tenable OT Security

USE CASE

SECURING YOUR BUILDING MANAGEMENT SYSTEMS

Background

Buildings are getting increasingly smart. From access control to fire safety, HVAC, lighting and humidity control, everything can be centrally managed and optimized to best fit the needs of each specific building and employee. The systems which make this possible are called BMS - Building Management Systems. BMS reduces building energy and maintenance costs. It also reduces the environmental footprint and improves the security and safety of the building occupants and property stored in it. Today's BMS have undergone significant and complex changes. Only a decade ago, BMS controlled HVAC and possibly a physical security system. Today, however, BMS control virtually every aspect of a smart building. Given smart technology delivers significant efficiencies and cost savings, adoption rates are on the rise.

In fact, risks are expected to geometrically increase as more buildings go "smart", more infrastructures converge, and IoT becomes the defacto standard in BMS. According to Data Bridge Market Research, the Global Building Management System Market accounted to USD 54.0 billion[1] in 2016 growing at a CAGR of 11.0% during the forecast period of 2019 to 2026. While BMS can yield huge benefits when it comes to streamlining processes and cutting down costs, it can be equally detrimental if security is not considered as part of its deployment and management.

Top Trends

- Increase of automated control systems to manage mechanical equipment (e.g. electrical, ventilation, lighting, power, fire, security)
- Emergence of legislation and initiatives to drive the development and adoption of BMS technologies
- Rapid adoption of IT/OT convergence
- Expanded connectivity of controlled systems that are accessible from outside

Key Challenges

- Secure design has not evolved into BMS
- Standard and publicly available protocols can be used to issue destructive commands
- Managed buildings often serve large crowds and unvetted visitors, creating risk for malicious physical access and tampering
- BMS systems require connecting controllers and IOs in many different locations so air gapping becomes nearly impossible

[1] Data Bridge Market Research, April 24, 2019

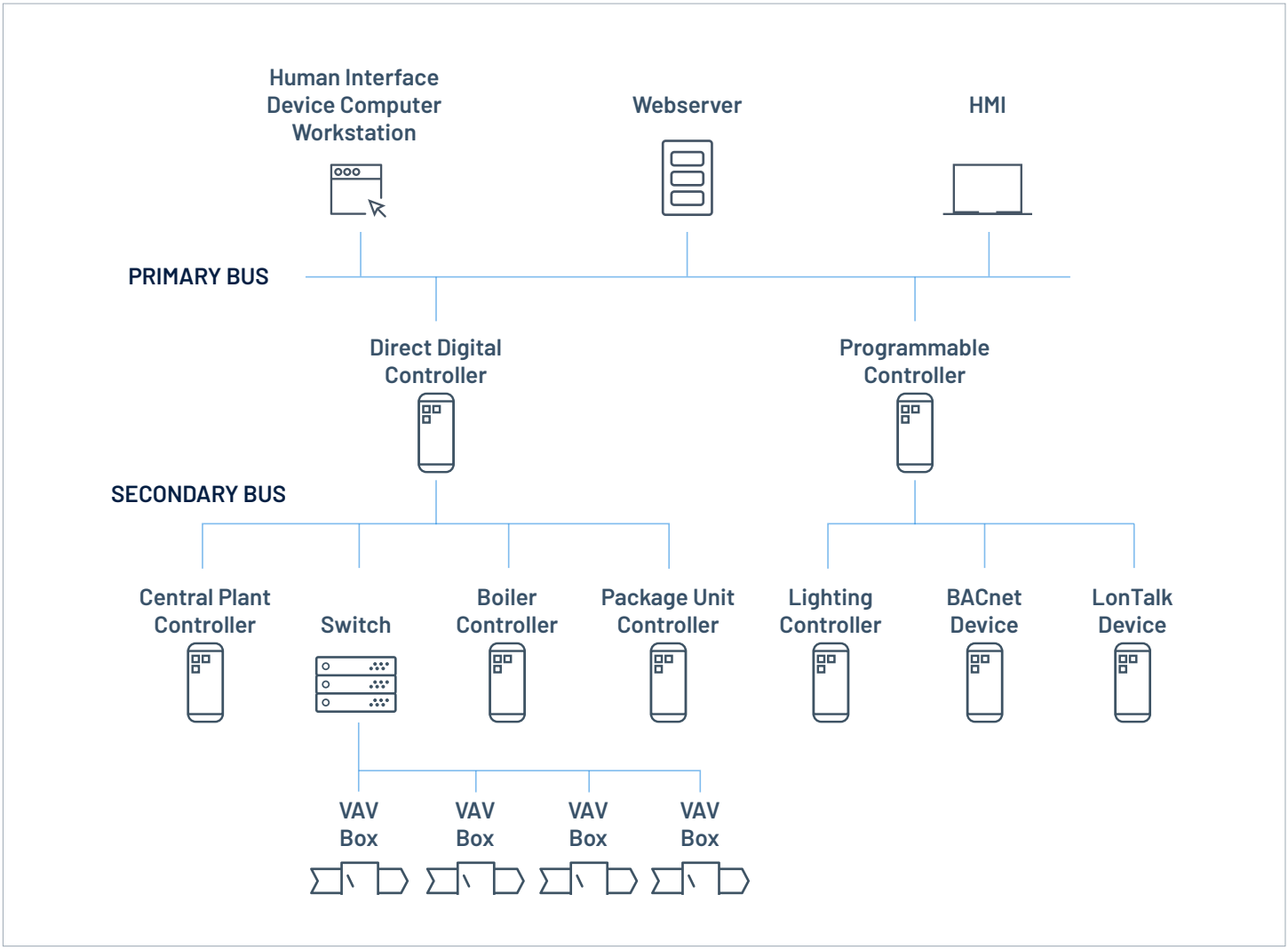
Anatomy of a Cyber Attack on BMS

- Initial physical or virtual infiltration to the BMS network
- Beachhead created in one of the assets in the network
- Reconnaissance activity to map out the targets and vulnerable devices or systems
- Propagation of other assets to reach the areas of interest
- Finalization of the "last mile" of the attack which disrupts building systems

Recent Events[2]

- **December 2018** - the FBI warned that unpatched devices on BMS networks were exposed to hackers exploiting vulnerabilities in FOX protocol which is common in BMS.
- **2014** - a hacker broke into the building control system of a five-star hotel in Shenzhen, China, to manipulate room control systems and steal customer data.
- **2013** - Retailer Target was breached resulting in millions of stolen credit card credentials. The breach was accomplished by using login credentials from a BMS HVAC system contractor.

Standard BMS Deployment



[2] Search Security Tech Target

Common Vulnerabilities in BMS

- Like other industrial verticals, BMS protocols were not designed with security in mind and are more easily exploited. For example, the FOX protocol used by some BMS systems has known vulnerabilities; a Shodan query identified 20,000 components directly connected to the internet via port 1911.
- Because many systems are older, they do not have proper documentation on how to close open vulnerabilities and may be completely unpatched with no new patches being issued. In a world where BMS is no longer air-gapped, these systems may be particularly vulnerable.
- Buildings are typically open to not only employees, but to a large heterogeneous audience. Poorly controlled physical security once in the building could result in unauthorized individuals gaining access to systems that run the building.
- With the widespread adoption of IoT and IT/OT convergence, the security that has been associated with air-gapped systems is dissolving resulting in everything being online and fully accessible.

Commonly Used Protocols

- **DeviceNet**
- **Niagra FOX**
- **XML**
- **BACnet**
- **LonWorks**
- **Modbus**
- **C-Bus**

Tenable OT Security has patented[3] active querying technologies and is also the first to specifically build **active querying engines for BMS**. The technology employs active querying for both standard and proprietary protocols to **achieve maximum coverage** of all devices in the distributed OT network.

Physical Access

Unlike traditional IT networks, buildings accommodate a wide, heterogeneous audience. Some of these individuals may be authorized employees. Many, however, may be visitors to the location (including suppliers, customers, maintenance workers, etc.) Most buildings have physical perimeter security set-up but once making it past the perimeter, these individuals may gain easy access to restricted areas of the building — including where BMS systems are housed. To counter the physical or on-site threat, a BMS security solution must periodically query individual devices at all locations to identify if any changes have been performed via physical connection to the device. It is also important to query servers, workstations, networking equipment, gateways, and any other devices that are critical to the regular network operations.

Smart and Secure Buildings

BMS networks tend to have a heterogeneous infrastructure. A multi-vendor scenario is generally the norm with different systems controlling everything from the elevator banks to the solar array on the roof. Many different devices can control one or several buildings on a more distributed campus using the same protocol. A solution should be able to utilize several discovery methods to create an accurate and realtime asset inventory. This enables you to secure the entire multi-vendor set of products that comprise BMS. What's more, you need to be able to account for dormant devices that are not communicating regularly over the network. Even if assets are not communicating over the network, there is the possibility that they will respond to a command. Deep knowledge, including visibility to all types of devices, patch levels, firmware versions and backplane information leveraging are essential. Tenable OT Security combines passive technology with its patented active device querying technology to account for not only network activity but also specific details on the devices that are part of the network.

[3]US Patent 10261489 - April 2019

About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

Catch Vulnerabilities Before They Are Exploited

BMS environments tend to contain a mix of legacy devices that may control older technologies, such as fire suppression and physical security. This occurs alongside devices from newer technologies such as living roofs, adaptive window tinting and more. With a multi-vendor, multi-generational environment, all the various patch levels across each device type are difficult to maintain. In addition, an up-to-date patch management program to assure protection from newly discovered vulnerabilities is equally cumbersome. If this were performed manually, it would not only consume a significant amount of time but would also be vulnerable to human error.

To achieve proper security, you need deep awareness of the state and characteristics of every device. You also need accurate matching between the specific condition of the devices and the available knowledge base on vulnerabilities to eliminate false positives. Because of the constantly changing threat conditions, this information should be updated regularly and kept in sync with newly discovered vulnerabilities. Tenable OT Security enables you to extract detail on devices (e.g. model, firmware, patch levels, installed software, serial number). This delivers the patch management required to keep all devices up-to-date.

Summary

Industrial cyber security is essential to eliminate many of the core risks associated with the new reality that is present in BMS environments. To mitigate that risk, it is essential to gain full visibility into all the operational assets that control the myriad of BMS systems inhabiting the building or campus. That includes HVAC, access control, fire suppression, lighting, physical security, elevators and other devices.

Tenable OT Security uses both passive detection as well as patented active query technology to detect any threat to your network. In addition, Tenable has developed a comprehensive policies mechanism that allows network management to create rules adapted to the routine of each individual network. Tenable OT Security uses both types of data acquisition methods. In addition to the policies mechanism, it leverages flexible deployment options to empower security teams to keep organizations running at peak efficiency and without unacceptable risk.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact