International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

SE based Secure Web Login Authentication using Android application

Prathamesh Raut[1], Bhushan Patil[2]

[1]*ME CNIS Student, Mumbai University, Rajiv Gandhi Institute of Technology, Mumbai (India)*

[2] *Assistant Professor, Computer Engineering Department, Mumbai University,*
Rajiv Gandhi Institute of Technology, Mumbai (India)

Abstract: *Mobile applications plays a major role by providing access to all content in systematic, arranged and analytically managed by considering all restrictions of mobile devices. Better accessibility, user experience and easy to use make mobile applications very common for people. With this, user enrolment becomes a challenge for all service providers. This paper presenting a secure way for user enrolment on web platform using mobile operating system android based platform. In this paper, we utilized fingerprint scanning and recognition technology with Secure Element available in mobile handsets for secure enrolment which help us to make and provide a secure solution for accessibility of web accounts using android application.*

Keywords: Fingerprint Authentication, Secure Elements, Trusted Login, User Enrolment, Web Security

I. INTRODUCTION

If we compare mobile handsets and their operating system with old devices and their operating systems, then we can confidently say that, today's mobile devices and operating systems running on it are much more capable and advanced. These devices become more powerful in terms of memory, operating systems and its power to handle multiple things at a time by utilizing less energy. Devices come with better enhanced hardware with enhanced architecture. We called today's mobile devices smart as new architecture and device hardware make them better. These all features help us to connect these devices with other devices in network [1]. This interconnected, smart devices are vital part of our daily life. Users access their bank account, social networks, e-mails, etc. on it [4].

Many service providers like Google, Yahoo, Microsoft and others provide their services online using web platform. Many users accessing their services freely or with some subscription charges for services [4]. But major challenge in front of all service providers is to identify their real users. For that service providers uses various authentication techniques like traditional authentication with login id and password, multi-factor authentication etc. Some providers go beyond and developed their own system to identify users by techniques like device authentication like. Sensor based device authentication, browser fingerprinting etc. [7] [3] [10]. These all techniques are used to identify user's device but still lack with user enrolment or identification on web platform.

Nowadays, Device manufactures provide various features to developers for user identification by providing access to devices hardware parts which were previously restricted through their software development kit (SDK) [4]. The famous one is fingerprint sensor which is present majority of the devices. Also, there are so many

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

components present in devices from long time but ignored like UICC commonly known as SIM, embedded chips, micro-SD cards etc. These components are to operate device on wireless mobile network and most ignored components while developing system for users security and identity [2]. In this paper, we are using UICC as a secure element with fingerprint sensor for user and device authentication for web application running over web platform. Use of fingerprint sensor and secure element UICC make this system secure in identifying user uses services running over web platform using his/her android device handset.

II. SECURE ELEMENTS AND MOBILE BIOMETRIC SECURITY SYSTEM

A secure element (SE) is a secure, tamper-resistant smart card microchip that is integrated into a mobile device. The SE is a secure component within the connected mobile device that provides the application, the network and the user with the appropriate level of security and identity management to assure the safe delivery of a particular service [13]. Going back almost three decades, the most common SE within the mobile space, and indeed the most widely used security platform in the world, is the SIM - or more accurately in today's world, the Universal Integrated Circuit Card (UICC) [2][4]. Fig.1. below showing the secure elements present in mobile devices.

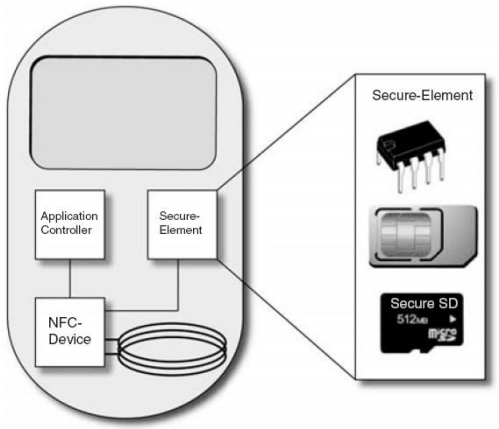

Fig.1. Secure Elements of Mobile Devices [13]

Secure Elements are present in mobile devices from very long time. But SE are the most ignored components while developing security system or application. We are using SE as unique part to for device fingerprinting. Using SE based device fingerprinting we'll be able to identify our user registered device which is registered with our secure server.

Biometric recognition system uses individual's chemical, physical or behavioural features to uniquely identify user. Considering mobile security features [4] [8]:

- SIM card with PIN code
- Numbered PIN lock and Pattern locks
- Various third party applications.

Biometric features are the unique features to identify user and that's why it is necessary to protect them very carefully. Traditional authentication system is not safe if mobile handset lost. Now day's majority of the manufactures make fingerprint sensors available in their devices and companies like Google, Samsung etc. are providing services with fingerprint detection like Google pay etc. These services are reliable and secure as user

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

don't need to remember any login id and password for it. According to market research 527 million devices are enabled with fingerprint sensors and app developer can utilize its features by services provided by service provider in their SDK's.

Mobile fingerprint sensors specially used in the following ways [4]:

- Mobile payments like Google Pay, Samsung collaborated with PayPal for password less payments using fingerprint detection technology on Samsung G5 devices.
- To open locked phone
- Most of the bank's app uses fingerprint detection with OTP in their application.
- Developers can use fingerprint detection in their apps where security concern.

III. SECURE ELEMENT AND BIOMETRIC AUTHENTICATION USING ANDROID APPLICATION

We know as per the research, 67% mobile devices having fingerprint sensors enabled. With increase in fingerprint enabled devices and access to it provided through SDK provided by service providers, make it interesting in developers and research institutions and persons to utilize fingerprint sensor for security work in multiple applications.

Many security measures have been developed to verify the user login identity for web sites in areas such as e-government, banking, and e-Learning. Some of these security measures are single use passwords, to login with identity information. Also, for some private educational sites, many users can participate in training with same username and password and that can be a security problem [4].

Our Android based Web Login Authentication application has been developed to use the mobile biometric feature login processes. The main purpose of the program is to produce a single use, time constrained password by fingerprint authentication with SE based device fingerprinting that will be used along with username and password for login to the related web site [4].

3.1. Operation of the application

This application is divided into two main parts. First, Web site or Web application and second is Android application. Android application plays an important role in this authentication for device fingerprinting and secure authentication, which generates the password for website. The operation of android application is as follows:

1. User needs to download the android application provided by service provider for the use web side of the service provider.
2. User needs to enter registered mobile number in android application for completion of the registration process. Fig.2. below showing registration page in app.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

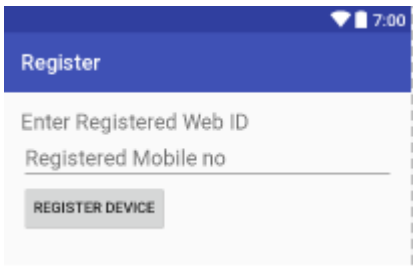

Fig.2. Android Registration Page

3. Here, Application check whether UICC is present or not. If available, then gets the ICCID number of it. Application uses Firebase notification service provided by Google. It generates the unique authentication id for each device. This unique id with registered mobile number and ICCID number of the UICC will get store in our secure web app server as well as in user's device for identification.
4. Now, whenever user login to service providers web platform. User will get a notification on registered mobile device.
5. If user clicks on notification, user will redirect to user authentication page of an android applications. If user is authenticated, then user will redirect to OTP generation page. Fig.3. below showing fingerprint authentication page.

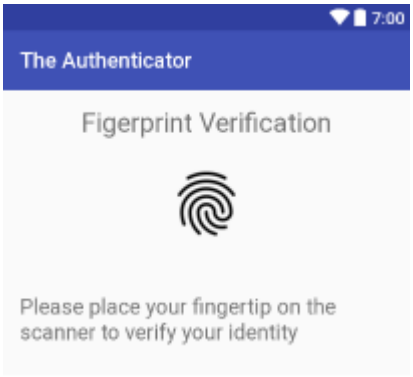

Fig.3. Fingerprint Authentication

6. Here, user gets a time based OTP. Time limit would be 30 seconds can vary depends on service provider requirement. If user failed to enter then s/he needs to login again to get OTP and needs to follow all steps mentioned above. Fig.4. below showing OTP page where user gets time based OTP.

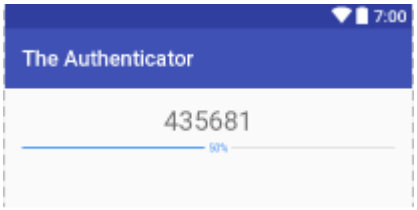

Fig.5. Time based OTP

7. If user has already downloaded and registered, then s/he only needs to verify generated him/herself to get OTP. The flowchart of the Android application program can be seen on below Fig.5.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

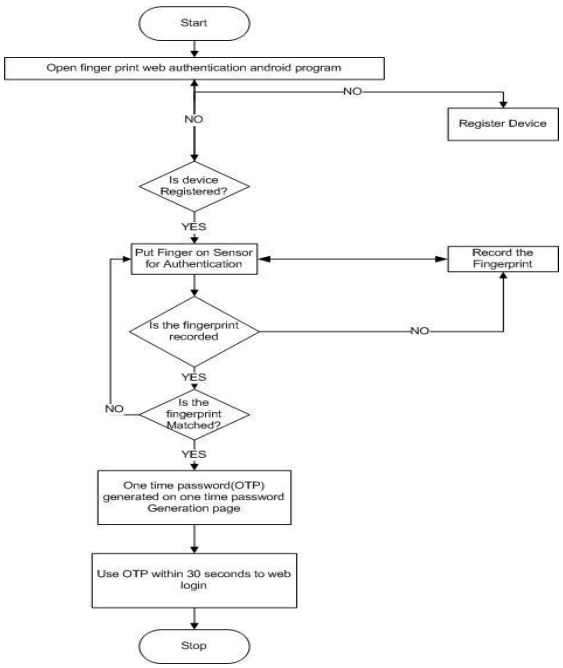

Fig.5. Flowchart of the program

First part of this system is Website. Below Fig.6. showing only login part as content of the whole site can be different with the service provider.

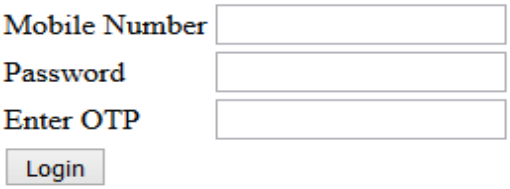

Fig.6. Login Page on Website

Here, we need to note, user can register maximum three fingerprints on device and user can use any fingerprint for successful use of the application [4].

3.2. Development of an Application

Here, we'll discuss more about the development of an application. We have used Redmi Note 3 device which is enabled with fingerprint sensor. For web application, we used WAMP as it is open source. Android application is designed and developed in Java with Google's official Android app development IDE Android Studio. We have used UICC/SIM as Secure Element and it plays important role in device fingerprinting of the device [3][7][9]. To access the state of UICC, we used Telephony Manager class which is available in the Android software stack. It helps to access information about the telephony services on the devices as well as to access subscriber information [15].

We have used Google's Firebase cloud service for notification management. It also helps to identify user's device by generating unique Firebase id and Fingerprint Manager class. It helps to access to the fingerprint hardware. Main properties of the Fingerprint Manager class that were used mentioned below [14] [15]:

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

- Register Fingerprint through enroll screen.
- Requesting Fingerprint recognition.
- Verify the current user provided by fingerprint with other stored fingerprints.

When user registered on the android application following process carried out are as follows:

1. User download the app, and it redirects to the registration page. On registration page, asks for the mobile number for as it is registered web id.
2. When user fills the required details and press register button, it checks the UICC is available in device or not. Here, two conditions occur:

- If App does not find UICC in device, app will redirect to error page showing error no UICC detected.
- If App detects the UICC then it'll fetch ICCID number of it.

3. If app get all details, then Firebase will generate unique firebase id for respective device and app sends it to secure app server for further identification.
4. Now, whenever user logged in to website user will get notification on device.
5. User needs to click on notification to get single one-time password. Once user click on the notification, user redirects to the fingerprint authentication page for user identification.
6. After successful identification, user gets the time based onetime password.
7. After one-time password generated, user needs to login to the website within the time limit given on app screen.

IV. CONCLUSIONS

In this study, we investigate that, use of secure elements and fingerprint sensor provide unique and secure way to web login authentication.

Our application is an example which showcase the benefits of using components of the mobile handsets with unique features which are ignored like UICC in secure app development from long time.

We have divided the authentication into two parts first in website and second in android app. By doing this, we have achieved the multilayer security. If attacker able to crack any security defence still s/he cannot able to gain the whole access on the user's system as other part of the authentication remain. Three main security feature are utilized in our application and they include Time based single time password, Secure Element UICC and Firebase Id for device identification and fingerprint sensor for user authentication. In this program, we managed to identify user as well as its device securely for accessing services running on the website.

Our study is expected to increase the use of untouched element like secure elements of the mobile device like UICC and biometric authentication for better and secure app development.

REFERENCES

[1.] Prathamesh Raut, Bhushan Patil, "Device Fingerprinting for Secure User Enrollment using TEE", in International Journal of Science and Research (IJSR) , Volume 6, Issue 3, March 2017 (ISSN: 2319-7064)

[2.] Michael Roland, Michael Hölzl," Open Mobile API: Accessing UICC on Android Devices",Jan 11, 2016.

[3.] Andreas Kurtz, Hugo Gascon, Tobias Becker, Konrad Rieck, and Felix Freiling, "Fingerprinting Mobile

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Devices Using Personalized Configurations" in Proceedings on Privacy Enhancing Technologies; 2016(1) : 4 – 19

[4.] Nilay_Yıldırım,Asaf Varol,"Android based mobile application development for web login authentication using fingerprint recognition feature", 23nd Signal Processing and Communications Applications Conference (SIU), May 2015(ISSN: 2165-0608).

[5.] Mohamed Sabt, Mohammed Achemlal, Abdelmadjid Bouabdallah." Trusted Execution Environment: What It is, and What It is Not." 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Aug 2015, Helsinki.

[6.] GlobalPlatform Inc, "Trusted Execution Environment: Delivering Enhanced Security at Lower Cost to Mobile Market", White Paper, June 2015

[7.] Vimal Khanna, "Remote Fingerprinting of Mobile Devices", IEEE Wireless Communications 22(6):106-113 December 2015

[8.] Frank Dickson "Hardening Android: Building Security into Core Mobile Devices", Secure Networking in Frost & Sullivan, Volume 2, Number 4, May 2014

[9.] Claudio Marforio, Nikolaos Karapanos, Claudio Soriente, "Secure Enrollment and Practical Migration for Mobile Trusted Execution Environments". [Online]. Available:https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2013/spsm_marforio.pdf

[10.] P.Eckersley, "How unique is your web browser?" [Online]. Available: https://panopticlick.eff.org/static/browser-uniqueness.pdf

[11.] https://developer.android.com/about/versions/marshmallow/android-6.0.html

[12.] https://www.globalplatform.org/mediaguideSE.asp

[13.] SIMalliance Open Mobile API, September, 2015[Online]. Available:http://simalliance.org/wp-content/uploads/2015/10/SIMalliance-Mobile-Open-API-Paper-V2_FINAL.pdf

[14.] firebase.google.com

[15.] developer.android.com