SIMULATED COGNITIVE CYBER RED-TEAM ATTACKER MODEL

Synthetic, offensive, cognitive agent that emulates real attackers by modeling the complex thoughts, decision-making, and understanding of a human interactive operator.

COGNITIVE AGENT

The agent’s knowledge is structured as a set of modular top level goals that can interleave in multiple ways to support different situations. The interleaving of goals and sub-goals for a particular attack generates a flexible, situation dependent “attack tree” structure. The current model generates a single “attack tree” trajectory, but the underlying knowledge representation has numerous placeholders ready to be populated with additional choices, representing a variety of Tactics, Techniques, and Procedures (TTPs). A cross-cutting representation of situational understanding supports the selection of goals and actions, as well as the interpretation of their results.

SC2RAM’s goal-seeking behavior results in a virtually unlimited range of realistic attacks.
EVENT LAYER

As SC2RAM agents attempt to achieve the goals of their missions, they communicate their intents to a layer that is responsible for translating them into real-world observable events. To do so, this event layer determines which of its available resources are appropriate, and then translates the agent’s intent into commands for those resources. The event layer is also responsible for providing the interface between SC2RAM and its teammates, be they human or synthetic.

HACKING TOOLKIT

The event layer uses middleware to communicate with off-the-shelf tools to perform specific offensive actions, such as port scanning, password cracking, or phishing. The hacking toolkit implements a layer of abstraction that permits such employment of real-world tools such as nmap or custom malware. The end result is the generation of real command-line arguments on real tools in a realistic manner. The modular nature of the toolkit facilitates the addition and removal of tools as needed.

PLATFORM

The system is implemented as a self-contained Virtual Machine (VM) called the SC2RAMbox. This VM can be easily introduced into any environment and quickly configured through a web-based interface. Even in the absence of any information about its target, SC2RAM is able to discover its environment and exploit systems within its capabilities. Given specific targets, goals, and constraints, its behavior can be very targeted.

DEVELOPMENT STATUS

SC2RAM is an Office of Naval Research (ONR) Phase II Small Business Innovative Research (SBIR) project. It was initially validated by performing a Denial of Service (DoS) attack in the Michigan Cyber Range (MCR). The current attacker agent can conduct multiple attacks including phishing with malicious documents, remote exploitation, and SQL injection. A custom remote access toolkit developed for this project provides additional persistent on-target capabilities.