Pacific Northwest
NATIONAL LABORATORY

Shadow Figment – Adaptive Strategic Deception

The challenge/need

Operational technology (OT) environments are increasingly becoming targets for cyberattacks. Monitoring and upgrading equipment deployed in the field is often still done via embedded devices like programmable logic controllers rather than technologies that afford full computer control.

This approach makes it difficult, slow, and costly to apply patches or update field equipment. As rapid patching has become a key tenet of strong cyber protections, this leaves OT environments particularly vulnerable to rapidly evolving cyberthreats.

APPROACH

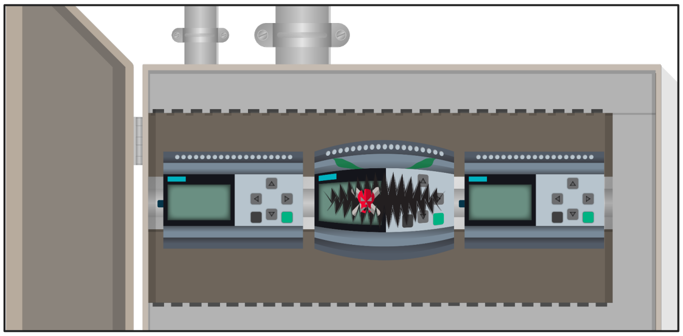
Pacific Northwest National Laboratory (PNNL) has developed a new approach to adaptive strategic deception through its Proactive Adaptive Cybersecurity for Control (PACiFiC) project.

PACiFiC combines adaptive principles, cross-domain information, and classic security best practices to deliver measurably more secure, reliable, robust, and resilient control systems while retaining business performance. By unifying disparate data and information across domains, including human, cyber, communications, and process physics, PNNL has defined and established secure design principles for use in all OT systems across multiple critical infrastructures.

Through sophisticated deception techniques, defenders can turn the tables on the attackers by distracting them, impeding their progress, and creating uncertainty. PNNL delivers these capabilities in a unique, patent-pending deception technology called Shadow Figment.

HOW IT WORKS

Shadow Figment is a model-driven cyber defense designed specifically for control system environments. The technology utilizes a distributed computational platform to define and deploy deceptive devices. Deployed decoys respond to protocol queries from an attacker with realistic, plausible return signals. As attackers interact with decoys, alerts are sent to defenders and incident responders to inform and educate them about active attacks.



Shadow Figment decoys mimic OT controllers in a networked system.

Shadow Figment provides model-driven decoys to convey realism and make the decoys appear to operate in coordination with real systems. Existing information-technology-based deception platforms only expose network services, such as network shares, that silently wait for an attacker to connect.

However, OT environments include sensors and controllers constantly interacting to manage a physical process. Devices that are not communicating are obviously suspicious.

Shadow Figment technology defines and deploys OT decoys that behave and can interact with real devices as if part of the real network.

To do this, models of the physical process are generated through machine learning using sensor data from actual OT settings. These models can then be expanded with new variables and functions and mapped to decoys, so the decoys appear to be interacting with the same process as the real devices.

In addition, Shadow Figment decoys accept control commands and setting changes so the hacker believes he's controlling an actual device within the OT system.

Specialized algorithms enable the Shadow Figment decoy to send realistic operational signals back to the attacker, showing a real-world physical reaction that would be expected.

The data engine predicts the system effects of those changes and further confounds the attacker with very realistic looking responses.

BENEFITS

Shadow Figment offers a platform to manage deployment of deceptive cyber-enabled control sensors specifically designed for OT environments and systems.

Novel breadcrumb concepts and scripts integrate with OT software and devices. Shadow Figment provides two options for deploying decoys. First is the System Copy Deception, and the second is a New System Deception. Each protects critical system components. This approach provides higher fidelity deception of control system environments compared to current-generation information technology deception platforms.

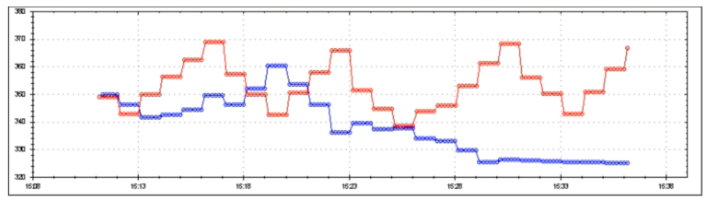
The Shadow Figment platform also includes a sandbox to collect data that can later be used to model attack goals and strategies.

IMPACT

Shadow Figment decoys shift attacker resources away from real cyber-physical systems in an OT environment.

Decoys draw the attacker toward apparent easier and higher value targets. Engaging the attacker with Shadow Figment decoys provides an early warning system for operators and preoccupies the adversary, slowing down the attack and allowing countermeasures to be employed.

Like a canary in a coal mine, Shadow Figment provides early, enhanced detection of adversarial behavior, while also frustrating the attacker's efforts by drawing their focus away from real targets.



The machine learning model is "good enough" to be convincing that it is part of a real system. The red line shows the real system status operating normally, while the blue line shows the decoy status as the decoy is being attacked to shut down the system. The downward slope convinces an attacker that they are achieving the desired effect of their attack.

For more information, contact

William Hofer
Principal Investigator
National Security Directorate/Computing & Analytics
Pacific Northwest National Laboratory
509.372.6229 | William.Hofer@PNNL.Gov

Thomas Edgar
Cybersecurity Researcher/Computing & Analytics
National Security Directorate
Pacific Northwest National Laboratory
509.372.6195 | Thomas.Edgar@PNNL.Gov

www.pnnl.gov