

Solving a National Problem

Intel® Security Critical Infrastructure Protection

The risk of cyberattacks on critical infrastructures is no longer theoretical. Grid operators are investing aggressively in both physical and information security systems, and there is accumulating guidance from governments worldwide on measures that should, and, in some cases, must be taken to secure the supply and delivery of electricity.

Building security into the grid can be challenging. Infrastructure elements can be very long-lived, and it might not be practical to replace equipment and applications with new versions that have security designed into them—which is optimum. In addition, availability of service is paramount for the grid, so common IT security measures, such as patching and rebooting, are inappropriate. Security for critical infrastructure needs to be non-invasive but simultaneously extremely robust.

An End-to-End Defense for Critical Infrastructures

Against this backdrop, Intel and two of its subsidiaries—Intel Security and Wind River—have been designing a solution to secure not only new, but also legacy infrastructures. Working with the Center for the Commercialization of Electric Technology (CCET) and the Electric Power Group (EPG), Intel has come up with a breakthrough solution: Intel Security Critical Infrastructure Protection (Intel Security CIP). The solution works by separating the security management functions of the platform from the operational applications so that the operational layer can be robustly secured.

The beauty of the Intel Security CIP approach is that it works for both new and existing infrastructures, and implementing it with existing systems is not only feasible, but also cost effective. This is a huge benefit—the solution can be applied without requiring any changes to business processes or application software, and it can be retrofitted onto existing systems. Intel Security CIP takes full advantage of hardware-based security fundamentals and a robust set of software technologies to monitor and protect critical systems end-to-end.

Field Trial: Protecting Synchrophasor Applications Is Critical

Since December 2013, the Intel Security CIP has been in a field trial at Texas Tech University (TTU), where it is demonstrating protection of EPG's synchrophasor applications, which analyze in real time power delivery failures such as those that would be caused by a cyberattack. By protecting the synchrophasor analytics, the heart and health of the system is protected from malicious cyberattacks and infrastructure attacks.

Product Brief

This solution also has undergone extensive and independent penetration testing by the university's computer science department engineers. Since the time it has been installed, the Heartbleed vulnerability and Havex attacks have further increased awareness of grid vulnerabilities. Since delivering panoramic situational awareness is key to the solution, engineers were able to prove how Intel Security CIP protects against these recent vulnerabilities.

Robust Security for New and Legacy Infrastructures

While the TTU field trial deploys the solution for securing synchrophasor analytics, the Intel Security CIP can be applied to many other critical infrastructure systems that need robust managed security. It would be equally effective for military applications, the oil and gas industry, and medical applications, to name just a few. Intel Security CIP addresses the fundamental security building blocks of device identity, malware protection, data protection, and resiliency—all tailored for today's machine-to-machine environments. And because this sophisticated and extensive solution can secure both new and existing infrastructures, it holds tremendous promise for securing the grid.

Learn More

For additional information on how Intel Security helps protect your critical infrastructure security, visit our embedded security software and solutions website (mcafee.com/embedded).