International Journal of Advanced Engineering and Innovative Technology (IJAEIT)
ISSN No 2348-7208   Special Issue on "Emerging Technology for Innovative India"

Ticket: Smartphone Enabled Secure Access to Multiple Entities (SESAME)

Harshalee D. Korde[1], Jyoti More[2]
Department of Computer Engineering, Lokmanya Tilak College of Engineering,
Koperkhairane, Navi Mumbai, Mumbai University, India
[1]harshaleekorde@yahoo.com
[2]jyotis8582@gmail.com

***Abstract*— Authentication is a process by which a system validates the identity of a user. User authentication is the mechanism for authentication and protects user data or unauthorized access of information. The most common computer authentication method is text-based passwords. Text based passwords are vulnerable to social engineering attacks, either weak-and-memorable or secure-but-difficult-to-remember. This method has been shown to have significant drawbacks. To address this problem some researchers have established authentication methods like alphanumerical passwords. Often alphanumerical passwords are combination of alphabets and numbers which makes the password greater in length and hard to remember. User can write our password in page or in computer file but if the page is damage or that computer file is corrupted then password is lost. Existing password scheme is easy to break through different attack i.e. dictionary attack, brute force attack, shoulder-surfing. A new hybrid graphical password based system is a combination of recognition and pure recall based techniques. This scheme is proposed for smart handheld devices like smart phone. Hybrid graphical password have been designed to make passwords more memorable and easier for people to use**

Keywords*— *Authentication, Graphical Passwords, Network Security, Smartphones, Hybrid

I. Introduction

Most Internet services like email, e-banking and social networking implement access control via a username password based authentication scheme. This creates an ambiguity to the user for which all passwords to remember and there's always a threat that the passwords may be hacked by someone. People even tend to write passwords on chits of papers and on diaries which can be hacked by someone to get the illegal and ill-legitimate access to the system. Textual passwords thus are likely to remain at least for now as the only way to authenticate a user to web services[4].

However, an adversary, by gaining knowledge of a user's password (e.g., by brute force attack), can compromise a user's access to such services. This concern can be largely alleviated by having users choose strong and complex passwords (which have high information entropy) for authentication[4]. In fact, some Service Providers have enforced password creation policies to make users choose such strong and complex passwords. However, there are two inherent issues with users being forced to choose stronger (or complex) passwords. First, studies such have indicated that enforcing stricter password rules causes users to take shortcuts like writing down the complex password in clear text, either on paper or electronically, as a memory aid. Thus, it is easy for an adversary to get hold of the complex password.

The second issue with complex passwords is the reuse or recycle of the same password for different services since remembering different passwords is burdensome. More than 34% of the people reused the exact password while almost 18% reused them with minor modifications. The study in also found that 41% of accounts from a university system could each be cracked in three seconds, using the knowledge of their expired passwords. A malicious entity can thus easily crack a user's password if she has the knowledge of password composition trends by the user or (and) if passwords are reused. To add to this, the risk of compromising her password either from shoulder surfing techniques or key loggers on end systems always exists, especially in public places or systems. In shoulder surfing, an adversary is able to watch a user keying in her credential by visually recording the user's keystrokes. Keyloggers are programs or hardware devices that record all keyboard strokes.

Perhaps the most serious problem today is that current authentication systems have no mechanisms to recognize the identity of the person who enters the password; in other words, there is no way of verifying if the person presenting the credentials is actually the person that she is claiming to be. Since the communication channels can be secured using protocols such as https, SSL, TLS, the weakest link which controls a user's access to web services today is the human factor due to the need of entering passwords. Hence, there is a clear need for a new system that secures the human computer interaction, especially for password entry in order to secure the end-to- end flow of data. One solution to the problem associated with passwords is to use biometrics as credentials to access web services. However, this would require an overhaul of the entire Internet and related web based services.

Addressing these issues amounts to essentially finding the right answers to the following two important questions:

1. How do we build a system that overcomes the security limitations of passwords?

2. How do we overcome the tough job of remembering complex passwords?

The Contribution of our system and current referred paper gives the solution for the system. Replace the textual passwords by image based passwords, and let the user use the passwords as images which will be a vivid set of images being displayed to the user randomly making difficult for the attacker and the person who shoulder surfs it. Assimilate emerging technologies such as Cloud Authentication using modern protocols like REST

The above two questions and answers for the questions only satisfies the replacement technique adapted by the proposed application, in fact this results only half of the system, later the proposed system creates a secure medium over a Bluetooth channel to cater the communication between the computer based application of which the user needs the access and the smart phone which acts as the key for that computer based application installed on the host.

II. OVERVIEW O PROPOSED SYSTEM

A user can access web application or a computer based desktop application on a Host Terminal via a smart device. Here the Host Terminal is used to view the web content while the smart device is used for authentication purposes. The Smart phone communicates with the host with Bluetooth channel, the smart phone application installed on the users smart phone will authenticate user on randomized image based authentication which will be authenticated over a Web Service.

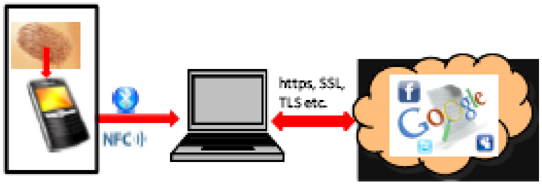

Fig. 1 Overview of Proposed System

Fig. 1 present's overview of SESAME (Smartphone Enabled Secure Access to Multiple Entities) which consists of a user accessing web application or a computer based desktop application on a Host Terminal via a smart device [4]. Specifically, we address the problem of entering credentials via a Host Terminal to access a service. Incidentally, addressing this specific problem also addresses the limitation of memorizing textual passwords. SESAME provides an avenue that is complimentary to textual passwords and their usage, mainly providing a way to better support its use while removing their limitations. A user here will choose a strong set of images from the given array of images. A set of three images can be chosen by the user for registration. Here images particularly means the type of the images which will be the part of the authentication mechanism these credentials will be stored on the server of the web service. And next time when the user of this system will login into the application will have to remember only the type of his images which a user had selected for registration in that application. Later the user will login into the app then he will have to choose that particular type of image that was chosen at the time of registration process. The images and location or position here will be different each time the user logins the system. The type of images remains the same, the system has a complex set of images each time he logs in, making it difficult for the person who shoulder surfs the password of the user of the application.

SESAME's concept for remembering passwords does that all, with advanced security measure in place sesame not only acts for our password remembrance but with its secured approach it also turns out to be something idea

III. ARCHITECTURE OF PROPOSED SYSTEM

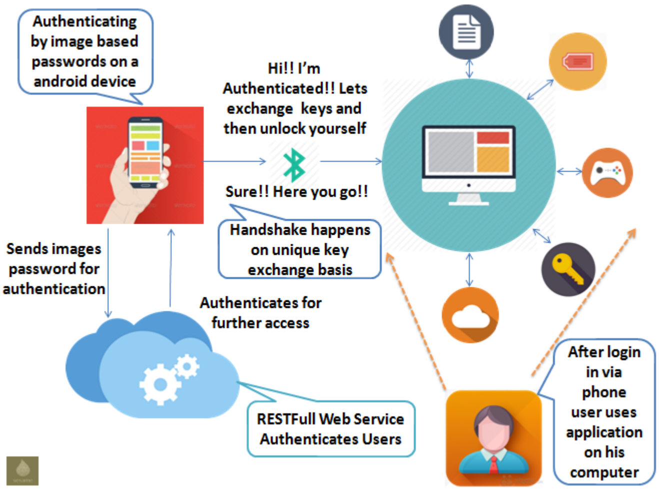
Authenticating by image based passwords on a android device
Hi!! I'm Authenticated!! Lets exchange keys and then unlock yourself
Sure!! Here you go!!
Handshake happens on unique key exchange basis
Sends images password for authentication
Authenticates for further access
RESTFull Web Service Authenticates Users
After login in via phone user uses application on his computer

Fig. 2 Architecture of SESAME

In Fig. 2 Architecture of SESAME a user of the system wants to access the secured high confidential data of his organization, he will first open App on the Phone and authenticate himself using easy to use image based password mechanism, basically here the phone is the key to that application.

He will then be authenticated via a web service. Then the user will be shown a screen on phone to connect to a host and another screen will display waiting for the device

In this process key exchanging process over Bluetooth is done. Here the person only with valid key i.e. only the person who is authenticated via a web service can only access the HOST application

Then the user seamlessly uses the computer application.

A. *Image based Authentication*

A user tends to forget passwords, with SESAME passwords which are not easy to remember. With RESTful Web Service in place, authentication is handled by the server with careful authentication mechanism. REST stands for Representational State Transfer, which is an architectural style for networked hypermedia applications; it is primarily used to build Web services that are lightweight, maintainable, secure and scalable [14]. A service based on REST is called a RESTful service. The images are sent to the web service. The web service checks that in MySQL Data base and tells whether the user is valid or not.

B. Android Aplication

After Authentication the device gets ready to tell the PC unlock you so that the user can securely use the Apps on PC in a secure way. The Android Application caters the Authentication Mechanism which is the heart of the Application. Here the user will authenticate user with his user name and the image pattern (pattern of 3 images out of grid of images). After entering the credentials user hits Log In. Image Categories are present so that user can choose his desired Pattern and that's with the twist, one's an image gets appeared the same image won't appear again, the image of that type will be displayed using a randomizer algorithm to randomize images from an array of vivid image categories, which cures the draw backs of shoulder surfing.

C. Wireless Communication

Once we have the passwords authenticated by the web service on the smart device, key exchanging needs to be done and keys need to be transferred securely to a host, so that the host can authenticate the user. This can be achieved by transferring credentials via the wireless medium using Bluetooth (BT) which were selected for SESAME. Smartphone manufacturers already plan on integrating NFC with their smart phones, many of which are already equipped with Bluetooth. SESAME uses either or both of these mediums to transfer user credentials.

Secure Token Transfer the new standards of Bluetooth provide a mechanism for encrypting all its data transfers which initially were vulnerable to DoS and MITM attacks. Another desirable aspect of Bluetooth is its short range communication and SESAME utilizes this short range to monitor the physical proximity of the user. This way a user and her smart device are virtually leashed to the Host Terminal. If the user moves away from the Host Terminal during the key exchange process, the virtual leash is broken, thus alerting the Host Terminal to lock the computer or log off the user. Similarly, due to advantages such as a very short communication range and resistance to eavesdropping, NFC is already used in financial transactions such as payments. In the current Android implementation, NFC transfers occur only when the device is unlocked (achieved only by an authenticated user). Further, NFC data rates can also transfer a user's credentials to the host device without any delay.

Even though NFC is a modern approach our system uses Bluetooth as a technology NFC can be integrated in the future scope of the application. NFC has not been so explored and not so many resources are available on the same.

IV. FLOW OF PROPOSED SYSTEM

For the shuffling of the images and shuffling of the position of the images a java rand () function is been used. With some mathematical combination the images are shuffled. The ways for authentication of the user over a web service is done by REST Protocol.

The flow of the system is shown in Fig. 3:

1. User uses app on smart phone to authenticate the application for further communication

2. If the user gets authenticated he will get a page getting ready for Bluetooth connection

3. Else he won't get an access to the service

4. After getting the success page the user will get a way to communicate with HOST by key exchanging mechanism

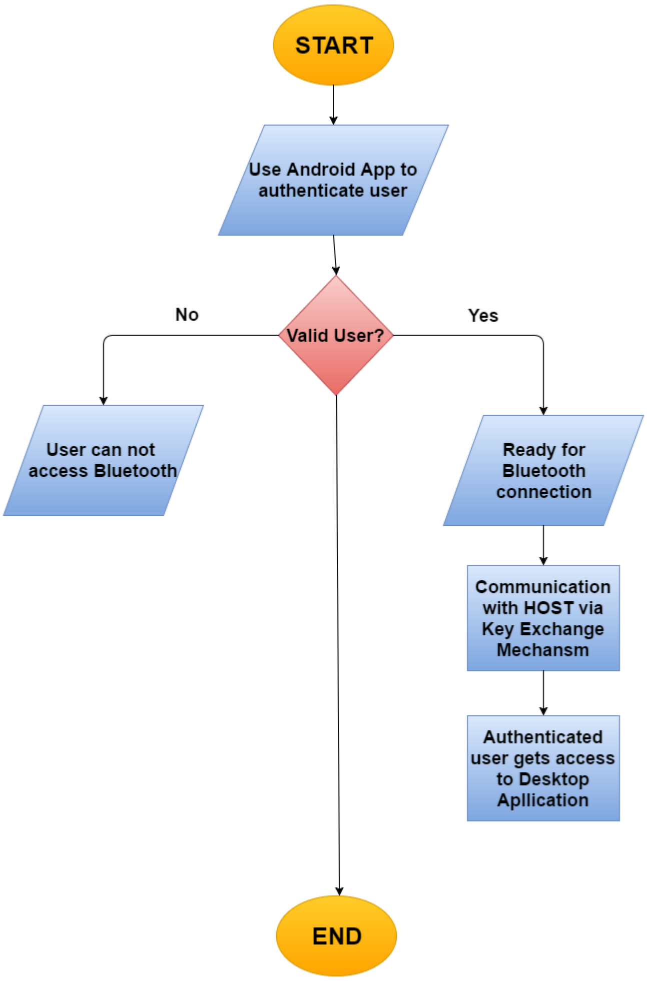
START
Use Android App to authenticate user
Valid User?
No
Yes
User can not access Bluetooth
Ready for Bluetooth connection
Communication with HOST via Key Exchange Mechansm
Authenticated user gets access to Desktop Apllication
END

Fig. 3 Flow of proposed system

5. If the user gets away for stop the communication of key exchanging process he won't get the access of the application on HOST terminal, he will have to redo the process

6. Else he will get the access of the HOST terminal.

V. SECURITY ANALYSIS

SESAME is an architecture that strengthens textual password based authentication schemes for accessing Internet based services. SESAME realizes scalability and configures durability without any major changes to the current Internet architecture or web services' authentication schemes. Further, there is no overhead on the user's part other than establishing the login credentials for the various web services and storing it securely on the smart device. Further, we discuss some aspects of SESAME. A. Security Analysis SESAME's design the philosophy of building a secure system using insecure components and is resilient against shoulder surfing and key logging attacks.

Shoulder Surfing: The most common computer authentication method is to use alphanumerical usernames and passwords [11]. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed [10]. On the other hand, if a password is hard to guess, then it is often hard to remember [12]. To address this problem, some researchers have developed authentication methods that use pictures as passwords [8].

Keyloggers attack: Keylogging is the practice of noting the keys struck on a keyboard, typically in a manner so that person using the keyboard is unaware that such action is monitored [13]. Software keylogger are installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. To avoid the thread from keyloggers many graphical password is used

MITM attacks for BT: The use Bluetooth transfer credentials precludes attacks such as eavesdropping by using secure communication channels. Further, by using Bluetooth for the pairing of the device and Host Terminal, we eliminate the MITM attacks. Bluetooth’s communication range makes it resilient against these attacks.

DoS Attacks: There have been no reports of DoS attacks targeting Bluetooth. Bluesmack, the only known DoS attack against BT exploited a specific make of devices. With newer standards, Bluetooth is also resilient to such attacks. Smart devices could present a vulnerability to DoS attacks that aim at accelerating energy consumption. However, the authors of [14] have demonstrated the ineffectiveness of such attacks, since modern smart devices have many modules that are optimized to conserve energy [4].

References

[1] Philip Inglesant & M. Angela Sasse The True Cost of Unusable Password Policies: Password Use in the Wild Department of Computer Science University College London

[2] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman : Of Passwords and People: Measuring the Effect of Password-Composition Policies Carnegie Mellon University Pittsburgh, PA National Institute of Standards and Technology Gaithersburg, MD

[3] Richard Shay _ Elisa Bertino A Comprehensive Simulation Tool for the Analysis of Password Policies International Journal of Information Security; Volume 8, Number 4; August 2009

[4] Sanzgiri Anandatirtha Nandugudi Shambhu Upadhyaya Chunming Qiao SESAME: Smartphone Enabled Secure Access to Multiple Entities Ameya Computer Science and Engineering, University at Buffalo, Buffalo, NY

[5] Adams, M. Sasse, and P. Lunt, “Making passwords secure and usable.” People and Computers, pp. 1–20, 1997.

[6] P. Inglesant and M. Sasse, “The true cost of unusable password policies: password use in the wild.” in Proceedings of the 28th international Conf. on Human factors in computing systems. ACM, 2010, pp. 383–392.

[7] “Smartphone-based authentication apps.” 2011. [Online].Available:http://www.msec.be/wiscy/ws2011/talks/talkboukayoua.pdf

[8] I.Sibiya, N.Sridivya, D.Suvitha, K.Saranya Hybrid Password Interference In Text And Cued Click Points-Based Graphical Passwords National Conference On Research Advances In Communication, Computation, Electrical Science And Structures

[9] Debnath Bhattacharya, Rahul Mahajan, Poaulomi Das, Taihoon Kim, Samir Kumar Biometric Authentication techniques and future possibilities Second International Conference of Science 2009.

[10] Abdul Rahim M Implementation of image based authentication to ensure the security of mail server Advanced Communication Control and Computing Technologies (ICACCCT), 2014

[11] Arash Habibi Lashkari Samaneh Farmand Dr. Omar Bin Zakaria Dr. Rosli Saleh Shoulder Surfing attack in graphical password authentication (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009

[12] Xiaoyuan Suo, Ying Zhu G. Scott. Owen, 2005, ‘Graphical passwords: a survey’, 21st Annual Computer Security Applications Conference.

[13] Sumit H. Wagh, Aarti G. Ambekar Shoulder Surfing Resistant Text-based Graphical Password Scheme International Conference on Computer Technology (ICCT 2015)

[14] RESTful Web Services:A Tutorial http://www.drdobbs.com/web-development/restful-web-services-a-tutorial/240169069