PROMETHEUS
SECURITY GROUP GLOBAL

Solutions

Markets

COMMAND AND CONTROL
C2 - IDS - ACS - Video

ZERO TRUST ARCHITECTURE
Cyber Secure from Sensor to C2

DOD

DOE

CRITICAL INFRASTRUCTURE

ZERO TRUST DATA ATHENTICATION
"from the EDGE to BDOC and beyond"
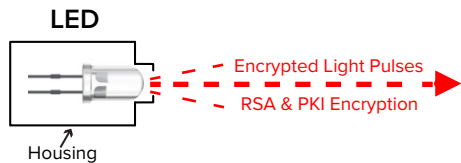
SCENE AUTHENTICATION

Product Overview

Scene Authentication is a PSG Patented product which provides real-time authentication of a video signal from its inception (video scene) to its delivery (viewing or storing). It is the first end-to-end authentication of its kind and simultaneously protects video signaling from spoofing, tampering and hijacking. Scene Authentication assures users that any instances of video produced by their surveillance system came from its cameras, at that the actual location at a specified point in time.

Features	Benefits
U.S. Patent Aug 2016	- Unique end-to-end protection
AES Encryption and RSA Signing	- Advanced encryption and protection
Automated Pairing and Tuning Algorithm	- Easy installation and configuration
Configurable Alerting	- Differentiates a real attack from an interruption
Environmental Tuning	- Reduces False Positives
Aware of time, spatial positioning	- Verifies Video Veracity
Metadata Validation	- Protects stored video with reversible audit
Integrated with ONVIF	- Federal Information Processing Standard (FIPS-140-2)
Available for OEM Integration	- Technology can be integrated into camera/encoder firmware
USB Host One to Many Programming	- Manage many devices from a single secure token
Industrially Designed	- -40° to +70° C operation, made for uptime and reliability

Active Transmitter in Field of View

Surveillance Camera

HPC

Viewer

LED

Encrypted Light Pulses

RSA & PKI Encryption

Housing

HTTPS (C2)

SRTP (AES Encryption)

Metadata Authentication

Authenticated Video/Metadata

- Supplies encrypted coded light signal
- Signal placed in the video scene
- Signal supplies geo-coordinates of emitter
- Spatial Location within video scene & time
- Public key loaded on emitter via USB
- PKI encryption secures data as transmitted
- Up to 4 emitters in a scene
- Tamper protected housing
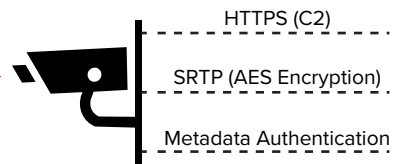
- Compliant with USAFI 31-101/AFMAN
  Section 9.15.3 regarding spoofing, bypassing,
  or system sabotage
- Receiver Software decrypts emitter metadata
- Detects Video Loops
- Detects covering of the emitter
- Detects injected video
- RSA signed data

- Decodes authentication signal
- Sends authentication metadata to storage
- Alerts guard of tampering
- Receiver software is a part of VICADS

- Authenticated Video from scene to viewer
- Emitter signal is masked out of the operator view

Acronyms:
- RSA Encryption - Asymmetric private / public key encryption
- PKI - Public Key Infrastructure to authenticate users and devices
- SRTP – Secure Real Time Protocol (AES Encryption for video)

Legend:
Red = Encrypted light from emitter
Black = Authenticated Video/Metadata over IP