HYBRID ENCRYPTION FOR SECURING SHARED PREFERENCES OF ANDROID APPLICATION

K.Venkateswarlu, Associate Professor Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP, India

VK.Mohith Kumar, Research Scholar, Dept.of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP, India

ABSTRACT:

Most mobile applications generate local data on internal memory with Shared Preference interface of an Android operating system. Therefore, many possible loopholes can access the confidential information such as passwords. We propose a Hybrid Encryption approach for Shared Preferences to protect the leaking confidential information through the source code.We apply Hybrid Encryption approach combining encryption approach with Android Keystore system, for providing better encryption algorithm to hide sensitive data.

Android's Shared Preferences interface provides a general framework that allows us to access and modify key-value pairs of primitive data types. This data persists across user sessions, even if the application is closed. By default, Android stores this data in an unencrypted XML file within the app's directory on the device's file system, with permissions that allow only the app to access this file.

Tools such as Android Debug Bridge (ADB) can be used to navigate to the directory where Shared Preferences are created.

KEY WORDS: Scan image, Scan Hand Written Data

INTRODUCTION

The Android working framework is an open source and source code discharge by Google under Apache permit license, based on Linux-Kernel designed for smartphones and tablets. Android is one of the most popular operating systems for smartphones [1,2]. Designed to be a complete software stack, Android includes an operating system, middleware, and core applications. Furthermore, it comes with an SDK that provides the tools and APIs necessary to develop new applications for the platform in Java. Android does not distinguish between its core applications and new applications developed with the SDK; in particular, all applications can potentially interact with the underlying mobile device and share their functionality with other applications. Device loss is a pervasive problem with mobile devices and leads to severe attacks. Android KeyStore System minimizes drawback of encryption approach but still leak the data on the device. For securing data on the device, we propose the Hybrid Encryption Approach with case studies.

STATEMENT OF THE PROBLEM:

The problem lies with existing system is Android's SharedPreferences interface provides a general framework that allows us to access and modify key-value pairs of primitive data types. This data persists across user sessions, even if the application is closed which makes it vulnerable to access by the attackers.

OBJECTIVE OF STUDY:

 \checkmark Most mobile applications generate local data on internal memory with SharedPreference interface of an Android operating system.

 \checkmark Therefore, many possible loopholes can access the confidential information such as passwords. I propose a Hybrid Encryption approach for SharedPreferences to protect the leaking confidential information through the source code.

 \checkmark I apply Hybrid Encryption approach combining encryption approach with Android Key store system for providing better encryption algorithm to hide sensitive data.

REVIEW OF LITERATURE:

Android allows create and store data within the application. This section describes Shared Preference interface, possible data security vulnerabilities with the help of test application. We discuss encryption approach taken to minimize the vulnerability and its drawback.

Android's Shared Preferences [3] interface provides a general framework that allows us to access and modify key-value pairs of primitive data types. This data persists across user sessions, even if the application is closed. By default, Android stores this data in an unencrypted XML file within the app's directory on the device's filesystem, with permissions that allow only the app to access this file. This is part of the concept known as "application sandboxing." In Android, shared preferences are used to store user's preferences for Android application such as display name, notification settings, vibration on/off, etc.

Developers can use Shared Preferences to store data on a device, and an attacker can access this data from a device as well. The need of protecting it is of much importance. Tools such as Android Debug Bridge (ADB) [4] can be used to navigate to the directory where SharedPreferences are created. ADB - Android Debug Bridge (ADB) is a versatile commandline tool that lets you communicate with a device. The ADB command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device.

ADB is included in the Android SDK Platform-Tools package. An attacker can download this package with the SDK Manager, which installs it at location android_sdk/platform-tools/. As it provides access to Unix shell of Android device, it helps an attacker to navigate to data directory and read or modify any unencrypted data including SharedPreferences

RESEARCH METHADOLOGY:

System Analysis is first stage according to System Development Life Cycle model. This System Analysis is a process that starts with the analyst. Analysis is a detailed study of the various operations performed by a system and their relationships within and outside of the system. One aspect of analysis is defining the boundaries of the system and determining whether or not a candidate system should consider other related systems. During analysis, data are collected on the available files, decision points, and transactions handled by the present system.

Logical system models and tools that are used in analysis. Training, experience, and common sense are required for collection of the information needed to do the analysis.



ARCHITECTURE:

MODULES:

- ✓ User Module
- ✓ Encryption Module
- ✓ Android Keystore Module
- ✓ Decryption Module

Page | 642

DESCRIPTION:

User

In this module, User can register and login to the system.Here, he can view the profile information and view the shared preference of this an android app.He can show that how the shared preferences are created in the android application.In the proposed system the user performing two types of logins, one normal login and second one is hybrid login.

Encryption Module

In this module, user can perform the hybrid login the system automatically encrypt the login information before storing in shared preferences. The proposed method uses symmetric encryption algorithm to encrypt the login information and store the private key in android keystore.

Android Keystore Module

In this module, the encryption key is stored in the android key store.

Android key store is root memory of android operating system which cannot accessed by external applications or external users. This is secure to store the data.

Decryption Module

In this module, when user performs login the app access the android key store and decrypt the data and verifies the data. This module is very efficient and it cannot be leak any data to third party applications.

RESULTS

The result analysis describes that the entire project was executed successfully and also having quality and performance by analyzing the flow of data and output screens. In my project the modules like User, Encryption, android keystroke and Decryption are independent modules. Because my project follows the top down approach and bottom up approach.

AES Algorithm

In this project to protect the video data we adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).



OUTPUT SCREENS



SCREEN 2

lig app
 manifests java jijava (porestard) jijava (porestard) jijava (porestard) jijava (porestard) jijava (porestard) echnity, browser.xml echnity, consul, login.xml echnity, consul, login.xml echnity, consul, login.xml echnity, portal, login.xml echnity, portal, login.xml echnity, segistration.xml <li< th=""></li<>

Dogo Rangsang Research Journal ISSN : 2347-7180

SCREEN 3

M Andreid as D = A	- Annie Land	A	ciant in the	the state of state		an manana	Charlen I.	100	Parise Elle Evelance			1.4	
udio III DeviceDiplorer III emulator-5554 III data III da	data ili cons Joginumi 1 cPa 2 cm 3 4 5 c/a	stencryphon m mattivity.login mattivity.login mattivity.login string name- string name- sp>	shared_press nxml 4 0' encodir "phoneKey" "pudKey">1	■ hybopret. hybdpref.xnf ge ⁻¹ utf-8 ⁺ s ¹ >GK7bRn4iipe HjbHtzaSb8hSi	zmi	<pre>ity_registrat 'yes' ?> YQ+= == </pre>	• ⊢⊾ Poet	·W2 ·W2 ing> g>	As + C C C C C C C C C C C C C C C C C C	T.1.1, API 25 Permissi drwa:	Date 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11 2020-03-11	Siz 10:30 4 10:30 4 10:30 4 10:31 4 10:32 4 10:32 4 10:33 4 10:34 4 10:35 4	C - +
Convy_splashami C									code_cache databases lides files webviewChromiu webviewChromu comvastwol.Nop imore comvastwol.Nop	drwxrwx drwxrwx drwxrwx drwxrwx rw-rw rw-rw rw-rw drwx f -rw-rw drwx f -rw-rw f -rw f -rw	2020-03-111 2020-03-111 2020-03-111 2020-03-111 2020-04-071 2020-03-111 2020-04-07 2020-03-111 2020-03-111 2020-03-111 2020-03-111 2020-03-11	0.31 4 0.31 4 0.33 4 0.56 4 13,28 13 10,56 15 10,53 12 10,30 4 10,30 4 10,30 4	K8 K8 K8 K8 88 78 K8 K8 K8
▶, \$ Run III TODO no. Profiler III § Logcat 1	II Terminal 🔨	Build							In drm In local In local In recla In media In media In media In misc In misc	drwxrwx drwxrwx drwxrwx drwxrwx drwxrwx drwxrwx drwxrwx	 2020-03-111 2020-03-111 2020-03-111 2020-03-111 2020-03-111 2020-03-111 2020-03-111 2020-03-111 	0:29 4 0:29 4 10:29 4 10:30 4 10:29 4 10:29 4 10:30 4	KB KB KB KB KB KB KB
Install successfully finished in 562 ms. Ann restart success	ful without requir	ing a re-install (17	minutes and							61	IF UT-1	4 spaces	1. 1
install successionly minimed in our rise reppirement success	rui mitrioui requi	ing a re-instant (17	minutes ago							9.1	LF STER	- spaces	-

SCREEN 4



SCREEN 5

m/ •				-
-		Device hile Explorer		.ų -
Hybrid Encryption	<pre>xml version="1.0" encoding="utf-8" standalone='yes' ?> " ap> cstring name="obcom/key">>6301525585c/string></pre>	III Emulator Pixel_XL_API_25 Android 7.	T.1, API 25	
		Name	Permissi Date	Size
	(string name="madKey">1234(/string)	Illif com.google.android.webs	drwx 2020-03-11 10:30	4 KB
	4 have 1	E Com opogle android yout	drax 2020-03-11 10:31	4 68
	maps.	T III comsisenception	drwx 2020-03-11 10-33	4 KB
	0	Elliano textures	drawney up 2020-03-11 10-33	ARR
	V	 III ann webview 	drwx 2020-04-07 10 57	4 KR
	1940	> III cache	dewareav 2020-03-11 10 33	4 68
	Ø	Im code cache	dewarea 2020-03-11 10.31	4 KB
		b. Bill databaser	downers 2020-03-11 10-31	4 KB
	171	> III files	drawney up 2020-03-11 10-33	AKE
		T is shared needs	dewy.eev.ux 2020-04-07 10-56	AKR
Newsell Londo		com sis encontion	-nu-nu 2020-03-11 13-28	136 R
A Normal Login	Q	hybdroef yml	-04-04-07 10-56	158.8
		Wahling Chenning	-50-50-03-11 10-33	127 R
	1	In the new later has	downers 2020-03-11 10-30	AKR
Encrypt Login	7	b in consent norman	dowy	AKR
1		E non chromium webview s	drag	AKR
	0	E III dem	drawnaw 2020-03-11 10-29	4 KB
		 Im Inval 	dewar-xx 2020-03-11 10-29	488
		> Im Instafound	drawney	4 KB
and the second se		h 🖿 media	dewarew 2020-03-11 10-30	4 KB
and the second se	Case -	mediadem	drwxrew 2020-03-11 10 29	4 KB
State of the second sec		misc	downey-+t 2020-03-11 10-29	4 10
the second se		> misc ce	drwarwat 2020-03-11 10:30	4 KB
		E misc de	drawrwat 2020-03-11 10:29	4 KB
		E De nativatest	dewartures 2020-03-11 10-28	4 KB
		> IIII ota	drwxrwx+ 2020-03-11 10:29	4 KB
		▶ IIII ota package	drwxreix 2020-03-11 10:29	4 KB
		> Im property	drwx 2020-03-11 10:30	4 KB
		in resource-cache	drwxrwx> 2020-03-11 10:29	4 KB
A Run II TODO (7) Profeer E & Logast	minal 🔨 Build		91	Event Lo
Install successfully finished in 662 ms : Ann restart successful	thout requiring a re-install. (15 minutes and)		61 LE UTUL 4 spa	ices 2

SCREEN 6

Hybrid Encryption	Q ¢ -			III Emulator Pixel_XL_API_25 Ar	vdroid 7.1.1, API 25	
Hybrid Encryption	Q Q - Al TextView Button			IIII Emulator Pixel_XL_AP1_25 Ar	xdroid 7,1.1, API 25	
Hybrid Encryption		 	H A 2			
Name 2	All TextView			Name	Permissi Date	1
Name	🕈 🔳 Button	The second se	Alla	> III acct	drwxr-xr-x 2020-03-11 10:29	ĩ
Name		197 AWALDO - C	b	▶ IIII cache	drvxrvx 2020-03-11 10:29	į.
Name 3	I ImaneView		2	► Im config	drwxt-xt-x 2020-03-11 10:29	ģ.
				> mit d	Inverse 1970-01-01 05:30	ŝ.
	i nesydenten _	the second se		► IIII data	drwxrwxx 2020-03-11 10:29	ġ.
Emulii	Co consignents			▶ IIII dev	drwxr-xr-x 2020-03-11 10:29	1
initian three duppend com-	ScrollView			▶ IIII etc	Invervoews: 1970-01-01 05:30	ŝ.
Mobile	=== Switch			► IIII mnt	drwxr-xr-x 2020-03-11 10:29	2
4201122100				> IIII oem	drwxr-xr-x 1970-01-01 05:30	5
Address				▶ IIII proc	dr-xr-xr-x 2020-03-11 10:28	8
Indiana	O			>> IIII root	drwx 2017-05-20 00:27	1
				▶ IIII sbin	drwxr-x 1970-01-01 05:30	ġ.,
		and the second se		▶ III sdcard	Investmention 1970-01-01 05:30	à.
		and the second se		storage	drwxr-xr-x 2020-03-11 10:30	8.
	Tree 🌣 —	and the second se		> IIII sys	dr-xr-xr-x 2020-03-11 10:29	ŷ.
	O avout (vertical)			system	drwxr-xr-x 1970-01-01 05:30	ð.
	login "Narmal Login"			⊨ liff var	Invervence 2020-03-11 10:29	9
	encent login Thront			Ill vendor	Invixrexrex 1970-01-01 05:30	8.
	Concipcodition and			10 bugreports	Invictive 1970-01-01 05:30	2
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	and the second se	in the second se	in charger	Invocework 1970-01-01 05:30	ŝ.,
	***	Press 1		efault.prop	-nw-rr 19/0-01-01 02:30	1
				file_contexts.bin	-rw-rr 1970-01-01 05:30	
			· π.	IDE and Pla	ugin Updates	
			100	Android St	udio is ready to update.	
• •			11	in interview.	DAMES IN TRADUCTION OF	
				in init envire		-
	1			init.goldfi 1 Plugin Upo	sate Recommended	
	/ · · · · · · · · · · · · · · · · · · ·			init ranch Android Gr	radle Plugin is ready to update.	
				init rancho-noencrypcit.		5
k, g Run III TODO 17) Profiler III § Logcat II	🗄 Terminal 🔨 Build				0	Ð
Install successfully finished in 662 ms.: App restart successf	ul without requiring a re-install. (2 minutes a	go)			CRLF UTF 4 sp	pa

CONCLUSION:

This project discussed the security leaks of an Android application due to XML files generated within the internal memory of application. This paper demonstrated the leak of the encrypted confidential data on internal memory with SharedPreference interface. We proposed a Hybrid Encryption approach for SharedPreferences combining encryption approach with Android Keystore system to protect the leaking confidential information from the Android device. The test results indicated that proposed Hybrid Encryption approach enables to secure local data on the device.

REFERENCES:

- 1. <u>https://www.tutorialspoint.com/android/android_resources.htm</u>
- 2. https://developer.android.com/guide/index.html
- 3. <u>https://www.engineersgarage.com/articles/what-is-android-introduction</u>
- 4. <u>http://www.beginandroid.com/intro.shtml</u>

5. <u>http://www.gcflearnfree.org/androidbasics/intro-to-android-devices/1/</u>

6. <u>https://en.wikipedia.org/wiki/Android</u>

REFERENCES

 "Number of Google play store apps 2016 statistic," Statista, 2014. [Online]. Available: http://www.statista.com/statistics/266210/numberofavailable-applications-in-the-google-play-store.
 "Smartphone users worldwide 2014-2020 statistic," Statista, 2016. [Online]. Available: https://www.statista.com/statistics/330695/numberofsmartphone-users-worldwide.
 "SharedPreference" [Online] Available:

https://developer.android.com/reference/android/content/SharedPreferences.html

[4] "ADB" [Online] Available: https://developer.android.com/studio/command-line/adb.html

[5] "CheatDroid application" [Online] Available: https://play.google.com/store/apps/details?id=com.felixheller.sharedprefseditor&hl=en

[6] "Android Keystore System" [Online] Available: https://developer.android.com/training/articles/keystore.html#SecurityFeatures

[7] Suchita Tayde, Seema Siledar, "File Encryption, Decryption Using" 2015 International Journal of Advanced Research in Computer Science and Software Engineering. [Online] Available: https://www.researchgate.net/publication/315669325_File_Encryption_Decryption_Using_AES_Alg orithm_in_Android_Phone

[8] Rohan Rayarikar, Sanket Upadhyay, Priyanka Pimpale, "SMS Encryption using AES Algorithm on Android" 2012 International Journal of Computer Applications [Online] Available: http://www.ijcaonline.org/archives/volume50/number19/7909-1038

[9] Tim Cooijmans, Joeri de Ruiter, Erik Poll, "Analysis of Secure Key Storage Solutions on Android."2014 Proceeding SPSM '14 Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices [Online] Available: https://dl.acm.org/citation.cfm?id=2666627

[10] Poonguzhali P., Prajyot Dhanokar, M. K. Chaithanya, and Mahesh U. Patil, "Secure Storage of Data on Android Based Devices." 2016 IACSIT International Journal of Engineering and Technology, Vol. 8, No. 3 [Online] Available: <u>http://www.ijetch.org/vol8/880-ST011.pdf8 m</u>

[11] Penchalaiah, P., & Rajasekar, P. An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data. International Journal of Future Generation Communication and Networking (WoS), ISSN, 2233-7857.