EN4720 - Security in Cyber-Physical Systems

Securing a Smart Building System - Milestone 1

Department of Electronic and Telecommunication Engineering
University of Moratuwa

Group: Cyberbullies

Name	Index Number
Amarasinghe Y.E.	200029B
Croos J.J.S.E.	200095V
Nimnaka K.W.H.	200426N
Vikkramanayaka A.G.P.S.	200683X

1 Introduction

Smart building systems are technologically advanced infrastructures that integrated with Internet of Things (IoT) devices, access control and data privacy mechanisms. This approach optimize security, energy efficiency, and overall operational efficiency. These buildings integrate various subsystems such as HVAC (Heating, Ventilation, and Air Conditioning), security cameras, access control mechanisms, smart lighting, and energy management systems.

While smart building systems offer unprecedented control and efficiency, they also introduce new cybersecurity risks due to their highly networked nature. Every connected device represents a potential attack surface, making them vulnerable to various security threats.

This report will focus on a commercially available smart building system, identifying its vulnerabilities and analyzing potential security threats. The vulnerabilities will be mapped to the Common Vulnerabilities and Exposures (CVE) database, and mitigation strategies will be proposed to enhance data privacy, authentication mechanisms, and cryptographic security within the system.

1.1 Honeywell as a commercially available smart building system 🔗

Honeywell International Inc. is a diversified multinational conglomerate that offers a wide range of products and services across various sectors, including aerospace, building technologies, performance materials, and safety solutions. Within the realm of Smart Building Systems, Honeywell has established itself as a leader by providing advanced solutions designed to enhance building efficiency, safety, and occupant comfort.

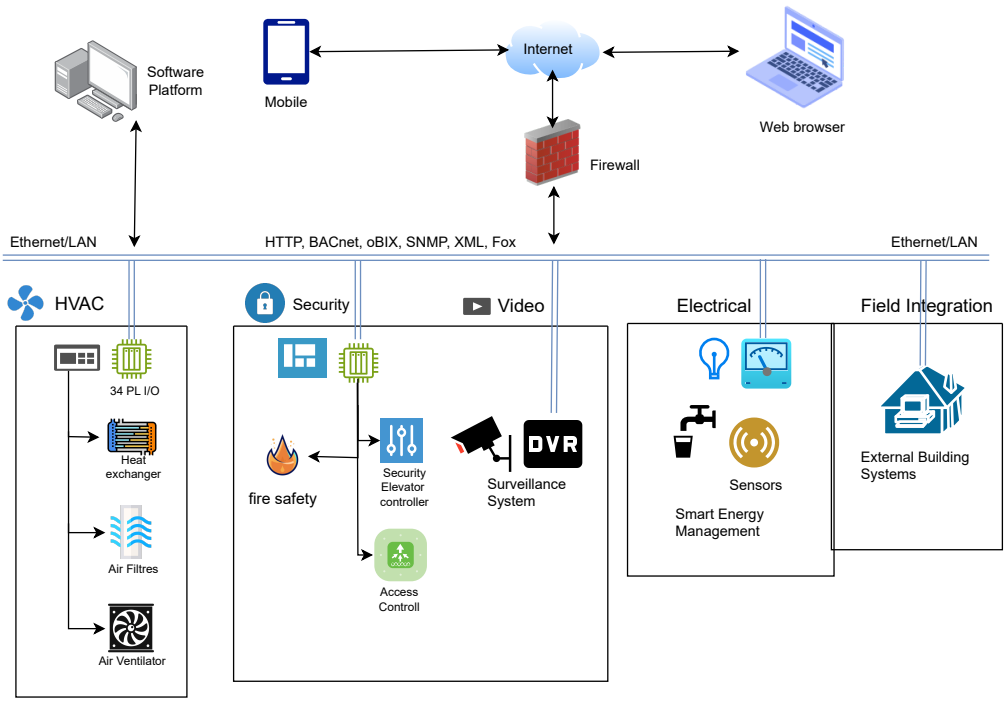

Figure 1: Architecture of the Honeywell smart building system.

Honeywell's Involvement in Smart Building Systems:

- **Building Management Systems (BMS):** Honeywell's BMS solutions integrate heating, ventilation, air conditioning (HVAC), lighting, and power control systems to optimize building performance. Utilizing open standards like BACnet and LonWorks, these systems ensure seamless interoperability with various building automation prosmart buidling systemducts, offering a flexible and future-proof platform.

- **Honeywell Forge for Buildings:** This comprehensive platform combines software, hardware, and services to deliver actionable insights for building operations. It aims to improve energy efficiency, enhance occupant experience, and streamline maintenance processes by leveraging data analytics and IoT technologies.
- **Advance Control for Buildings:** Launched in early 2024, this platform represents a significant advancement in building controls innovation. It features built-in cybersecurity measures, faster network speeds, and tools designed to make buildings smarter, safer, and more sustainable. The system automates processes and improves energy efficiency, addressing the growing demand for more connected and efficient building management solutions.
- **Trend Building Energy Management Systems (BEMS):** Trend, a brand under Honeywell Building Technologies, offers modular BEMS solutions that can adapt to changing usage patterns, user requirements, and new legislation. These systems provide visibility and control over energy use and building conditions, contributing to a frictionless occupant experience and powerful insights into building usage.
- **Niagara Framework:** Developed by Tridium, a Honeywell subsidiary, the Niagara Framework is a universal software infrastructure that allows integrators and contractors to build custom, web-enabled applications for accessing, automating, and controlling smart devices in real-time. This framework facilitates the integration of diverse building systems, promoting interoperability and centralized management.

2 Identified Vulnerabilities

- **Insecure Encryption Practices**
  Some Honeywell systems have been found to utilize weak encryption mechanisms, making them susceptible to data breaches. For instance, vulnerabilities in the Honeywell XL Web II controller allowed attackers to access sensitive information due to inadequate encryption protocols.

  Justification: Encryption is fundamental to protecting sensitive data, but weak encryption leaves systems vulnerable to attacks. Weak or outdated cryptographic implementations can allow attackers to intercept and decrypt confidential information. In Honeywell systems, older encryption mechanisms were found to be insufficient against modern brute-force and cryptanalysis techniques. The risk is especially high in IoT-driven systems where data integrity and confidentiality are critical.
- **Weak Key Management**
  Improper handling and storage of cryptographic keys can lead to unauthorized access. While specific instances in Honeywell systems are not detailed in the provided sources, weak key management remains a common concern in industrial control systems.

  Justification: Even if strong encryption is used, poor cryptographic key management can make a system highly vulnerable. Storing keys insecurely (e.g., in plaintext configuration files) or failing to implement key rotation allows attackers to compromise encryption protections. Many IoT devices lack secure key storage mechanisms, leading to unauthorized decryption and manipulation of data.
- **Weak Password Policies**
  Systems with default or easily guessable passwords are prime targets for attackers. The Honeywell XL Web II controller, for example, had vulnerabilities that could be exploited due to insufficient password protection mechanisms.

  Justification: Weak or default passwords significantly increase the likelihood of unauthorized access. Attackers often exploit weak credentials using brute-force attacks or credential stuffing.

Many Honeywell systems have historically relied on default or easily guessable passwords, which compromise system security. This makes enforcing strong password policies essential for protecting sensitive building control systems.

- **Improper Access Control Configurations**
  Flaws in access control can allow unauthorized users to manipulate system settings. The Honeywell MPA2 Access Panel had a cross-site scripting vulnerability (CVE-2023-1841) that could be exploited to bypass access controls.

  Justification: Poor access control mechanisms allow attackers to escalate privileges and tamper with building management systems. In some cases, improperly configured role-based access control (RBAC) enables lower-privileged users to execute administrative functions. The Honeywell MPA2 Access Panel vulnerability demonstrated how improper access controls can lead to system compromise, reinforcing the need for strict enforcement of least privilege access policies.

- **Remote Code Execution (RCE)**
  Certain Honeywell systems, such as the ProWatch 4.5, contained vulnerabilities that could allow standard users to execute arbitrary system code, potentially compromising the entire system.

  Justification: RCE vulnerabilities are among the most severe as they allow attackers to execute arbitrary commands on a target system, potentially gaining full control. In Honeywell ProWatch 4.5, an RCE vulnerability allowed attackers to compromise the system, which could lead to disabling security controls or deploying malware. Such vulnerabilities must be mitigated through secure coding practices, software updates, and stringent network segmentation.

3 Mitigation Strategies

- **Enhance Encryption Protocols:**
  Implement robust encryption standards, and ensure secure key management practices to protect data integrity.

  - **Adopt strong encryption standards** such as **AES-256** for data transmission and storage.
  - Implement **end-to-end encryption** to protect data as it moves between devices.
  - Use **Transport Layer Security (TLS 1.3)** to secure communication between components.
  - Ensure **secure cryptographic key management**, including:
    * Using **hardware security modules (HSMs)** for secure key storage.
    * Implementing **automatic key rotation** to prevent compromised keys from being misused.

- **Strengthen Password Policies:**
  Enforce complex password requirements, mandate regular password changes, and eliminate default credentials to reduce unauthorized access risks.

  - **Mandate complex passwords** with a mix of uppercase, lowercase, numbers, and special characters.
  - Implement **multi-factor authentication (MFA)** to add an extra layer of security.
  - Enforce **automatic password expiration** to require users to update passwords periodically.

  - Disable default credentials and enforce **unique passwords** for each device or system component.

- **Regular Software Updates:**
  Keep all systems and firmware up-to-date to address known vulnerabilities promptly. For instance, Honeywell released firmware updates to mitigate identified security issues.

  - Establish an **automated patch management system** to update Honeywell devices.
  - Monitor **CVE (Common Vulnerabilities and Exposures) databases** to stay informed about newly discovered threats.
  - Apply **firmware updates from Honeywell** as soon as they are released.
  - Use **virtual patching** as a temporary measure to protect unpatched vulnerabilities.
  - Enable **automatic rollback** mechanisms in case an update causes system instability.

- **Implement Comprehensive Access Controls:**
  Define and enforce strict access control policies, ensuring users have the minimum necessary privileges to perform their roles.

  - Implement **role-based access control (RBAC)** to ensure users only have access to functions required for their role.
  - Enforce the **principle of least privilege (PoLP)** to minimize unnecessary access.
  - Use **strong authentication mechanisms**, such as biometric verification or **hardware security tokens**.
  - Regularly audit **access logs** to identify and remove **inactive or unnecessary accounts**.
  - Deploy **network segmentation** to limit access between different subsystems, ensuring a compromised device cannot affect critical operations.

- **Deploying Network Security Measures:**
  Smart buildings are **highly networked**, making them vulnerable to cyberattacks like **man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, and unauthorized remote access**.

  - **Deploy firewalls and intrusion detection systems (IDS/IPS)** to monitor network traffic and detect anomalies.
  - Use **network segmentation** to isolate **IoT devices** from corporate networks.
  - Implement **VPN (Virtual Private Network) solutions** for secure remote access.
  - Enforce **network access control (NAC)** policies to verify the security posture of devices before allowing them to connect.
  - Conduct **regular network penetration testing** to identify and fix vulnerabilities.

4 Best Practices for Enhanced Security

To strengthen smart building security, the following best practices should be followed.

- **Zero Trust Architecture (ZTA):**
  The Zero Trust Architecture (ZTA) operates on the principle of *"Never trust, always verify."* Instead of automatically trusting devices or users inside the network, ZTA requires verification at every access request.

  How It Works:

  - Every device, user, and application must be authenticated and authorized before accessing resources.
  - Uses Multi-Factor Authentication (MFA) and strong identity verification methods.
  - Implements least privilege access to ensure users and devices get only the required access.
  - Continuously monitors network activity and dynamically adjusts permissions based on risk levels.

  Benefits:

  - Prevents unauthorized access.
  - Reduces the risk of internal threats.
  - Limits the impact of data breaches and lateral movement by attackers.

- **IoT Device Segmentation:**
  IoT (Internet of Things) devices in smart buildings, such as security cameras and HVAC controls, often have weak security mechanisms. IoT device segmentation ensures that IoT networks are isolated from the main corporate network.

  How It Works:

  - Uses Virtual LANs (VLANs) or firewalls to separate IoT traffic from critical business systems.
  - Implements network access control (NAC) to prevent unauthorized device connections.
  - Creates separate security policies for IoT devices, limiting their access.

  Benefits:

  - Prevents IoT-based attacks such as DDoS.
  - Enhances network performance.
  - Limits damage in case an IoT device is compromised.

- **Real-time Intrusion Detection:**
  Cyber threats evolve rapidly, making it crucial to detect attacks in real time before they cause significant damage. AI-based intrusion detection systems analyze network activity and detect abnormal behaviors.

  How It Works:

  - Uses machine learning algorithms to identify unusual patterns in network traffic.
  - Deploys Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor and block suspicious activities.
  - Analyzes historical data to detect zero-day attacks.

- Sends alerts to administrators if an attack is detected.

Benefits:

- Detects and blocks cyberattacks in real time.
- Reduces the risk of data breaches and ransomware attacks.
- Helps organizations respond to threats quickly.

- **Regular Security Audits:**
  Cybercriminals continuously find new ways to exploit vulnerabilities in smart buildings. Regular security audits help identify weaknesses and ensure systems remain resilient.

  How It Works:

  - Conducts penetration testing to simulate cyberattacks and uncover vulnerabilities.
  - Performs vulnerability scans on IoT devices, firewalls, and access control systems.
  - Evaluates software and firmware updates to ensure outdated versions are patched.
  - Reviews access control policies and logs for suspicious activity.

  Benefits:

  - Identifies security gaps before attackers exploit them.
  - Ensures compliance with security standards (e.g., ISO 27001, NIST).
  - Strengthens the overall security posture of the building.

- **User Awareness Training:**
  Even with advanced security measures, human error remains one of the biggest threats. User awareness training educates employees and building occupants on recognizing and avoiding cyber threats.

  How It Works:

  - Conducts phishing simulation tests to train employees on identifying scam emails.
  - Educates users on password best practices.
  - Provides training on social engineering attacks such as impersonation fraud.
  - Encourages secure device usage.

  Benefits:

  - Reduces the risk of social engineering attacks and phishing scams.
  - Empowers users to identify suspicious activity.
  - Creates a culture of cybersecurity awareness.

5 Common Vulnerabilities and Exposures (CVE)

5.1 Most Wanted List for Software Bugs!

Common Vulnerabilities and Exposures (CVE) is a system that provides a standardized method for identifying and naming publicly disclosed cybersecurity vulnerabilities and exposures. Each CVE entry is assigned a unique identifier, known as a CVE ID, which allows security professionals and organizations to efficiently share information and coordinate responses to security flaws.

5.2 Mapping to CVE Database

CVE ID	Description	Security Goal Breached (CIA Triad)	Real-Life Incident
CVE-2023-1841	A cross-site scripting (XSS) vulnerability in Honeywell MPA2 Access Panel, which could allow attackers to bypass access controls.	Confidentiality and Integrity	https://www.cve.org/CVERecord?id=CVE-2023-1841
CVE-2020-7479	Remote Code Execution vulnerability in Honeywell ProWatch 4.5, allowing attackers to execute arbitrary code remotely, compromising the system.	Availability and Integrity	https://www.cve.org/CVERecord?id=CVE-2020-7479
CVE-2019-12966	Weak password vulnerability in Honeywell WebAccess, which could allow attackers to exploit default or weak passwords.	Confidentiality	https://www.cve.org/CVERecord?id=CVE-2019-12966

Table 1: Vulnerabilities Identified in Honeywell Systems

6 Conclusion

Securing smart building systems is essential to prevent cyber threats that can compromise data, operations, and occupant safety. This report identified key vulnerabilities in Honeywell systems, including weak encryption, poor password policies, and improper access controls. To mitigate these risks, stronger encryption, stricter password policies, regular updates, and better access controls are necessary. Implementing best practices like Zero Trust Architecture, IoT segmentation, and intrusion detection further enhances security. Proactive measures and continuous improvements are crucial for ensuring smart buildings remain safe, efficient, and resilient against evolving cyber threats.

Appendix

- Best smart home systems in 2025: Reviews and buying advice.
- Honeywell | Building Automation
- CVE Database
- RedHat