ISSN 2250-3153

Improving Password Security Using Location –Based Intelligence.

Samuel Ojode Oluoch

Jomo Kenyatta University of Agriculture and Technology, School of Computer and Information Technology

Abstract- Information technology users are increasingly dependent on mobile devices while computers are stationed in offices and cyber cafes. Most of these mobile devices like smartphones use location applications such as Google maps for reporting their locations. With computers in offices and cyber cafes, and people able to log in to other accounts in their mobile devices, it is likely that a trusted workmate who gets access to your authentication credentials i.e. user name and password to use them to access, interfere, or copy your work in your absence. With the mobile device able to report your location, security can be improved by integrating location based intelligence with password authentication. This technique works by comparing the location of a person's mobile device and where the log in attempt is being made. If the two match then log in succeeds but if the two locations are different, log in does not succeed.

Much research has already gone into the field of information security more so, password management, and location based authentication. These methods look at strength of passwords and ability to log into a system within a particular location.

The proposed system tends to apply a technology where the location of a mobile device possessed by a user is compared with the location of the other device where log in attempt is being made. Access is only granted when the two devices are in the same location.

Index Terms- passwords; authentication; location-based intelligence; location

I. INTRODUCTION

In this information technonoly age, computer and information security is an important issue when businesses conduct transactions online, host customer accounts, and field officers accounts. Authentication is the most ubiquitous form of identification method as user access control to a system [2]. User authentication is the combination of username and password [3]. A username is identity by which a user is identified. A password is information associated with user name that confirms the user's identity, which may be used to grant or deny access to user from a secure connection.

The use of a user identification and password is not an absolute proof of a user's identity. The use of a specific user identification and password by a user only means that the user is aware of the existence of the user identification and associated password; it does not necessarily mean that the person using the identity and password is the person associated with this user identification and password.

Meanwhile, smart phones are gaining popularity all over the world [1]. Most of these smart phones are equipped with inbuilt global positioning system (GPS) chips that can accurately detect the location of the user. This is evidenced by the explosion of location-based services, such as Google Maps. In addition, a lot of innovation is constantly occurring in the area. Companies such as Skyhook, Google and Apple continually improve their location detecting technologies by creating large databases of wireless access point and cell tower locations. The overall results have been the improvement in the accuracy of the detected locations. It is now feasible to determine the location of a user within meters of his/her actual location [1].

Integrating location-based intelligence in password authentication benefits the user in the following important ways:

• If an unauthorised user attempts to authenticate from a location far from the user's mobile phone, an authentication mechanism can reject the attempt even if he/she has the right username and password.

• A user does not have to worry about storing or writing down the password. It is difficult to memorize passwords hence the user can write them down and still be secure.

Based on these facts described above, smart phones can be a potential solution for integration of location-based intelligence with password authentication. Smart phones can be used to detect and send the location of a particular user to back-end servers, which shall verify the location as a factor for authentication and authorization purpose.

This project carries out research on password protection mechanisms and weaknesses, then goes ahead to discuss a technique which ensures that the person using a user identification and password is the actual person to whom this user identification and password belongs.

In the described technique, location based intelligence is integrated in the authentication process.

II. RELATED WORK

1n 2006 Willem G. de Ru, and Jan H.P. Elof presents a methodology for reinforcement of password authentication through the installation of typing biometrical mechanisms. This technique analyses the keystroke patterns unique to each user. The analysis is done transparently indiscernible to the user while typing to gain system access via a password authentication mechanism in the normal way ie. through entering of a user identification and password string. It then shows that the integration of fuzzy logic based typing biometrics with current password mechanism which constitute the most universal authentication device, can only serve to enhance security.

They further conducted an experiment to identify the ability of the system to identify an intruder and to identify a genuine user.

The system was however not able to do these at 100% accuracy, since an intruder can still log in using credentials that do not belong to him. It is as a result of this that this proposed system identifies the location of where the log in is being done, and where the user is with a mobile device which may be a phone.

In 2013, Shazia Rahman Obedur says that passwords are a critical part of information security. Then goes ahead to say that passwords when poorly chosen can be compromised and put the entire work at risk. Many users do not understand why good passwords and password management are important for information systems. Using a password or having a password policy is not enough. Understanding and practicing the policy is important to keep accounts secure. The author has ten conducted a survey to check password habits for user accounts on 113 subjects. This survey allowed the author to understand password habits of users according to sensitivity of their accounts, and revealing some critical issues associated with password choice. The author has considered data on password strength, types, and length of passwords chosen and how they vary by site and sensitivity.

The author further identified that that selecting a strong password continues to be a problem to most users, those who create strong passwords tend to reuse them for several accounts hence putting them at risk.

The proposed system will tend to secure the use of simple passwords, or even strong passwords which are written down. If someone has to access an account then the actual user as to be around with his mobile device. If in a different location, access will not be granted even if someone has the password.

Takamizawa and Kaijiri proposed and designed an authentication method using location information obtained from mobile telephones that is suitable in web-based education applications. A student who wants to login into the web-based application, in addition to using username and passwords, has also to provide his/her location through a mobile telephone in order to prove the authenticity. In their method, location from a mobile phone is determined using GPS. For that, mobile phone must be equipped with a GPS receiver and a clear view of the sky is needed for the process to work. QR codes are also used for web applications to prompt the mobile phone for the location. The user has to scan the code from the screen using his/her mobile phone and therefore a phone needs a camera. In addition, the authors did not pay attention to security threats and vulnerabilities for their location–based authentication method and as such the mechanism may be susceptible to trivial attacks. For example, the location could be easily spoofed or modified.

Despite the security features that they offer, most of these solutions however have suffered from problems such as practicality, usability, reliability and cost. In addition since the location signature depends on GPS, the mechanism suffers a lot of reliability issues especially indoors or in places where there is no clear view of the sky. Others have proposed protocols, which however apply only to specific scenarios or require specific devices. A general and flexible approach that can be applied in different situations is still lacking.

A method that takes advantage of the recent advancement in location–sensing technologies, especially provided by smart phones, is needed. These advancements have led to the improvement and reliability of location information and thus rendering it more useful. Earlier approaches have relied on technologies, once considered state–of–the–art, but currently either obsolete or mainly not adequate. In addition, these approaches require extensive user involvement making them less user–friendly. With the current technology it is possible to make this technology transparent and convenient for users.

III. STRUCTURE AND COMPONENTS

The proposed solution comprises four components, which are combination of various servers and applications:

• ***Reference Local Location server (RLLS)***

This is component which stores the location information of the computer where log in attempt is being made. It provides location registration, authentication and authorization services;

• ***Authentication server***

This provides authentication service for all participants whose username and passwords are stored in it. It stores usernames and passwords of users and is connected with the RLLS server and SP server to provide location-based authentication service.

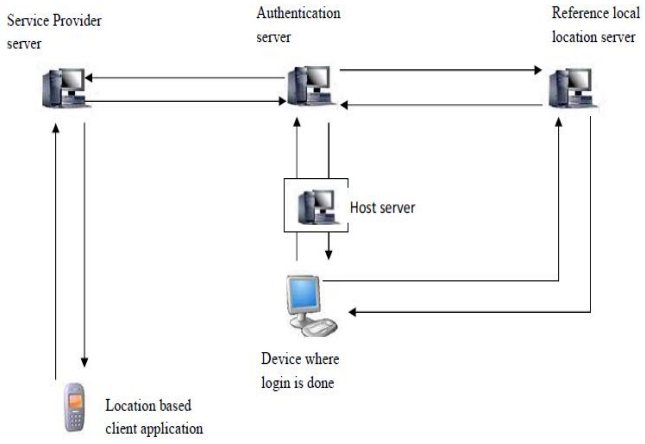
• ***Service Provider (SP) server***

These are the providers of various mobile services. They provide the information on location of the mobile phone of the users.

• ***Location-based Client (LBC) Application***

This is an application running on user's mobile device, capable to collect location information from trusted Location Providers (LP) and relay the same to the authentication server.

The architecture components are as shown in the diagram below



IV. PROTOCOLS

The design of the proposed system takes into consideration the fact that the registration process is already complete. It is therefore designed with one protocol i.e. authentication protocol.

Only one protocol is proposed in the system since during email or account registration, mobile phone numbers are always captured. It is this mobile phone number whose location will be determined each time a log in is requested. Authentication is performed at the beginning of each session, based on principles of single sign–on protocol. In our system, two types of location information are used: reference location and mobile location. Reference location refers to the location of the device being used to log in and stored in the database on RLLS server for future comparison during authentication. Reference location usually remains the same until it is explicitly changed by the user. Mobile location refers to the location information captured every time when user requests access to some resources or accounts. Mobile location always changes based on the user's movement and current location. The location information (both mobile and reference) that is captured by the LBC and sent to the server comprise four parameters: longitude, latitude, range of location accuracy and the underlying technology that was used to determine the location. In addition, the reference location also contains the user specified location range that specifies the area within which if the user is present user's account log in attempt can be authenticated successfully. The longitude and latitude are used to identify a specific precisely a geographical location. Every location estimate contains a level of uncertainty as the result of the location sensing technology used. The range of location accuracy is used to express this uncertainty to the server in order to facilitate in making valid authentication decisions.

V. AUTHENTICATION

This is when the actual location comparison process is performed. The protocol is performed every time when the user requests access to some resources or service from the system. Our solution can be integrated with any existing authentication systems. In this case, there is the authentication server providing the existing authentication service. The proposed solution can be integrated with them.

The process begins when the user tries to access the protected resource (e.g. login into his/her account). The process is initiated by user sending a service request to the authentication server. The server verifies the username and password, and if they are correct, sends location information request to the user's mobile phone and Reference Local Location server to compare location information then goes ahead to authenticate the user.

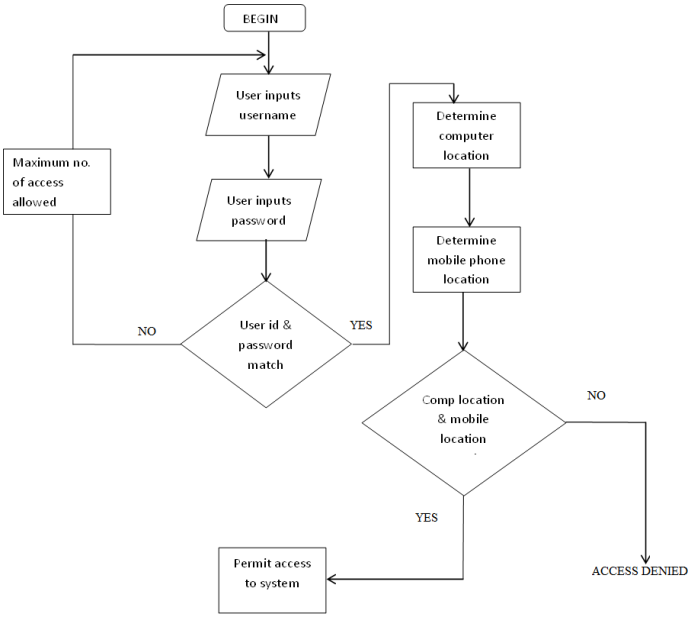


Fig 2. Summary on the whole authentication process.

The Authentication server sends a location information request to the user's mobile phone. The phone responds back to the Authentication server with the location information for the authentication purpose, which can be any existing mechanism depending on the implementation of the particular system.

It then compares user's location information with the log in device location data stored in its database during the installation phase, namely compare reference location with mobile location. If the authentication succeeds, authentication server sends authorization request, comprising user's access request and user's location information, to the host server. The server first performs existing authorization mechanisms, based on the locally stored policies [1]. After that, host server decides whether to approve user's service request based on the authorization result.

VI. LOCATION VERIFICATION

One of the most crucial steps in a location-based authentication mechanism is the verification of the location provided by the user's phone [1]. The security of the whole systems can either succeed or fail depending on the effectiveness of this step. The decision whether a user is authenticated or not depends on the validity of his/her presented location. When a user's mobile authenticates to the system he/she presents his/her location, which has been captured and calculated by the location sensing client. The verification algorithm then has the responsibility to check the reported location, verify its validity, compare it to the reference location and make a decision whether the user is authenticated or not. The goal of this process is to prevent location mismatch of location information and make sure that the clients' reported location is the actual locations that they are so that someone may not have access yet the actual user is not nearby.

VII. CONCLUSION

In this paper a technique for strengthening password security using location-based intelligence proposed and described. The proposed solution provides a system for ensuring that the person login in using a password is the actual owner of the password.For location verification, we propose an approach, which focuses on checking if the mobile number is in the same location as the computer where login is being attempted. This technique for integrating password authentication with location based intelligence improves the confidence of using and storing passwords, compared with other solutions where a long or complicated password has to be used, and where a password is not supposed to be written down but to be memorized. As a result, our system of integrating location based intelligence to password authentication comes out as more secure and valid.

REFERENCES

[1] Feng Zhang et al, Location-based Authentication and Authorization Using Smart Phones

[2] Shazia Rahman Obedur, Strategies for password Management, 2013

[3] Hans-Joachim et al, Authentication methods; 2010

[4] Wayne Jansen et al, Proximity Based Authentication for mobile devices, 2011.

[5] Shraddha D. Ghogare et al, location based Authentication: A new Approach towards providing security. International Journal of Scientific and Research Publications;volume 2, issue 4, April 2012.

[6] Mariana Hentea, intelligent Systems for information Seccurity Management:Architecture and design issues vol 4;2007

AUTHORS

First Author – Samuel Ojode Oluoch, Msc Computer Systems, Jomo Kenyatta University of Agriculture and Technology, samoj2000@yahoo.com.