Lunera Smart Lamps: Our Approach to Security

Whenever the topic of the Internet of Things comes up, the concern of security quickly follows. As it absolutely should. Security is at the forefront of every decision we make. Lunera takes the security of our cloud, our customers, and our lamps and customer data very seriously. And although no system can ever be perfectly secure, Lunera is committed to be an industry leader in security and transparent about our practices.

This document provides a high-level technical overview of what Lunera does to ensure that our devices are trustworthy, and that our lamp-to-cloud communications are as protected as possible.

This begins with our architecture, which provides a secure, scalable IoT infrastructure for smart buildings, and includes secure features at these levels:

- Hardware, Secure Boot and Keys
- Upgrade
- Lamp Ecosystem
- Operations

Hardware, Secure Boot and Keys

Each Lunera Smart Lamp features a microcontroller with flash storage on the same die, inside which the device's code and keys are stored. To protect this storage from external access, the microcontroller unit's debugging interfaces (JTAG and SWD) are permanently disabled, along with external boot methods and device firmware update (DFU) mode. Note: This protection cannot be disabled.

The Lunera firmware image prevents any access to the key storage area using the ARM Cortex MPU, helping to ensure that out of bounds memory accesses cannot reach sensitive information.

Because all code execution is from on-die memory, the boot process does not expose any attack vectors via the external memory bus as with many other systems.

Every lamp contains a number of per-device unique keys which are used to validate a device's identity, and a hardware-based RNG is used to provide entropy for the cryptographic libraries.

Upgrade

In order to preserve security, devices must be able to accept over-the-air (OTA) firmware upgrades. The firmware image of the lamp will reject any firmware upgrade that is not correctly signed and encrypted, or any image which represents a rollback of the security epoch.

All firmware update images are AES encrypted and signed with PKCS#1 v2. Upgrades are stored as image files on a server within the cloud.

Each lamp holds within its on-die storage an RSA-4096 public key, which is used to verify the signatures within firmware updates downloaded from the upgrade server. The private key that signs firmware images is protected within a FIPS140-2 compliant HSM and requires multiple parties, smartcards, and pass phrases in order to generate a correctly signed image.

The Lunera Smart Lamp's firmware verifies, decrypts and stores the upgrade in its on-die storage. Code is never executed without the matching signatures. And interrupting or corrupting the upgrade does not result in incomplete, unverified code being executable at any point.

The Lunera Ambient Compute platform, in turn, manages the on-board connectivity hardware of each lamp to deliver secure communications with the cloud.

Smart Lamp Ecosystem

Lunera Smart Lamp firmware provides a secure, sandboxed virtual machine (VM) in which the lamp's partner applications are run.

This is similar to a Java VM; meaning the application code can only interact with the outside world (including external hardware, module software and all communications channels) via pre-defined APIs delivered by the Lunera Ambient Compute platform itself. The platform also provides an abstraction layer through which lamp applications interface with the lamp hardware.

Operations

Lunera exercises best practices and cutting-edge cloud operations to minimize attack surface areas in both the service layer and data. We monitor and test our infrastructure regularly for potential vulnerabilities. We use a sophisticated dev-ops system of automated deployments, containers, and service checks to automatically ensure servers are up-to-date and running only the expected applications. Servers are protected with a variety of automatic intrusion detection software to discourage automated attacks.

Additionally, Lunera engineers routinely destroy and re-provision boxes to reduce the risk or scope of any undetected issues or lingering old versions of libraries or other software. Human access to these boxes is limited to a trusted server operations team, and that access is granted only via a single bastion host, which is strictly monitored. Additionally, Lunera disallows the execution of arbitrary code in our lamps, which prevents attackers from impersonating our lamps, and finally, we ensure that the lamp installation process in the field is secure, as well as, lamp-to-cloud communications afterwards.

Execution of Arbitrary Code

In many cases, exploits involve the execution of arbitrary code; trapping these operations helps deal with unforeseen attack vectors, and is generally considered to be a key part of a robust security methodology.

In order to help protect against bugs that might allow malicious code to perform unauthorized actions in the platform (network stack, security stack, etc.), the memory protection unit within the CPU core is enabled.

The unit's protections fall into three groups: (1) The use of asymmetric RSA keys prevents any leakage of the on-die image from enabling an attacker to build valid upgrade files and hence execute untrusted code on any other device; (2) All executable code is placed in a read-only area, so it cannot be altered by a malicious attack; (3) All writable RAM is marked: 'No Execute.' This disallows instruction fetches from these areas to prevent code execution from any source that could be influenced by an attacker.

Also, any illegal accesses are trapped and reported to the server over the secure TLS channel. This allows Lunera to analyze attacks that may be made on connected smart lamps.

Lamp-to-Cloud Communications

No data or code ever leaves the Lunera Smart Lamps without first being encrypted. Local network wireless encryption is handled by the wireless chip, but Lunera does not rely on this security in any way. Instead, we use TLS encryption (version 1.2).

Currently, Lunera uses AES-128 link encryption for the TLS connection to the server with mutual authentication: the client verifies that the server's certificate is valid based on an embedded X.509 CA certificate within the lamp's firmware. The server requests the client's certificate and verifies that it is valid using another embedded X.509 CA certificate. If either certificate fails validation, the connection is dropped.

Certificates used are all generated by Lunera and deployed to the various servers, load balancers and firmware build processes.

Lamp-to-cloud server communications perform an ephemeral elliptic curve Diffie-Hellman key exchange (ECDHE) to achieve forward secrecy for the link (using the NIST P-256/secp256r1 curve; expected to provide a 128-bit security level). A compromise of long-term server authentication keys at a later date will not break the security of earlier captured communications.

On each new TLS session a ECDHE handshake occurs. The session is kept open as long as possible. In the event of connectivity issues, a new session is initiated. TLS session resumption is supported to improve reconnection times for lamps that poll (sleep and wake); the session tokens are stored within on-die RAM.

Commissioning Lamps for End-use

Every smart lamp in the field must be commissioned if it is to be put to use. Commissioning involves providing the lamp with any information it needs to first connect to a local network and then authorizing access to the cloud. Lamps which are not commissioned, or which are rejected during the authorization phase, will not be able to connect to the cloud.

The communications credentials (WiFi SSID, password, proxy setup, etc.) to Lunera Smart Lamps are transmitted via BLE and are encrypted via a secret key that is unique for each lamp and stored in the cloud for that specific lamp. This key is changed after every use, and is transmitted using the BLE from the Lunera mobile installation app. The Lunera mobile installation app also requires authentication. Neither the mobile app nor the user knows the key, which is obtained via the cloud over https and allowed only after a secure authentication. This key is unique for every smart lamp.

About Lunera

Lunera is an IoT infrastructure company that delivers simple, affordable and valuable networked command and control solutions for commercial and industrial buildings through lighting.

Our Smart Lighting Platform of connected LED lamps and cloud-based software applications, is a universal IoT gateway infrastructure, enabling indoor GPS and real-time location-based services while, delivering coordinated energy management of lighting, HVAC and plug loads throughout a facility.

The Smart Lighting Platform architecture is built on open standard and is highly scalable. A robust set of applications are available in the expanding, cloud-based Lunera Applications Marketplace.

The Smart T8 lamp is based on LED light bulbs due to its low cost of deployment, immediate energy savings, ubiquity, density and always-on power. Lunera is redefining traditional LED lighting to catalyze change and realize a vision for location/context aware ambient computing at the edge.

https://www.lunera.com/smart-lighting-platform

1615 Wyatt Drive, Santa Clara CA 95054 | 408.495.5600 | lunera.com