A Layered Approach for Securing “Internet of Things” Devices in Transportation

A strategic technology perspective

Alcatel·Lucent
Enterprise

Background

Transportation networks have been evolving with the desire to increase public safety, provide increased passenger/traveler services, while at the same time, trying to reduce network complexity and lower operating costs. In order to improve the passenger experience and increase ridership, transportation operators are increasingly providing additional services. These include services such as Internet access, video on demand, and free e-books, either directly, or via advertising sponsors. Passengers are using smart phones, tablets, laptop computers and a multitude of connected devices while on the go. This phenomenon, known as "Bring Your Own Device" (BYOD), reflects users needs and desires for mobility.

IoT (Internet of Things) is now adding an extra layer of complexity and pressure to transportation entities. For example, Intelligent Transportation Networks (ITS) provide drivers with advanced warning information on road conditions via digital signage for speed notification, traffic accident information, and road hazard awareness. Rail is looking at safety systems such as Positive Train Control (PTC) systems, to remotely and automatically slow down or stop runaway trains. Airports are looking at more efficient methods of servicing planes while away from their gates, and the shipping industry is looking to streamline cargo asset tracking.

All of these solutions involve some type of sensors, devices and/or hardened equipment. However, with mobility come security challenges for network infrastructure managers. The scale of the problem gets much bigger with more than 20 billion objects expected to be connected to networks by 2020. As described in the article "BYOD Was Merely an Appetizer; IoT is the Main Course," the nature of the problem has changed as there is often no user behind IoT connected devices.

Here is an overview of the layered security approach that ALE (operating under the Alcatel-Lucent brand) uses to secure IoT devices in Transportation:

Protection against denial of service

One of the most common security issues that results from IoT devices is denial of service (DoS). A DoS is a security attack aimed at devices that are available on a private network or the internet. Your first line of defense against these attacks starts with your network switches, which should filter DoS attacks by default. This attack filtering is standard on every Alcatel-Lucent OmniSwitch®. Some attacks seek out system bugs or vulnerabilities, while other types of attacks involve generating large volumes of traffic such that network service is denied to legitimate network users. A recent ALE blog discusses these types of attacks and provides a list of things you can do to prevent or mitigate the effects of an attack. For example, a network switch should be set to detect various types of port scans by monitoring for TCP or UDP packets sent to open or closed ports.

Most network vendors have ways of protecting against DoS attacks. However, important ALE differentiators are the default enabled DoS filtering features. From the moment a switch is turned on, network access is secure. These basic DoS filtering features strengthen the foundation and ensure secure connectivity and IoT device operation.

Secured network

ALE provides a unique network architecture design that helps reduce human configuration errors – a leading cause of security vulnerabilities. This unique capability is called iFab (Intelligent Fabric). iFab offers a single layer (called a POD/MESH) that provides a unique, nearly linear scalability from 50 to 14,000 10GigE ports. Moves, adds, and changes are fully automated, dramatically reducing human configuration errors.

iFab is based on the IEEE 802.1aq Shortest Path Bridging standard (SPB), which provides multi-link topology. This means that all links are active with load sharing. SPB enables large Layer-2 topologies with a shorter convergence time.

SPB is not new. It is an amendment to IS-IS, which is a mature protocol used by carriers for the past 25-30 years. IS-IS is built over Ethernet, and not over IP over Ethernet. Consequently, SPB does not need an IP address. This means it's possible to build a network backbone of 100 switches without an IP address, so core switches are invisible from hackers. IP-based attacks are therefore impossible. Only Ethernet-based attacks are possible, but they are complex to execute, and more importantly they effect only one hop in the network.

SPB should be deployed in a service-based approach. Each service is created and IS-IS distributes the service information and automatically builds the topologies to connect all the endpoints (IoTs) to the service. Each SPB service represents a single Layer-2 virtual network.

The protocol can scale up to 16.7 million separate services using a 24 bit service description field. This easily enables highly virtualized networks that far exceed the 4K limit of the traditional VLAN tag format. By separating and containing HVAC sensor traffic from CCTV, for example, an IoT attack on one object type will affect a only a portion of the network, thus reducing network downtime and in most cases eliminating unplanned network outages.

Secured service

ALE provides additional security measures at the service level (which is the IoT level).

IoTs are authenticated via IEEE 802.1X network-based authentication, MAC-based authentication or other mechanisms. The object is then automatically assigned to a specific "HVAC" or "CCTV" profile, for example. These profiles contain parameters such as access control lists (ACLs), VLAN, QoS, and

bandwidth limitations. This ensures that only multicast CCTV type of traffic is forwarded on the network from an object authenticated as “CCTV”. Any other type of traffic from such an object will be automatically discarded even before entering the network. This is configurable and several types of traffic can be defined in a very granular manner.

Only authorized traffic will enter the correct SPB virtualized portion of the network. In essence, the specific object will be restricted to the appropriate container.

When coupled with access switches, a layer 2-7 deep packet inspection at wire-speed knows the exact traffic status, by object and by user. ALE presents this in an easy-to-read format for managers. Managers are then able to make the right decisions on network upgrades. Of course, this provides user and object data, which is today’s gold mine.

Embedded software – Ethernet switch security

Intelligent networks now require an increasing number of software capabilities that every piece of network equipment must support. And of course, the larger and more complicated the software program, the more likely it is to have vulnerabilities and backdoors.

One way that ALE addresses this situation is with the Alcatel-Lucent Operating System (AOS) software, which is embedded in all ALE network switches, and hardened to provide network-level integrity. The AOS software is verified and guaranteed by LGS Innovations, an independent organization.

LGS provides:

- Independent code verification to remove backdoors and vulnerabilities
- Code diversification reduces the risk of hacking via scanning of well-known maps by compiling code multiple times using different memory maps. Each time an ALE integrator downloads a new firmware version from a support site, the user receives a randomly generated version.
- A secured supply chain (available in the USA only) guarantees non-alteration of the code when downloaded by a partner or customer.

Network securing technology is here today

ALE has always been at the forefront of embedding and offering security features in LAN and WLAN network infrastructure products. With more than 15 years of innovations, ALE solutions are resonating with transportation system integrators. As tomorrow’s world of billions of connected objects on network infrastructures increasingly become a challenge, Alcatel-Lucent Enterprise LAN and WLAN solutions, with embedded security functionalities, are ideal for multi-level IT security:

- Embedded security firmware in network switches
- Embedded protection against denial-of-service attacks
- Secured network at both the core and access layers
- Secured network service for IoT

Transportation networks can now simplify the deployment of IoTs while providing a good security base. ALE enables network infrastructure managers to manage deployments themselves as long as the IT department provides the right network profile for users and devices, and the right network containment strategy for the IoT.

Alcatel·Lucent Enterprise