Secure Building Automation — Case Study

Last Revised: September 2021

Introduction

Veridify Security and its partner, KMC Controls, have deployed their secure building solution in several commercial buildings across the US. This case study describes our early proof-of-concept (PoC) deployment in a 32-story office building in downtown Manhattan (for security reasons, we have not disclosed the exact location). Prior to our deployment, this building experienced a costly cyber-attack. As a result, the building owners were very motivated to have us secure their building.

Building with no security

At the project's inception, the building's HVAC contractor provided us with a layout of the automation components together with the building automation network topology. This building uses automation for HVAC only, but a planned upgrade will also put their lighting, elevators, and access control on the automation network. The building automation network communicates over *BACnet*, the leading building automation communications protocol.

A building management system (BMS) is installed on the 7th floor that talks to BACnet/IP routers on the 5th, 14th, and 32nd floors (see Fig. 1.). Not shown are several other BACnet devices located on all floors that communicate with the BMS by way of the routers.

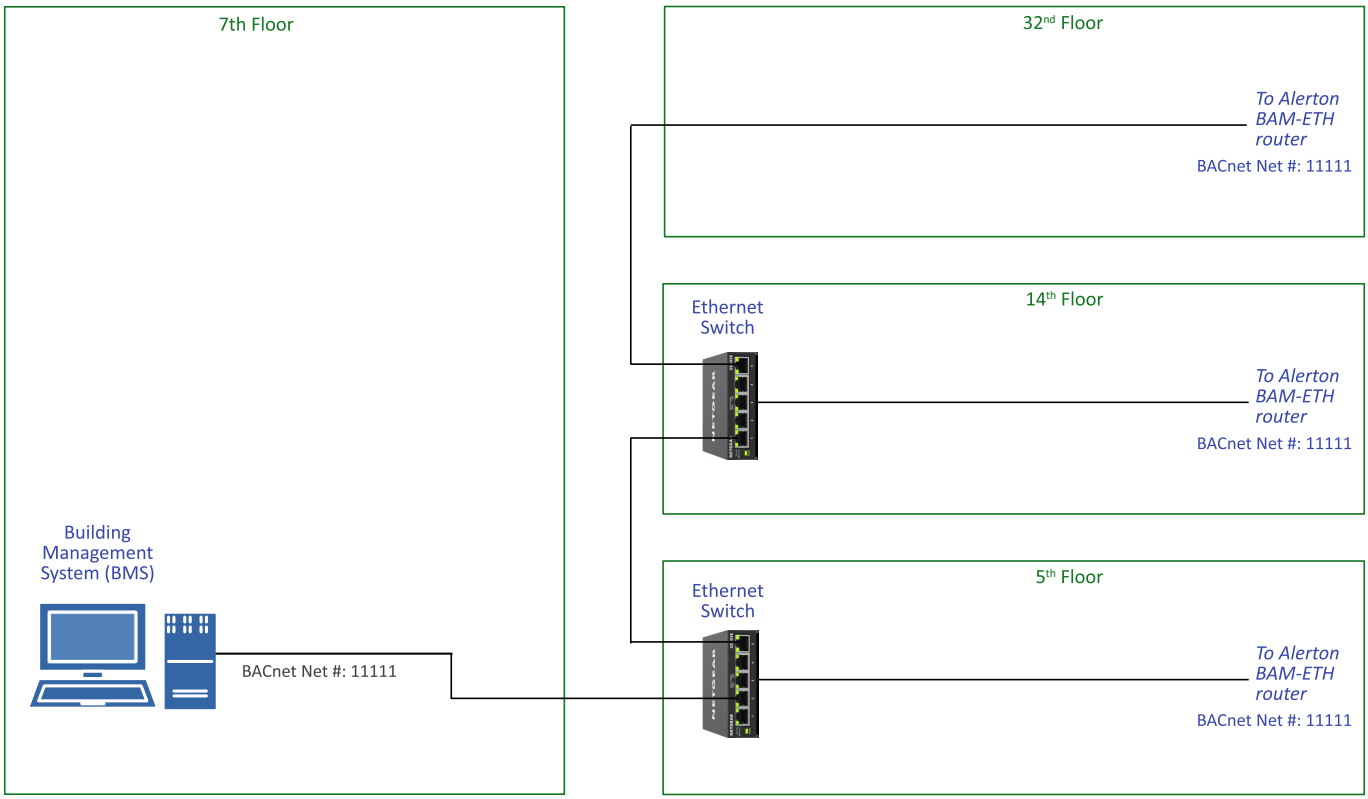

Fig. 1. Building automation network with no security

Building with security deployed

Fig. 2. shows the components installed by Veridify and KMC. The most important are the DOME Sentry's which are Bump-in-the-Wire (BITW) security gateways that provide security for all of the building automation components. With security gateways installed, when the BMS on the 7th floor wants to issue a command to the BACnet router on the 32nd floor, for example, the security gateways on the 7th and 32nd floors will authenticate each other using cryptographic methods, then set up a secure tunnel to encrypt and deliver the message from the BMS to the router. In this way, an attacker who gains access to the automation network cannot read or modify messages sent between critical automation components. What's more, the automation components will not act on messages sent by an attacker (because the security gateways will block such messages).

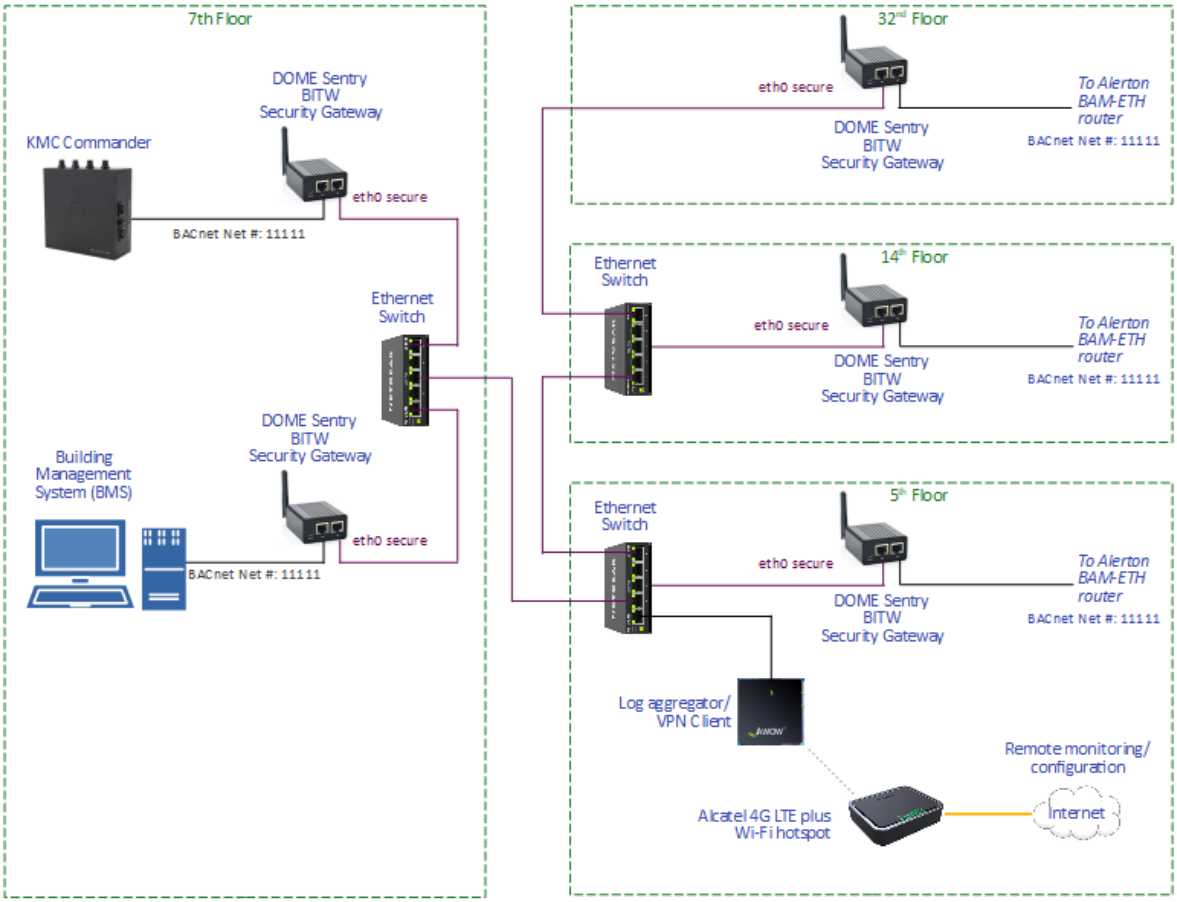

Fig. 2. Building automation network with security

Fig. 3. contains actual traffic captured on April 14th to show how the DOME Sentry secures critical messages. This traffic represents a typical transaction between a building management system and a building automation component.

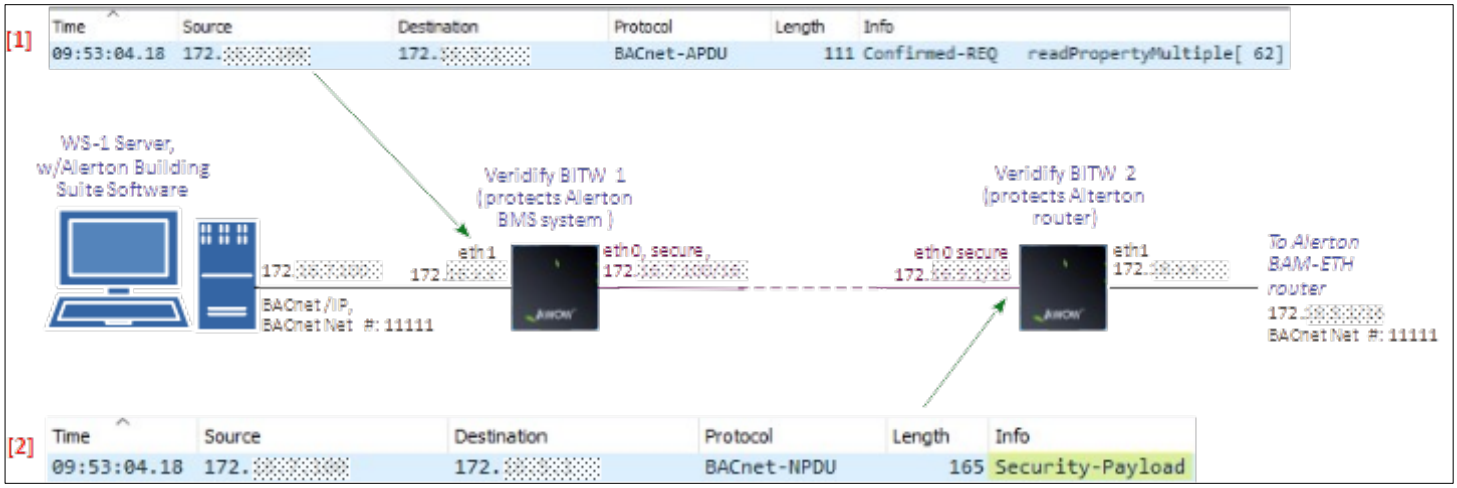

Fig. 3. Building automation traffic secured by DOME Sentry Gateways

In step [1], the BMS sends a message to a device on the 5th floor asking for its current readings via the standard BACnet command "readPropertyMultiple". The message is processed by DOME Sentry 1 and encrypted resulting in a "Security Payload" packet. In step [2], that message is sent to DOME Sentry 2 located on the 5th floor. Because the message is encrypted, an eavesdropper who taps into the building's network wiring or who otherwise obtains access to the network traffic is unable to decipher the message.

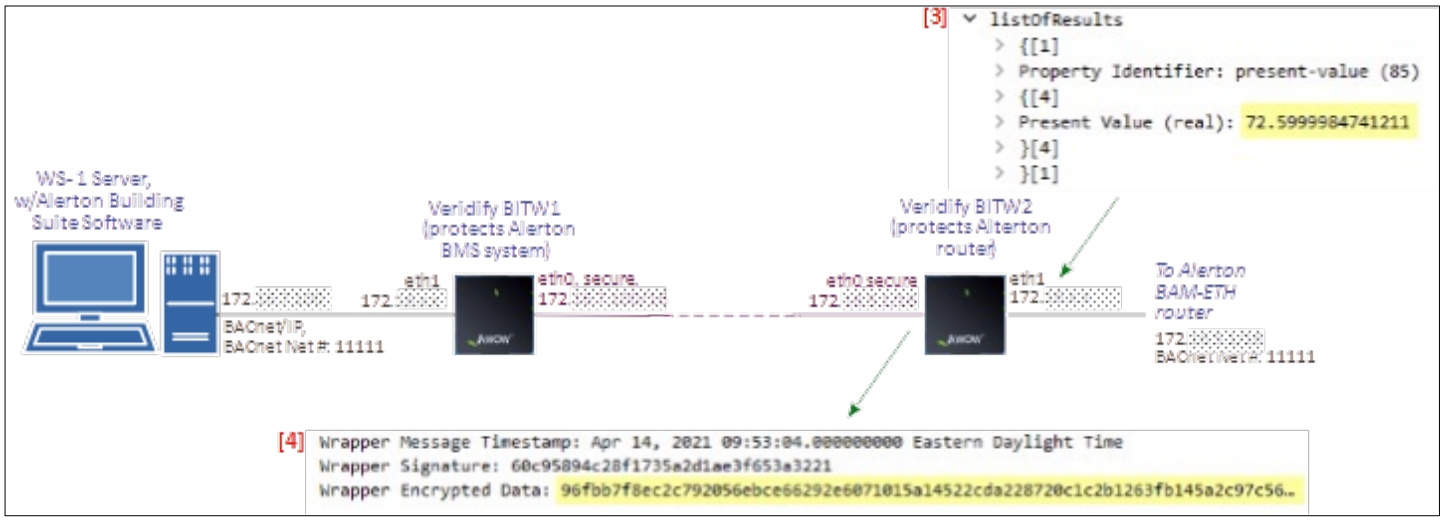

Fig. 4. Building automation traffic secured by DOME Sentry Gateways continued

In step [3], the queried device responds back via the Alerton ETH router. Note that one of the values is a temperature reading: 72.599 degrees. In step [4], that message is encrypted by DOME Sentry 2 located just a few inches away and transmitted to the DOME Sentry on the seventh floor. If an attacker gained access to that message without the security provided by the DOME Sentry, the attacker could change the reading to suit their purpose. For example, the attacker could force a setpoint temperature of an IT server room to be 120 degrees while spoofing the BMS into thinking the temperature was only 65 degrees. But with security, an attacker would have no idea what the message was for or what it said.

In addition to the DOME Sentry Gateways, Veridify and KMC have installed a KMC Commander BMS system as a more secure and modern alternative to the legacy BMS system previously in use. Lastly, we have installed a monitoring capability that provides a security dashboard for the building superintendent. Because all of the building automation traffic must pass through the DOME Sentry Gateways, those devices are in a unique position to detect break-in attempts and other anomalies and to report on the overall security health of the building. Fig. 5. shows a screenshot of the security dashboard configured for this building.

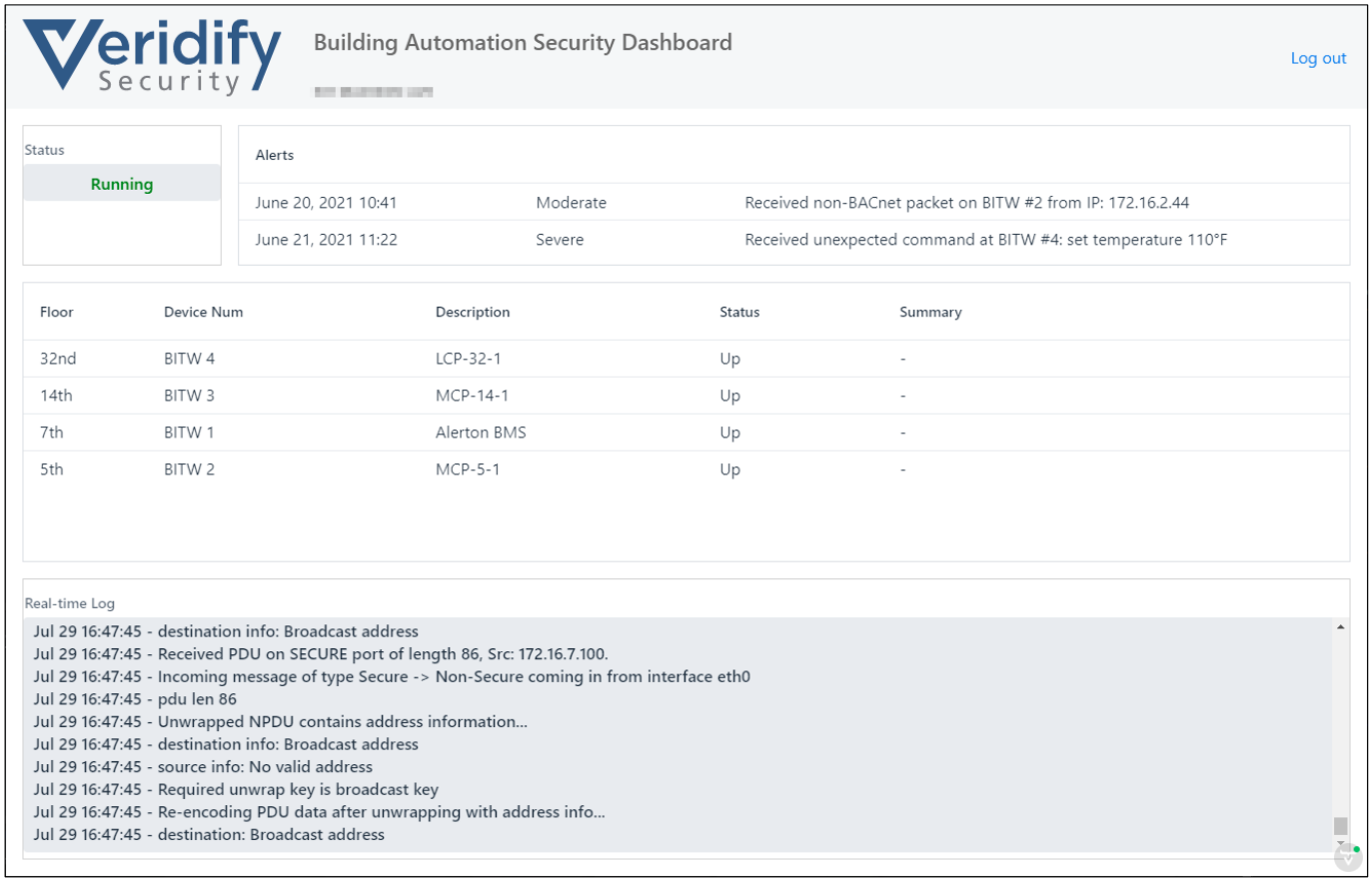

Fig. 5. Security Dashboard

DOME Sentry Gateway

The DOME Sentry prototypes being installed are based on an Intel® MAX® 10 development kit. Veridify has worked with an Intel partner to package the board together with a power converter (see Fig. 6). The power converter, shown on the left-hand side of the enclosure, is required to convert the 24 VAC that building automation components use to the +12VDC required by the MAX 10 board. The MAX 10 FPGA is ideal for this application since it offers the flexibility to handle communications protocols other than those based on Ethernet. For example, with just three pins, the MAX 10 can interface with a myriad of building components that communicate over the EIA-485 serial interface. More importantly, the MAX 10's on-chip flash memory can securely store secret cryptographic keys in a way that prevents access from outside the chip.

Veridify is working with building component OEMs to produce a custom printed circuit board for a smaller, more cost-effective DOME Sentry solution.

Fig. 6. DOME Sentry prototype based on MAX 10 (shown with cover removed)