How Insecure Building Management Systems Are Putting Organizations At Risk

ISASecure Webinar

November 6th, 2019
Webinar Panel

Gjoko Krstic
Senior ICS Security Consultant
@ Applied Risk

Scott Thomas
Senior ICS Security Consultant
@ Applied Risk
About Applied Risk

Applied Risk is driven to secure critical infrastructures and their underlying Operational Technology (OT) powering our digital society.

Based in The Netherlands since 2012, Applied Risk services an extensive range of industries globally, delivering solutions for asset owners, suppliers and system integrators throughout the entire lifecycle of their assets. This is aligned with internationally recognised best practices and standards.
BMS, IEC 62443 & ISASecure

- IEC 62443 is relevant for securing building automation components, management and governance
- IEC 62443 standards are based on stakeholder viewpoints and the system lifecycle
- IEC 62443 standards are useful in securing the supply chain for off-the-shelf automation technology used in BMS
- Complies with many best practices applicable in traditional Operational Technology environments
- Relevant standards for BMS automation products include IEC 62443-4-1 Product development requirements and IEC 62443-4-2 Technical security requirements
What is a BMS?

- Building Management Systems control a facility’s technical systems and services.

- They can be:
  - Standalone
  - Connected to corporate Intranet
  - Internet-connected

- As an example - they can be found in the following locations:
An example of BMS services

- Security cameras
- Access control systems
- Fire alarms and suppression
- Heating and ventilation control systems
- Power/Lighting Control Systems
- Elevator Controls
What are the challenges?

- Individual components can be provided by diverse suppliers that makes the BMS as a whole more challenging to setup, maintain and secure.
- Increased attack surface (IIoT)
- Accountability, ownership, often poorly defined
- BMS are not traditionally viewed as attack vectors
- BMS insecurity may allow sidestep into IT/OT environments
- Security not a priority during development
How can this impact my business?

A malicious actor could:

▪ Gain unauthorized access to restricted areas (Access Control manipulation)
▪ Disable fire alarms, manipulate lighting, manipulate cooling and heating system
▪ Access confidential information about people, processes, procedures
▪ Modify gas sensor readings to cause physical damage
▪ Intercept CCTV surveillance streams
Common findings – what is exposed?

There is a significant number of BMS components directly accessible from the Internet.

Different BMS components share similar built-in vulnerabilities.

Discovered vulnerabilities suggest that the suppliers, system integrators and end users make similar oversights.
Who is responsible for BMS Security?

**BMS suppliers** often do not adhere to security by design principles. They provide functional solutions, which unfortunately contain weaknesses such as hardcoded and default credentials, and backdoors.

**BMS system integrators** often use the devices out of the box, that is, they do not change the default settings. Security should be taken into account when designing the BMS solution.

**End users of BMS** solutions are responsible for the safety and security of the facility they are managing. Contracts with BMS system integrators typically do not address security. Once integrated, the BMS is kept as-is without changing the provided settings.
Case Study: Major Airport

Considerations:

- Access gates
  - Block travelers for boarding
- Alarm systems
  - Evacuation system
  - Fire and safety
  - Public announcement system
- Elevator
  - Disrupt workflows and convenience
Threat Scenarios

Case Study: Hospital

Considerations:

- Lighting
  - Turn off the lights while surgery is ongoing
- Power management system
  - Disrupt power / life-support off-line
  - UPS (uninterruptable power supply)
- Ventilation
  - Hazardous waste (specific rooms have to have pressurized to prevent spread of contagions)
Threat Scenarios

Case Study: Data Centre

Considerations:

- Disrupt air conditioning
  - Overheat and damage systems
  - Potential loss of client and process data
- Access to CCTV streams and controls
  - Gather sensitive information
  - Disable surveillance
- Access control
  - Unlock restricted area (server rack door)
Supplier/Vendor Recommendations

- Remove “development consoles” (backdoors) from deployed BMS components.
- Address application security controls of your product.
- Select secure protocols and interfaces to protect data in transit and at rest.
- Enforce strong security policies to address hardcoded, default credentials, as well as password complexity.
- Force changing all default passwords upon installation of new software, particularly for administrator accounts and control system devices.
- Develop and provide security baseline for your products.
- To improve the maturity level of the product, consider implementing SSDLC - Secure Software Development Life Cycle
System Integrator Recommendations

- Adopt suppliers' recommended security baselines as necessary.
- Educate engineers about security best practices and raise the awareness level about BMS security issues.
- Deploy BMS networks and components behind firewalls and segregate them from the business network.
- Embed security assessment as part of factory acceptance tests (FAT) and site acceptance test (SAT).
- Use secure methods for remote access, e.g., VPNs, two-factor authentication (2FA), SSL.
- Use strong and expiring passwords.
- Change all default passwords upon installation of new software, particularly for administrator accounts and control system devices, even when this is not requested.
- Implement logging and monitoring solutions, which can detect and prevent malicious activities in BMS networks.
- Provide the end user with detailed documentation about the BMS solution.
- Supply backup configurations for all BMS components, including network devices, controllers, operating systems.
End user recommendations

- Educate staff about BMS security as part of the ongoing IT/OT security awareness campaigns.
- Ensure that suppliers and system integrators develop and build the BMS in line with the project security requirements.
- Perform regular security assessments
- Address roles and responsibilities (IT, OT or Corporate security) in relation to BMS.
- Enforce strong security policies regarding devices connecting to BMS.
- Always regularly update your software.
- Isolate your BMS from any untrusted networks.
- Minimize network exposure for all control system devices and/or systems
- Use only strong passwords.
- Change all default passwords upon installation of new software, particularly for administrator accounts and control system devices.
- Do not allow for shared usernames and passwords.
- Check for unusual system activity within your network
- Have a security incident response plan
I Own Your Building (Management System)

- Over 100 zero-day vulnerabilities discovered in commonly used building automation and access control devices during security research
- Includes in-depth technical discussions and recommendations for securing your building management systems
- Technical whitepaper available next week for download - free from www.applied-risk.com
Q&A Session