Automated Login Method Selection in a Multi-modal Authentication System

Login Method Selection based on User Behavior

CHANG PEI SHAN
Security Information Lab
Mimos Berhad
Kuala Lumpur, Malaysia
ps.chang@mimos.my

DAHLIA DIN
Security Information Lab
Mimos Berhad
Kuala Lumpur, Malaysia
dahlia.din@mimos.my

WONG HON LOON
Security Information Lab
Mimos Berhad
Kuala Lumpur, Malaysia
hl.wong@mimos.my

SEA CHONG SEAK
Security Information Lab
Mimos Berhad
Kuala Lumpur, Malaysia
cssea@mimos.my

LEE KAY WIN
Security Information Lab
Mimos Berhad
Kuala Lumpur, Malaysia
kw.lee@mimos.my

***Abstract*— An intelligent model is proposed to automate selection of login authentication method in a multi-model authentication system based on user behavior profile. The proposed protocol analyzes the user behavior data to minimize the process in real time and prevent untrusted attempt, meanwhile, it able to facilitate frictionless user experience in a multi-modal authentication system. The proposed system determines a user at a log-in interface and retrieves the user's behavioral historical data as its determinant factors, matching user behavior based on data retrieval from database. Wherein the behavioral data includes the user's login sessions time, geolocation, accessed application and type of user-agent used. The system processes the behavioral data to generate a user profile by a profiling module, at that point, evaluates the user's profile by factoring in environmental parameters of the user terminal to select an authentication method by an evaluation module. The selected authentication method will be displayed for the user to complete the authentication process. On the other hand, the system will updating the user profile with data relating to a new successful login session for future evaluation.**

Keywords - Automated Method Selection, Multi-modal Authentication system, User Historical Profile, Profiling Module, Environmental Parameters, Evaluation Module, Normalized Distribution

I. Introduction

In the past couple of years, we have witnessed the rapid development of technology especially on cloud and network computing and it has significant impact on the world today. Users enjoy the technology to reduce the operating time, improve operation efficiency and other convenience by registered and stored all their confidential personal data in cloud application or others web-based programs. Unfortunately, the vast majority of network attacks are initiated, the cloud terminal of the weight loss caused by the end user security environment weakened, the client is more susceptible to viruses and Trojans infected, the user password is stolen incident has increased, all of this lead to face with more severe information security challenges [1].

Hence, the user authentication is essential requirement for current protected web-based applications nowadays. The common ways of authentication is through passwords (knowledge-based security), fingerprint or face (inherence factors) and ID cards (token based security) which are normally accustomed limit access to a variety of systems [2]. Initially, a traditional authentication mechanism provides a sole authentication method for user to proceed in a secure web page access. However, current development in information technology manages to decouple authentication function from application, thus allowing for new possibilities for the application to counter the internet fraud in a more cost effective way [3]. In this case, the traditional identity authentication and content authentication cannot meet the basic security needs of the web-based application and cloud computing environment [4].

Therefore, multifactor authentication is required which is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction [5]. Then again, to let user must aware and able to provide "what the user has" and "what the user knows", a multi-modal authentication system called MIMOS Unified Authentication Platform (Mi-UAP) is being introduced by author's team member. Multi-modal means, multiple authentication methods are provided for user to access a web application. Stand arise this multi-model authentication system, user able to select a login option they confident to provide for the current situation for completing a successful authentication. Furthermore, the current development phase is to generate an automated selection of login method for user in a multi-modal authentication system for facilitating frictionless and improve user experience.

The rest of the paper is organized and structured as follows. In Section II, we look into the background of our authentication system Mi-UAP platform. We define the related work by introduce the experimental environment and user historical data analysis from our production in Session III. For session IV, we introduce solution by describe the architecture and flow of our design idea, as

978-1-5386-8546-4/19/$31.00 ©2019 IEEE

well as the analysis results based on collected historical data. In Section V, we include the major findings relate to the analysis we have done. Finally, we describe the benefits and limitations of the proposed protocol, also the future work in the conclusion section.

II. Background

A. Platform Architecture

The organization Information System Security research lab has developed a multi-modal authentication platform named Mi-UAP to provide a convenient and user-friendly service for both organizations and individual users [6]. Mi-UAP provides an infrastructure which able deliver authentication services to applications with the authentication mechanism decoupled from application implementation. This is a self-managed system which incurs zero administrative effort [3]. Besides, a user has an option to use any login method based on user's preference as six authentication login options is available for users to select.

The authentication method implemented in our platform depicted in Figure 1 includes four common authentication methods used today which is password, certificate, One Time Password (OTP) token and OTP SMS; and other two proprietary authentication methods was introduce and developed by the authors which is Time-Constrained Key (TCK) and 2DBarcode. The development and production spanned for eight years. The authentication methods are progressively added, case by case basis, either as new project requirements or to solve problems raised from previous authentication method [4].

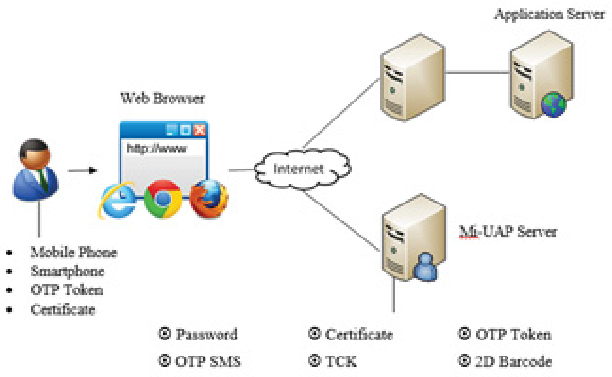

Fig. 1: Mi-UAP Platform Architecture

The benefits of the authentication platform utilizes Single Sign-On (SSO) for a seamless environment operation and adaptive authentication with threat response without modifying existing applications [6]. Mi-UAP also able support two factors authentication, which following a successful first authentication, a second single authentication method is displayed to challenge user in the new single web page. The goal of two factor authentication is to create a layered defense and make it more difficult for an unauthorized person to access a target

B. Problem Statements

While providing flexibility to the users, multi-modal authentication can lead to some adverse effects:

1. Confusion and annoyance as unregistered authentication methods are shown in front of user.
2. Undesirable friction in user experience which need to perform an additional step to choose the authentication method as others common authentication system doesn't behave the same.

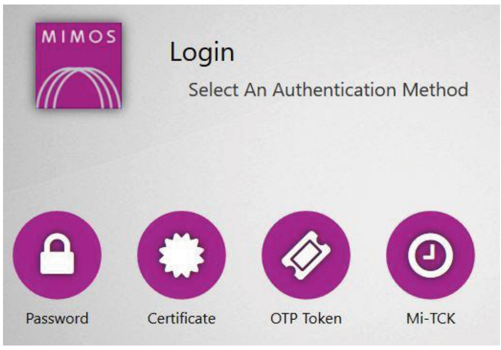

Fig. 2: Login Options in Mi-UAP

Refer to Figure 2, the multi-modal authentication system shows a list of login methods when user tries to login their application. There have been pass experiences where user forget the methods they registered on the particular gateway. Hence, user has to spend some times for the login process to recall their registered login method and credential.

Accordingly, it would be desirable and convenient to provide a system that can automatically select a login method for a user based on the behavior characteristics of a current session when compared to the user's historical profile.

III. Related Work

A. The Environment

For the authentication platform system, it is supported by a physical host with 8 mandatory Virtual Machines (VM) with different functionality as shown in Figure 1. For the physical host, it is using a 24-core CPU, 96B RAM and 1.1TB disk storage. All the Virtual Machines (VM) are deployed Ubuntu version 16.04LTS as the operating system.

B. Collected Data Based on User Behavior

This paper is an industry case study of the development on multiple authentication methods as an authentication service for 16638 registered users. This case study is unique because the data is extracted from a live production system with registered users inside multiple system logs. Since this paper emphasizes on user behavior for multi-modal authentication, related analytic is measured based on scenario of users performing authentication to access the production secure portal. The authentication system log contained the information such as process time, authentication method selected, application which to access, geolocation and user agent. The log duration is 3 months, which is from July 2018 to Sept 2018. As review purpose in this paper, 1 user who named as User C is selected for the user behavior analytics based on 100 successful access from authentication logs last 3 months.

Table 1: User C Preference Method based on Browser

User Agent	Selected Authentication Method			
	Password	*TCK*	*OTP Token*	*Certificate*
Firefox	12	5	8	28
Internet Explorer	5	0	0	0
Chrome	31	9	2	0

Based on Table 1, User C prefers to use Firefox as default browser with Certificate login method. Secondly is Chrome, while prefer login method is password. It might because the user certificate is stored under Firefox.

Table 2: User C Preference Method based on Application

Application	Selected Authentication Method			
	Password	*TCK*	*OTP Token*	*Certificate*
Myprofile	27	0	0	3
MyEss	11	14	10	25
IDPAA	10	0	0	0

Table 2 shows that User C used to access MyEss application most of the time with certificate login method. Whereas, password is the prefer method of User C when go to others application.

Table 3: User C Preference Method based on Location

Location	Selected Authentication Method			
	Password	*TCK*	*OTP Token*	*Certificate*
Geolocation 1	44	10	10	27
Geolocation 2	1	1	0	0
Geolocation 3	1	3	0	3

Geolocaion 1: Kuala Lumpur Geolocation 2: Petaling Jaya
Geolocation 3: Seri Kembangan

Table 3 shows that User C normally access from Geolocation 1 by using both favorite login method which is password and certificate.

Table 4: User C Preference Method based on Timestamp

Timestamp	Selected Authentication Method			
	Password	*TCK*	*OTP Token*	*Certificate*
Timestamp 1	23	7	4	19
Timestamp 2	17	4	6	8
Timestamp 3	3	3	0	6
Timestamp 4	0	0	0	0

Timestamp 1: 6am – 12pm Timestamp 2: 12pm – 6pm
Timestamp 3: 6pm – 12am Timestamp 4: 12am – 6am

Table 4 indicates that User C access application mostly on Timestamp 1 with password login method follow by certificate login method.

IV. Solution

Figure 3 is a full diagram illustrating a representative environment in which an automated method selection in a multi-modal authentication system may be implemented.

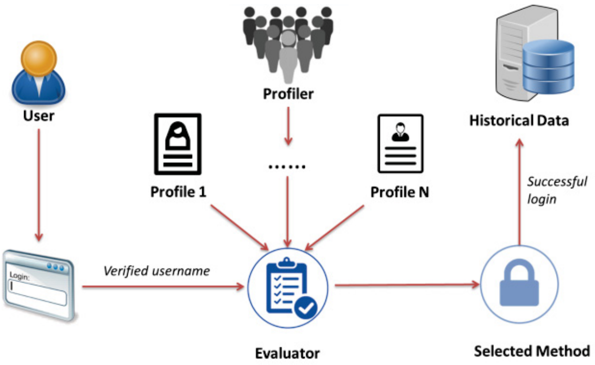

Fig. 3: Proposed Framework Diagrams

The paper's idea discloses a computer-implemented method to automatically select an authentication method for a user based on a plurality of historical profiles corresponding to user identifier in a multi-modal authentication system. In another aspect, a protocol that comparing behavioral characteristics of the user during current session with the user behavioral profile that previously developed based on prior usage patterns of the user through the historical login session. User behavior profile included device location, usual login timestamp, internet service provider and application.

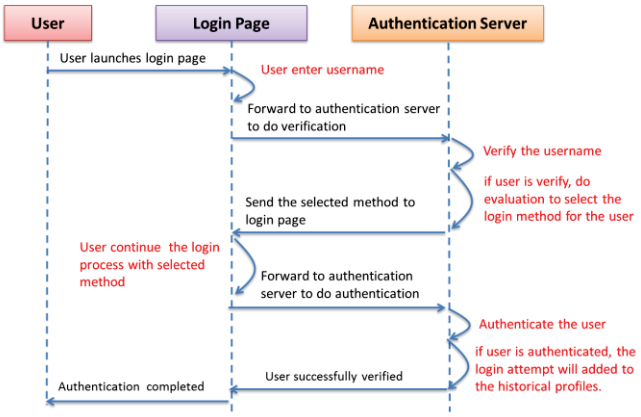
User
Login Page
Authentication Server
User launches login page
User enter username
Forward to authentication server to do verification
Verify the username
if user is verify, do evaluation to select the login method for the user
Send the selected method to login page
User continue the login process with selected method
Forward to authentication server to do authentication
Authenticate the user
if user is authenticated, the login attempt will added to the historical profiles.
User successfully verified
Authentication completed

Fig. 4: Overall Process Flow

Figure 4 is the overall process flow of the proposed protocol in this paper. First, user comes to an authentication gateway to login for an application. The authentication system will ask the user to enter her/his username first instead of show a list of login method to let user select. After user enters their username, the system only will start the enable the automated method selection flow if the username is verified by the system. The authentication system automatically selects a login method for the user based on a plurality of historical profiles related to his/her username inside the database. If the user continues and completed login with the selected method, the successful login attempt is added to the historical profiles.

Alternatively, user may wish to skip the selected method, at that moment, the automation authentication system will evaluate the profile of user again by exclude the skipped method as show in Figure 5.

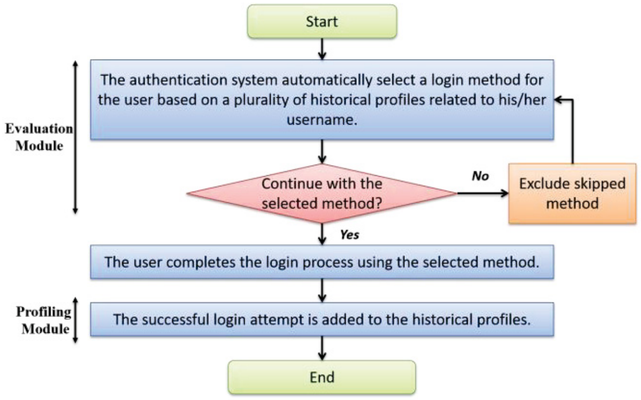
Start
The authentication system automatically select a login method for the user based on a plurality of historical profiles related to his/her username.
Evaluation Module
Continue with the selected method?
No
Exclude skipped method
Yes
The user completes the login process using the selected method.
Profiling Module
The successful login attempt is added to the historical profiles.
End

Fig. 5: Process Flow when user skipped selected method

In some scenarios, two or more methods may have the same plurality of historical profiles; hence, the system will pick the last used method from most recent login based on the timestamp table which will explain more in the following session.

Basically, the proposed process flow shows in Figure 3 depends on 2 modules as following:

1. **Profiling Module**, wherein processing the behavioral data includes the user's login sessions, geolocation, and type of browser used to generate a user profile
2. **Evaluation Module**, wherein evaluating the user's profile by factoring in environmental parameters of the user terminal to select an authentication method.

A. *Profiling Module.*

Profiling process extracts the data that is received, stored and transmitted by authentication server after user is verified. Successful login data are profiled based on the environmental parameters, e.g. access application, browser, and geolocation.

Table 5 shows the normalized distribution implemented on a profile based on user agent from User C from Table 1. Normalized distribution equation are obtained from below based on password method in Firefox browser.

$$\frac{\text{Password login in Firefox}}{\text{Total login in Firefox}} = \textit{Normalized Distribution of Password login in Firefox}$$

$$\frac{12}{12+5+8+28} = 0.226$$

Table 5: Normalized Distribution of User C based on browser

User Agent	Selected Authentication Method			
	Password	*TCK*	*OTP Token*	*Certificate*
Firefox	0.226	0.094	0.152	0.528
Internet Explorer	1	0	0	0
Chrome	0.738	0.214	0.048	0

On the other hand, the profiling module also stores the timestamp table of each method for every successful login attempt as illustrated in the table 6 below. It is stored to use when system obtain more than one favorite method for user after the evaluation module.

Table 6: Last Successful Login Timestamp of each method

Password	TCK	OTP Token	Certificate
30/9/2018	12/9/2018	31/8/2018	29/9/2018
1.39pm	4.50pm	9.15am	10.02am

B. *Evaluation Module*

Automated authentication system based on user behavior profile then the system analysis an overall distribution for the current session user. After analysis the highest normalized distribution, one of login method appear which is based on user-defined preference regarding their respective apparatus activities. For example A, if User C in Seri Kembangan and wish to access application MyEss by using Chrome browser on 1pm, the overall distribution of each method, is calculated as example equation below and tabulated in Table 8.

$$\textit{Overall distribution on Password Method}$$

$$= 0.738x0.183x0.484x0.486 = 0.0318$$

Table 7 : Overall Distribution of each Method in Example A

Environmental Parameters	Authentication Methods			
	Password	*TCK*	*OTP Token*	*Certificate*
Chrome	0.738	0.214	0.048	0
MyEss	0.183	0.233	0.167	0.416
Geolocation 1	0.484	0.11	0.11	0.3
Timestamp 2	0.486	0.114	0.171	0.229
Overall Distribution	***0.0318***	***0.0006***	***0.0002***	***0***

Based on table 7, Password method is selected for user C to login as it has the highest normalized distribution (HND) when user C having situation in Example A.

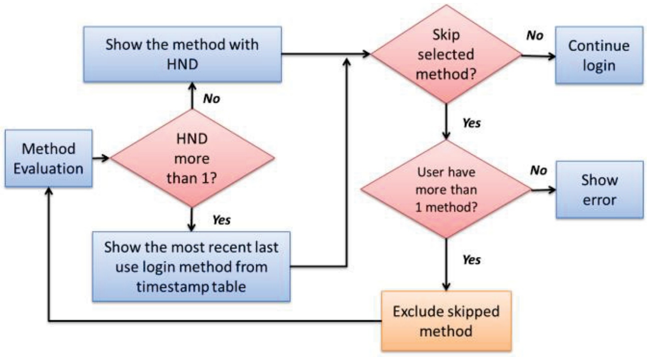

Fig. 6: Evaluation Process Flow when selected method is skipped

Alternatively, for some scenario as shown in Figure 6, if more than one method having same highest normalized distribution (HND), the automated authentication system will select the recent last use method based on the timestamp table which stored during every successful login attempt of the user in profiling module as shown in Table 6 and the overall distribution cannot equal to zero. Otherwise, system will directly show the HND login method only.

However, user is allowed to skip the selected method. If user skips the selected method but the user only having one login method, then system will show related error to user. While if user has activated more than one login method previously, the system will exclude the skipped method and do evaluation again to select another login method for user. Hence, if user do not skip the selected method and continue login, the related environment data will stored by the authentication server to keep as profiling module.

As in Example A. if user C skipped the Password Method, automated authentication system will select TCK as next login method for User C as TCK method having the latest login, while Password method is excluded and overall distribution of certificate method is equal to zero.

V. DISCUSSION

The aim of this paper is to attempt an intelligent method which allows user the flexibility to select its own preferable login method when access a restricted web service [7].

From the finding in Table 1 to 4 shares that every user have their own behavior when they access the authentication system in different authentication factor such as location, timing, application to access, user agent and etc. These end-user behavior is credible data analytic to mature one of the important research content for our paper. The findings from Table 5 to 6 which involve the normalized distribution formula indicate user C favorite methods are password and certificate while depends on which browser is using. For example, the system will prompt user C certificate login method when user C access service with Firefox browser. The results clearly show that the automated authentication system able to select user prefer login method in different scenarios based on the two module which is profiling and evaluation as shown in session IV.

VI. CONCLUSION

Clearly, the requirement for reliable techniques for user authentication has enhanced within the wake of heightened considerations regarding security and fast advancements in communication, quality and networking [8]. A large kind of applications need reliable verification schemes to verify the identity of a person requesting their service.

Current proposed protocol is to provide user login method automatically based on user's historical profile to facilitate the multi-modal authentication process of a user. At the same time, it able to proliferate the security level which based on user historical behavior data. Firstly, the authentication system automatically selects a login method for the user based on a plurality of historical profiles related to his/her username inside the database. If the user continues and completed login with the selected method, the successful login attempt is added to the historical profiles.

As summary of the results we discussion in session V, it indicates that the proposed approach is able to select login method for user automatically based on their historical behavior, it positively facilitates the undesirable friction in user experience. The results also show that confusion and annoyance will not occurred as unregistered authentication methods are shown.

However, the automated authentication system do have limitation especially for new user. It is because no behavior data able to collect since the user is newly registered. Hence, the automated authentication system cannot proceed to evaluation module. Furthermore, the current proposed protocol is based on the user historical behavior from first day register, so it may not precise for users that change their recent behavior which possible caused by many environment factor such as change laptop, work relocation and etc.

For future work, we are planning to deploy the proposed protocol in this paper, along with its implementation and experimentation in real testbeds. Correspondingly, the team will study to design a better approach for increasing the design complexity and overcome the limitations but at the same time, remains improving the end-user experience.

Conclusively, when this application is fully deployed, the intelligent protocol will be able to prompt user favor login method based on their historical behavior. This will save time for user while still able provide positive identification, also, the multi-modal authentication system will serve as a data repository for evaluating the user historical behavior.

ACKNOWLEDGMENT

We acknowledge the support provided by Dr Cheong Hoon Sin for providing the advice on the idea and framework related of this paper. Also, Mr. Wong Hon Loon to provide the authentication logs from the production platform as reference on user behavior analytics to accomplish this paper.

REFERENCES

[1] Chengyuan Zhang, Haishui Xu, "Research on user behavior authentication model based on stochastic Petri nets", Proceeding of the American Institute of Physics

[2] Garg, Suneet & vig Savita gupta, Renu, "Multimodal Authentication System: An Overview", International Journal of Control Theory and Applications, Vol 10, Page 111 to 119, 2017 https://www.researchgate.net/publication/319292208_Multimodal_Authentication_System_An_Overview

[3] Sea Chong Seak, Ng Kang Siong, Wong Hon Loon, Galoh Rashidah Haron, "A Centralized Multimodal Unified Authentication Platform for Web-based Application", WCECS 2014, Proceedings of the World Congress on Engineering and Computer Science

[4] Galoh Rashidah Haron, Dharmadharshni Maniam, Latifah Mat Nen, Nor Izyani Daud, "User Behaviour and Interactions for Multimodal Authentication", PST2016, published by IEEE.

[5] Margaret Rouse, "Multifactor authentication (MFA)", March 2015, https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

[6] Sea ChongSeak, Chang PeiShan, Wong HonLoon, Dahlia Din, "Research Institution Software Development Process Improvement to Produce High Quality Research Software & Assessment on Technical Software Package Installation", ISAI2018, published by IOP

[7] Anusiuba Ifeanyi, Anigbogu S.O., Onyesolu Moses, Okonkwo, "Multimodal Authentication Techniques For Staff Identification And Tracking", December 2014, proceeding of West African Journal of Industrial & Academic Research.

[8] Stacy Lyn Stubblefield, "System and method for utilizing behavioral characteristics in authentication and fraud prevention", 15 March 2013, US9275211 B2

[9] David M. Grigg, Peter John Bertanzetti, Michael E. Toth, Carrie Anne Hanson, "User authentication based on historical user behavior", 7 Feb 2014, US9185101 B2

[10] Zhengyou Zhang, David W.Williams, Yuan Kong, Zicheng Liu, David Kurlander, Mike Sinclair, "Multimodal authentication", 29 June 2005, US8079079B