SURVEY ON ANDROID SECURITY MODEL

[1]Kavita , [2] Rekha, [3] Preeti

[1,2,3]Computer Science & Engineering Department, M.D.U. (India)

ABSTRACT

This paper presents the study of Android Security Model. . In this paper a study of various papers is done, and in the reviewed paper we explain the application of android system. Intents, Activities, Broadcast Receivers, Services, Content Providers and Binder. As android is open source we should also have this code available to us. Both the java and C code is critical for understanding how Android works, and is far more detailed than any of the platform documentation

Keywords*: *Android Tool, Android, API, Access Permission, Security

I. INTRODUCTION

In present days people carry mobile devices rather than desktops or mainframes computer. So the importance of data and services support the increasing vulnerability.

Android provide a platform for usable security infrastructure. Android has been developed by open Handset Alliance(led by Google).It provide a base operating system, application middleware layer, java software development kit(SDK) and collection system application. As we know Android SDK has been available since 2007. Traditional desktop and server operating systems have tried to securely integrate personal and business applications and services on a single platform. And when we did it on a mobile platform such as Android it remains nontrivial. Many researchers observe that it provides a clean slate devoid of the complications that legacy software can cause. Android doesn't officially support applications developed for other platforms: The applications execute on top of a Java middleware layer running on an embedded Linux kernel, so developers wishing to port their application to Android must use its custom user interface environment. Additionally, Android restricts application interaction to its special APIs by running each application as its own user. This article attempts to show the complexity of Android security and summary some possible development pitfalls which can be showed while defining an application 'security. We conclude by attempting to draw some aspects and identify opportunities for future scope that should be showed in clarity and correctness entity.

Android is a widely anticipated open source operating system for mobile devices which provides a base operating system, an application middleware layer, a Java software development kit (SDK), and a collection of system applications. Android has a unique security model that focuses the user work in control of the device. Android devices provide the open nature of the platform allows for proprietary extensions and changes.

II. BRIEF DESCRIPTION OF ANDROID SECURITY MODEL

Android is a program having Linux platform with java. It enhanced its own security. It combines OS features like multitasking, Unix User Identifier (UID) and file permission. It is familiar with class library and safe java language. This model is like multi-user server than sandbox found on J2ME or blackberry platform. The Android GUI environment has some novel security features that help support this isolation. Mobile platforms are rapidly increasing which results in having complex requirements including regulatory compliance [6].

Android supports building applications used by phone feature quality while protecting users by minimizing the consequences of bugs and software. Android's process isolation results the need for complicated policy configuration files for sandboxes. This gives flexibility to applications to its use native code without compromising Android's security or granting the application rights. Android permissions are necessary for the given applications which allow them to do things like take pictures, use the GPS or make phone calls. When installed applications having unique UID, and the application will always execute as that UID on that particular device. The UID of an application is used to secure its data and developers have needed to be explicit about sharing data with other application [7]. Applications can allow users to work or entertain with graphics, playing music, and launch other programs without special permissions. Malicious software is reality software on popular platforms, and with its features Android tries to minimize the impact of malware. However, even unprivileged malware which gets installed on an Android device pretending to be useful can still temporarily allows the user's experience [8]. Users in this unfortunate state will have to identify and remove the hostile application.

III. ANDROID APPLICATION CRITERIA

Application framework mainly enforces on structure to developers. It does not have main () function. Instead of using main () function developers design application in terms of components. For explaining this we can take example or described as the Friend Viewer application are used to retrieve the stored geographic coordinates and view friends on a map. Both applications contain multiple components for performing their respective tasks the components themselves are classified by their component types. An Android developer chooses from predefined component types depending on the component's purpose (such as interfacing with a user or storing data). An application developer defines one activity per "screen." Activities start each other, possibly passing and returning values. In this application only one process can be running like keyboard work and all other are suspended. In the working of Android application there are two functions performed i.e. component protection and component interaction. In Component Interaction there are two components there is System server which has two components system service and location manager. System service communicates with boot receiver and location manager communicate with friend tracker.

After that boot receiver get contacted with friend tracker then friend provider used to read or write the function and friend tracker control perform the functioning of start/stop with friend tracker.

In component protection, friend tracker, friend viewer and contact are three applications which get communicated with ICC reference monitor. Android protects application and data through enforcement mechanism on the System level as well as at ICC level. Generally, each application runs as unique user identity.

IV. ACCESS PERMISSION

For developing Android application developer have to assigns some permission access. The permission assigned via XML manifest file which accompanies every package application.

In this framework, developer assigns permission to define application security and write permission

This permission can be explained at various levels. The Access permission are as follows-

Protection Permission

Broadcast permission

Content Provider

V. SECURITY

In this phase main aspect is to make process secure. In this phase, developer focuses on how their code will keep user safe as well as how to get behave with constrained memory, processing and power of battery.

Developer has to secure input data into device with their application and did not allow malware to access application without special permission. The big trick in android development is that every application runs with different UID. In Android, the system has given its own UID rather than every person.

For example, an application wants the READ_CONTACTS permission to read the user's address book. A contact manager application wants the READ_CONTACTS permission, but a block stacking game should not keep the model simple. It is possible to secure the use of all the different Android inters- process communication (IPC) mechanisms with just a single kind of permission. Starting Activities, connecting to Services, accessing Content Providers, sending and receiving broadcast Intents, and invoking Binder interfaces can all require the same permission. Therefore users do not wants to understand more than ―My new contact manager needs to read contacts.

VI. CONCLUSION

Android application can communicate with different ways. In this paper, we conclude that we can make our data and communication security by allowing special permission. Android applications have their own identity given or enforced by the system. Application can be communicated with the mechanism provided by the system like file, activities and content provider.

While communicating with other program makes sure that how much you can trust your input and validate the identity of services you used up.

VII. ACKNOWLEDGMENT

We express thanks to all the departments' personals and sponsors who give us an opportunity to present and express my paper on this level. We wish to place on my record my deep sense of gratitude to all reference papers authors for them valuable help through their papers, books, websites etc.

REFERENCES

[1] J.P. Anderson, Computer Security Technology Planning Study, tech. report ESDTR-73-51, Mitre, Oct. 1972.

[2] M.A. Harrison, W.L. Ruzzo, and J.D. Ullman, "Protection in Operating Systems," Comm. ACM vol. 19, no. 8, 1976, pp. 461–471.

[3] L. Badger et al., "Practical Domain and Type Enforcement for UNIX," Proc. IEEE Symp. Security and Privacy, IEEE CS Press, 1995, pp. 66–77.

[4] J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," Proc. IEEE, vol. 63, no. 9,S 1975, pp. 1278–1308.

[5] I. Krstic and S.L. Garfinkel, "Bitfrost: The One Laptopper Child Security Model," Proc. Symp. Usable Privacy and Security, ACM Press, 2007, pp. 132–142.

[6] N. Li, B.N. Grosof, and J. Feigenbaum, "Dele gationLogic: A Logic-Based Approach to Dis tributed Authori zation," ACM Trans. Informa tion and System Security,vol no.1, 2003, pp. 128–171.

[7] W. Enck, M. Ongtang, and P. McDaniel, Miti Android Software Misuse before It Happens, tech.report NAS-TR-0094-2008, Network and Security Re

search Ctr., Dept. Computer Science and Eng., Pennsylvania State Univ., Nov. 2008.

[8] Chu, E. (2008, August 28). Android Market: a user driven content distribution system. Re trieved August

30, 2008, from Android Devel oper's Blog.
[9] Google Inc. (2008, August 29). Security and Permissions in Android. Retrieved August 30, 2008, from An droid - An Open Handset Al liance Project.
[10] Burns, Jesse (2009, October) developing secure mobileapplications for android.
[11] Royce, Winston (1975), "Managing the Development of Large Software Systems", Proceedings of IEEE WESCON, 26 August, 1975.
[12] Richard N. Taylor, Will Tracz, and Lou Coglianese(1995),"*Software development using domain-specific software architectures," SIGSOFT Softw. Eng. Notes*, vol. 20, no. 5, pp. 27–38, 1995.
[13] Rajendra Ganpatrao Sabale, Dr. A.R. Dani(2012)," *Comparative Study of Prototype Model For Software Engineering With System Development Cycle Model*", IOSR Journal of Engineering (IOSRJEN),Volume 2, Issue 7,July 2012.