

# Research Statement

Jose Andre Morales

May 2008

Detection of unknown computer viruses upon their initial infection attempt on a computer system is the focus of my research. My main contribution in this area is the creation of a proactive behavior based virus detection approach for self-reference replication (*SR-replication*) [3]. This form of replication occurs when a process attempts to write or copy itself to some other location of a computer system. The process attempting this will invoke read and/or write operations with the only source (“from”) parameter referring to the process itself that is invoking the operation. When this occurs the process has attempted to replicate itself by self-referencing in one or more read/write operations. This behavior is assumed unique to viruses and not commonly occurring in benign processes.

Another novel contribution of my research has been to identify and characterize the *self-reference property (SR)* [3] which is essential to virus replication. *SR* operations are a read or write operation that passes a reference to the caller process as the only source parameter. An *SR* process executes *SR* operations. The majority of viruses belonging to several different virus classes replicate using *SR* which I term *SR-replication*. In its present form, my detection approach is capable of detecting file infecting viruses which is the largest class of known viruses and the detection works well under several different execution conditions. Detection is performed with the creation of a call graph containing all read and write operations of a process with their arguments as the nodes. When a path on the graph appears from the file of the caller process to a target file, the process is flagged as a possible virus for exhibiting *SR-replication* behavior. The path on the call graph shows a transitive relation between the virus file and the newly infected file, this transitive property between files is the fundamental detection property of *SR-replication*. Currently a prototype titled SRRAT has been built for Microsoft Windows which tracks Win32 API calls invoked by all currently running processes on a local computer. Testing has shown SRRAT capable of detecting both known and unknown viruses and has not produced any false positives or false negatives during testing. System resource use has not been high with CPU usage and memory consumption not resulting in an overall slowdown of the local computer.

The majority of virus infected computer systems fall victim to fast spreading unknown viruses. These viruses infect and injure vulnerable computers within minutes or seconds of initial release. The most commonly used form of virus detection today is signature based detection. This form of detection is very effective in identifying known computer viruses but perform poorly in detecting unknown computer viruses and modified forms of known computer viruses [1]. Behavior based virus detection shows great promise in detecting unknown viruses. This form of detection monitors the execution behavior of a process and decides if it is possibly a virus based on an evaluation of a virus characteristic such as a process attempting to delete protected files. The shortcomings of behavior based virus detection are the lack of a virus characteristic allowing for detection of viruses under several execution conditions and that belong to many different virus classes. In my recent work, a rigorous study of execution behavior of a computer virus was conducted [2] where *virus replication* was identified as a virus characteristic with the potential to overcome the

shortcomings of behavior based virus detection because it is the qualifying fundamental characteristic present in all viruses where one specific form is *SR-replication*.

## **Moving Forward**

A key focus of my future work is extending my detection approach to other classes of viruses such as memory resident viruses, worms that replicate across systems and viruses that do not use *SR-replication*. I will also implement prototypes for wireless and embedded devices such as PDA's, cellular phones, GPS systems, appliances and other systems. The addition of self healing to compliment my proactive detection approach is another area of future research. My long term research goal is the continued formulation of effective detection against yet unknown viruses employing novel anti-detection techniques. This is an ongoing research evolving in synergy with emerging technologies that is realized in a lab environment. In the future I envision computer systems that detect, remove and self heal from virus attacks with minimal if not any human intervention. The most recent President's Information Technology Advisory Committee report (PITAC) stated cyber security to be a top prioritization in need of federal funding in the private and academic sectors to further secure the current national security infrastructure. The report recommended long term research funding in the areas of monitoring and detection of intrusions on a system and securing emerging technologies such as wireless, embedded and handheld devices. The report further states a need to develop new security models from the ground up that are integral to a system and just perimeter protection. The latest Federal Plan for Cyber Security and Information Assurance from the National Science and Technology Council named attack protection, prevention and preemption along with automated attack detection, warning and response as two of the top funding priorities noting a need for development of proactive behavior based systems. My research addresses these issues which makes it a potential candidate for government research funding.

[1] **“Testing and Evaluating Virus Detectors for Handheld Devices”**, Jose Andre Morales, Peter J. Clarke, B.M. Golam Kibria, Yi Deng. Journal in Computer Virology Special Issue on Mobile Malware and Anti-malware Technologies, Springer Paris, Volume 2/Number 2, November 2006, pg. 135-147.

[2] **“Characterization of Virus Replication”**, Jose Andre Morales, Peter J. Clarke, B.M. Golam Kibria, Yi Deng. Journal in Computer Virology Special Issue on Theory of Computer Viruses Workshop, Springer-Verlag 2008.

[3] **“Detecting Self-Reference Virus Replication”**, Jose Andre Morales, Peter J. Clarke and Yi Deng, Proceedings of the 17th Annual European Institute for Computer Anti-Virus Research (EICAR) Conference, May 3-8 2008, Laval France.