CREE ⬍ LIGHTING

FAQ: SmartCast Intelligence Platform™ and IoT Cybersecurity

Just as LED lighting control systems have become smart, connected and networkable, the Internet of Things (IoT) is poised to give companies rapidly expanding data, information and insights through network-connected smart devices and systems.

If you develop, plan, specify or select commercial LED lighting systems, this has four important implications:

1. You must assume every lighting control network will eventually be connected to other enterprise networks and/or the Internet.
2. Any lighting control network that doesn't provide enterprise-level cybersecurity may compromise the company and put valuable assets and resources at risk.
3. Not all lighting manufacturers give cybersecurity the same priority.
4. Since every IoT-enabled lighting network will require the blessing of the corporate IT department, you'll want to choose a lighting vendor with cybersecurity that will earn IT department approval.

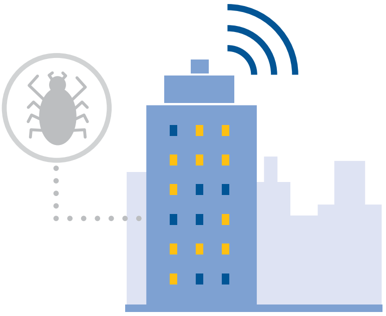
Here's the good news: Cree Lighting's SmartCast Intelligence Platform™ was developed from the ground up with IT-grade cybersecurity features and has passed rigorous independent evaluation. In fact, a global cybersecurity firm ranked the cybersecurity measures of the SmartCast Intelligence Platform™ in the top 10% of all technology companies they've tested, which includes the leading technology companies that you use every day.

Here is a summary review of the most common security questions about connected lighting control networks and the IoT, and some quick answers to potential IT questions about Cree Lighting's SmartCast Intelligence Platform™ security features.

Why is IoT cybersecurity an issue for connected lighting control networks?

The smart lighting networks you use to control dimming, task-tuning and daylight harvesting can also collect environmental data through embedded sensors to give you actionable business insights beyond lighting. But the real payoff begins when this lighting network is connected to other networks. For instance, by providing a building's HVAC system with occupancy data from the lighting network, heating and cooling loads can be adjusted to only condition those spaces that are in use. Similarly, a connected lighting network can interoperate with security systems, fire control systems, maintenance schedulers and other building networks for improved safety, responsiveness and convenience.

But connected lighting networks are no different from any other computer network: they can be hacked or hijacked by disgruntled users, corporate spies or outside actors. As these networks are connected to other networks, smart devices and the Internet, the number of potential entry points by which hackers can access critical data and systems continues to grow.



By 2020, more than **25% of identified attacks in enterprises will involve the IoT,** although the IoT will account for less than 10% of IT security budgets**.**

What are the most common cyber threats?

Cyber threats range from sensitive data stored on IoT devices being stolen or exposed to IoT devices themselves being hijacked and used as 'botnets' to carry out a distributed denial of service (DDoS) attack (overwhelming a system with traffic from multiple sources). Perhaps the most dangerous threat: hackers commandeering IoT devices then sending malicious commands — e.g., disabling the brake-by-wire system in an automobile or de-calibrating a home health monitor. Also on the rise: "ransomware" extortions whereby an attacker surreptitiously encrypts a company's data to effectively lock the enterprise out of its own information, then demands a hefty ransom under threat of total data erasure. MIT predicts that ransomware attacks will soon become one of the top threats to cloud computing.[1]

Other common threats include:[2]

- Brute-force password attacks (trying billions of combinations of passwords)
- Vectoring (using an unsecure networked system to gain access to other systems in the network)
- Sniffing (reading and/or maliciously modifying data that is not encrypted)
- Invasions of privacy

The Open Web Application Security Project (OWASP) lists the top ten security issues for the IoT as:

1. Insecure web interface
2. Insufficient authentication/ authorization
3. Insecure network services
4. Lack of transport encryption
5. Privacy concerns
6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software/firmware
10. Poor physical security

What are the main IoT security concerns?

According to McAfee, 70% of IoT devices have security exposures. Even worse, as cybersecurity and IT experts often point out, is that many IoT device manufacturers don't address security as a fundamental part of their development process. Building a connected network system without cybersecurity is like constructing an office building without plumbing and electricity — adding it later is expensive and difficult, if not impossible.[3]

The IoT will also rapidly increase the volume of security patch applications needed to keep all those new smart devices and systems updated. Before the IoT, IT departments typically worried about server, computer and software updates. As Internet-connected devices become ubiquitous, IT departments will be faced with providing timely updates to everything — from smart lighting to IoT-enabled vending machines, trash receptacles, coffee machines and window blinds — requiring new, additional updating/patching tools and processes.

What is the current state of security in most networked lighting controls?

A number of networked lighting control systems have 128-bit AES encryption and meet the National Institute of Standards and Technology 's (NIST) FIPS 140-2, Level 1 requirements — a basic security standard. But these are frequently not enough to satisfy enterprise-level IT departments, especially those with higher standards for encryption, modes of access, passwords, etc. When we compared the connected lighting control networks of seven leading Cree Lighting competitors, only two require HTTPS and none include LDAP integration, containerization or are capable of continuous patching.

[1] https://www.computerweekly.com/news/450432488/Ransomware-to-hit-cloud-computing-in-2018-predicts-MIT

[2] https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-files/top-five-cyber-risks.ashx; https://www.energy.gov/sites/prod/files/2018/06/f52/cyber_security_lighting.pdf

[3] https://www.itproportal.com/features/top-ten-cybersecurity-predictions-for-2019/

How is the SmartCast Intelligence Platform™ different?

Unlike traditional lighting companies, Cree Lighting is a "digital native," expressly created at the heart of the Internet revolution to innovate and manufacture LED lighting.

As you'd expect from a leading technology provider, we built the SmartCast Intelligence Platform™ around the security principles and practices we knew corporate IT would want to see — especially following the BSIMM9 (Building Security in Maturity Model) framework: the ninth iteration of an adaptive model based on quantified software security best practices.

By engineering cybersecurity directly into the core of the product, Cree Lighting successfully made the SmartCast Intelligence Platform™ more resistant to vulnerabilities and exploitable flaws across the system. As a result, Cree Lighting's cybersecurity was recently rated by a global cybersecurity group as among the top 10% of all technology companies they've tested, which includes the leading technology companies that you use every day.

What security features set the SmartCast Intelligence Platform™ apart?

Notable features and benefits include:

- Unique keys/passwords for each SmartCast Link™
- Secure boot and password storage (including salting)
- An encrypted datastore for sensitive information
- LDAP integration
- Containerization
- Continuous patching
- HTTPS protocols required everywhere (even on "intra-container" networks)

What should IT departments know about the SmartCast Link™ API?

An application programming interface key (API key) is a code passed in by computer programs calling an API to identify the calling program, its developer, or its user. SmartCast Link's API is protected with dynamically-generated API keys that must be presented with each and every user request. SmartCast Link's Role-Based Access Control (RBAC) then determines the level of administrative function or "role" associated with each API key. Thus each key is individually assigned the right level of access, such as "read," "write" or "admin."

What should IT departments know about our encryption?

While in recent years some enterprises have migrated to 256-bit encryption, the power requirements of using 256-bit encryption in IoT devices such as smart luminaires are too demanding. That's not to say 128-bit keys are in any way insecure: security experts agree that cracking AES 128-bit encryption will remain beyond any conceivable technology available in the foreseeable future. The current estimate of the time required to crack a 128-bit cryptographic key using a brute force attack utilizing a state-of-the art supercomputer is 500 billion years.[4]

Why is SmartCast® Technology an open and interoperable system?

There is debate about the merits of "closed" versus "open" system architectures and IoT security. A closed system architecture is built on proprietary code shielded from public view and might seem to offer a security advantage. An open architecture is just that – an open book allowing anyone to view the source code. Does an open architecture's greater potential for growth, scalability and collaboration outweigh any security advantage offered by a "closed" system? In a word, we say 'yes'.

[4] https://medium.com/@drgutteridge/whats-the-deal-with-encryption-strength-is-128-bit-encryption-enough-or-do-you-need-more-3338b53f1e3d

Cree Lighting agrees with industry experts who emphasize that interoperability will be essential for companies to fully realize the potential of IoT applications. Further, experts agree that "closed" systems tend to yield more bugs and security flaws due to the limited number of developers and testers who are allowed to scrutinize the software source code. In contrast, the software in open architectures can be reviewed and tested by anyone. Security vulnerabilities are much more likely to be discovered and publicized, forcing greater accountability and quicker remedies. That's why the SmartCast Intelligence Platform™ is built on a secure, open intelligence platform optimized for connectivity and data integration. It's also why Cree Lighting is working alongside IT security companies and industry groups to ensure secure architectures and protocols are in place to safely open the door to a fully connected IoT world.

What are the security trends to watch?

Security standards for networked lighting controls are emerging. The American National Standard Institute (ANSI)/UL 2900 is a series of standards providing measurable criteria for the testing of network-connected devices that send, store or transmit data to/from networked devices. UL 2900-1 focuses on cybersecurity for appliances including lighting. According to the U.S. Department of Energy, the DLC is revising the Networked Lighting Control System Technical Requirements to incorporate cybersecurity requirements (current draft version 3 includes ANSI/UL 2900-1). Although not a federal requirement, sites might need to use ANSI/UL 2900-1 lighting products to qualify for a rebate.

Product testing is also on the rise. The UL Cybersecurity Assurance Program and other 3rd-party testing labs now can test product software for vulnerabilities, analyze source codes, conduct robustness testing for all external interfaces and communication protocols, and do limited "white hat" penetration testing (penetration testing that simulates real-world attack scenarios to discover and exploit security gaps).

In fact, Cree Lighting is currently unique among lighting manufacturers in doing 3rd-party penetration testing for the SmartCast Intelligence Platform™ to help determine how to best mitigate security risks and protect data and connected networks from cybersecurity attacks.

Visit **creelighting.com/smartcast** or contact a Cree Lighting representative to learn more.

CREE LIGHTING
A COMPANY OF IDEAL INDUSTRIES, INC.