Unlocking a Building's IoT Potential With Secure, Smart Lighting

arm

White Paper

The concept of smart lighting once meant automatically turning the lights off when you left a room. But today's sensor and LED-based smart lighting systems can reduce energy costs and improve organizational efficiency and productivity, redefining what it means to be smart.

IoT Technology Makes Lighting Smart

Smart lighting in action

"IoT-powered lighting offers the ideal infrastructure for collecting data about a building and its occupants," says Aniruddha Deodhar, Director, Connected Spaces at Arm. "There are no better 'eyes and ears' for harnessing data." In fact, Boston Consulting Group estimates that 25 percent of all luminaires will be "smart" by 2020.[1]

While any organization can benefit from networked lighting systems, rates of adoption and use cases vary by industry. Cities, universities, corporate campuses, and stadiums are steadily implementing IoT-enabled lighting. By controlling lighting remotely, these institutions can achieve huge energy efficiencies and cost savings.

For example, as part of a smart city initiative, the city of San Diego is upgrading 14,000 of its 60,100 street lights with LED lights, which is expected to save the city approximately $2.4 million per year in energy costs.[2] And at Atlas Global Solutions, a global protective packaging company in Sutton, Massachusetts, simply upgrading to an intelligent LED system in one of its warehouses could translate to energy savings of $34,000 per year.[3] Building owners are also reducing energy costs by integrating smart lighting systems with thermostats, HVAC controllers, and occupancy sensors for complete automation.

"IoT-powered lighting offers the ideal infrastructure for collecting data about a building and its occupants. There are no better 'eyes and ears' for harnessing data."

Aniruddha Deodhar, Director, Connected Spaces, Arm

The Future of Smart Lighting

Office Security

Space Optimization

Asset Visibility

Building Automation

Object Detection

Wayfinding

Arm Improves Productivity With Smart Lighting

In 2017, Arm installed hundreds of sensor-embedded smart lights in its San Jose, CA headquarters. Together, these sensors collect bits of data 65 times per second, enabling Arm's building managers to control everything from conference room lighting to individual sensors. This allows Arm to dim or brighten a boardroom depending on how many people are in it, or how much outdoor light the room receives.

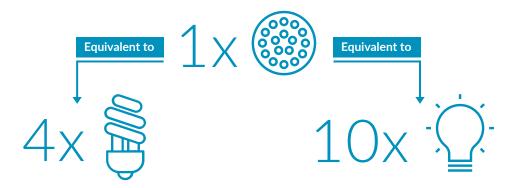Since implementing the programmable system, Arm says its ROI extends beyond lighting, which generally accounts for 65 percent of its overall energy expenses. A smart lighting sensor can detect when a room is vacated and automatically send a message to employees letting them know it's available. In a large office with hundreds of people and limited conference rooms, this type of functionality improves organizational efficiency and employee productivity.

By migrating to an IoT-enabled lighting system, Arm also reduced its overall lighting maintenance costs. LED lights last 4 times longer than fluorescents and 10 times longer than traditional incandescent light bulbs. Moreover, by using smart lighting sensors to collect occupancy and foot-traffic data, Arm can now better optimize its employee working environments for improved productivity.

Equivalent to — 1x — Equivalent to

4x — 10x

Emerging Technologies Extend Smart Lighting Capabilities

IoT-powered lighting systems extend beyond connectivity. These sophisticated systems often incorporate a wide variety of advanced technologies and capabilities.

1

Energy harvesting

Advanced, multi-function sensors offer energy-harvesting technologies that generate electricity from kinetic, light, and thermal energy and energy-sipping features that put devices into "sleep" mode when not in use.

2

Computer vision technology

By capturing and analyzing digital images in real time, computer vision technology is opening up a new realm of possibilities in facility management and security. Computer vision technology can track and count people in a building, generate heat maps to show space usage, and even control facility access for employees and contractors.

3

Artificial intelligence (AI)

Smart lighting systems with built-in artificial intelligence can learn occupancy patterns over time and dim a conference room or illuminate a cafeteria based on actual usage, rather than using rigid, predetermined schedules.

4

Advanced IoT platforms

In their efforts to securely harness enterprise data, organizations are investing in advanced IoT platforms that surpass ordinary, heterogeneous software and technology stacks. These IoT platforms are interoperable with other building systems, offer strong device-to-cloud security, and help streamline data management for end-user applications.
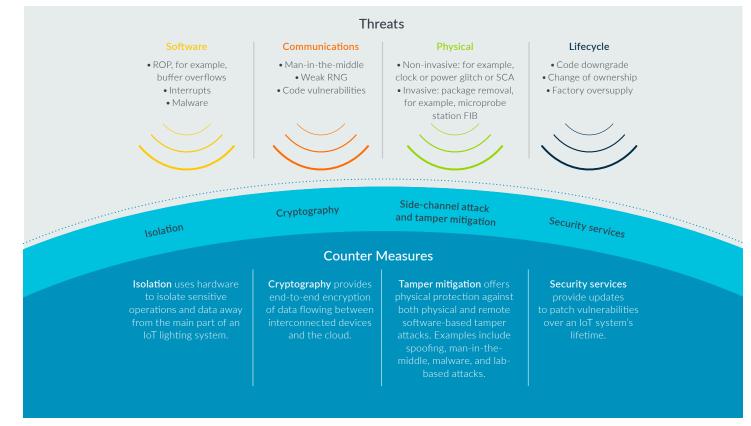
How to Overcome the Security Challenges of Smart Lighting

Despite the many benefits of IoT-enabled lighting, its ubiquity and connectivity also make it a target for cybercriminals. "Smart lighting is typically connected to a building's IT and business infrastructure," warns Deodhar. "When these systems share connectivity, a business's entire operations can be vulnerable to compromise."

Additionally, by hacking into a poorly-secured smart lighting system a cyber criminal "can potentially gain access to a company's entire IT operations and bring down its email system, servers, and business operations, gaining access to confidential data. All it takes is one bad actor with access to your data to create havoc, from sending phishing emails to securing access to private consumer data."

Case in point: the Mirai botnet caused a nationwide internet outage in 2016 by waging a massive distributed denial-of-service attack using hundreds of thousands of compromised IoT devices, including home routers, air-quality monitors, and personal surveillance cameras. Hackers have even been known to hijack the internet-connected controls of heating and air-conditioning systems.

A security framework for smart lighting success

Threats

Software
- ROP, for example, buffer overflows
- Interrupts
- Malware

Communications
- Man-in-the-middle
- Weak RNG
- Code vulnerabilities

Physical
- Non-invasive: for example, clock or power glitch or SCA
- Invasive: package removal, for example, microprobe station FIB

Lifecycle
- Code downgrade
- Change of ownership
- Factory oversupply

Isolation

Cryptography

Side-channel attack and tamper mitigation

Security services

Counter Measures

Isolation uses hardware to isolate sensitive operations and data away from the main part of an IoT lighting system.

Cryptography provides end-to-end encryption of data flowing between interconnected devices and the cloud.

Tamper mitigation offers physical protection against both physical and remote software-based tamper attacks. Examples include spoofing, man-in-the-middle, malware, and lab-based attacks.

Security services provide updates to patch vulnerabilities over an IoT system's lifetime.

Secure smart lighting: where to begin

The benefits of a smart lighting system generally outweigh the risks. But organizations should take steps to secure IoT-enabled devices, their connection to the cloud, and the data that flows between and among them. You can begin with a threat model and security analysis (TMSA). This step examines the assets requiring protection, identifies potential threats, and flags individuals and groups most likely to pose a threat.

Critical questions to ask:

✛ What threats do we need to consider and which assets should we protect?

✛ What is the attack surface and how broad is it?

✛ What type of breach do we need to prepare for?

Although security needs vary by industry, it's critical that you build a solid security model that aligns with your overall strategic goals, unique security challenges, and industry trends.

Principles for protection

Once you identify potential cyber threats, you need to build a strong baseline of IoT security centered on the following four principles.

Immutable device identity
An IoT device's identity must be authorized, authenticated, and verified. Cryptographic functions, such as a set of keys, should be built directly into the chip to prevent unauthorized access to a device's firmware. This is more efficient than bolting on security measures postimplementation.

A trusted boot sequence
A trusted boot sequence builds integrity into an IoT system by preventing the execution of unauthorized code when a device powers up.

Certificate-based authentication
Certificate-based authentication helps ensure a device connects only to authorized servers, peers, and cloud-based services.

Secure over-the-air updates
By patching vulnerabilities remotely, secure, over-the-air updates enable cost-effective, realtime resolution to time-sensitive security threats.

The Arm Equation

As business costs continue to rise, more organizations seek the cost savings, energy efficiency, and productivity benefits of smart lighting. The following set of Arm solutions can help you build a secure and efficient smart lighting system.

Mbed OS

Mbed OS is a free, open-source embedded operating system that includes all the features needed to design and develop IoT devices, including:

- Standards-based security and connectivity stacks
- RTOS kernel
- Middleware for storage and networking
- Remote device management

Developed in collaboration with our 300,000+ developer community, Mbed OS supports a wide range of chips, boards, and modules from the world's top semiconductor vendors.

Pelion IoT Platform

The Arm Pelion IoT Platform provides a secure and efficient foundation that enables IoT capability at scale, powering new discoveries and data-driven decisions. It's a device-to-data platform designed to help enterprises grow. The three key components of the Pelion IoT platform are:
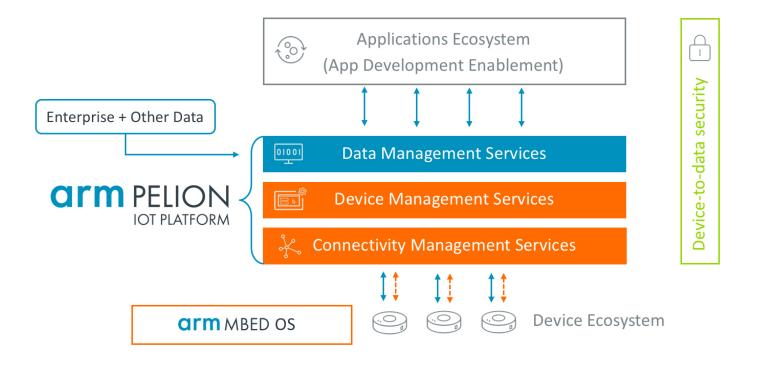
✛ **Connectivity Management**

The Pelion connectivity management enables enterprises to easily, securely, and cost-effectively connect devices for a global IoT deployment, reducing the time and effort required to scale devices on multiple network standards. It also provides connectivity management as a service to mobile network operators.

✛ **Device Management**

The Pelion device management lets customers securely and reliably onboard new devices, connect them to the network, and update devices throughout their lifecycle. The platform's device management capabilities support whatever device, cloud vendor (public, private or hybrid cloud), or communication protocol a customer may require.
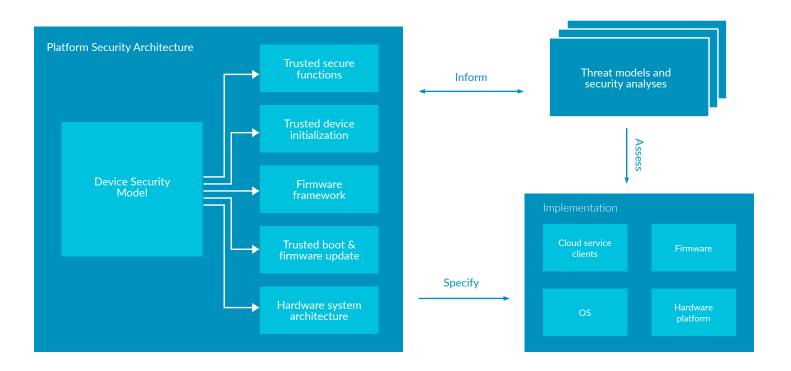
✛ **Data Management**

Pelion data management makes it easy to ingest and integrate large volumes of IoT device data with enterprise and 3rd party data. The unique insights enabled by this data management capability often help businesses discover new revenue potential, improve operational efficiency, and make critical decisions with confidence.

Platform Security Architecture (PSA)

Arm's Platform Security Architecture (PSA) offers a scalable approach that includes a set of threat models, documentation, hardware and firmware architecture specifications, and an open-source firmware reference implementation.

Platform Security Architecture

Device Security Model	Trusted secure functions
	Trusted device initialization
	Firmware framework
	Trusted boot & firmware update
	Hardware system architecture

Inform

Threat models and security analyses

Assess

Implementation

Cloud service clients	Firmware
OS	Hardware platform

Specify

Arm TrustZone

Arm TrustZone provides a platform for system-wide security and protects assets from software and hardware attacks through a secure and non-secure partition. Semiconductor designers can build TrustZone's hardware-based security technology directly into their SoCs for secure end-points and a device root-of-trust.

Arm Security IP

Arm has a range of security IP that can protect against security threats. Arm has also extended its security IP portfolio to protect against both invasive and non-invasive attacks.

Project Trillium

Project Trillium is a suite of IP that enables machine learning (ML) for many devices and processors. It includes a ML processor and a set of open source software libraries.

Conclusion

Today's organizations expect lighting systems to illuminate their business operations — not just rooms. Smart lighting systems provide the perfect IoT backbone for a range of intelligent applications, from occupancy-based facility services, to computer-vision-based security. Whatever the use case, by automating lighting and connecting it with other building systems, such as heating and cooling, organizations can achieve enormous business benefits, from reduced operational costs and energy bills to space optimization and enhanced employee productivity.

And in the world of IoT, the ubiquity and connected nature of the smart lighting system make the LED lights, and the business itself, vulnerable to cyber attacks. End-to-end security is non-negotiable. It must be baked into devices and enforced throughout the devices' lifecycle. By doing so, organizations can take advantage of the benefits of smart lighting while continuing to support a secure world of interconnected systems.

Learn more about how the IoT is bringing intelligence to not just lighting, but a range of environments and infrastructure. www.arm.com/smartlighting

arm

1. How to Win in a Transforming Lighting Industry, Boston Consulting Group, November 12, 2015

2. "GE, Intel, and AT&T Are Putting Cameras and Sensors All Over San Diego," Reuters, February 22, 2017, http://fortune.com/2017/02/22/sandiego-ge-intel-att/

3. Michelle Davidson, "Case study: IoT lighting system cuts energy costs, improves productivity," IDG Communications, Inc., July 26, 2016, https://www.networkworld.com/article/3099682/internet-of-things/case-study-iot-lighting-system-cuts-energy-costs-improves-productivity.html

Learn more:

arm.com/smartlighting