IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003188

Arresting the Advertisements Behaviour in Android Application

Ashok Kumar K, Nikhill, Santhosh S, DR.K.Anbazhagan

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Associate Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: Nowadays, app developers tend to integrate advertisement libraries (or ad libraries) into their apps to get revenue from ad networks. However, researches have shown that both ad libraries and ad contents could raise serious security and privacy concerns. In this paper, we propose Ad Capsule, a user-level solution to practically confine advertisements, including ad libraries and ad contents. Our solution does not need to change the Android framework, nor requires the root privilege, thus can be readily deployed. Specifically, we propose the permission sandbox, which isolates the permissions used by ad libraries from the host app, and the file sandbox, which separates the file operations of advertisements. The ad library and ad content cannot read or write any file outside this sandbox. We have implemented a prototype of Ad Capsule. Our evaluation results indicate that Ad Capsule can successfully enforce security policies to block attempts of accessing private information or manipulating files of the host app, and the performance overhead introduced by Ad Capsule is low

KEYWORDS: Andriod Application, Ad-capsule, Adagency, Adprovider, Malicious advertisements detection

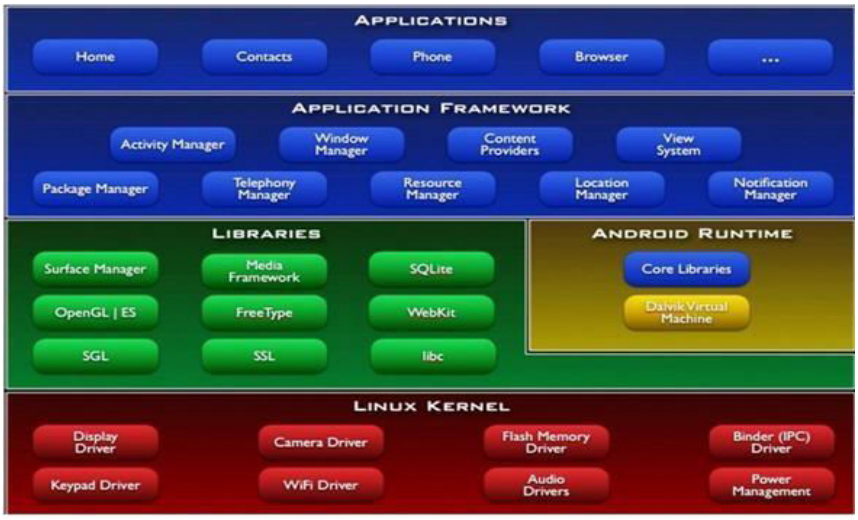
I. INTRODUCTION

The main aim of this paper is to have control of the in app advertisements in order to restrict the unauthorized access of personal information.Due to the proliferation of mobile phones in recent years there are many advantages and some disadvantages in smart-phones usage. Many applications like Ecommerce, Social media and games get access of user's permission to use some privileges. Normally while installing any application we used to grant permission to the particular application to access all the privileges. So when the applications which we install in our smart-phones have some tie-up with some advertisement company. So that for the benefits of the app developer those ads will run in our app. Here in this case the advertisements can behave maliciously some times. This malicious behavior extracts personal information like user's contact and files by using the permission access policy of particular app. This data theft may happen without the knowledge of user; the malicious ad will upload the collected information to the desired server. We propose a third party Server to validate the advertisement before the ad get loaded into the app.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003188



II. LITERATURE SURVEY

[1] PScout: Analyzing the Android Permission Specification
Author Name: Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang and David Lie
Year of Publishing: 2012
Android, Developed PScout, a tool that extracts the permission specification from the Android OS source code using static analysis. PScout overcomes several challenges, such as scalability due to Android's 3.4 million line code bases, accounting for permission enforcement across processes due to Android's use of IPC, and abstracting Android's diverse permission checking mechanisms into a single primitive for analysis

[2] Efficient Privilege De-Escalation for Ad Libraries in Mobile Apps
Author Name: Bin Liu, Bin Liuy, HongxiaJin, Ramesh Govindanz
Year of Publishing: 2015
Pedal, contains a novel machine classifier for detecting ad libraries even in the presence of obfuscated code, and techniques for automatically instrumenting by tecode to effect privilege de-escalation even in the presence of privilege inheritance. We evaluate PEDAL on a large set of apps from the Google Play store and demonstrate that it has a 98% accuracy in detecting ad libraries and imposes less than 1% runtime overhead on apps.

[3] FLEXDROID: Enforcing In-App Privilege Separation in Android
Author Name: JaebaekSeo, Daehyeok Kim, Donghyun Cho, TaesooKimy, Insik Shin
Year of Publishing: 2016
Mobile applications are increasingly integrating third-party libraries to provide various features, such as advertising, analytics, social networking, and more. Unfortunately, such integration with third-party libraries comes with the cost of potential privacy violations of users, because Android always grants a full set of permissions to third-party libraries as their host applications.

III. PROPOSED METHODOLOGY AND DISCUSSION

EXISTING SYSTEM:
Normally while installing any application we used to grant permission to the particular application to access all the privileges.In the existing system,the applications we install in our smart-phones have some tie-up with any advertisement company and for the benefits of the app developer those ads will run in our app.Here in this case the advertisements can behave maliciously some times. This malicious behavior extracts personal information like user's contact and files.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

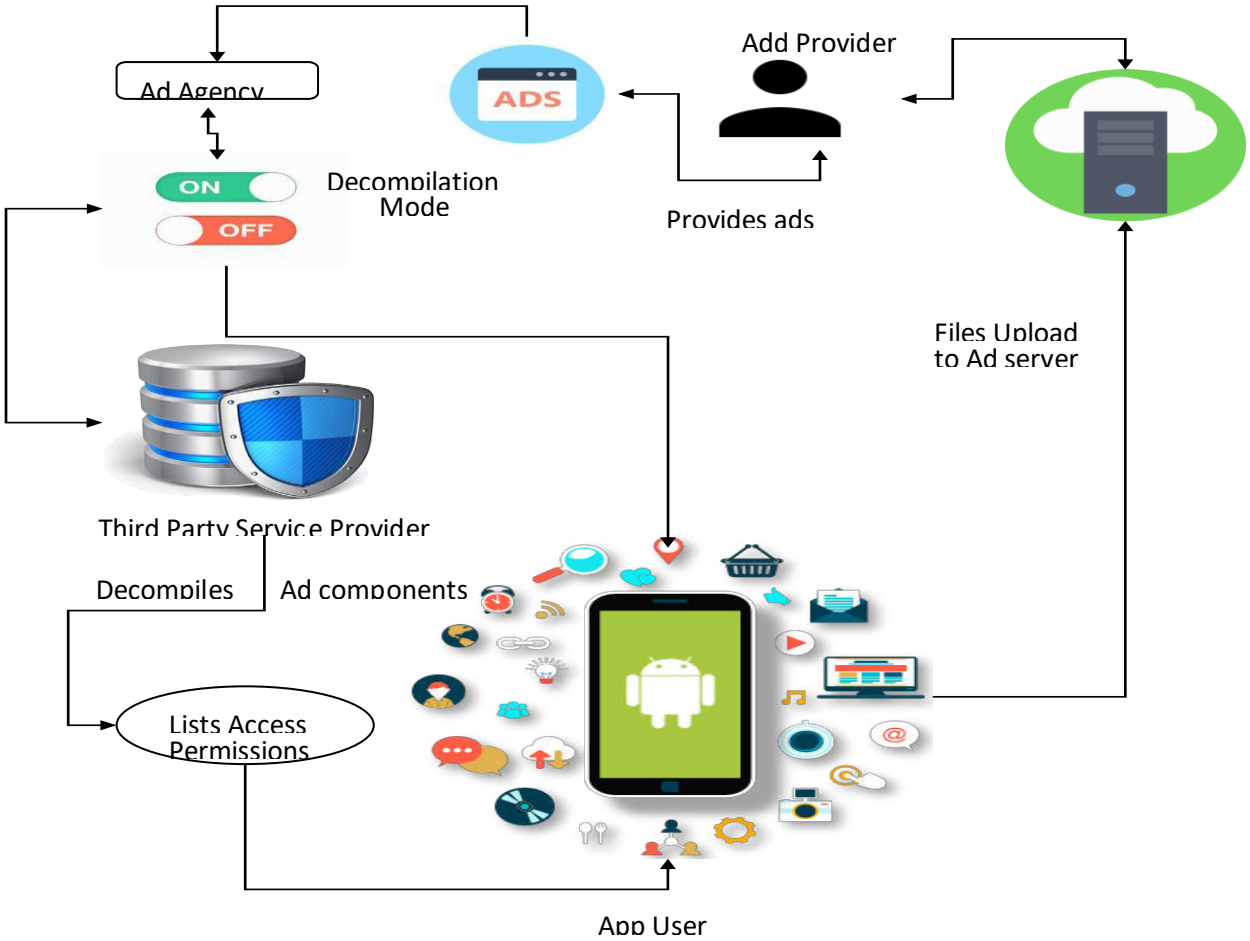
|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003188

PROPOSED SYSTEM

We propose a third part service advertisement library, Here the User whenever install any new application the third party service will start checking the incoming adds. So before loading a new advertisement into the application our system will analyze the triggering components inside the ads and its behavior.our system is capable of detecting that kind of ads and restrict their access,then pop up the required access permission list to the user. Only when the user accepts that permission it will allow the ad to run inside the hosted app. Otherwise our system will block the malicious ads.

Architecture of the proposed system



Adding Application in Ad agency

In-order to use our application the users need to do user registration. After Ad Agency user Authentication the users or application developers will add their applications to the AdAgency portal. While adding an application they has to give basic information about the app like number of downloads, number of daily user logins, ratings, and App Id is mandatory. After that when an Ad-Agency admin sign-in into the portal the requested applications for advertisements will be shown. Here the admin has the privilege to set amount for the requested applications..

Ad provider Purchasing App Bundle

After the Ad Provider User registers into Ad Agency, The Provider as well as Agency has to generate new bank account using our Bank application. After accounts created successfully they can do money transfer for any desired accounts. Then the Ad Provider has to sign-in the Ad-Agency page and look for apps satisfying their criteria. They can select the apps in a bundle by applying filters based on their type of advertisement content, ratings, cost , number of downloads and number of daily users. After filtration an app bundle will be formed with Agency's applied offers. So now the Ad Provider has to purchase the app bundle.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003188

Hosting Ad in APP Bundle

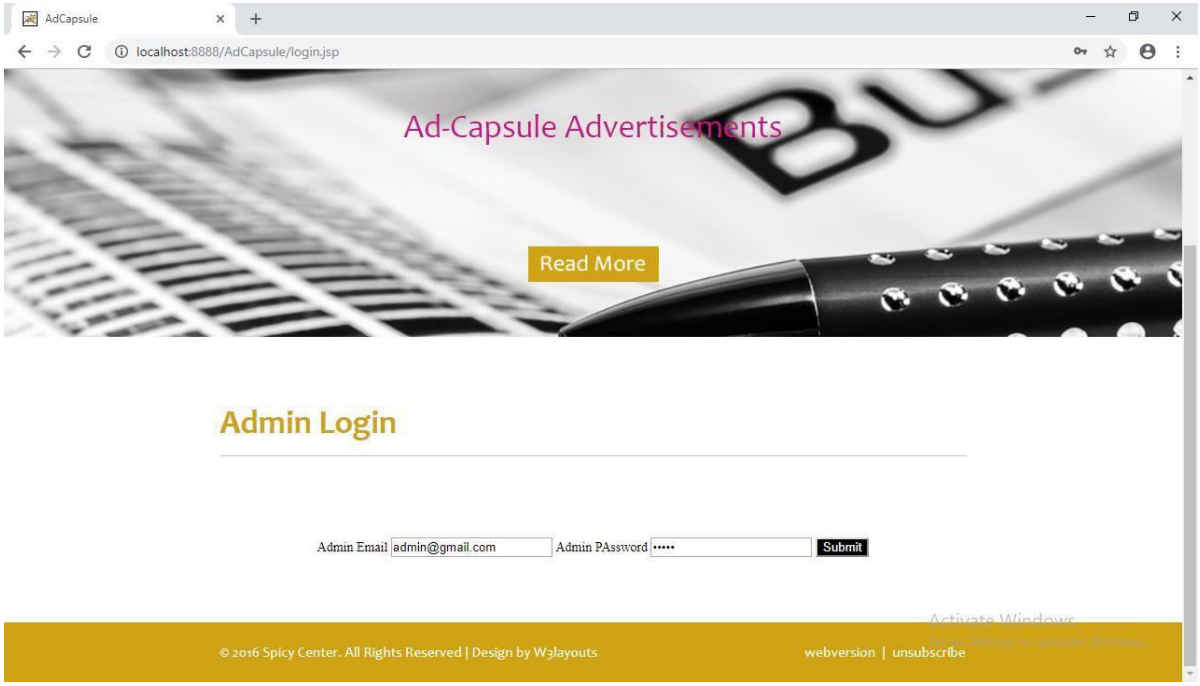
After bundle purchase the Provider has to upload the suitable ad content which is of types transport, education or health. After uploading the ad content into Agency, it will be 32 automatically loaded into the end applications whose app id is there in the selected bundle. For each category of application we will be showing a related category Android Application. For example we run a health related app. Once an advertisement gets hosted into that application the ad content will start initiating its malicious behavior. If the application uses permission like sms or contacts the ad-content will make use of it and send all user's sms or contacts to their ad-Server automatically without user's knowledge in background.

Third-Party Service Provide

We implement a Third Party Service Provider in Ad-Agency side to verify the malicious contents of incoming advertisements .So whenever a new adcomponent is loaded into the empty spaces allocated for specific ads. The ads get loaded into certain locations inside the host apps. We need to do a preprocessing technique in our proposed Third party Service Provider. So when an advertisement is loaded first into the application the Service provider will check or process all the running components using decompilation and find out the possible permission access that the ads going to get from the hosted application. Then the Third party application will send a request to the application user in order to grant permission for authorized access. A popup will be shown to the app user and get the authorized access. Hereby we can restrict the ad components from getting access to user's sensitive data. Thus we can handle the ads from misbehaviors. This is known as confinement of advertisements

IV. EXPERIMENTAL RESULTS

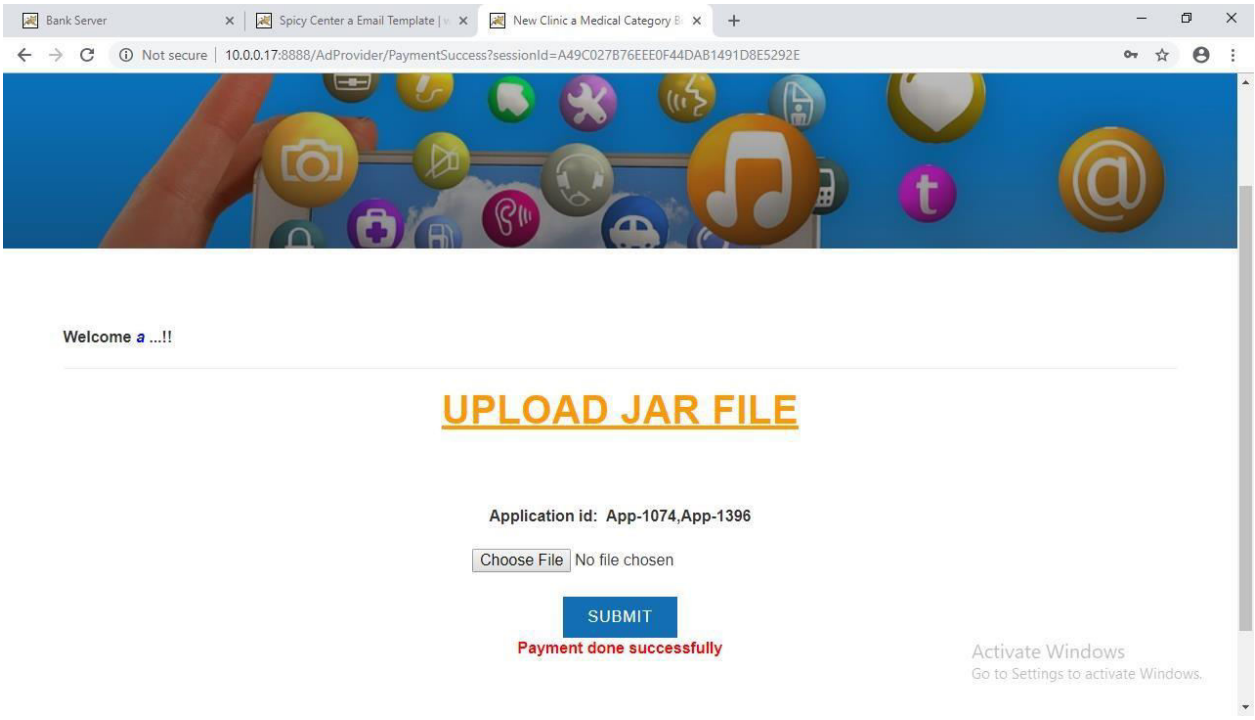
SCREENSHOTS

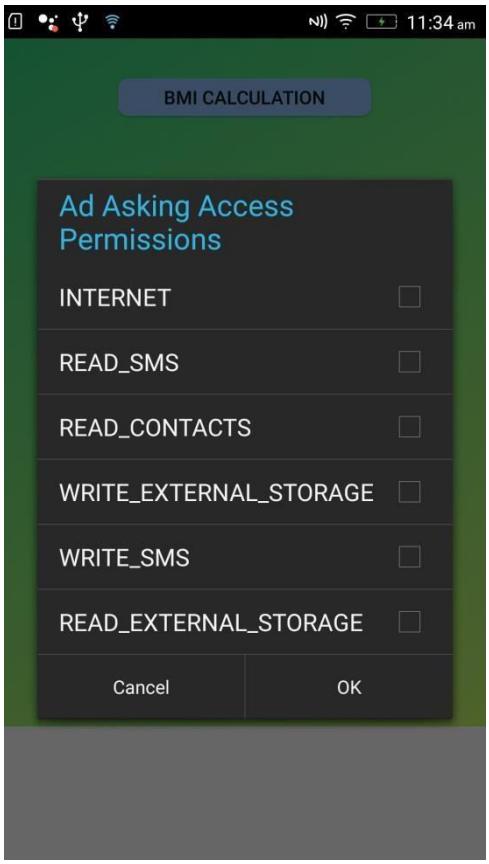


| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003188





| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003188

V. CONCLUSION

The AdCapsule protects the users from malicious ads which can steal user's information. The user can trust apps which is registered with AdCapsule as it is more safe and secure in protecting users data.

Future WORKS

In the future, we can implement the third party ad service in other operating systems like ios,linuxetc protecting users information. A cloud based system for the third party ad server can be added in the future.

REFERENCES

[1] "Number of Android applications." https://www.appbrain.com/stats/number-of-android-apps.
[2] "Free vs. paid Android apps." https://www.appbrain.com/stats/free-and-paid-android-applications.
[3] "Security Alert: New Stealthy Android Spyware – Plankton – Found in Official Android Market." https://www.csc.ncsu.edu/faculty/jiang/Plankton/, 2011.
[4] "PontiFlex Ad Library - Remote JavaScript Command Execution." https://labs.mwrinfosecurity.com/blog/pontiflex-ad-library-remote-javascript- Cmmandexecution/, 2013.
[5] "Setting the Record Straight on Moplus SDK and the Wormhole Vulnerability." http://blog.trendmicro.com/trendlabs-securityintelligence/setting-the-record-straight-on-moplussdk-and-the-wormhole-vulnerability/, 2015.
[6] S. Demetriou, W. Merrill, W. Yang, A. Zhang, and C. A.Gunter, "Free for All! Assessing User Data Exposure to Advertising Libraries on Android," in Proceedings of the 23rd Annual Symposium on Network and Distributed System Security, NDSS, 2016.
[7] M. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi, "Unsafe Exposure Analysis of Mobile In-App Advertisements, "in Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks, ACM Wi sec, 2012.
[8] S. Son, D. Kim, and V. Shmatikov, "What Mobile Ads Know about Mobile Users," in Proceedings of the 23rd Annual Symposium on Network and Distributed System Security, NDSS, 2016.
[9] N. Daswani and M. Stoppelman, "The anatomy of clickbot. a," in Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, pp. 11– 11, USENIX Association, 2007.
[10] A. Dewald, T. Holz, and F. C. Freiling, "Adsandbox: Sandboxing javascript to fight malicious websites," in Proceedings of the 2010 ACM Symposium on Applied Computing, pp. 1859–1864, ACM, 2010.
[11] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna, "The dark alleys of Madison avenue: Understanding malicious advertisements," in Proceedings of the 2014 Conference on Internet Measurement Conference, pp. 373–380, ACM, 2014.
[12] X. Dong, M. Tran, Z. Liang, and X. Jiang, "Adsentry: comprehensive and flexible confinement of javascriptbased advertisements," in Proceedings of the 27th Annual Computer Security Applications Conference, pp. 297–306, ACM, 2011.
[13] T. Book and D. S. Wallach, "An empirical study of mobile ad targeting," CoRR, vol. abs/1502.06577, 2015.
[14] S. Han, J. Jung, and D. Wetherall, "A study of thirdparty tracking by mobile apps in the wild."

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details