Michael Poplawski and Adam St. Lawrence

Stress Test Cybersecurity lessons emerge from a recent study of connected lighting

One of the key issues raised by the emergence of connected lighting is cybersecurity. Increased data, and connectivity-based access to that data, introduce cybersecurity risks that are new to the lighting industry and that must be addressed if integrations with other systems are to be widely implemented. Pacific Northwest National Laboratory (PNNL) has conducted the first in a series of studies intended to educate lighting-industry stakeholders on specific cybersecurity practices and characterize the implementation of those practices in commercially available connected lighting systems (CLS) with varying system architectures, network communication technologies and maturities (**Figure 1**). Based on tests conducted in partnership with Underwriters Laboratories (UL) at PNNL's Connected Lighting Test Bed (CLTB), the first study explores authentication practices and their implementation in five CLS.

Authentication is the process of verifying an identity claim and is sometimes followed by authorization, which is the process of verifying whether a request for subsequent access to other systems, networks or data falls within the authenticated party's permitted privileges. The most-common authentication mechanism is the traditional combination of username and password, also known as a credential set. People and machines are both capable of using credential sets as well as other authentication mechanisms, such as cryptographic keys and tokens.

> The connected lighting systems being brought to market have varying levels of vulnerability

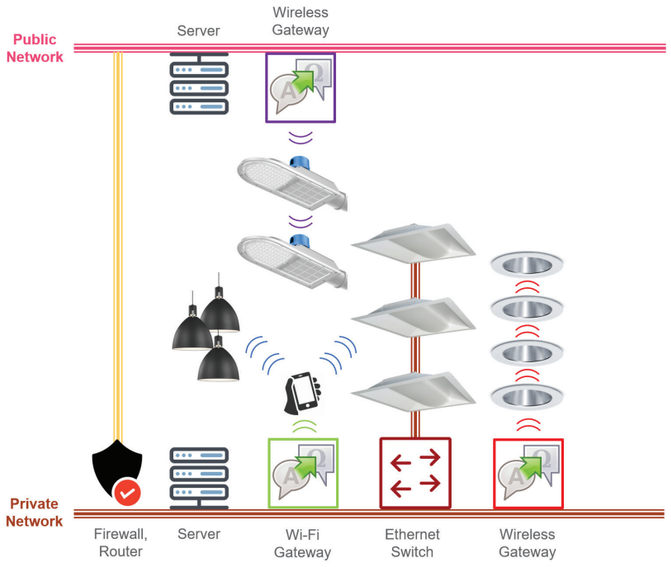

Figure 1: Conceptual representation of different connected lighting systems, showing common system architecture variations and technology implementations.

Attackers looking to exploit authentication vulnerabilities target weaknesses in the communication medium used to transport secrets, in the secrets-storing mechanism or in the authentication mechanism itself. Communication mediums, wired and wireless, may be susceptible to what are known as "sniffing" attacks, in which an attacker is able to observe secrets due to a lack of adequate cryptographic protections. Cryptographic protection may be implemented insecurely (i.e., it may be misconfigured), or the cryptographic mechanism itself may have weaknesses, such as weak or broken ciphers. The same cryptographic concepts apply to the storage of secrets.

Five connected lighting systems, spanning a range of vintages, system architectures, network implementations and other characteristics, were initially targeted for authentication testing (**Table 1**). The developed test-method suite was not suitable for one of the CLS because it did not have an integral authentication mechanism and, for cybersecurity, relied on the mechanism implemented for the host computer. The suite was run on the remaining four CLS, although not all tests were applicable to every CLS. The CLTB test setup used to identify authentication vulnerabilities consisted of a computing device with multiple operating systems, multiple web browsers, a login cracker, a web vulnerability scanner, a packet analyzer and an over-the-air Zigbee packet sniffer (**Figure 2**).

Table 1: Connected lighting systems selected for authentication testing.

	CLS A	CLS B	CLS C	CLS D	CLS E
Vintage	2015	2015	2019	2019	2018
System architecture	Web-App, accessed via on-premise server; CLS devices connected via wireless gateway	Web-App, accessed via on-premise server; CLS devices connected via wireless gateway	Web-App, accessed via Cloud server; CLS devices connected via wireless gateway	Web-App, accessed via Cloud server and 2) iOS App; CLS devices connected via direct wireless	Web-App, accessed via on-premise server; CLS devices connected via wired switch
Network connectivity	Wireless, Zigbee based Mesh	Wireless, Zigbee based Mesh	Wireless, 2G Cellular	Wireless, Bluetooth Mesh	Wired, Power-over-Ethernet (PoE)
Physical layer	IEEE 802.15.4	IEEE 802.15.4	GPRS	Bluetooth Low Energy	IEEE 802.3

A total of 18 tests were developed by UL and implemented by PNNL to characterize the four CLS that were evaluated. The tests explore the implementation of basic authentication best practices (e.g., establishing a secure communications channel prior to transmitting sensitive data such as credentials) as well as known technology-specific practices (e.g., the use of Zigbee default trust center, or the implementation of JSON Web Token, also known as JWT replay protections). As a result, not all tests are applicable to all CLS (because not all CLS use Zigbee or JWT technology). Six of the 18 tests were not applicable to any of the CLS that were evaluated in this investigation, due to their non-use of the targeted technology (JWT, MQTT, Bluetooth). A total of 40 out of 72 (4 x 18) possible tests were applicable for the four evaluated CLS (**Table 2**), and the CLS collectively passed 26 of the remaining 40 tests (63%). While pass/fail ratio is a simple way of reporting test results, it's not really a relevant metric. Cybersecurity vulnerability testing is a risk analysis practice; the relevance of passing or failing a certain test is best evaluated in concert with an understanding of the risk associated with that vulnerability in a specific implementation. Nevertheless, pass/fail ratios give some indication of the range of performance found in market-available CLS.

Looking ahead, there are numerous existing frameworks and guidelines for evaluating cybersecurity vulnerability, such as the National Institute of Standards and Technology (NIST) cyber framework, the NIST 800 series, the International Electrotechnical Commission 62443 series, International Organization for Standardization 27001 and 27002, and UL 2900-1. While these may apply to CLS in whole or in part, there is currently no mandatory requirement for cybersecurity testing or certification.

The lighting industry, including technology developers and specification organizations, are evaluating the suitability of these frameworks and guidelines for CLS. Based on the limited results of the PNNL study, it appears that the connected lighting systems that are being brought to market have varying levels of cybersecurity vulnerability. PNNL plans to conduct more authentication testing as well as initiate related authorization testing. It is hoped that these evaluations support and perhaps accelerate industry discussions on what cybersecurity

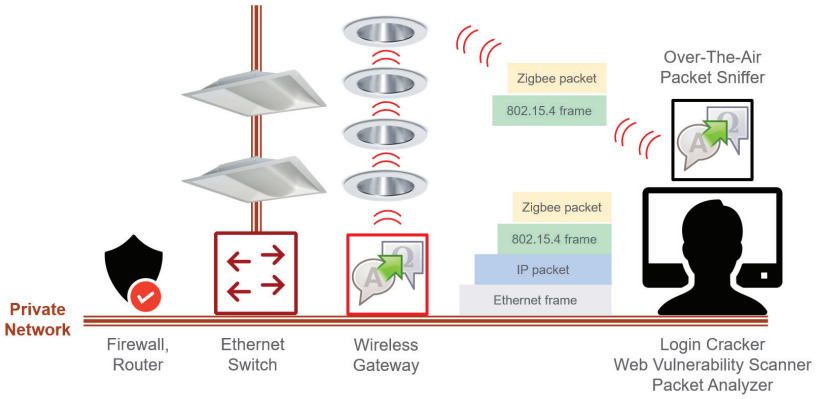

Figure 2: Authentication vulnerability test setup.

Table 2: Test results summary.

	Summary	CLS A	CLS B	CLS C	CLS D
Applicable	40	9	11	10	10
PASS	26 (63%)	3	9	7	7
FAIL	14 (37%)	6	2	3	3

vulnerabilities should be protected by best practices in CLS, and whether any such practices should be mandatory.

Michael Poplawski is a senior engineer at Pacific Northwest National Laboratory, where he supports the U.S. Department of Energy Solid-State Lighting program, primarily in the areas of connected lighting system technology evaluation and demonstration, standards and specification development, and the estimation of lighting energy end-use consumption.

Adam St. Lawrence is a senior security analyst at Underwriters Laboratories, where he provides standards-based security testing, penetration testing, training and advisory services to a wide variety of industries.