CARLOS III UNIVERSITY OF MADRID

HIGHER TECHNICAL SCHOOL



MASTER IN CYBERSECURITY

MASTER THESIS

TARGETED EXERCISER FOR ANDROID MALWARE AND GRAYWARE

**Author**: Mario Herreros Díaz

**Mentors**: Juan E. Tapiador, Guillermo Suarez-Tangil

**September, 20th, 2016**

**Abstract**

Nowadays each person has one or more mobile device (smartphones, tablets, wearables, etc) with similar characteristics and performance of a personal computer. Many people use these devices to check their email or make bank transfers. For this, these devices store a lot of sensitive information that it could be very attractive to an attacker.

Mobile devices share same security troubles can be found in a conventional computer as malware hidden inside apps or users that don’t use nor protect their correctly.

Malware has evolved and is able to by pass protection systems and works only under certain circumstances to avoid detection. Some kind of malware is activated depends of network connection, device location, apps installed, calls received or other type of events.

The purpose of this Master Thesis is to study the behavior of malware on mobile devices depending of the device context, focusing on Android operating system. It has developed a system that allows dynamic and automatic generation of many different contexts to study the behavior of Android malware in each of the scenarios.

It has been designed a technique based on new language which defines each of the scenes and events to execute over the device to analyze the malware, in order to study their behavior depending on the characteristics of each context. In this way, it can detect the context features that makes triggering the malicious malware or greyware actions.

This Thesis focuses on analyzing all possible Android events to define a language and developing a system available to understand it and generate automatic executions to launch these events. With this system it is possible detect malware and grayware that a convetional static and dynamic analysis could not detect.

*Keywords: Malware, Greyware, Android, Context, Malware detection, Dynamic analysis, Mobile device*

1. **Introduction**

Los dispositivos móviles se han expandido notablemente en la sociedad actual. La mayoría de las personas posee uno o más dispositivos móviles (graficas de uso de dispositivos móviles) de los cuales Android es un porcentaje importante.

Se bajan no se cuantas aplicaciones de Android al día. Actualmente esto supone una atractiva puerta para los atacantes para introducir código malicioso en apks que aparentan ser legítimas (ejemplo de pokemon go). Muchos de los atacantes se centran en focalizar sus actividades maliciosas en usuarios que cumplen una serie de características o tienen un hábito de consumo y uso del dispositivo móvil determinado.

1. *Motivation*
2. *Main contributions*
3. *Structure of the document*
4. **Related Work**
5. **TargetDroid**
6. *What is?*
7. *Events*
8. *Contexts (t= -1, t = 0, t > 0)*
9. **Discussion**
10. **Conclusion**
11. **Future Works**

**References**

**Appendix A : json-schema**

**Appendix B: event list**

**Appendix C: Planning and budget**

In order to comply with the regulations of MsC Thesis by Universidad Carlos III de Madrid, this appendix presents the Planning and Budget of the Thesis.

First, it is going to be presented a planning that defines this project in different tasks. It has been generated a typical Gantt chart presenting in a graphical form the duration of each phase.

The resume of the phases is shown in Figure X with its start and end date. Gantt chart with detailed information is shown in Figure X+1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Duration | Start Date | End Date |
| Definition of goals |  | 15/01/2016 | 22/02/2016 |
| Analysis |  | 01/03/2016 | 15/04/2016 |
| Design |  | 24/05/2016 | 10/06/2016 |
| Development |  | 11/06/2016 | 04/07/2016 |
| Testing |  | 5/07/2016 | 10/07/2016 |
| Report |  | 16/07/2016 | 1/09/2016 |

Last, it is going to be presented the budget. It is broken down into various estimations by type cost:

* Personal cost:
* Software cost:
* Indirect cost:
* Total cost:

Note: VATs are included.

|  |  |  |  |
| --- | --- | --- | --- |
| Concept | Time | Fees | RRHH cost |
| Security Engineer |  | 50 €/hour |  |
| PhD |  | 55 €/hour |  |
| TOTAL | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Concept | Units | Unit price | Estimated life time | Airtime | Cost |
| Acer Aspire 5740 | 1 | 600 € | 60 months | 3 months |  |
| TOTAL | | |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Concept | Units | Unit price | Estimated life time | Airtime | Cost |
| Ubuntu Linux | 1 | 0 € | - | 3 months |  |
| Sublime Text 3 | 1 |  |  |  |  |
| SmartGit Hg 7.1 | 1 |  |  |  |  |
| Github | 1 |  |  |  |  |
| Bitbucker | 1 |  |  |  |  |
| Latex Editor?? |  |  |  |  |  |
| TOTAL | | |  |  |  |