Prometheus Security Group (PSG) Global

Securing Critical Infrastructure Points (CIP) and Homeland Security

In today's world, video technology is developing at a rapid pace as user expectations, data traffic and storage requirements are greater than ever. Historically, security systems utilized a fixed sensor-based mindset where a user interfaced with a centralized head-end platform and video was used as a confirming subsystem. This paradigm is rapidly changing as users are demanding dynamic, multi-layered, combined information with "eyes on the scene". Advanced video analytics more accurately process time, spatial positioning and patterns to provide enhanced information for decision making. "Video is no longer regarded as an add-on subsystem but rather a core component. Why? because 'seeing is believing', and video is vital in bringing our eyes to the scene," explains Daniel Griego, Director of Cyber & Network Services at Prometheus Security Group (PSG) Global.

Griego references an incident in 2013 when the Crown Casino in Melbourne, Australia fell victim to an elaborate heist involving video manipulation; these scenes, once thought to occur only in Hollywood films, took the unexpected and made it an astonishing reality. This event is sobering because it has simultaneous insider and external attack potential. This demonstrates a very real and present threat to our homeland's military, government facilities, command and control centers, power plants, flight lines and other critical infrastructure points (CIP). This threat outlines the need for even more advanced methods of video signal verification and protection.

Jeremy Freeze-Skret, Vice President of PSG Global touches upon the challenges faced by one agency–the International Atomic Energy Agency (IAEA) in ensuring safeguards. The IAEA carries out 2,000 inspections on the ground, with more than 20,000 seals, over 1,000 attended/unattended monitoring and measuring systems in the field. "It's clear that authentic surveillance imagery could assist in addressing the massive auditing challenges," says Freeze-Skret. While the acceleration of new video based technology is a positive enhancement to overall security, it has simultaneously exposed infrastructure to a myriad of attack entry points where new threats can be introduced. "The authenticity of the video chain of data transmitted over networked systems is crucial to the entire security solution," Freeze-Skret adds.

PSG Global has developed a patented product called 'Scene Authentication' that addresses this concern. This is the first-ever, comprehensive real-time protection of the surveillance video data chain from its inception (video scene) to its delivery (viewing or storing). Combining a unique technology and drawing on

a standards-based approach to cryptography, the video chain is continuously verified, validated and can be trusted. Scene Authentication ensures video scenes are live, authentic, and have not been manipulated by any entities. The technology leverages an encrypted, external light source produced by an active transmitter positioned in the video scene. Using the camera as a sensor, the encrypted signal is subsequently read by a paired receiver. The data generated is uniquely encoded with the video stream and the frames are digitally signed with Ravinder-Shamir-Adleman (RSA) in real-time. The technology functions like an 'invisible fingerprint' or silent bank alarm for video–it remains ever present and ever vigilant even in video storage. With this technology, the enterprise is safe-guarded while video operations remain unaffected.

PSG Global offers an edge network appliance known as the Talon which integrates the breakthrough Scene Authentication technology. Talon is an ultra-high security multi-function, embedded security appliance. The device delivers FIPS 140-2 compliant encryption with real-time, secure video and control data over an IP network. Kevin Bray, Director of Sales at PSG Global says "I'm very excited about the OEM potential for this technology. We've proved a small embedded device can deliver these advanced analytics which means it can also be integrated into most IP surveillance devices. CR