White Paper for MOSAICS JCTD Industry Day

TRIPLiot

Patching and Updating IoT Remotely, Securely, and at Scale

Deep…Hardened…Isolated

For Security Inside the IoT Device Where it Belongs

InZero Technologies
September 2020

Problem Statement

IoT, with its fleets of connected devices, has brought incredible capabilities while also exposing a large, vulnerable attack surface. The number and nature of these devices has complicated the security and management of the enterprise. It is well known that to date, IoT cyber security has been largely an afterthought. These devices must be made fundamentally more secure and more defendable.

TRIPLiot Executive Summary

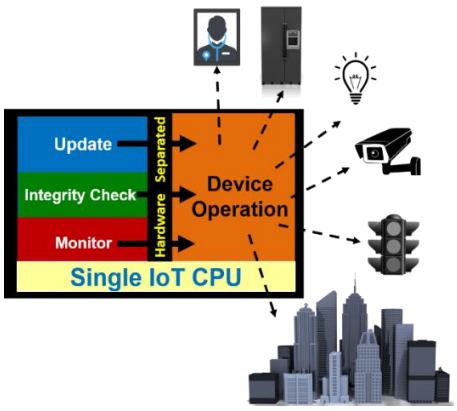
TRIPLiot is an in-device HARDWARE-ENFORCED data separation technology for entire fleets of IoT/ICS devices which enables remote:

- Isolated real-time firmware updates
- OS patching and updates
- Only signed updates are allowed
- Code integrity checks
- Ongoing data traffic monitoring
- Hot swap updates so downtime is seconds or less
- Blocking of unauthorized internet traffic to deployed devices
- Immediate mitigation and active defense against hacks
- Remote updates and remediations

TRIPLiot thus provides advanced enterprise update and security management for IoT, ICS, sensors, and drones.

Benefit to the ICS Operator

TRIPLiot greatly increases the security, reliability, resiliency, and availability of sensor, drone, and IoT systems. This provides the ICS community more reliable systems with greater security and improved capabilities.



Overview

TRIPLiot establishes A SEPARATE IN-DEVICE MINI-VM/OS THAT IS INACCESSIBLE TO ANY INCOMING MALWARE. This eliminates the need for physical device access for firmware updating, and the isolation provides advanced protection against internet-borne malware. The TRIPLiot VM/OS automatically checks firmware update electronic signature to prevent against unauthorized alteration. Importantly, the TRIPLiot VM/OS is independent and inaccessible from the host OS, making it immune to malware which may effect the device OS. The SYS ADMIN can access the TRIPLiot VM/OS remotely across the entire deployed fleet of devices (sensors, SCADA/ICS, autonomous systems/drones, or IoT node).

TRIPLiot overcomes THE KNOWN UNRELIABILITY AND DELAYS that typically occur when IoT devices are infected and expose the enterprise to a widespread breach. It also addresses the situation where adversaries take advantage of the delay and burden of IoT device correction to disrupt systems in order to damage or degrade operations of US and Coalition forces. In short, TRIPLiot puts important device security inside the device, where it belongs. Should a device running TRIPLiot become compromised,

TRIPLiot allows the SYS ADMIN TO REGAIN CONTROL OF THE INFECTED DEVICE remotely by automatically rolling back to a known good OS configuration or a new patched firmware.

TRIPLiot's mini-VM/OS is launched in parallel to the device OS during normal operation. Security and integrity checks, patches, and updates are run during normal operation. Once the Sys Admin is confident of the stability of the updated configuration, the OS's are hot-swapped. This means the device is only down for a second or two (or less). This is done remotely and can be done across an entire fleet of devices simultaneously.

TRIPLiot can be ported to any device running on a chip big enough to supports System-On-a-Chip (SoC). The amount and frequency of access to enterprise processing resources that are needed varies according to the number of devices.

Requirements and Technical Details

Software only. No additional hardware needed.

Target device must be running on a chip that support system on a chip (SoC).

No additional enterprise hardware needed. Periodic access to enterprise cloud needed for updates.

No change to device size or weight.

No additional power source needed.

Sys Admins already have the basic skills needed to work with TRIPLiot. Should only need familiarization with the capabilities and interface.

Cost is TBD.

References

InZero Technologies: https://www.inzerosystems.com/

Instructional video: https://youtu.be/pnOrwEgdemM

Patent: https://patents.justia.com/patent/20190014128

Contact Info

Matthew Dosmann – VP Strategy and Business Development
443.510.7260
InZero Technologies
100 Carpenter Drive, Suite 203
Sterling, VA 20164
703.636.2048