SECURE WIRELESS LIGHTING CONTROL

Legrand's new Wattstopper Wireless Digital Lighting Management (DLM) system is the first wireless lighting control solution designed and built for secure large-scale IoT deployments.

OVERVIEW

Connected devices are now found everywhere, including commercial buildings. In 2014, there were just under 14 billion connected devices worldwide. That number is expected to reach 50 billion by 2020. This means the average number of connected devices per person will double from two in 2014 to four in 2020 (source: Cisco).

As the number of these devices increase and the flow of data travelling through buildings becomes more complex, buildings need to adapt.

At Legrand, we see this as an opportunity to provide our customers with added value. The Internet of Things (IoT) is a reality that we have taken on board. Legrand already has more than 22 million nodes installed around the world. The Eliot (Electricity + IoT) program was formed to ensure that these connected devices are delivering on Legrand's commitment to:

1. Deliver solutions that are intuitive and easy to use and install
2. Enhance the product's value in use
3. Respect the user through security and confidentiality of data

The third point in particular is very important because wireless IoT devices are indeed more vulnerable to the threat of cyberattacks. In recent years, there have been multiple instances of hackers entering a corporate network via a compromised IoT device resulting in expensive and problematic security breaches for the companies involved. These security breaches are usually traced back to a device or system where security was poorly implemented. The result of many of these issues is loss of revenue and productivity, theft of private customer information, erosion of customer confidence, and bad publicity for the client and manufacturers, designers, and even installers of the product.

Implementing security into products and solutions requires very specialized knowledge and most organizations do not have the necessary competence in-house. And while security challenges can be addressed more easily in small installations, security is often why large-scale deployments of IoT are held back due to the high implementation costs.

Security considerations start from system design and continue well after the IoT devices are installed. These devices need to be managed and maintained with secure firmware updates throughout their lifetime, which can be 10–20 years — or even longer. Therefore, designing IoT devices that have strong, enterprise-grade security is paramount to Legrand's approach. The engineering team at Wattstopper (a product line of Legrand) has spent more than two years developing a wireless lighting control solution specifically designed for advanced IoT security during the entire life of the system from installation and commissioning through the long-term operation and use by building occupants.

This solution is called Wireless DLM and it employs several unique security technologies that fall under the umbrellas of Secure Commission and Secure Control.

SECURE COMMISSION TECHNOLOGY

Commissioning is the process of bringing a new system into working condition as intended based on the project design and requirements. This is a pivotal phase in the project when security is configured for the wireless devices being installed in the space. If the security is not set up properly by the contractor, the system could be vulnerable to security breaches and hacks so it is imperative that attention is paid to getting this right.

SECURE COMMISSION TECHNOLOGY (continued)

With *Secure Commission* technology, the security is built into the device at the time of manufacture and is automatically activated when it is powered on, thereby relieving the contractor of the responsibility of making sure that the devices are secure. There are three core components of *Secure Commission* technology. Let's look at each in more detail.

Device Authentication:

All wireless lighting control systems rely on some form of encryption to protect communication between devices on the network. And while encryption is necessary, it is not sufficient on its own. Encryption prevents eavesdropping but does not identify whom you are communicating with. *Authentication* allows you to verify both the origin and the identity of the communicating device. Identity-based authentication ensures that a device only communicates with an authorized server and prevents it from downloading malicious software (malware) and becoming a security risk. Mutual authentication, encryption, and ability to securely download firmware are key building blocks of device security.

With Wireless DLM's "Device Authentication," the device must be authenticated via a *trusted hardware chip* containing the proper key to be able to join the Wireless DLM IPv6 mesh network. Trusted hardware is a secure cryptographic microchip that is programmed with digital certificates and manufactured into each wireless device. It automatically enables a series of critical security capabilities without requiring any installer involvement.

With trusted hardware, device security is always automatically enabled from the moment the device is first turned on until it is eventually decommissioned, preventing any outside devices from being able to connect to the lighting control network. This means best-practice driven secure provisioning steps are automatically completed during the commissioning process, eliminating the need for the contractor to program security into every device and the possibility of insecure implementations that can result from relying on the installer's knowledge of cybersecurity.

Many wireless lighting control systems were developed before it was cost effective to include trusted hardware and may require a complete redesign to support it. Managing network security without trusted hardware makes it difficult to know or control who can access your network because it assures that there is a manual process somewhere along the way that could compromise the security of the system.

Zero Touch Encryption Provisioning:

Network-layer encryption is the first line of defense to prevent someone from reading or breaking into the network. Encryption provides a structure for private communication by translating the communication between devices into a code that the device receiving the information can decrypt if the two devices share the same "key."

Before going into "zero touch" encryption provisioning, a short primer on encryption will be beneficial.

First, there are two kinds of cryptographic keys: symmetric and asymmetric. A *Symmetric key* refers to a single algorithm which is used for both encryption and decryption. This symmetric algorithm can also be referred to as a "secret key." The challenge with symmetric encryption is mainly the key management, which becomes increasingly complicated as the number of IoT devices grows.

Asymmetric algorithms are considered "public keys" which use different, mathematically related keys for encryption and decryption. Asymmetric encryption largely solves the key distribution problem. When used in concert with one another the public key is used for encryption and is shared with all devices in the system, while the private key is used for decryption and kept a secret on the individual device.

The use of this type of public key infrastructure (PKI) is a very proven, scalable, and standardized technology, and originally intended for enterprises and computers. The premise behind PKI cryptography is that it should be computationally infeasible to obtain the secret private key by knowing the public key. The longer the key, the more computational resources and time would be needed for a hacker to break the encryption. In practice, the key length depends on the security requirements of a specific application. So, the cryptographic keys required for securing a connected light bulb in your home against a hacker with limited resources would be very different from the keys required for securing a closely guarded national military secret against state-sponsored cyberattacks.

SECURE COMMISSION TECHNOLOGY (continued)

In general, the higher the security, the higher the cost, so there is a tradeoff between the required level of security and key length, and the cost of providing that security.

Standards-based PKI with asymmetric encryption working in tandem with certificate authority-issued digital certificates stored on trusted hardware chips is highly scalable and considered the gold standard for IoT device security. Elliptic-curve cryptography (ECC) keypairs and certificates, which include a private key to generate digital signatures and a public key to verify digital signatures offer the benefit of a smaller key size to reduce storage and transmission requirements. With trusted hardware, the ECC keypairs and certificates are built in so that these shared keys can be created randomly, on the fly, and only shared when encrypted.

In other wireless systems, the shared keys often must be set or "provisioned" on every device or every zone of lighting. This can be an enormous task during commissioning that is time consuming, prone to error, and often unmanageable over the life of the system. More troublingly, it exposes the security keys to the installer's tools and sometimes to the installer themselves. Without using keypairs to prove identity, devices that receive the public key are *assumed* to be authentic. There's no way for another device or an app to challenge them with any other type of secret to make certain they are not an imposter.

This brings us to the unique approach taken by Wireless DLM. Zero touch encryption provisioning provides a pre-loaded digital identity and security profile making the system automatically secure. The contractor never has to set up security keys — this happens automatically. This is why it's called "zero touch." Embedding strong security into commercial lighting controls and building systems makes it possible for contractors to install wireless lighting systems in a matter of hours, compared to several weeks for traditional wired systems or older wireless systems without this technology.

Lighting Network Isolation:

In late 2013, during the peak of the retail season, hackers breached Target's private network and accessed credit card data for thousands of consumers. The hackers gained entry using network credentials stolen from a provider of refrigeration and HVAC equipment to Target. It is incidents like this that make it important to maintain separation from the client's network. For this reason, the Wireless DLM system is designed to operate on a parallel network that never intersects with the client's private network.

Depending on the precise network configuration, this separation will be a physical air gap or a robust firewall that separates the Ethernet ports on a Tridium Jace. The Jace has two Ethernet ports: one for lighting controls and one for the client's BAS with a firewall in between. The only communication that happens is when the client system asks for data on the lighting system to be supplied. This separation between the two networks ensures that it is simply impossible for a hacker to gain access to a client network through the Wireless DLM lighting control system.

SECURE CONTROL TECHNOLOGY

After the installation and commissioning are done and the building is turned over to the occupants, the Wireless DLM system's security features continue to work via a suite of technologies we call *Secure Control*. There are three core components under this umbrella term so let us unpack each of them and understand why they are important.

Cloud Authentication:

After installation and even well into building use, a commissioning tool is needed to adjust the lighting control system for sequence of operations adjustments, system tuning, or providing user level control. Almost all wireless lighting control systems leverage proprietary mobile apps as a convenient way for enabling these tasks to be completed.

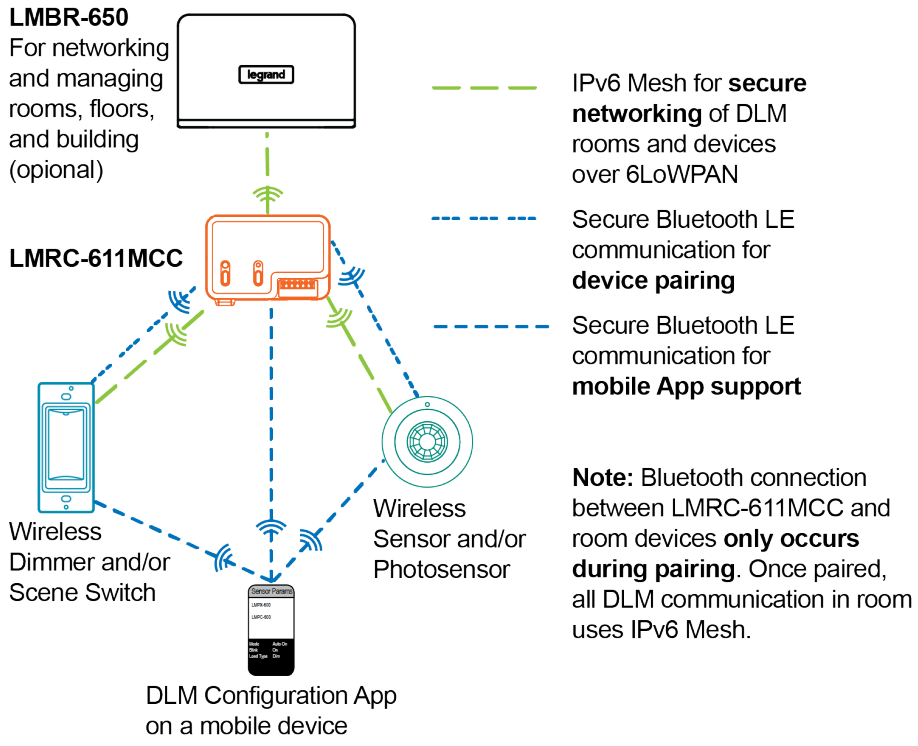
SECURE CONTROL TECHNOLOGY (continued)

Though mobile apps are a great tool, they can also be a major security risk due to the number of different types of uses and users. Most apps are made publicly available in the App Store™ and Google Play Store™ and can therefore be downloaded by anyone. To manage the risk caused by this convenience, it is imperative that all mobile apps have a managed user authentication methodology.

As a best practice, unverified users should have minimal and specific access to the system. As an example, installers may have permission to pair devices that are in factory defaults to complete an initial setup but once commissioned they can only see the devices in the room and not make any changes. Users download the app and create a free account. At this point, any actions are at least tracked to the account. But until the account is verified to be a real installer, as opposed to a foreign hacker, a competing contractor, or even a fifth grader in a classroom with a connected lighting system, escalated advanced permissions should not be granted. This helps prevent anyone from making unauthorized changes using the app. Otherwise, access from an app might as well be a wide-open portal for anyone to exploit.

For this reason, Wireless DLM employs role and time-based user authentication so that facility managers can control who has system access. Having a methodology for controlling how much access a user has is very important to ensure security and stability of the system. Technicians may have access to reset rooms, devices, and programming. Facility managers may just want access to adjust basic settings. Finally, users may just have access to specific rooms or zones to control light levels or to get status.

Technology is sufficiently advanced to allow this granularity and so any strategy from only granting access to facility teams on down to individual rooms to individual users can be accomplished using the same technologies. Phones and tablets already use this model for many other things so the mechanisms to have access expire automatically are again based on standard technologies that have been available for years – just not very prevalently for lighting and controls. The diagram below illustrates the secure wireless connectivity between the DLM Configuration app and the Wireless DLM products.



SECURE CONTROL TECHNOLOGY (continued)

The Wireless DLM cloud-based authentication model is a great method for managing who has access to what and for how long. It's also a great asset for adjusting access as employees enter or leave a company. Being able to remove or provide time-based access that expires automatically is ideal for maintaining a secure stable solution since this centralizes the user accounts and provides the opportunity to have installers cycle off access from a particular project without losing the rights they have with other active projects or having to re-verify their account. They are still valid, but when that job is finished their access expires. Preventing even well-meaning unauthorized access can go a long way towards guaranteeing the service level from the manufacturer since no changes can be made without it being obvious to all involved in the support process who is making changes when and what the changes are.

AES Encryption:

As previously stated, network-layer encryption is extremely important as the first line of defense. If a wireless lighting control manufacturer can't share what their encryption standard is, beware, because it often means it is an older proprietary standard or non-existent. If a manufacturer says they use AES 128, be sure to ask how it is deployed. AES128 implementations are so standardized that typically the method of key protection during deployment is often more important than the level of encryption itself.

For Wireless DLM, it begins with zero touch encryption provisioning as we've already outlined. But it is also important to note that all ongoing communication between devices is also encrypted. When devices communicate, they are using symmetric keys. Symmetric keys are randomly generated on the fly through a random number generated by a Federal Information Processing Standard (FIPS) certified true random number generator stored on the secure IC and only shared to devices that can pass a mutual authentication challenge using securely stored certificates and a device-unique public/private keypair.

The devices in a Wireless DLM system understand each other because every device in the network encrypts and decrypts with the same 128-bit number. The method in which Wireless DLM shares the number everywhere in a room or in a larger Personal Area Network (PAN) is also very unique. Asymmetric ECC keypairs are used to generate a shared secret key. Since all the devices share a parent in the trust chain, they will get the same answer and will be able to communicate with one another while any outside devices will be locked out.

When used with trusted hardware, devices contain a verifiable identity to keep imposters out and to share the symmetric secrets via encrypted sessions. Wireless DLM trusted devices use their unique cryptographic information to establish trusted encrypted Datagram Transport Layer Session (DTLS) anytime IPv6 mesh or Bluetooth low energy wireless data is transmitted. Whether traffic is being sent device to device, device to mobile app, or to a mesh network of devices, the DTLS standard ensures that the communication session is always encrypted and protected from unauthorized access. Wireless DLM uses the following measures for secure AES encryption deployment:

- The private key for each device is safely stored in secure hardware and should never leave the module where it is stored.
- IoT devices use cryptographic verification of the authenticity and integrity of new software (code signing) before they download it.
- Logistics behind provisioning of keys and corresponding certificates are packaged into the hardware at the factory, making implementation simple and turn-key.
- Simplicity of implementation saves cost and time to market making secure IoT much more attractive to implement across the entire product line.
- Embedded certificates and keys in IoT devices allow network servers to implement secure policies to more effectively control network access and ensure ecosystem integrity.

SECURE CONTROL TECHNOLOGY (continued)

When implemented this way, AES 128 becomes virtually impossible to hack because the key that is needed to join the network is randomized and created within trusted hardware where it cannot be stolen. Since stealing keys is the most successful method used to compromise a network, manually setting keys is a mistake.

Updateable Firmware Over the Air (OTA):

Since technology in the IoT space is advancing extremely rapidly and new cybersecurity threats continue to emerge, it is important that the firmware on wireless lighting control devices can be updated with as little hassle as possible after installation. For this reason, Wireless DLM has been engineered to enable firmware updates over the air. All firmware over-the-air upgrades are securely transmitted with DTLS and verified by trusted hardware for authenticity. When paired with a Wattstopper RACCESS remote support modem (as part of Wattstopper Lighting Control System Services) the firmware updates can be pushed remotely by Wattstopper technicians in the Remote Operations Center (ROC). This functionality helps to avoid downtime or the need for contractors to physically go to the site.

CONCLUSION

Security was a major consideration during the development of Wireless DLM. Each of the six different technologies that are featured under Secure Commission and Secure Control help make Wireless DLM the most secure wireless lighting system on the market. The engineering team at Legrand has worked hard to ensure that robust security is built into the product from the outset so that specifiers, contractors, building owners, and facility managers can rest assured that the system is secure without any action being needed on their part.

For more information on the Wireless DLM system, please visit https://www.legrand.us/wattstopper/digital-lighting-management-solutions.aspx.

ABOUT WATTSTOPPER

Wattstopper, a product line of Legrand, offers the most comprehensive line of simple, scalable and flexible energy efficient lighting controls and solutions for commercial and residential applications. The Wattstopper range of products, programs, and services have been helping customers save energy, meet green initiatives and comply with energy codes for more than 30 years. www.legrand.us/wattstopper

ABOUT LEGRAND AND LEGRAND, NORTH AND CENTRAL AMERICA

Legrand is a global specialist in electrical and digital building infrastructures. Its comprehensive offering of solutions for use in commercial, industrial, and residential markets makes it a benchmark for customers worldwide. Innovation for a steady flow of new products with high added value is a prime vector for growth, including, in particular, connected devices stemming from Legrand's global Eliot (Electricity and IoT) program. Legrand reported sales of $6.2 billion (USD) in 2017. Legrand has a strong presence in North and Central America, with a portfolio of well-known market brands and product lines that includes AFCO Systems, C2G, Cablofil, Chief, Da-Lite, Electrorack, Finelite, Luxul, Middle Atlantic Products, Milestone AV, Nuvo, OCL, On-Q, Ortronics, Pass & Seymour, Pinnacle, Projecta, QMotion, Quiktron, Raritan, Sanus, Server Technology, Solarfective, Vaddio, Vantage, Wattstopper, and Wiremold. Legrand is listed on Euronext Paris and is a component stock of indexes including the CAC40, FTSE4Good, MSCI World, ASPI, Corporate Oekom Rating, and DJSI (ISIN code FR0010307819). www.legrand.us