CMU Ghosts to Simulate a User Environment and Detect Novelty

Dr. Holder, Vincent Lombardi, Timothy Reidy

PROBLEM STATEMENT

As the world becomes even more tech focused, there is a need for detecting possible security threats that cannot be detected be a person or team..

CMU Ghosts

A framework built for simulating a user environment. Creates agents and their interactions similar to how an office or company would interact.

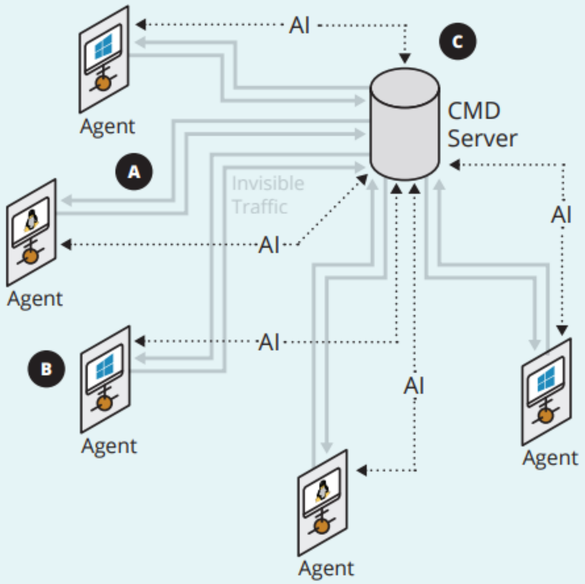
We are using this framework to develop an AI that can detect novel situations. More specifically, we want this AI to be able to detect possible insiders who are compromising security of the simulated environment.

-What is Novelty?

-Novelty is described as a situation or data that differs from the previous data, or data that has been introduced previously.

-What is an Insider?

-An insider would be an agent that is acting differently than other agents but attempting to hide their actions, similar to how someone in real life could sell secrets or volatile information.



GHOSTS Highlights

GHOSTS provides the realism that is missing in cyber environments that lack random, independently generated traffic from multiple sources to multiple destinations.

A. GHOSTS uses vTunnel to hide the connection to the central command server from exercise participants.

B. Artificial intelligence powers non-player characters to create realistic and self-directed communications.

C. Event managers can give instructions to any number of GHOSTS clients from a central command server.

Expansions on the System

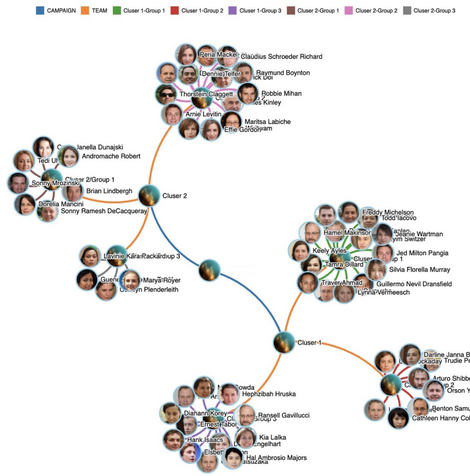
it is also possible to use this system to create active intervention scenarios, in which an AI or person could actively intervene as opposed to just using an AI to interpret data like we are using the system. The figure above describes how this scenario would be organized. In the future, this is an idea that we could adapt our approach to consider depending on viability.

References

-Software Engineering Institute, CMU, “Ghosts, A Framework for Realistic NPC Organization”

Ghosts Groups

Ghosts has the capability to simulate groups as well, such as teams inside of a company, or a department. This structure can be seen in the figure below.



How our System Works

-Multiple machines running VM’s to allow ghosts to run consistently for as long as required.

-Each VM gets “taken over” by the Ghosts system, and it will do actions as dictated by the host, such as opening an excel document, sending an email, etc.

-In the future, we would like to get a sort of portal set up, so our collection of machines can be accessed from anywhere, and we can run experiments more conveniently.