DOMATIC

Why Consumer-Grade Smart Home Systems Fall Short for Buildings

3.10.25

San Mateo, California - In recent years, smart home technology has transformed modern living, offering convenience and control over our environments. With the ease of purchasing and installing such devices, it's easy to assume they can be added after a building is completed and managed by a property manager.

However, this mindset has serious drawbacks—like insufficient data security, lack of robustness, and limited support, to name a few. Long-lasting smart building systems should be designed with the developer's involvement from the early stages of the project. This allows smart systems to be integrated into the infrastructure, benefiting all stakeholders (owners, investors, property managers, and tenants) by enabling smooth operation and upkeep, ultimately extending the life of the building.

Aside from some high-end solutions, most consumer-grade smart home systems available online simply don't measure up.

The Empty Promise of Consumer Smart Home Devices

It's important to understand why consumer-grade devices are so attractive and where their hidden flaws lie. These devices often promise:

- **Quick setup on the resident network**: Configure the Wi-Fi credentials, and devices are connected to the home network for immediate use.

Reality: Each ecosystem varies, and many users face difficulty setting things up. A lot of devices only work on single-frequency 2.4GHz networks, requiring users to configure their Wi-Fi routers. Later, if the user changes their SSID or password, they'll need to reconfigure every device again.

- **Immediate availability**: Thousands of devices are available for purchase online, something will work.
  Reality: Often, users must try multiple devices to find a solution. Once a device works, it typically operates within its own app or ecosystem, which makes integration with other systems challenging (or impossible). For instance, what if you want your HVAC system to coordinate with your window blinds? While secondary control systems like SmartThings can bridge these gaps, they require advanced technical skills and often result in platform lock-in.Bullet 2
- **Convenient battery power**: Battery-operated devices eliminate the need for hardwiring, making installation easy for the average consumer.
  Reality: Batteries eventually die and need replacing. This is manageable for a homeowner with a few devices but becomes problematic when managing a large property. If tenants are responsible for maintaining batteries, they likely won't do it, which leads to system failures.

These issues are manageable for a single end-user with just a few devices. But at the scale of a multifamily residential property, it becomes a nightmare. While it's possible to build a consumer-grade system for large-scale use, it's fragile and often unreliable. When the system breaks down, maintenance falls by the wayside, and residents stop using or relying on it. Even worse, when a critical failure occurs, the property manager, faced with angry tenants, may decide it's easier to tear out the system than replace it.

Let's dive into these shortcomings in more detail, and see how a solution like Domatic addresses each issue.

Shortcoming 1: Weak Security

As previously mentioned, the quick conveniences of consumer-grade devices become glaring issues at scale. But security is a significant concern regardless of the project's size, and it must be addressed seriously whether you're dealing with a handful of users or a large building. Leaving security in the hands of residents or property managers is a recipe for disaster. Here are some reasons why consumer-grade solutions fall short:

1. Dubious root-of-trust

Problem: Many consumer smart devices collect vast amounts of personal data and store it on third-party servers, which may be at risk if they aren't properly secured. Some devices, such as video cameras, transmit data to unknown servers, often located overseas. Where are these servers hosted? Can we trust the country and the company overseeing the data? Often, these questions go unanswered.

Solution: Domatic stores and encrypts its data on databases directly managed by the company and hosted on US-based servers. These servers are subject to strict US laws around personal data and must follow protocols for

research and development purposes. This means Domatic will never use customer data without explicit consent for a clear and stated purpose.

2. Lack of regular updates and patches

Problem: Security is an ongoing process, yet many manufacturers fail to provide timely updates or patches, leaving known vulnerabilities unaddressed. This is especially true for systems that lack maintenance programs or consequences for breaches. A property manager certainly doesn't want the hallway lights to be held ransom by a hacker demanding payment in Bitcoin (yes, that's a real issue happening with unsecured databases today).

Solution: Domatic, as a smart building system, takes security seriously because the impact of downtime is substantial for its clients. Security is never a finished task; Domatic continually updates its system and monitors for anomalous behavior. Its team has over 30 years of experience securing network systems, and ensuring ongoing protection.

3. Inadequate authentication and encryption

Problem: Wireless systems are inherently public—anyone nearby can intercept the signal. The security of these systems relies on Wi-Fi authentication and passwords, which often aren't set up properly. Some systems use outdated or weak encryption standards, leaving them vulnerable to attacks, and most people are unaware of these risks. Home networks are also frequently insecure because users stick to default settings without further securing their routers.

Solution: Domatic embeds security into the design of its system. Domatic devices are hardwired into the network, making them far more secure than consumer devices broadcasting wireless signals. Even if a malicious actor gains physical access to the network, the encrypted traffic will be unreadable to them.

Real-World Examples of Security Challenges

To highlight the risks of consumer-grade security, here are a couple of notable incidents:

Mirai Botnet Attack: In 2016, the Mirai botnet exploited vulnerable connected devices to launch one of the largest DDoS (Distributed Denial of Service) attacks in history. The attackers scanned the Internet for IP addresses of connected devices, then used a list of default usernames and passwords to log in and install malware. Once infected, the devices were controlled by the attacker and used to bombard websites with traffic, making them inaccessible.

Smart Doorbell Hack: Consumer reports have revealed that hackers can easily gain access to smart doorbell cameras, spying on families and even communicating with children. Many of these devices, which are widely available online, lack encryption and expose users' home IP addresses and Wi-Fi network names. In some cases, anyone with physical access to the doorbell can pair their phone to it and take control of the device.

Both of these situations could have been avoided with Domatic's approach. The Domatic hub acts as a gatekeeper, encrypting all communications on the network. Devices only communicate through the hub, ensuring no device can act independently or coordinate an attack. Domatic's system is supported by a security team with over 30 years of experience.

Shortcoming 2: Lack of Robustness

1. Connectivity problems

Problem: One of the most common issues with smart home devices is connectivity. They rely on a stable Wi-Fi (or Zigbee/Z-Wave) connection to the resident or building network (or smart hub) to function properly. When connectivity is unreliable, as it often is in large environments, devices may become unresponsive or fail to communicate, requiring frequent resets. In addition, changing the SSID for a group of connected devices often breaks their functionality, necessitating reconfiguration.

Solution: Domatic employs a separate wired network from the resident's network, ensuring reliable, stable connections. This wired network is robust and completely isolated from other building networks. Additionally, Domatic's system doesn't rely on the Internet for basic building functionality like turning on lights or controlling heating and cooling. Even if the Internet goes down, the Domatic system will continue to operate locally.

2. Battery life concerns

Problem: Many smaller smart devices, like sensors and locks, run on batteries, which need to be replaced or recharged. Over time, batteries lose their capacity, leading to degraded performance or device failure. Having critical devices like flood sensors run on batteries is risky, as problems often arise when you least expect them.

Solution: Domatic uses low-voltage wiring to power devices, meaning no need for regular battery changes. The same cables provide both power and communication, reducing maintenance while improving reliability. Additionally, Domatic supports battery-less wireless protocols like EnOcean when needed.

3. Aging devices and obsolescence

Problem: As smart home technology evolves, older devices often become obsolete or incompatible with newer systems. This creates issues when integrating new devices into an existing system. Many older devices, for instance, only support 2.4GHz Wi-Fi and can't handle modern blended networks. We may need to replace devices, which increases costs.

Solution: All Domatic-compatible devices installed in the field will remain compatible with the Domatic system, even as it evolves. Domatic's standards are future-proof, ensuring that older devices can work alongside new ones.

Shortcoming 3: Lack of Support

1. Silos of control

Problem: Devices targeting consumers aren't designed to integrate with building management systems. Instead, they rely on separate apps and platforms like Apple HomeKit, Google Assistant, and Amazon Alexa, each with its own ecosystem. Managing a grid of apps on a phone is cumbersome for homeowners, let alone property managers. Devices that work well within one app may not integrate easily with others, creating a fragmented experience.

Solution: An integrated system is key to effective management. Domatic's Device Classes serve as a foundational layer, enabling seamless communication between devices from different manufacturers. These Device Classes ensure interoperability, allowing property managers and developers to select the right devices for their specific project, without worrying about app compatibility or fragmented control.

2. Inconsistent APIs

Problem: Many consumer-grade smart devices offer limited APIs, making it difficult to integrate them into broader building systems. While proprietary systems like Amazon's Alexa or Google Assistant are designed for residential use, they lack the depth of integration necessary for professional-grade environments. To get these systems to work in commercial settings, developers must write custom software to integrate each device's API, increasing complexity and cost.

Solution: Domatic offers a truly open smart building system with open APIs for integration, meaning third-party systems can communicate and exchange data with Domatic's ecosystem with minimal friction. This level of openness and accessibility reduces the complexity of integrating new devices and software.

3. Device incompatibility

Problem: Consumer-grade devices often fail or are discontinued without notice, leaving property managers scrambling to find compatible replacements. Tenants might buy smart locks, thermostats, or lights, but what happens if those brands are discontinued? Maintaining consistency across apartments is difficult if tenants are purchasing their own devices. As devices fail, replacements are difficult to find, and management becomes a mess.

Solution: Domatic's ecosystem ensures that all devices are compatible with each other, reducing the risk of obsolescence or incompatibility. Whether tenants bring in their own devices or rely on the building's smart infrastructure, Domatic provides consistency and compatibility across all apartments.

Conclusion

While consumer-grade smart home devices offer convenience and appeal for DIY projects or small households, they are not suitable for managing the complexity and demands of a large-scale smart building. These systems are fragile, often lack proper security measures, and have limited support, making them more of a headache than a solution in large multifamily environments.

A robust system like Domatic, designed with security, reliability, and future-proofing in mind, is essential for managing smart buildings efficiently. Domatic's integrated approach allows property managers and residents to enjoy the benefits of a smart building without worrying about vendor lock-in, security risks, or constant maintenance headaches. By breaking down silos and ensuring that devices communicate seamlessly across a unified system, Domatic creates a better living experience for residents and a more manageable operation for property managers and developers alike.