MULTI-AGENT ARCHITECTURE WITH DYNAMIC MODEL CHECKING FOR MALWARE DETECTION SYSTEM

Imtithal Alnour Saeed, Prof. Dr. Ali bin Selamat
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia
imtithal_s@hotmail.com, aselamat@utm.my

ABSTRACT
In spite of the huge development in computer security technology, but still there are many problems face this development. Malicious software attacks growing up is the biggest challenges that threaten computer and information security. Manufacturers do huge efforts to produce improved detection systems for malicious programs every time, but malcodes programmers compete with themselves to invent new types of malwares that evade detection programs. Briefly there is fast racing between antivirus software producers and malware programmers. The major problems in the current detection systems are: first of all the current antivirus software need to be updated periodically, using internet batch update or any other way, to make the program capable to defend against the given viruses. Secondly new viruses are not recognized by old antivirus, because they neither have detection tools to identify them, nor these viruses contained in their databases. Manufacturers of operating systems and antivirus producers use many ways to detect against virus, that ranging from check sum, carry bit, virus signature (which depends on special stamp that enough to add the program in the list of virus to be treated by the antivirus), reaching to software programs that use heuristic scanning techniques methods for detecting unknown and complex viruses. All of the current methods are not successful to provide high performance effective antivirus tool. In this thesis I will try to invent an algorithm, to detect any type of viruses effectively with high performance. I will work combining the approaches of multi-agent and model checking to construct architecture for malware detection system. My research aims to combine these two emerging research areas in order to overcome drawbacks of the current technologies used for structuring malware detection system. The first approach, multi-agent model, is to distribute the whole control task over several small execution objects (agents), which communicate by sending rules and protocols using the second approach. The model contains four agents types: Sniffer agents which are responsible of capturing data from the main memory, classification agents which are responsible of identifying items by applying classification model on them, reporter agents who are responsible of issuing reports about decision made by classification agents and finally the coordination agent which is dynamically control communication between agents using dynamic model checking approach.

KEYWORD
multi-agent, dynamic model checking, intrusion detection, malware detection