SCHOOL BUS & MASS TRANSIT LEVEL PROTECTION

CYBERSECURTIY SOLUTIONS FOR THE **BUS AND MASS TRANSIT INDUSTRY** SEAMLESSLY INTERGRATED DURING PRODUCTION OR **RETROFITTED** IN THE **AFTERMARKET** AS A SIMPLE PLUG IN

PROTECTION IN THE FACE OF VEHICLE HACKING

As vehicle complexity and connectivity requirements increase, the need for post-production scalability and extensibility is rising. Furthermore, a secured end-point within the vehicle becomes increasingly vital to the automotive value chain as well

Today's buses are heavily connected and outfitted with numerous sensors, management systems, tracking devices, and other technologies that relay data with the intent to travel as safely as possible. However, connectivity is changing busing operations as each new connected technology adds new cybersecurity vulnerabilities. When we are transporting millions of children and passengers each day, cybersecurity must be viewed as an extension of safety and not be viewed as a 'patch in' solution.

Deterministic cybersecurity must be employed for cyber health with a holistic and defense-in-depth approach as buses and other forms of mass transit transport human lives. There is no room for risk, false positives or errors when lives are at stake.

CYBERSECURITY OF SCHOOL BUSES AND OTHER MASS TRANSIT FLEETS

Cybersecurity must be treated as a necessity rather than a luxury in order to maintain the control and integrity of the vehicle and fleet as a whole while simultaneously serving as the foundational layer to enable services, applications, data analytics and more. Current levels of connectivity in buses and other forms of mass transit create a large attack surface that can compromise the safety of the vehicle, its passengers and the data produced. Furthermore, advanced fleet management relies on the constant flow of accurate data directly from the vehicles to the fleet manager's data center. Successful vehicle hacking attacks could result in:

- Loss of command and control communication with vehicles
- Inability to access location data and services for route planning
- Disabled functions in the vehicle leading to loss of life

Buses generate a plethora of operational data, indicative of behavior, maintenance, functionality, health and more. GuardKnox's Secure Network Orchestrator (SNO™) maintains the vehicle and data cyberhealth and integrity, saving fleet managers from costly downtime while ensuring the longer life cycles needed in the industry.

GUARDKNOX'S METHODOLOGY, WHICH PRIORITIZES AND PROTECTS **SAFETY-CRITICAL SYSTEMS**, HAS BEEN PROVEN IN THE ISRAELI AIR FORCE AND **ADAPTED** AND **OPTIMIZED** FOR THE MODERN **MASS TRANSIT** FLEET

www.guardknox.com | info@guardknox.com | 2 Hahazon St. PO Box 320, Ramla, Israel 7210202

SCHOOL BUS & MASS TRANSIT LEVEL PROTECTION

UNDERSTANDING THE NEEDS OF THE SCHOOL BUS & MASS TRANSIT INDUSTRY

School buses in the United States are the largest singular form of mass transit, with around 25 million students riding over 450,000 buses each day. Public transportation which encompasses public buses, metro systems, trains, and more transports over 34 million riders every weekday in the United States. Globally, 53 billion people took public transportation in 2017. Telematics and fleet management solutions enable bus operators and school districts to monitor, filter, and better understand usage and safety. When we factor in other forms of mass transit buses, there are even more lives at risk if proper cybersecurity measures are not practiced.

Large ransomware attacks are a major cause for concern when it comes to the safety of children, especially when there can be upwards of 70 passengers on board. Disablement of a school bus could block traffic, create chaos, and even endanger lives. Additionally, with the levels of connectivity to other buses, there is always the risk that one compromised vehicle could be used as a stepping stone to shut down an entire fleet.

GUARDKNOS'S UNIQUE **VALUE PROPOSITION** BRINGS SOLUTIONS TO THE INDUSTRY THAT PARSE ALL IN-VEHICLE COMMUNICATIONS AND DROP ANY IMPROPER MESSAGES IN REALTIME. OUR PLATFORM PROVIDES A **SECURE END POINT** FOR DATA HOSTING, PROCESSING AND STORING

LOCAL SECURE NETWORK ORCHESTRATOR (SNO™)

The GuardKnox SNO™ is a cybersecure and optimized computing platform. The comprehensive hardware and software approach enables heavy customization in realtime without any compromise to security.

Guardknox's collaboration with Palo Alto Networks enables true end-to-end solution and protection by using Palo Alto Networks expertise in network and cloud security with GuardKnox's expertise in automotive security. Manufacturers can secure OTA communications between the vehicle, the cloud, and their operational centers.

The SNO™ is an especially attractive solution for buses, as it can be seamlessly integrated into the fleet without needing to take the buses out of daily service. The SNO™ is a simple plug-in that can easily be installed in the OBD port during vehicle manufacturing or retroactively in the aftermarket.

USE CASES

Fleet Management Protection: Create the secure environment to ensure no vulnerability or ransomeware attack is used as a stepping stone to take control of the entire fleet

Secure Telematics ECU (TGU): Secure functioning from any external cyber threats as well as securing data obtained from the device