International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Single Sign On (SSO) using User Specific Security Features

Josvin Thomas John[1], Albert Mathew[1], Jibin Jose[1], Done Boben[1]
[1] UG Scholar, Department Of Information Technology, Amal Jyothi College Of Engineering, Kanjirapally,

***Abstract*— In the android system almost everything is considered as an application and this project proposes a common sign in or single sign on app for android system. Through this application it is possible to sign in to different websites which require the credentials of the user. In this application the user can login to different websites where login is required by a single sign on with user specific security feature. After successful login to this application the user is allowed to select the websites to be used and through this system the user is allowed to successfully access different websites without any further login. By using this application the user is allowed to add new websites to his home screen and change the username and password whenever there is a change in credentials outside the system. The user is also allowed to speak and if it is a valid word, it will redirect to the site of his choice.**

Keywords—Single Sign On, One Time Login, Pattern Lock, Face Recognition, PIN Unlock, Speech Recognition.

I. INTRODUCTION

The management of multiple user-names and passwords is not only an annoying aspect of the current Internet, it is also one of the most serious security weakness. Each system requires that a client registers himself in order to access to the services. But rather often a user is registered in several web sites under the same user-name and with the same or closely related passwords, which is not a secure practice. They may often forget their user-name and password and the user management system sends an unencrypted e-mail with these confidential data.

Single Sign-On (SSO) protocols tackle the problem by enabling companies to establish a federated environment in which clients sign in the environment once and yet are able to access to services offered by different companies. The SSO project aims to simplify authentication procedures and reduce the number of passwords in a heterogeneous platform and application environment. These steps should enhance security administration in a multiplatform, multi-application environment. An SSO solution must address two distinct functions: authentication and authorization. Authentication verifies user identity, whereas authorization grants access rights to an already authenticated user. Traditional applications combine these two functions and incorporate them in the same modules. SSO helps to login to different websites. It reduces the burden of signing-onto different websites. It reduces the time lapse.

It gives user a wide option of security features which include Face Recognition, Pattern match, Speech recognition etc. In this application, the user can login to different websites where login is required, using a single sign on with user specific security feature. After the security login, the user is allowed to select the websites to be used and through this system the user allowed to successfully access different websites without any further login.

By using this application the user is allowed to add new websites to his/her home screen and change the username and password whenever required.

II. EXISTING SYSTEM

In the existing system the security feature for sign-in to application is mainly restricted to setting password. This security feature wouldn't be enough as some one who breaks the password can get access to the entire websites.The choice for the user to add different websites is restricted. Simplifying user authentication procedures is an SSO project's first goal, but adding an SSO tool to existing systems introduces new complexity. Security isn't the only issue for an SSO infrastructure. An SSO project must also support new authentication methods and accommodate new types of applications and devices [1]. In new e-commerce applications, single authentication is essential. Different SSO tools and technologies are available, and new standards are emerging.

Authentication: recognizes who you are.

Authorization: know what you are allowed to do, or what you allow others to do.

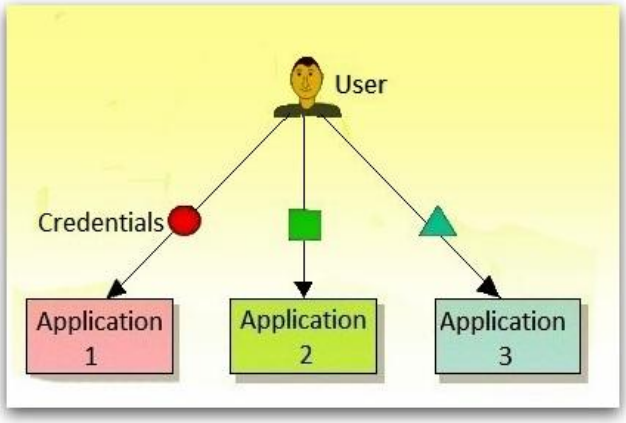

Fig. 1. Traditional logon procedure with multiple credentials (User ID & password pairs)

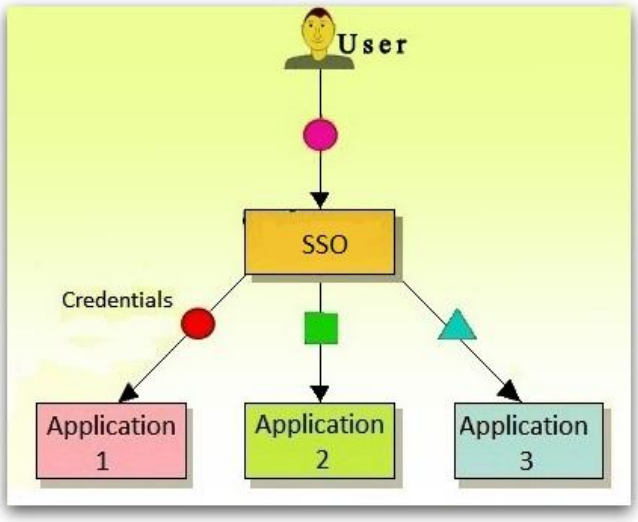

Fig. 2. Single logon procedure for a user employing an SSO Tool, where credentials come from the SSO tool

A. SSO TECHNOLOGIES

Traditional SSO tools assist users in the authentication process [1]. All credentials required for authentication—user ID, password, procedures or scripts for target systems, and so on—reside on an authentication server, as shown in Fig 3. From the target application's standpoint, nothing has changed. The local SSO agent, rather than the user, provides the credentials.

All SSO tools provide a software development kit so that customers can develop interfaces to their legacy logon procedures. The most popular general purpose SSO tools are PassGo SSO from Axent, Platinum SSO from Computer Associates (formerly Platinum), eTrust SSO from Computer Associates, Global Sign-On from IBM/Tivoli, and AccessMaster SSO from Bull. Hewlett-Packard and Novell have also proposed SSO solutions. Products may differ on the platform and standard acceptance level (LDAP, X.500, X.509). The Open Group has also issued a specification for SSO solutions known as XSSO.

In all of these tools, the authentication server manages a complex database containing confidential data such as passwords, access rights, and scripts. This database must be highly protected but also available continuously and scalable. The SSO system generates and automatically manages passwords for target systems. This method enhances access security but can also lead to a single point of failure because users can log in only via the SSO tool [5].

Network operating systems (NOSs) became major players when they adopted X.509 standards for certificates. As NOS directories and PKI technologies converge, security management will get easier, and NOSs will probably become strategic platforms supporting authentication and authorization in company networks. However, migrating to a PKI and Web-application paradigm will require new software and hardware, revision of the company's security model and policies, and implementation of an internal certification authority.

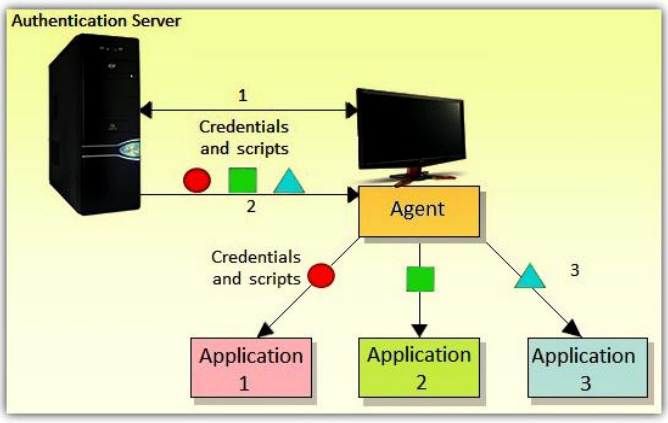

Fig. 3. An SSO System

Fig. 3. Shows an SSO System in which (1) a user logs onto the authentication server. The SSO Agent on the client platform retrieves the list of available applications from the server to display a special or customized desktop. When the user wants to first execute an application, (2) the SSO Agent retrieves credentials (User ID and password pairs) and scripts from the server, then (3) executes the logon procedure as a script or set of instructions.

III. PROPOSED SYSTEM

An SSO solution must address two distinct functions: authentication and authorization. Authentication verifies user identity, whereas authorization grants access rights to an already authenticated user. Traditional applications combine these two functions and incorporate them in the same modules. It gives user a wide option of security features which include Face Recognition, Pattern match, Speech Recognition etc.

By using this application the user is allowed to add new websites to his/her home screen and change the username and password whenever required.

A. Authentication and Authorization

An SSO solution must address two distinct functions: authentication and authorization. Authentication verifies user identity, whereas authorization grants access rights to an already authenticated user. Traditional applications combine these two functions and incorporate them in the same modules. SSO systems usually focus only on authentication, leaving authorization to the underlying systems or applications.

Authentication systems are traditionally based on pairs of user IDs and passwords. However, the landscape for applications and devices is expanding, and new methods are emerging, such as public-key infrastructure (PKI), tokens, one-time password systems, smart cards, and biometrics. As these technologies continually evolve, developing central administration and SSO systems may require adapting legacy applications or building special-purpose authentication middleware. You can also expect different types of applications and devices, each requiring an authentication process—and, therefore, an SSO solution—as shown in Fig 2. Of course, authentication is necessary, not only for applications, but also for firewalls, virtual private networks, extranets, mobile devices, personalization access systems,

navigation systems, security or data-encryption systems, and content-management systems. The rapid development of technologies will generate new communication models and devices requiring authentication from inside and outside the company [5].

B. *Internal and external applications*

Differentiating between internal and external (Web) applications adds another dimension to the problem of choosing an SSO strategy. An expanding application scope, coupled with increased user mobility, generates challenges related to access authorization, such as access rights, content protection, and security policies. Users should be differentiated, not only by their physical (internal or external) location, but also—in fact, mainly—by their adherence to groups or roles and their rights to access particular information.

Moreover, because electronic commerce demands that applications provide users maximum comfort, single authentication is essential. In traditional systems for internal users, the main focus is cutting costs and improving security. In the Web context, however, quality of service is crucial. Furthermore, Web applications tend to be more recent and, therefore, based on technologies that facilitate SSO implementation.

Our application focuses mainly on external (Web) applications or sites. The user can store the credentials of his favorite sites and access them easily without any trouble.

C. *Speech Recognition*

This is a very simple feature. Once the user is logged onto his home screen, he can trigger Android's Speech to Text Intent which shows a dialog to take speech input. It will have a button with Mic symbol. The speech input is then converted into text. The text is then displayed as a toast message and if it is present in the website list created by the user immediately you will be redirected to the respective website. Otherwise the result is displayed as a toast message. If unable to recognize the website we return error "unable to recognize". We can also close the speech dialog box at any time.

IV. SECURITY

A. *Face Unlock*

Android 4.0 introduces a completely new approach to securing a device, making each person's device even more personal — Face Unlock. It is the biometric identification by scanning a person's face and matching it against a library of known faces. It is a new screen-lock option that lets you unlock your device with your face. It takes advantage of the device front-facing camera and state-of-the-art facial recognition technology to register a face during setup and then to recognize it again when unlocking the device. Just hold your device in front of your face to unlock, or use a backup PIN or pattern.

Facial feature identification is the necessary step before many computer vision systems including emotion detection, face tracking and face recognition [2]. The facial feature identification algorithm presented is based on an anthropometric face model, box-blur filtering, and non-maximum suppression to find eyes corners, mouth corners and nose center. Skin color detection is used to find regions in the image that have a higher potential of containing eyes [3]. The anthropometric face model is used to reduce the computational complexity involved in localizing facial regions. This algorithm is designed to be compatible with the limited hardware and memory capabilities of mobile devices.

Skin segmentation is done to identify skin like regions in the image. It is assumed we have a picture containing shoulder and frontal face. The skin like region is therefore assumed to be the part of the region that contains the face. The RGB color image is transformed into the YCrCb color image. The extraction of the eyes is the most important part of this algorithm. All other features are found based on the position of the eyes and the intra-ocular distance. Once the skin region is found, eyes are to be found in that skin region. The skin region could consist of not only the face but also the neck and sometimes part of the chest. It is possible to extract the extract the face by using the following golden ratio formula,

$$h/w = phi \quad (1)$$

where h is the height of the head, w is the width of the head and phi is the symbol representing the golden ratio 1.618. The width of the skin region is to be measured and considered to be the head width [2].

The distance between the two eyes is D. The following rules are applied:

1- $N/D = 0:33$ (2)

where N is the vertical distance between the eyes and the nose tip.

2- $M/D = 1:10$ (3)

where M is the vertical distance between the eyes and the mouth center.

3- The width of the nose E is 0.8D.

4- $E/L = phi$ (4)

where E is the nose width and L is the distance from the nose to the mouth.

5- $K/E = phi$ (5)

where K is the length of the lips.

6- The width of the eyes is similar to the nose width.

B. *Pattern Unlock*

Pattern unlock involves a grid of 6 dots on which you draw a pattern. It should be something easy to remember and can be done one-handed. This is probably the easiest method, but isn't the most secure. You don't want to create one that's too easy to figure out — just as with a PIN — but you also don't want to make it so complex that you forget it.

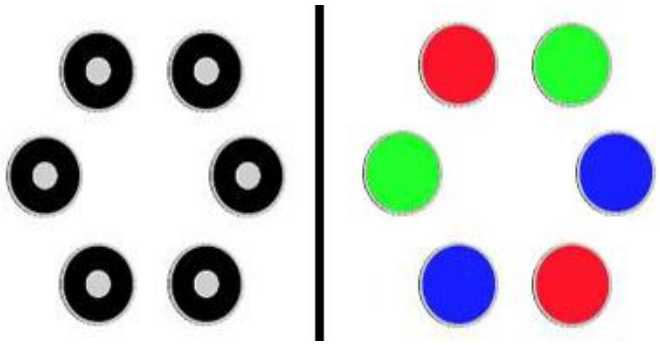

Fig. 4. Pattern Lock

This Lock Screen is shown in Fig 4. Redundancy input (re-touching the circle) is allowed and when the circle is touched more than once, it changes color (maximum of seven times) so that the user can identify the correct input [4]. In our demonstration we allowed 20 inputs and were able to make over one quadrillion passwords. Once you enter your pattern and the screen says Pattern Recorded! Hit Continue. At any time before this you can hit Retry to draw a different one or Cancel to start over. The security power depends upon the size of the key space; the bigger the key space, the more difficult is a brute force attack.

Comparing our system to the Pattern Lock and number password systems, the Pattern Lock has about one million key spaces, the number password system has about 10,000 key spaces, and our Lock Screen system has about ten million (6^9 = 10077696) key spaces. It can also be made larger by increasing the number of repetitive touches.

Once the pattern is saved Android will return you to the Security screen where you have to re-enter the Pattern to access the app.

C. PIN Unlock

Most people are familiar with PIN numbers for their ATM card and voicemail, and this is pretty much the same. Unlocking with a PIN means numbers only. You can use just 4 or up to 16 numbers. The more numbers you use, the harder it will be to crack. If you already have a PIN number you use for other things you may be tempted to apply it to your Android phone as well. I suggest adding an extra number at the beginning or end to add a layer of security.

After you enter the PIN you've chosen, press Continue and confirm by entering it again. Once you hit OK the PIN is set. At any time before this you can hit Cancel to start over. Once the PIN is saved Android will return you to the Security screen where you have to re-enter the PIN to access the app.

CONCLUSION

Single Sign-On (SSO) helps the users to sign-on to different websites. It helps the user to move directly to the home page of different websites without having to enter user credentials each time. As the user does not need to log-in each time, it helps the user to set strong passwords. In this application the user can login to different websites where login is required by a single sign on with user specific security feature. After securely logging onto this application the user is allowed to select the websites to be used and through this system the user is allowed to successfully access different websites without any further login. It employs various security features such as Face Lock, Pattern Lock and PIN Password. It even employs Speech Recognition to select websites for the user.

FUTURE WORK

As the latest gadgets provide Fingerprint Detection, we can encrypt the SSO using the user's Fingerprint so as to replace text password. As Banking Sites work using Sessions, hence once the session expires the user has to login again. So the feasibility of banking sites with SSO is less. To overcome this limitation, once the user logs into the Banking site using his username and password, it will be stored in the database of the phone and encrypted using some encryption standard.

REFERENCES

[1] Andrej Volchkov, "Revisiting Single Sign-On A Pragmatic Approach in a New Context", IT Professional, vol. 3, pp. 39-45, Feb 2001.

[2] Josette. C. Tagatio Mawafo, W.A. Clarke and P.E. Robinson, "Identification of Facial Features on Android Platforms" , Cape Town, 2013 IEEE International Conference on Industrial Technology (ICIT), pp. 1872 - 1876, 25-28 Feb 2013

[3] P. Campadelli, R. Lanzarotti, and G. Lipori, "Automatic facial feature extraction for face recognition", Kresimir Delac and Mislav Grgic (Ed.), InTech Education and Publishing, pp. 31-58, 1 July 2007.

[4] Kwang Il Shin, Ji Soo Park, Jae Yong Lee, Jong Hyuk Park "Design and Implementation of Improved Authentication System for Android Smartphone Users", Fukuoka, 2012 26th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 704 – 707, 26-29 March 2012.

[5] P. Charden, "The New Face of Single Sign-On", Network Computing, pp. 1-9, 22 March 1999.

[6] J.Bankston,"Keeping Gatecrashers away from Your Web Site", Network World Fusion, 18 Oct. 1999, www. nwfusion.com/reviews/1018rev.html