's International Journal of Information Technology*, February 2014

[5]. Dilbag Singh and Ajit Singh, A Secure Private Key Encryption Technique for Data Security in Modern Cryptosystem, *BVICAM's International Journal of Information Technology*, December 2010

[6]. Mohammad Ubaidullah Bokhari and Shams Tabrez Siddiqui, A Comparative Study of Software Requirements Tools for Secure Software Development, *BVICAM's International Journal of Information Technology*, December 2010

[7]. RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, http://tools.ietf.org/html/rfc4226

[8]. Rui Wang, Shuo Chen, and XiaoFeng Wang. "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services".

[9]. S.K.Muttoo and Sushil Kumar, Data Hiding in JPEG Images, *BVICAM's International Journal of Information Technology*, June 2009

[10]. Ahn, Luis von; Blum, Manuel; Hopper, Nicholas J.; Langford, John (2003). "CAPTCHA: Using Hard AI Problems for Security". *Advances in Cryptology — EUROCRYPT 2003*. Lecture Notes in Computer Science 2656. pp. 294–311. doi:10.1007/3-540-39200-9_18. ISBN 978-3-540-14039-9.

[11]. The Register article. The Register article (2005-10-12). Available: http://www.theregister.co.uk/2005/10/12/outlaw_phishing/

[12]. Neelabh, Tracking Digital Footprints of Scareware to Thwart Cyber Hypnotism through Cyber Vigilantism in Cyberspace, *BVICAM's International Journal of Information Technology*, December 2012