Shadow Figment technology foils cyberattacks

2 June 2021, by Tom Rickey

Keeping electricity flowing without disruption from a cyber attack is one aim of Shadow Figment. Credit: Urbans | Shutterstock.com

Scientists have created a cybersecurity technology called Shadow Figment that is designed to lure hackers into an artificial world, then stop them from doing damage by feeding them illusory tidbits of success.

The aim is to sequester bad actors by captivating them with an attractive—but imaginary—world.

The technology is aimed at protecting physical targets—infrastructure such as buildings, the electric grid, water and sewage systems, and even pipelines. The technology was developed by scientists at the U.S. Department of Energy's Pacific Northwest National Laboratory.

The starting point for Shadow Figment is an oft-deployed technology called a honeypot—something attractive to lure an attacker, perhaps a desirable target with the appearance of easy access.

But while most honeypots are used to lure attackers and study their methods, Shadow Figment goes much further. The technology uses artificial intelligence to deploy elaborate deception to keep attackers engaged in a pretend world—the figment—that mirrors the real world. The decoy interacts with users in real time, responding in realistic ways to commands.

"Our intention is to make interactions seem realistic, so that if someone is interacting with our decoy, we keep them involved, giving our defenders extra time to respond," said Thomas Edgar, a PNNL cybersecurity researcher who led the development of Shadow Figment.

Exploiting attackers' 'success'

The system rewards hackers with false signals of success, keeping them occupied while defenders learn about the attackers' methods and take actions to protect the real system.

The credibility of the deception relies on a machine learning program that learns from observing the real-world system where it is installed. The program responds to an attack by sending signals that illustrate that the system under attack is responding in plausible ways. This "model-driven dynamic deception" is much more realistic than a static decoy, a more common tool that is quickly recognized by experienced cyberattackers.

Shadow Figment spans two worlds that years ago were independent but are now intertwined: The cyber world and the physical world, with elaborate structures that rely on complex industrial control systems. Such systems are more often in the crosshairs of hackers than ever before. Examples include the takedown of large portions of the electric grid in the Ukraine in 2015, an attack on a Florida water supply earlier this year, and the recent hacking of the Colonial Pipeline that affected gasoline supplies along the East Coast.

Physical systems are so complex and immense

that the number of potential targets—valves, controls, pumps, sensors, chillers and so on—is boundless. Thousands of devices work in concert to bring us uninterrupted electricity, clean water and comfortable working conditions. False readings fed into a system maliciously could cause electricity to shut down. They could drive up the temperature in a building to uncomfortable or unsafe levels, or change the concentration of chemicals added to a water supply.

Shadow Figment creates interactive clones of such system in all their complexity, in ways that experienced operators and cyber criminals would expect. For example, if a hacker turns off a fan in a server room in the artificial world, Shadow Figment responds by signaling that air movement has slowed and the temperature is rising. If a hacker changes a setting to a water boiler, the system adjusts the water flow rate accordingly.

Shadow Figment: undermining ill intent

The intent is to distract bad actors from the real control systems, to funnel them into an artificial system where their actions have no impact.

"We're buying time so the defenders can take action to stop bad things from happening," Edgar said. "Even a few minutes is sometimes all you need to stop an attack. But Shadow Figment needs to be one piece of a broader program of cybersecurity defense. There is no one solution that is a magic bullet."

PNNL has applied for a patent on the technology, which has been licensed to Attivo Networks. Shadow Figment is one of five cybersecurity technologies created by PNNL and packaged together in a suite called PACiFiC.

"The development of Shadow Figment is yet another example of how PNNL scientists are focused on protecting the nation's critical assets and infrastructure," said Kannan Krishnaswami, a commercialization manager at PNNL. "This cybersecurity tool has far-reaching applications in government and private sectors—from city municipalities, to utilities, to banking institutions, manufacturing, and even health providers."

"The development of Shadow Figment illustrates how PNNL technology makes a difference in so many lives," Krishnaswami added. "The Laboratory's research provides protection against an array of threats, including cyberattacks."

Provided by Pacific Northwest National Laboratory

APA citation: Shadow Figment technology foils cyberattacks (2021, June 2) retrieved 29 November 2021 from https://techxplore.com/news/2021-06-shadow-figment-technology-foils-cyberattacks.html