perspecta LABS

SecureSmart cyber emissions monitor

True air-gapped and continuous autonomous monitoring

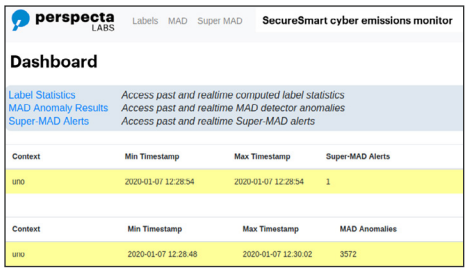
Internet of Things (IoT) and industrial control systems (ICS) are becoming increasingly vulnerable to cyberattacks. Most devices on these networks are susceptible to evolving threats and are not protected by traditional cyber monitoring or prevention techniques. In today's expanding threat environment, it's not a matter of if, but when these devices will become compromised. And at that time, how will the attack be detected? Utilities and other industries need a fast, reliable and easy to deploy monitoring and detection solution capable of defending critical embedded devices against malware.

Perspecta Labs' cyber emissions monitor, part of the SecureSmart™ critical infrastructure solution line, is a highly portable, anomaly detection system that can assess the integrity and operational state of protection system equipment based on non-intrusive monitoring of device radio frequency (RF) emissions in a substation and other ICSs. All electronic processors produce unintended side effects such as power consumption, electromagnetic leakage and sound. Our solution analyzes and correlates these side effects with device behavior to determine if a device is operating normally or if it has been compromised.

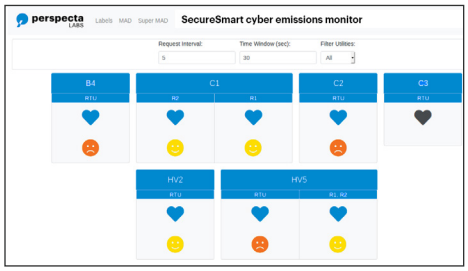
How it works

The SecureSmart cyber emissions monitor provides a true air-gapped defense that has no electrical path between the monitoring system and the devices being monitored. This means that an attacker cannot examine an exploited device for signs that it's being monitored; preventing the attacker from identifying and then attacking the monitoring system.

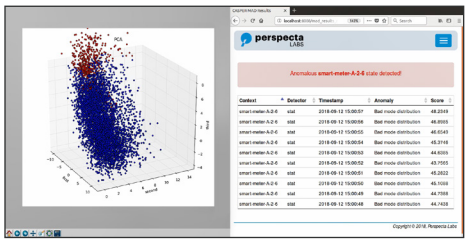
Our solution uses a small antenna attached near the protected device(s) to capture its RF emissions. The solution then analyzes the emissions and tracks them against a baseline model of normal RF activity from the same device. If an anomaly is detected,



The cyber emissions monitor dashboard displaying the total anomalies as well as the collectors detected and alerts sent



Sample display of all network devices monitored



Monitor GUI showing 3D visualization of the device side effects. The red dots indicate previously unseen behavior which generates an anomaly report displayed in the dashboard

the solution's sensors will send alerts over a forensics network to activate monitoring platforms.

The novel technology employed by the tool can be used in electric distribution, IoT and ICS networks as an early warning system to rapidly detect potentially compromised devices and better focus security monitoring resources and tools to diagnose and repair infected devices. The solution can be deployed permanently in substations or used as a portable "magic wand" for spot-checking devices.

About SecureSmart

The SecureSmart critical infrastructure solution line is a suite of industry-changing technologies that help defend critical infrastructure and smart energy systems with comprehensive integrated operations, engineering, security monitoring, anomaly detection, protection, analysis and troubleshooting capabilities for energy management systems (EMS), supervisory control and data acquisition (SCADA), and advanced metering infrastructure (AMI) and distribution automation (DA) field networks.

Why Perspecta Labs

At Perspecta Labs, we refuse to think inside the box. As the innovation hub of Perspecta, we are molding the future of emerging technologies. Our experts conduct leading applied research into cybersecurity, mobile communications, machine learning and internet of things technologies that provides customers with transformative insights and real-time situational intelligence. With our finger on the pulse of next-gen technology, you'll gain an essential edge.

Perspecta Labs is a wholly owned subsidiary of Perspecta Inc., a proven provider of information solutions, engineering and analytics for the U.S. Government.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920