Malware Detection In Android: Assignment 1

Nagadevara Venkatesh
p.no: 942011-6551
vena15@student.bth.se

patta siva venkat prasad
p.no: 931221-7137
sipa15@student.bth.se

ABSRACT

In this report we will see and compare various criteria that a good article should posses. Fulfilling these criteria Incorporating them in our article would create a good impact in the readers mind. Hence forth we will see and compare three different articles and provide a brief description about them.

I. INTRODUCTION

In recent years there is a increase in android based smartphones. As it is a open source project, it has become a open arena for malware developers. There is a increase in android malware in recent years. As all mobile phones contains users information such as contacts, banking details, personal data and messages. Android malware such as premium rate sms Trojan, spyware, botnets, aggressive adware are some of the attacks reported in Google play store and android also supports third-party market applications there is a high risk. Google play does not verify the uploaded apps manually. They depend on bouncer which is a dynamic environment which protects against malware attacks it does not check vulnerability of uploaded apps. So malware authors take this as an advantage of such vulnerable apps and try steal users data.

II. LITERATURE SEARCH

After selecting the problem area, we framed some key words such as android, security, malware, detection and searched the scientific databases like ACM, INSPEC, Scopus, IEEE. The results are not so relevant the selected topic . We got relevant papers in IEEE explorer. There are about 110 relvant papers to the selected topic. So we limited the search to year 2015 we got three papers. It contains of two conference papers and one early access article.

III. COMPARITIVE STUDY

1. What is the problem area being addressed in each of these articles?

   They have same problem addressed in three articles that is malware detection in android. To be precise article [1] is “A Survey of issues, Malware Penetration And Defenses”. The problems specified in article [2] is”Malware Detection in Android by Traffic analysis”. Article [3] specifies about “An Automated Virtual Security Testing Platform For Android Mobile Apps”.

   Identified problem is well stated in each paper and the approaches for solving the problem are good in each article.
2. How is research question formulated?

   The authors from three articles had well specified research question. According to us the research questions specified are in article [1] is “What are the present issues, penetrations and defenses”. In article[2] is “How to detect malware applications by network traffic analysis”. In article [3] is “ To find malware in a virtual emulated environment”.

3. What are method or methods used in the reported study?

   The methods used in article [1] is empirical approach it is well defined. In article [2] the method is the authors proposed a framework based on experimental approach and is well justified. In article [3] we proposed a experimental approach.

4. How and why are methods chosen?

The author of Article [1] considered all cases and choosen a better method for app verification. In article [2] and article [3] proposed an experimental approach, but in article [3] author does not state any methods.

5. How were these methods applied in the study?

In article [1] is a case study and it describes about of existing methods. He proposed that behavioral approach to guard the centralized app markets from malware authors. And discussed about Android Security Architecture.

In article [2] author proposed a malware detection by monitoring network traffic analysis. This is a better method but it is not efficient every time.

In article [3] author proposed that he would produce a emulator that will help to verify apps but did not tell about any methods for the tool.

6. How are the results presented in each study?

In article [1] the author expressed all the causes and given a solution to the problem in form of a distributed mechanism.

In article [2] the author proposed an experimental approach by analyzing network traffic

In article [3] the author expressed did not give result but he told that he is going to develop a software that would analyze malware in apps.

7. How do the presented results relate to the problem area and stated research question being addressed?

In article [1] the presented results are related to the problem area and the chosen research question.

In article [2] the presented results are related to the problem area and the chosen research question.

In article [3] the presented results are not related to the problem area and the chosen research question.

8. How are the references used in each study?

In article [1] presented references are more accurate and more detailed, they are promising and are useful for future research.

In article [2] presented are some what useful and not so helpful for future research.

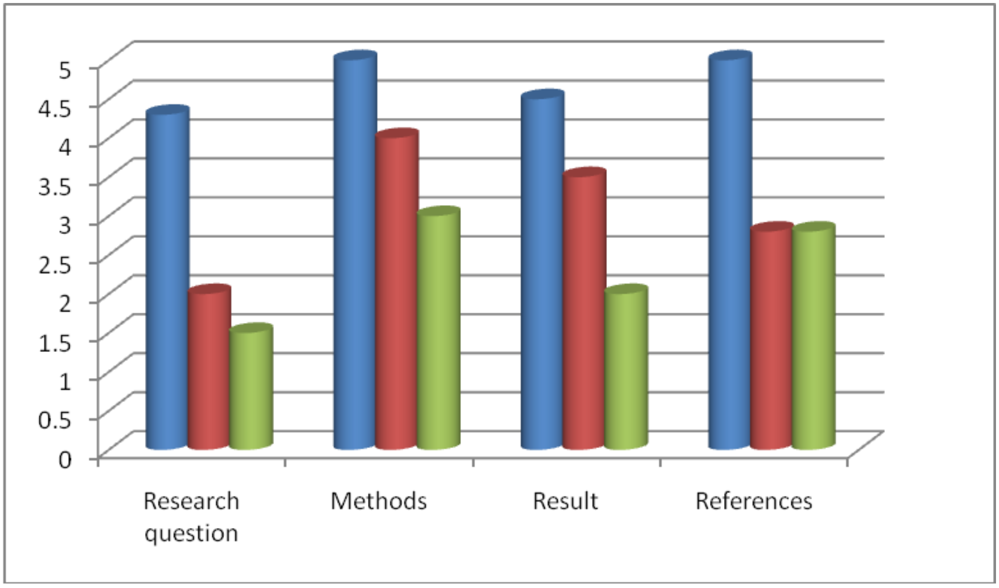
In article [3] presented are some useful and not so useful for future research.

IV. CONCLUSIONS

The graph below representation of the selected area that are present in the selected papers.

BLUE – ARTICLE [1]

RED – ARTICLE [2] GREEN- ARTICLE [3]



]

V. REFERENCES

[1] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. Gaur, M. Conti, and R. Muttukrishnan, “Android Security: A Survey of Issues, Malware Penetration and Defenses,” *IEEE Communications Surveys & Tutorials*, pp. 1–27, 2015

[2] M. Zaman, T. Siddiqui, M. R. Amin, and M. S. Hossain, “Malware detection in Android by network traffic analysis,” in *Networking Systems and Security (NSysS), 2015 International Conference on*, 2015, pp. 1–5

[3] Y. Wang, “An automated virtual security testing platform for android mobile apps,” in *Mobile and Secure Services (MOBISECSERV), 2015 First Conference on*, 2015, pp. 1–2.