Undetectable Computer Virus

# Project Report – Week 1

## Work Done

* We've explored various aspects, from the origins of computer viruses to how they spread and impact digital systems.
* We delved into the different generations of viruses, tracing their evolution from simple to highly sophisticated forms.
* Reading up on research papers about undetectable computer viruses. This involves understanding the latest tricks and techniques used by cybercriminals to create viruses that slip under the radar.
* We are keeping an eye on emerging technologies like AI and machine learning, which are crucial in the fight against viruses.
* Considering and understanding the ethics of this field, pondering the implications of creating and distributing viruses.

## Papers Referred:

1. Towards an undetectable computer Virus
   1. – Priti Desai
   2. – Presented to the faculty of Department of Computer Science San Jose State University
2. An Undetectable Computer Virus
   1. – David. M. Chess and Steve. R. White
   2. – IBM Thomas J. Watson Research Centre Haw thorne, New York USA

## Summary

Paper 1 discuss the development of an undetectable compute virus through the use of code obfuscation techniques. While paper2 focusses on the discussion about the limitations of views detection algorithm and presents a program that fails to detect a specific virus due to a faulty subroutine implementation. The paper emphasizes the need for a more realistic notion of virus detection. In paper 1, we explore the implementation of metamorphic engine that can generate highly diverse morphed copies of a base vires making it difficult for signature – based virus scanners to detect. The paper also investigates the use of Hidden Markov Models (HMMs) as a potential detection tool for metamorphic viruses. Experimental results show that commercial virus scanners are unable to detect the metamorphic viruses generated by the engine. The metamorphic engine in this paper generates diverse morphed copies of a base virus by using code obfuscation techniques such as equivalent instructions, substitutions, dead code insertion and rearrangement of instruction order. These techniques manipulate both the control flow and data section of the program to produce different looking copies of the original virus.

The engine also incorporates a transformation module that replaces instructions or blocks of instructions with code, further contributing to the diversity of the morphed copies.

## Conclusions

The paper’s exploration of using Hidden Markov Model (HMMs\_ as a potential detection tool for metamorphic virus is interesting. While the results showed that the HMM was able to classify the morphed copies as belonging to the same family a s the base virus it is worth noting that the morphed copies were still able to evade direction by commercial virus scanners. This highlights the effectiveness of the metamorphic engine in generating diverse and undetectable variant. Dynamically changing the virus signature using some AI/ML algorithms we can make this metamorphic virus kind of undetectable.

## Future Works

* Understanding the inner workings of ML/AI algorithms to grasp how viruses, such as metamorphic viruses, can adapt based on a computer's activity.
* Exploring the problem statements and requirements relevant to this field. This foundational knowledge is essential for effectively addressing the challenges in cybersecurity.
* Investigating advanced behavioural analysis methods to predict and counteract malicious activities more effectively.
* Continuously evaluating the ethical implications of research in this field, ensuring responsible use of knowledge.

Project Supervisor

Dr Modi Chirag

Aryan Shrivastav (20CSE1005)

Aditya (20CSE1002)