Enhancing Cyber Resilience in Smart Buildings

Akın AYTEKİN
Information Security Engineering
Gazi University
Ankara, Türkiye
ORCID: 0000-0002-0783-7597

Prof.Dr.Aysun COŞKUN
Department of Computer Engineering
Gazi University
Ankara, Türkiye
ORCID: 0000-0002-8541-9497

Prof.Dr.Mahir DURSUN[1,2],
1[2]Department of Electrical and Electronics Engineering, Faculty of Technology, Gazi University, Ankara 06560, Türkiye.

[2]Azerbaijan University of Architecture and Construction, Baku AZ1073, Azerbaijan;
ORCID: 0000-0003-0649-2627

Abstract— Building Automation Systems (BASs) are essential components of smart buildings, functioning as the core intelligence that enables efficient and intelligent operations. To support capabilities such as remote monitoring, cloud-based analytics, and integration with smart grids, BASs increasingly rely on connectivity—both within the building and with external networks like the Internet and cloud platforms. The shift toward open communication protocols has made remote access to BASs more common, improving convenience and operational efficiency.

However, this rise in connectivity also increases exposure to cybersecurity risks. Many BASs were originally designed as closed, isolated systems with minimal attention to cyber threats. As a result, these systems are now vulnerable to various attacks that could disrupt building operations, cause occupant discomfort, increase energy waste, or lead to equipment failure. The growing reliance on interconnected digital infrastructure in buildings makes it critical to address these security challenges.

To ensure safe and resilient building environments, it is necessary to enhance cyber-physical security frameworks for BASs and implement effective strategies to detect, prevent, and respond to cyber threats.

Keywords— Smart Buildings, Building Automation Systems (BASs), Cybersecurity, Resilience.

I. INTRODUCTION

Smart buildings represent a significant advancement in the way buildings are managed and operated, bringing improvements in energy efficiency, comfort, and sustainability. These buildings use internet-connected sensors to link systems like HVAC (heating, ventilation, and air conditioning), lighting, security, and access control. By working together intelligently, these integrated systems help reduce energy use, streamline daily operations, and improve the overall experience for those inside the building. However, this increased connectivity also introduces new cybersecurity risks that must be addressed.

As buildings adopt greater levels of connectivity and automation, their exposure to cyber risks also increases[1]. The convergence of operational technology (OT) and information technology (IT) in smart buildings creates an expanded attack surface that malicious actors can exploit. This expanded vulnerability can result in significant issues, such as system failures, data leaks, unauthorized access, and threats to the physical safety of occupants[2-3].

This paper highlights the cybersecurity challenges facing smart buildings, with a particular focus on the communication protocols used between various systems and devices. It examines the vulnerabilities inherent in these protocols and presents a cyber maturity–based approach to help building owners, managers, and security professionals strengthen the overall security posture of smart building environments.

II. SMART BUILDING SYSTEMS AND THEIR BENEFITS

A smart building leverages technology to automate and optimize various building functions through a network of connected devices and systems[4-5]. These systems collect and analyze data to make intelligent decisions about building operations, often without human intervention.

Key components of smart buildings

1. Building Management Systems (BMS): Centralized platforms that monitor and control various building systems, including HVAC, lighting, and security.

2. Internet of Things (IoT) Devices: Sensors, actuators, and other connected devices that collect data and execute commands throughout the building.

3. Automation Systems: Systems that automatically adjust building parameters based on predefined rules or AI algorithms.

4. Integration Platforms: Software that enables different building systems to communicate and work together seamlessly.

5. Data Analytics: Tools that process and analyze data from various sources to identify patterns, optimize operations, and predict maintenance needs[6-7-8].

Benefits of Smart Building Implementation

Smart buildings offer numerous benefits to building owners, operators, and occupants:

1. Energy Efficiency: Smart buildings can reduce energy consumption by 15-30% through automated control of HVAC, lighting, and other systems based on occupancy, weather conditions, and time of day[9].

2. Cost Savings: Reduced energy consumption and more efficient maintenance lead to significant operational cost savings.

3. Enhanced Occupant Comfort: Personalized environmental controls and automated adjustments improve comfort and productivity.

4. Improved Maintenance: Predictive maintenance capabilities identify potential issues before they cause failures, reducing downtime and repair costs.

5. Sustainability: Optimized resource usage contributes to reduced environmental impact and helps meet sustainability goals.

6. Space Utilization: Data on space usage patterns helps optimize layout and allocation of building resources[10].

7. Safety and Security: Integrated security systems provide enhanced protection through coordinated access control, surveillance, and emergency response[11].

III. CYBER THREAT LANDSCAPE FOR SMART BUILDINGS

Despite their many benefits, smart buildings face a range of cybersecurity threats that can compromise their operation, safety, and the privacy of their occupants.

Types of Cyber Actors Targeting Smart Buildings

1. Nation-State Actors: Sophisticated threat actors with significant resources who may target critical infrastructure, including smart buildings, for espionage, sabotage, or as part of broader geopolitical conflicts.

2. Cybercriminals: Financially motivated attackers who may target smart buildings for ransomware attacks, data theft, or to gain access to corporate networks through building systems.

3. Hacktivists: Ideologically motivated individuals or groups who may target buildings to make political statements or disrupt operations of organizations they oppose.

4. Insiders: Current or former employees with legitimate access who may misuse their privileges intentionally or unintentionally.

5. Opportunistic Attackers: Less sophisticated actors who exploit easily accessible vulnerabilities in poorly secured systems[1,12].

Common Attack Vectors

1. Unsecured Network Connections: Many building automation systems connect to the internet without proper security controls, creating entry points for attackers.

2. Protocol Vulnerabilities: Communication protocols used in building automation often lack robust security features, making them susceptible to various attacks.

3. Default Credentials: Many devices and systems retain factory-default passwords, providing easy access to attackers[14].

4. Outdated Software: Building systems often run on legacy software that may not receive regular security updates.

5. Physical Access: Unsecured access to building automation equipment can allow attackers to tamper with devices directly.

6. Social Engineering: Attackers may manipulate building staff to gain access to systems or information.

7. Third-Party Connections: Vendors and service providers with remote access to building systems can introduce security risks if their own security practices are inadequate[13].

Potential Impacts of Cyber Attacks

1. Operational Disruption: Attacks can disable critical building functions, causing discomfort, business interruption, or even building evacuation.

2. Safety Risks: Compromised building systems could create unsafe conditions, such as disabling fire detection systems or manipulating access controls.

3. Privacy Violations: Attackers could access occupancy data, surveillance footage, or other sensitive information.

4. Financial Losses: Attacks can result in direct costs for remediation, as well as indirect costs from business disruption and reputational damage.

5. Lateral Movement: Building systems can serve as entry points to corporate networks, enabling attackers to access more sensitive systems and data[1,15].

IV. SMART BUILDING PROTOCOLS AND THEIR VULNERABILITIES

Smart buildings rely on various communication protocols to enable different systems and devices to interact. These protocols often prioritize functionality and interoperability over security, creating vulnerabilities that attackers can exploit[16-18]. The overview of the protocols used in Smart Buildings is shown in Table 1.

Protocol	Smart Building Protocols Summary Table		
	Description	***Key Vulnerabilities***	***Mitigations***
BACnet	Building automation protocol for interoperability between systems	• No authentication • Lack of encryption • Broadcasting vulnerability • Token-passing risks	• Implement encryption • Network segmentation • Use BACnet/SC • Strong authentication
Modbus	Industrial control protocol used in building systems	• No authentication • No encryption • Default configurations • Lack of authorization	• Regular security assessments • Data encryption • Access controls • Firmware updates
KNX	Open standard for building control, popular in Europe	• Account lockout issues • Unencrypted communication • Physical access risks	• Follow KNX Secure guidelines • Set BCU Keys • Network isolation • Secure physical access
MQTT	Lightweight messaging protocol for IoT devices	• Default unencrypted • Poor authentication • Misconfiguration risks	• Use TLS/SSL • Implement authentication • Proper authorization policies
Zigbee	Wireless protocol for IoT device connectivity	• Open trust model • Key management issues • Default link keys	• Proper key management • Secure trust center • Avoid default keys
Z-Wave	Wireless protocol for home or building automation	• Radio jamming • Rogue node inclusion • Replay attacks	• Monitor heartbeat signals • OOB authentication • Use S2 Security
OPC UA	Machine-to-machine	• Trust list weaknesses	• Proper trust list implementation

Protocol	Smart Building Protocols Summary Table		
	Description	*Key Vulnerabilities*	*Mitigations*
	protocol for industrial automation	• HTTP(S) server risks • Implementation flaws	• Use Sign or SignAndEncrypt mode • Certificate management

Table 1. Summary of Common Smart Building Protocols, Vulnerabilities, and Mitigation Strategies

V. CYBER MATURITY FRAMEWORK FOR SMART BUILDINGS

Enhancing the cybersecurity of smart buildings requires a structured approach that addresses the unique challenges of these environments. A cyber maturity framework provides a roadmap for organizations to assess their current security posture and identify areas for improvement.

Understanding Cyber Maturity

Cyber maturity refers to an organization's level of cybersecurity capability to protect against cyber attacks and effectiveness of an organization's readiness[19]. It encompasses not only technical controls but also governance, processes, and people aspects of security. A mature cybersecurity program is characterized by:

1. Proactive Approach: Anticipating and addressing security risks before they materialize
2. Comprehensive Coverage: Addressing all aspects of security across the organization
3. Continuous Improvement: Regularly assessing and enhancing security capabilities
4. Integration: Security embedded into all aspects of operations, not treated as an afterthought
5. Resilience: Ability to detect, respond to, and recover from security incidents effectively

Maturity Levels for Smart Building Cybersecurity

The following maturity levels provide a framework for assessing and improving the cybersecurity posture of smart buildings:

Level 1: Initial/Ad-hoc

- Basic security measures implemented inconsistently
- Reactive approach to security incidents
- Limited awareness of vulnerabilities
- Minimal documentation and processes

Level 2: Managed

- Security measures implemented with some consistency
- Documented processes for common security activities
- Basic risk assessment performed
- Some security awareness among staff

Level 3: Defined

- Standardized security processes implemented consistently
- Comprehensive risk assessment and management
- Regular security training and awareness programs
- Documented security policies and procedures

Level 4: Quantitatively Managed

- Security metrics collected and analyzed
- Data-driven security decisions
- Regular testing and validation of security controls
- Continuous monitoring and improvement

Level 5: Optimizing

- Proactive security posture (preventive defense mindset)
- Automated security processes
- Advanced threat intelligence and analytics
- Continuous adaptation to emerging threats

VI. CONCLUSION

As smart buildings continue to evolve and proliferate, the need for robust cybersecurity measures becomes increasingly critical. The interconnected nature of these systems, combined with the use of protocols that often prioritize functionality over security, creates significant vulnerabilities that malicious actors can exploit.

By understanding the specific vulnerabilities of common smart building protocols and implementing a comprehensive cyber maturity framework, building owners and operators can significantly enhance their security posture. The cyber maturity overview provided in this article guides a structured approach to addressing these challenges, enabling organizations to systematically improve their defenses against cyber threats.

Ultimately, enhancing the cyber maturity of smart buildings requires a holistic approach that addresses not only technical controls but also governance, processes, and people aspects of security. By adopting such an approach, organizations can enjoy the many benefits of smart building technology while minimizing the associated cybersecurity risks.

Future research should explore the development of standardized security protocols tailored specifically for smart building environments, balancing functionality with robust cybersecurity. Additionally, investigating AI-driven threat detection and automated response mechanisms could further enhance proactive defense capabilities. Long-term studies on the integration of cyber maturity frameworks into smart building lifecycle management would also provide valuable insights for industry-wide adoption.

REFERENCES

[1] Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K. S., & O'Neill, Z. (2023). "A critical review of cyber-physical security for building automation systems" Annual Reviews in Control, 55, 237-254. https://doi.org/10.1016/j.arcontrol.2023.02.004

[2] Higgins, K. J. (2021). Lights Out: cyberattacks shut down building automation systems. Retrieved June 3, 2025 from https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems.

[3] McMullen, D. A., Sanchez, M. H., & Reilly-Allen, M. O. (2016). "Target security: A case study of how hackers hit the jackpot at the

expense of Institutional Review of Business and Finance Studies, 7(2), 41–50.

[4] Goldstein, P. (2024). The Benefits of Smart Buildings for State and Local Government Campuses. Retrieved June 4, 2025 from https://statetechmagazine.com/article/2024/06/smart-buildings-leverage-automation-perfcon

[5] Yeşilata, Y. (2024). Smart Building Platforms 101: Everything You Need to Know. Retrieved June 4, 2025 from https://sensgreen.com/smart-building-platforms-101-everything-you-need-to-know/

[6] Aliero, M. S., Asif, M., Ghani, I., Pasha, M. F., & Jeong, S. R. (2022). Systematic Review Analysis on Smart Building: Challenges and Opportunities. Sustainability, 14(5), 3009. https://doi.org/10.3390/su14053009.

[7] Taboada-Orozco, A., Yetongnon, K., & Nicolle, C. (2024). Smart Buildings: A Comprehensive Systematic Literature Review on Data-Driven Building Management Systems. Sensors, 24(13), 4405. https://doi.org/10.3390/s24134405.

[8] Ambroziak, A., & Borkowski, P. (2025). "Temperature and humidity model for predictive control of smart buildings." *Journal of Building Engineering*, *100*, 111668. https://doi.org/https://doi.org/10.1016/j.jobe.2024.111668

[9] Uzair, M., Yacoub Al-Kafrawi S., Manaf Al-Janadi, K. and Abdulrahman Al-Bulushi, I. (2022) "A Low-Cost IoT Based Buildings Management System (BMS) Using Arduino Mega 2560 and Raspberry Pi 4 for Smart Monitoring and Automation" International Journal of Electrical and Computer Engineering Systems, Volume 13, Number 3, 219-236. https://doi.org/10.32985/ijeces.13.3.7

[10] Jing, T., & Zhao, Y. (2024). Optimizing energy consumption in smart buildings: A model for efficient energy management and renewable integration. Energy and Buildings, 323, 114754. https://doi.org/https://doi.org/10.1016/j.enbuild.2024.114754

[11] Graveto, V., Cruz, T., & Simões, P. (2022). Security of Building Automation and Control Systems: Survey and future research directions. *Computers & Security*, *112*, 102527. https://doi.org/https://doi.org/10.1016/j.cose.2021.102527

[12] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, 2019, pp. 28-33, doi: 10.1109/JEEIT.2019.8717449.

[13] Kaspersky. (2019). Smart buildings threat landscape: 37.8% targeted by malicious attacks in H1 2019. Retrieved September 7, 2022 from https://www.kaspersky.com/about/press-releases/2019_smart-buildings-threat-landscape.

[14] Holmberg, D. G., & Evans, D. (2003). "BACnet wide area network security threat assessment". US Department of Commerce, National Institute of Standards and Technology.

[15] Sridhar, S., & Manimaran, G. (2010). Data integrity attacks and their impacts on SCADA control system. In *IEEE PES general meeting* (pp. 1–6). IEEE, 1-6.

[16] M. K. McGowan. (2019) "Building automation systems: Addressing the cybersecurity threat," Retrieved June 4, 2025 from https://www.ashrae.org/technical-resources/ashrae-journal/featured-articles/building-automation-systems-addressing-the-cybersecurity-threat.

[17] txOne Networks. (2023). Ten Unpatched Vulnerabilities in Building Automation Products Identified by TXOne Networks. Retrieved June 5, 2025 from https://www.txone.com/blog/ten-unpatched-vulnerabilities-in-building-automation-products-identified-by-txone-networks.

[18] IOT Security Foundation. (2019). "Can You Trust Your Smart Building? Understanding the security issues and why they are important to you.". Retrieved June 5, 2025 from https://www.iotsecurityfoundation.org/wp-content/uploads/2019/06/IoTSF-Smart-Buildings-White-Paper-PDF-1.pdf.

[19] Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. Business & Information Systems Engineering, 1(3), 213-222. https://doi.org/10.1007/s12599-009-0044-5.