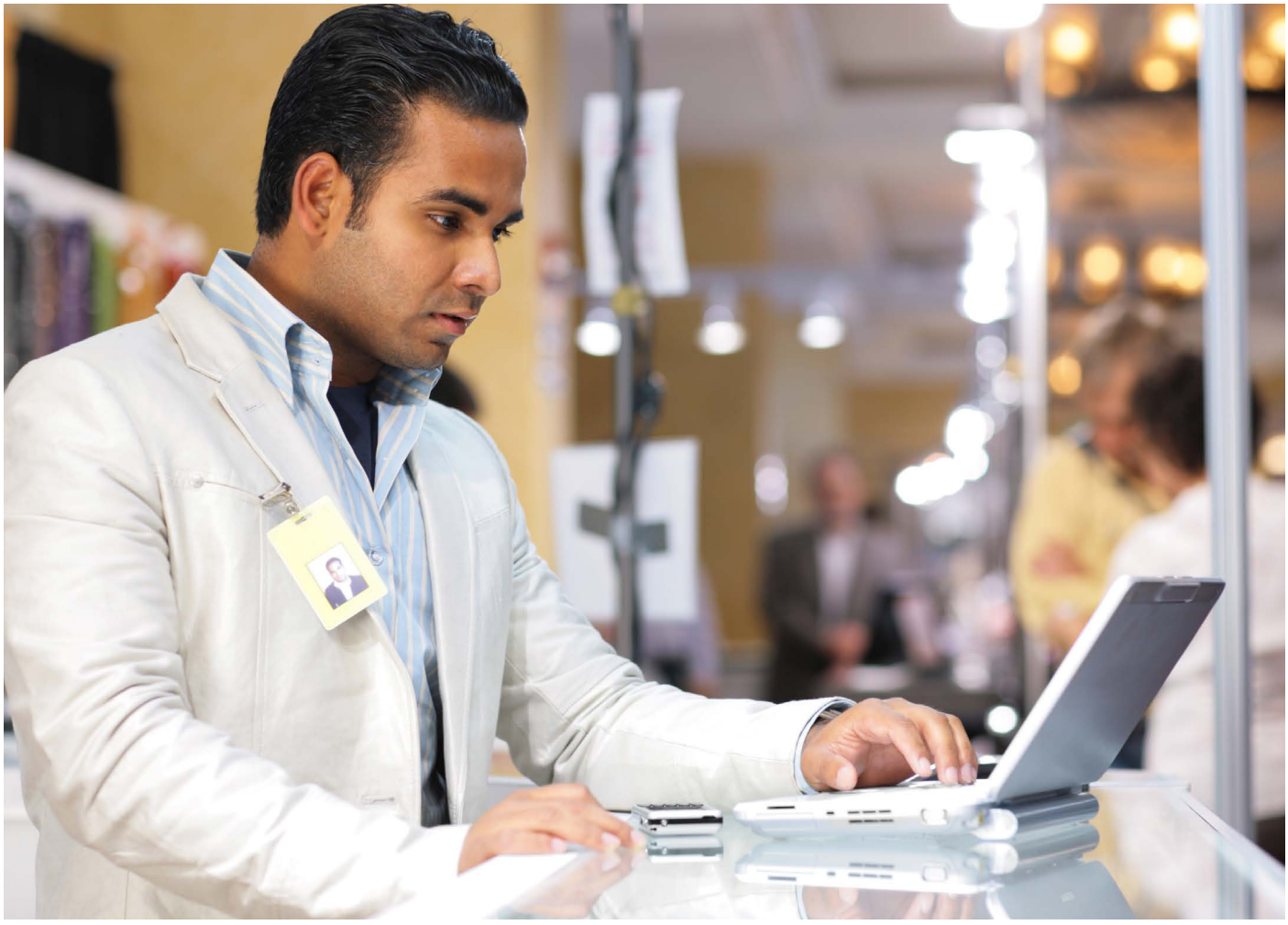
A Layered Approach for Securing "Internet of Things" Devices in Healthcare

A strategic technology perspective



Alcatel·Lucent
Enterprise

Background

Hospital networks have been supporting Electronic Medical Records (EMR) for some time and more recently, the requirement to support multiple mobile devices for clinicians, patients, administrative staff and visitors, has placed an increased burden on these same networks. This phenomenon, known as "Bring Your Own Device" (BYOD), reflects users needs and desires for mobility. Clinicians are looking at EMRs and making diagnoses on the go, patients and visitors want Wi-Fi internet connectivity and administrative staff are increasingly using mobility for their workflows.

Hospitals are also preparing for the onslaught of new devices and sensors that will help improve the patient pathway, like patient health monitoring at home, clinician/patient tracking and diagnostic equipment monitoring (status, maintenance schedules, etc.), but with mobility comes security headaches for CIOs. 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, because unlike BYOD, there is often no user behind IoT connected devices.

The following is an overview of the layered security approach that ALE uses to secure IoT devices in Healthcare.

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 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, an important difference that ALE offers are DoS filtering features that are enabled by default. From the moment a switch is turned on, network access is secure. These basic DoS filtering features strengthen the foundation for secure connectivity and operation of IoT devices.

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 making IP-based attacks impossible. Only Ethernet-based attacks are doable, but they are complex to execute and more importantly, they have an effect on 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, and 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 very limited portion of the network, thus limiting network downtime and in most cases eliminating many unplanned network outages.

Secured service

Additional security measures ALE provides are at the service level, meaning the IoT level. IoTs are authenticated via IEEE 802.1X network-based authentication, MAC-based authentication or other mechanisms. The object is automatically assigned to a specific profile, for example, "HVAC" or "CCTV". 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.

Such authorized traffic will only enter the right 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 (operating under the Alcatel-Lucent Enterprise brand) addresses this situation is to have the Alcatel-Lucent Operating System (AOS) software, which is embedded in all ALE network switches, hardened to provide network-level integrity. The AOS software is checked and guaranteed by LGS Innovations, an independent organization.

LGS provides:

- Independent code checking 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

Although ALE is not a security vendor providing firewalls or Unified Threat Management (UTM) solutions, ALE provides technology to help secure networks and mitigate cyber attacks – something every hospital should implement.

ALE has always been at the forefront of embedding and offering security features in LAN and WLAN network infrastructure products. 15 + years of innovations are now resonating with hospital CIOs as tomorrow's world of billions of connected objects on network infrastructures increasingly become a challenge. Alcatel-Lucent Enterprise LAN and WLAN solutions, with their embedded security functionalities, make them ideal for multi-level IT security:

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

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

Alcatel·Lucent Enterprise