**CSE306 Research – Project Plan**

**Bisesh Shrestha**

**219570044**

**Computer system engineering**

**International School of Management and Technology**

**Mobile malware and it detection**

**Word Count: 1502**

1. Justification for the Proposed Research

Technology is always improving and moving forward. At times, technology is also ahead of its time and pushes humanity into new realms. Thanks to technology, we have all conquered modern civilization. In this modern civilization, Malware has had a significant influence on a lot of computer equipment. Malicious software, or malware, is created with the intention of achieving the negative goals of a malicious attacker. Malware may breach networks, damage vital infrastructures, compromise computers and smart devices, and steal sensitive data. These programs include ransom ware, rootkits, spyware, bots, viruses, worms, and Trojans. From $3.3 billion in 1997 to $13.3 billion in 2006, according to Computer Economics, financial damage as a result of malware assault has increased by a factor of four. The criteria for defining a Year of Mega Breach must be updated periodically in light of assaults committed during that year. In 2016, the WannaCry ransom ware virus completely destroyed computers in over 150 countries and cost various businesses money. Cyber security Ventures calculated in 2016 that the entire cost of malware assaults was $3 trillion in 2015 and would rise to $6 trillion by 2021. (Rathore, et al., 2018)

In our daily lives, mobile phones are a necessity since they provide us with access to a wide range of services. Thus, mobile gadgets are sometimes referred to as smart phones. The usage of mobile devices like phones and personal digital assistants (PDAs) has more than doubled since 2000, and the market for these gadgets has increased enormously in recent years. Mobile phone ownership has surpassed 1.5 billion users, or a fourth of the world's population, even if slower growth is anticipated in the future. The latest wireless communication technology is 4G, while other options include GSM, GPRS, Bluetooth, Wi-Fi, and 3G. (S & S, 2017) It has attractive features that enable online banking, internet access, and the installation of several apps. A crucial concern is if these devices will now have another resemblance with the PC and become the target of viruses, worms, and other malware programs as a result of these pathways into the devices being opened up and their processing capabilities becoming more equivalent to desktop PCs of a few years ago. (Furnell, 2005)

Malware developers frequently come up with innovative concepts. They create malware in such a manner that it changes itself periodically in order to avoid detection. The goal of malware developer is to create programs that are difficult to detect. As time has gone on, they have effectively improved the tactics used to hide or morph the malicious code. These concepts begin with straightforward encryption before moving on to oligiomorphic, polymorphic, and metamorphic viruses. These malwares are detected via Trojan detectors, and antivirus scanners are one method of detection. Malware detectors utilize a variety of them, however with advancements in malware production methods, ways to mitigate the negative impacts of these programs. (Tahir, 2018) Therefore, we provide a full analysis of the development and widespread distribution of mobile malware, as well as the attack pathways and different malware detection techniques.

1. The Project's Aim

This project goal is to Identify and detect the different types of malwares in a mobile devices which may affect mobile application with its possible detections measures and solution for reducing those malware.

1. The Project's objective
2. Discuss on malware’s evolution.
3. Identify different taxonomy of malwares.
4. Detection approach of malwares.
5. Identify the challenges while detecting malwares using specific approach.
6. Discuss future threats from those malwares.
7. Solution/reduce of malware after it detection.
8. Publish the project's conclusions.
9. Practical Outcomes for Client

The project's main objective is to identify various malware types using various detection approach. After the completion of different detection approach testing will be done and result will be evaluated using different detection approach then client will receive a specific detection approach which will be more effective to detect malware easily and help them to reduce or be aware of them.

1. The Proposed Methodology

This project aims to detect various malware types using various detection approaches. In order to accomplish this project's aim, the project objectives will be completed according to the timetable that was accurately projected using a Gantt chart. It will take 600 hours, approximately 16 weeks, to finish the project and will start with requirement collection through research and examination of various publications and papers.

In the initial weeks of research, various publications and papers were examined. A report will be created to document these discoveries as we learn more about the different kinds of malware. After third week of research and studying papers, different detection approaches will be discussed and will analyses different challenges faced while using different approaches.

After all the data has been gathered, specific detection approach will be studied and after the study of different detection approach testing will be done showing how it will be effective and how will it be more effective than other detection approach. After week 9, we will interview the network specialist so that we can discuss about different types of malware and how it will affect the mobile application. After interview with network specialist we will note the important information and analyze those important information then we will make an important note from obtained notes from interview.

As the first core concept of the project, the hypothesis will be built. Prior to the commencement of the real testing, an assumption will be made to produce an idealized result and it will be reported. Finally at last and second last week draft of the project will be produced and it will be sent for the review. Once the review is complete, the research article is finalized and published in scholarly journals.

1. The Evaluation Plans

In order to evaluate the proposed methods, many research and paper will be evaluated. Due to the limitations of the currently available malware detection approaches, machine learning and data mining techniques are coupled with them to increase the detection process' efficiency. In spite of their effectiveness in detecting known malware, signature-based detection techniques are unable to identify polymorphic and unknown malware since these threats can alter their signatures. Because new malware's signatures have not yet been generated, signature-based detection also cannot detect them. Heuristic-based detection techniques may find new, well-known, and undiscovered viruses, but they have a high percentage of false positives and negatives, which motivates us to create more precise detection techniques. Heuristic-based detection approaches are paired with machine learning methods to boost malware detection efficiency and accuracy as a result of the exponential growth of polymorphic malware. A survey form will be used to collect feedback on the detection strategy once all the experiments and testing have been completed. The information will highlight the aspects of the strategy that needed to be strengthened as well as its shortcomings.

1. Scientific Justification

The purpose of this project clearly identifies the objective of this research proposal, and the procedures are structured in a way to concentrate on that target. As a result, this project exhibits a high degree of purposiveness. A certain degree of testability exists; by gathering response information from both systems, the outcomes may be compared and contrasted to assess the success or failure of the new approach. The assessment also retains a level of rigor since when the findings are gathered, they undergo a critical examination to demonstrate how the new approach outperforms the existing one. The suggested assessment has a high degree of repeatability since the criteria for ambiguity are stated, as are all of the questions used to test the system. As a result, other researchers might compile control groups of the same criteria and use the same questions to evaluate a technique in this fashion. The evaluation also had generalizability since the results were based on activities and questions that were appropriate for the detection methodologies; these tasks and questions would be performed nearly every day by mobile device users all over the world. Overall, as seen above, this study follows excellent scientific standards and results in a research proposal that is supported by the available scientific evidence.

1. Ethical Justification

I come to the conclusion that my study proposal does not violate any ethical norms after reviewing my research technique and evaluation and using a different detection approach. By conducting expert interviews, identifying the challenging, and focusing the research on a single objective, the quality of the study is maintained. This guarantees that the study is carried out in a wholly legal manner, receiving the network specialist's full consent by conducting the necessary interviews and conversations as necessary. Since there will be independent assistants present who can make sure each participant understands their task before agreeing to it, there is no violation of the mental capacity statute. Each network specialist is treated equally, the research is conducted neutrally, and no special treatment will be offered. This study will have a good significance by helping all mobile devices in detecting and reducing malware.

# References

Furnell, S., 2005. Handheld hazards: The rise of malware on mobile devices. *Computer Fraud & Security.*

Rathore, H., Agarwal, . S., Sahay, S. K. & Sewak, M., 2018. Malware Detection Using Machine Learning and Deep Learning.

S, K. & S, K., 2017. A Survey on Rise of Mobile Malware and Detection. *international conference on innovation in information, embedded and communication system.*

Tahir, R., 2018. A Study on Malware and Malware Detection Techniques. *I.J. Education and Management Engineering,* Volume 2, pp. 20-30.

1. Schedule

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Task Title** | **Effort**  **(hour)** | **Planned**  **Start Date** | **Planned**  **End Date** | **Actual**  **Start Date** | **Actual**  **End Date** | **Deliverable** |
| **1** | **Discuss on malware’s evolution** | **85** |  |  |  |  |  |
| 1.1 | Research on who invented malware | 20 | 29/08/2022 | 19/09/2022 |  |  | Research notes |
| 1.2 | Study on how malware was created | 20 | 29/08/2022 | 19/09/2022 |  |  | Research notes |
| 1.3 | Compare of rise of malware in different time period | 35 | 29/08/2022 | 26/09/2022 |  |  | Summary notes |
| 1.4 | Report writing | 10 | 19/09/2022 | 26/09/2022 |  |  | Evaluation Report |
| **2** | **Identify different taxonomy of malwares** | **85** |  |  |  |  |  |
| 2.1 | Research on different types of malware | 25 | 29/08/2022 | 03/10/2022 |  |  | Research notes |
| 2.2 | Read article research papers, | 35 | 29/08/2022 | 26/09/2022 |  |  | Significant details on the research papers |
| 2.3 | Make significant notes on writing. | 15 | 26/09/2022 | 10/10/2022 |  |  | Evaluation Report |
| 2.4 | Report writing | 10 | 03/10/2022 | 10/10/2022 |  |  |  |
| **3** | **Detection approach of malwares** | **100** |  |  |  |  | Evaluation Report |
| 3.1 | Find important research articles on the detection of malware. | 35 | 12/09/2022 | 17/10/2022 |  |  | A set of research articles |
| 3.2 | Analyze the data gathered from articles on malware detection study. | 15 | 26/09/2022 | 17/10/2022 |  |  | Exact notes |
| 3.3 | List out the different types of detection approach | 25 | 03/10/2022 | 24/10/2022 |  |  | Detections types |
| 3.4 | Select of specific detection approach | 15 | 10/09/2022 | 24/10/2022 |  |  | Selection |
| 3.5 | Report writing | 10 | 17/10/2022 | 24/10/2022 |  |  | Evaluation Report |
| **4** | **Identify the challenges while detecting malwares using specific approach** | **100** |  |  |  |  |  |
| 4.1 | Find important research articles on the challenges while detecting of malware. | 25 | 10/10/2022 | 24/10/2022 |  |  | A set of research articles |
| 4.2 | Write notes on challenges while detecting malwares. | 10 | 17/10/2022 | 24/10/2022 |  |  | list of challenges |
| 4.3 | Meet the network specialist regarding challenges. | 30 | 31/10/2022 | 14/11/2022 |  |  | Notes from the interview |
| 4.4 | Obtain the comments from network specialist | 15 | 31/10/2022 | 14/11/2022 |  |  | Remarks on feedback |
| 4.5 | Evaluate the obtained comments | 10 | 14/11/2022 | 28/11/2022 |  |  | Evaluation Report |
| 4.6 | Report writing | 10 | 21/11/2022 | 28/11/2022 |  |  | Evaluation Report |
| **5** | **Discuss future threats from those malwares** | **75** |  |  |  |  |  |
| 5.1 | Find the most recent studies on various malware threats. | 25 | 24/10/2022 | 14/11/2022 |  |  | A set of research articles |
| 5.2 | Analyze the research articles and their findings. | 30 | 24/10/2022 | 28/11/2022 |  |  | Exact notes |
| 5.3 | List out the different threats | 10 | 21/11/2022 | 28/11/2022 |  |  | list notes |
| 5.4 | Report writing | 10 | 28/11/2022 | 05/12/2022 |  |  | Evaluation Report |
| **6** | **Solution/reduce of malware after it detection** | **100** |  |  |  |  |  |
| 6.1 | Identify the malware | 20 | 24/10/2022 | 14/11/2022 |  |  | Research notes |
| 6.2 | Analyze the note prepared on malwares | 15 | 31/10/2022 | 14/11/2022 |  |  | Exact notes |
| 6.3 | Meet the network specialist. | 30 | 14/11/2022 | 28/11/2022 |  |  | Notes from the interview |
| 6.4 | Produce a hypothesis for a new methods that will reduce the malware | 25 | 28/11/2022 | 12/12/2022 |  |  | Documents with written hypotheses |
| 6.5 | Report writing | 10 | 05/12/2022 | 12/12/2022 |  |  | Evaluation Report |
| **7** | **Publish the project's conclusions.** | **55** |  |  |  |  |  |
| 7.1 | Draft the paper. | 20 | 05/12/2022 | 12/12/2022 |  |  | Unfinished research document |
| 7.2 | Send the paper for review | 10 | 05/12/2022 | 12/12/2022 |  |  | Examining notes |
| 7.3 | Finalize the research paper. | 25 | 12/12/2022 | 19/12/2022 |  |  | A complete  Research paper |

1. Gantt chart

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | Task Title | Effort  (hour) | W  1 | W  2 | W  3 | W  4 | W  5 | W  6 | W  7 | W  8 | W  9 | W  10 | W  11 | W  12 | W  13 | W  14 | W  15 | W  16 |
| **1** | **Discuss on malware’s evolution** | **85** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.1 | Research on who invented malware | 20 | 10 | 5 | 5 |  |  |  |  |  |  |  |  |  |  | 1 |  |  |
| 1.2 | Study on how malware was created | 20 | 5 | 10 | 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.3 | Compare of rise of malware in different time period | 35 | 10 | 10 | 10 | 5 |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.4 | Report writing | 10 |  |  | 5 | 5 |  |  |  |  |  |  |  |  |  |  |  |  |
| **2** | **Identify different taxonomy of malwares** | **85** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.1 | Research on different types of malware | 25 | 5 | 5 | 5 | 5 | 5 |  |  |  |  |  |  |  |  |  |  |  |
| 2.2 | Read article research papers, | 35 | 10 | 10 | 5 | 10 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.3 | Make significant notes on writing. | 15 |  |  |  | 5 | 5 | 5 |  |  |  |  |  |  |  |  |  |  |
| 2.4 | Report writing | 10 |  |  |  |  | 5 | 5 |  |  |  |  |  |  |  |  |  |  |
| **3** | **Detection approach of malwares** | **100** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.1 | Find important research articles on the detection of malware. | 35 |  |  | 5 | 5 | 15 | 5 | 5 |  |  |  |  |  |  |  |  |  |
| 3.2 | Analyze the data gathered from articles on malware detection study. | 15 |  |  |  | 5 | 5 | 2 | 3 |  |  |  |  |  |  |  |  |  |
| 3.3 | List out the different types of detection approach | 25 |  |  |  |  | 5 | 8 | 9 | 3 |  |  |  |  |  |  |  |  |
| 3.4 | Select of specific detection approach | 15 |  |  |  |  |  | 5 | 5 | 5 |  |  |  |  |  |  |  |  |
| 3.5 | Report writing | 10 |  |  |  |  |  |  | 5 | 5 |  |  |  |  |  |  |  |  |
| **4** | **Identify the challenges while detecting malwares using specific approach** | **100** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.1 | Find important research articles on the challenges while detecting of malware. | 25 |  |  |  |  |  | 10 | 10 | 5 |  |  |  |  |  |  |  |  |
| 4.2 | Write notes on challenges while detecting malwares. | 10 |  |  |  |  |  |  | 3 | 7 |  |  |  |  |  |  |  |  |
| 4.3 | Meet the network specialist regarding challenges. | 30 |  |  |  |  |  |  |  |  | 10 | 10 | 10 |  |  |  |  |  |
| 4.4 | Obtain the comments from network specialist | 15 |  |  |  |  |  |  |  |  | 5 | 5 | 5 |  |  |  |  |  |
| 4.5 | Evaluate the obtained comments | 10 |  |  |  |  |  |  |  |  |  |  | 2 | 5 | 3 |  |  |  |
| 4.6 | Report writing | 10 |  |  |  |  |  |  |  |  |  |  |  | 5 | 5 |  |  |  |
| **5** | **Discuss future threats from those malwares** | **75** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5.1 | Find the most recent studies on various malware threats. | 25 |  |  |  |  |  |  |  | 5 | 5 | 10 | 5 |  |  |  |  |  |
| 5.2 | Analyze the research articles and their findings. | 30 |  |  |  |  |  |  |  | 7 | 8 | 5 | 2 | 3 | 5 |  |  |  |
| 5.3 | List out the different threats | 10 |  |  |  |  |  |  |  |  |  |  |  | 8 | 2 |  |  |  |
| 5.4 | Report writing | 10 |  |  |  |  |  |  |  |  |  |  |  |  | 5 | 5 |  |  |
| **6** | **Solution/reduce of malware after it detection** | **100** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6.1 | Identify the malware | 20 |  |  |  |  |  |  |  | 3 | 7 | 5 | 5 |  |  |  |  |  |
| 6.2 | Analyze the note prepared on malwares | 15 |  |  |  |  |  |  |  |  | 5 | 5 | 5 |  |  |  |  |  |
| 6.3 | Meet the network specialist. | 30 |  |  |  |  |  |  |  |  |  |  | 5 | 15 | 10 |  |  |  |
| 6.4 | Produce a hypothesis for a new methods that will reduce the malware | 25 |  |  |  |  |  |  |  |  |  |  |  |  | 10 | 10 | 5 |  |
| 6.5 | Report writing | 10 |  |  |  |  |  |  |  |  |  |  |  |  |  | 5 | 5 |  |
| **7** | **Publish the project's conclusions.** | **55** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7.1 | Draft the paper. | 15 |  |  |  |  |  |  |  |  |  |  |  |  |  | 5 | 10 |  |
| 7.2 | Send the paper for review | 10 |  |  |  |  |  |  |  |  |  |  |  |  |  | 3 | 7 |  |
| 7.3 | Finalize the research paper. | 30 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 5 | 25 |
|  | Total hour per week | 600 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 40 | 39 | 36 | 40 | 28 | 32 | 25 |