ABSTRACT AND MOTIVATION

The alarming rise in the number of computer security incidents since the late 80's had inspired researchers to devise new mechanisms for detection and containment of malwares like worms and viruses. Traditional approaches like worm signatures are helpless against new age polymorphic and metamorphic worms. Design and implementation of an anomaly based detection system seems to be a herculean task due to the difficulty in defining a normal model.

There have been attempts to generate polymorphic and metamorphic resilient vulnerability signatures but they still suffer from low coverage. Protocol level vulnerability signatures are one of the newest approaches. One of the open issues that need to be addressed is effective generation of compact signatures that are resilient to polymorphic and metamorphic variations of attacks.

In this project, we make an attempt to develop new algorithms and techniques for effective and fast generation of protocol level vulnerability signatures; and finally, our main aim is to develop a defense system against internet worms, which are also resilient to the polymorphic and metamorphic variations of attack. In our approach, we plan to generate protocol level vulnerability signatures, which will offer better coverage than other approaches as they will work at the protocol level, which automatically covers all the paths to the vulnerability point. We also attempt to minimize rates of false positives and false negatives.

In this semester, we made an attempt to extract the input dependent branch conditions from the disassembly of a binary (executable) file, by statically analyzing the CFG of the binary and finally mapping the jump instructions of the decision nodes with the corresponding branch conditions.