Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M15-167P^
Published: 2/26/2020

Inventors

Paulo Shakarian
Eric Nunes
Casey Buto
Christian Lebiere
Robert Thomson

Contact

Shen Yan
shen.yan@skysonginnovations.com

Data Driven Malware Task Identification

Malicious software, or malware, is a type of coded program designed to damage/hack computer systems. Often, malware disables a user's computer control, consequently leaving a user's sensitive information vulnerable. Even though various types of firewall, anti-virus, and network security software all serve as layers of defense, they only define a malware's binary features (attributes) such as, referencing/not referencing a set of data, starting/stopping a process, etc. However, identifying the higher-level purpose (tasks) malware may perform (e.g. logging key strokes, taking a screenshot, establishing remote access, etc.) requires trained analysts. With malware programmers making more complex and resistive codes, computer scientists look to improve malware task identification by shifting toward a more automated method.

Researchers at ASU have developed an automated way of identifying malware tasks by combining dynamic malware analysis with cognitive modeling. Scientists dubbed this method, "Adaptive Control of Thought–Rational (ACT-R)," due to the human-based, cognitive modeling method. The system compares a given malware's traits to existing malware families in a database. For any families the malware could belong to, the system assigns a probability and returns a set of predicted tasks the malware will perform. Any new malware traits remain in the system for future comparison. The system's human-based functionality can apply various traits from different malware families to characterize new, unknown malware. The cognitive, dynamic analysis approach effectively models an analyst's decision-making ability, easily adapts to unknown malware, and ultimately prevents computer system hacking and damage.

Potential Applications

- Network and computer security
- Computer software
- Data mining and storage

Benefits and Advantages

- Lower Cost – utilizes an iterative, computerized approach that reduces both the cost of computational algorithm and the need for human interaction
- Faster – the system stores data in a knowledge base for future comparison, leading to an increased processing speed
- Effective – ACT-R identified malware more accurately compared to a leading malware-detection program
- Proactive and Preventive – the method's growing reference database allows it to characterize unknown malware types and prevent computer system damage/hacking

For more information about the inventor(s) and their research, please see:

Dr. Paulo Shakarian's directory webpage