SSL

Paul Francik, Michael Poplawski, and Travis Ashley

Assessing the Threat Weaving cybersecurity into the building development process

Today's connected lighting systems have the potential to reduce energy consumption and operational costs via the use of the data they collect and share with other building systems (e.g., HVAC, building automation, security). However, many market-available products are new to being networked, and when networked components in lighting and other building systems are not sufficiently secured, they present opportunities for adversaries to exploit. Further, security vulnerabilities in one system can be used as lateral stepping-stones that allow access to other prized assets on the same network. These cybersecurity concerns could deter the adoption and use of connected systems, which then could jeopardize long-term national objectives for reduced energy usage.

We conducted a series of studies here at Pacific Northwest National Laboratory (PNNL) using industry-standard tools to analyze cyber risks associated with connected lighting systems. The analysis provides a model for product developers as well as building owners and suppliers to assess cyber threats and determine who is responsible for the controls or mitigations that should be implemented to remediate or reduce the threat potential.

Cybersecurity threats present in a networked system can be categorized in a variety of ways. Microsoft developed a categorization known as the STRIDE framework (**Table 1**), a pneumonic for six threat categories—Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privileges. Cybersecurity professionals have developed software tools that model a networked system and identify threats associated with specific device types and system architectures.

PNNL recently used one such software application, the Microsoft Threat Modeling Tool, to characterize threats that might exist in networked street lighting systems. We modeled six different street lighting systems with varying system architectures and network management technologies. The attack surface was characterized from an adversarial perspective, looking for entry points to the connected assets. We identified 57 unique threats spanning all six STRIDE categories—77% of the threats applied to all six lighting systems. Supervisory and network routing devices used to communicate with the lights (e.g., servers, routers, gateways) served as the source of 65% of threats, whereas the remaining 35% existed in the end-use devices (i.e., the streetlights). The attack surface was examined by calculating the cumulative threats that applied to each of the six connected lighting systems (CLS A through CLS F in **Figure 1**) across each STRIDE category. Hybrid systems consisting of both cloud and on-premises gateways (E and F) created a larger attack surface and more opportunities to attempt infiltration as opposed to systems consisting of homogenous systems that utilize either cloud (B, D) or on-premises gateways (A, C). The impact of two approaches (A, B vs. C, D) to authentication was also accounted for in the attack surface analysis.

> Wariness need not harden into fear and paralysis

Analysis revealed that 63% of the recommended mitigations could and likely should be addressed by manufacturers during product development. The remaining 37% would become the responsibility of building owners and operators.

Threat profiles and attack surfaces can be used by system specifiers to compare different solutions and estimate the cybersecurity actions necessary for securing those solutions to achieve a particular reduced risk level. Many system owners and operators struggle, however, to characterize their risk sensitivity to the degree necessary for deciding what threats should be mitigated and what threats can be left uncontrolled. Attackers often look for and target "known

	Threat	Violation	Threat Definition	Example
S	Spoofing Identity	Authentication	Impersonating something or someone else	Pretending to be a website, service, or user to gain access
T	Tampering with Data	Integrity	Modifying data or code	Intercepting data in transit and modifying with malicious code or false text
R	Repudiation	Non-repudiation	Claiming to have not performed an action	"I didn't visit that website," "I never ordered that," "I didn't modify that file"
I	Information Disclosure	Confidentiality	Revealing information to someone not authorized to see it	Publishing a list of customers to a website, allowing someone to read the source code of software
D	Denial of Service	Availability	Denying or degrading service to users	Crashing a website, SYN (synchronize) floods, rerouting packets
E	Elevation of Privileges	Authorization	Gaining access without proper authorization	A normal user gaining admin privilege, an external remote user accessing and running commands

Table 1. The Microsoft STRIDE framework, a method for characterizing and prioritizing the evaluation and control (i.e., mitigation) of cybersecurity threats.

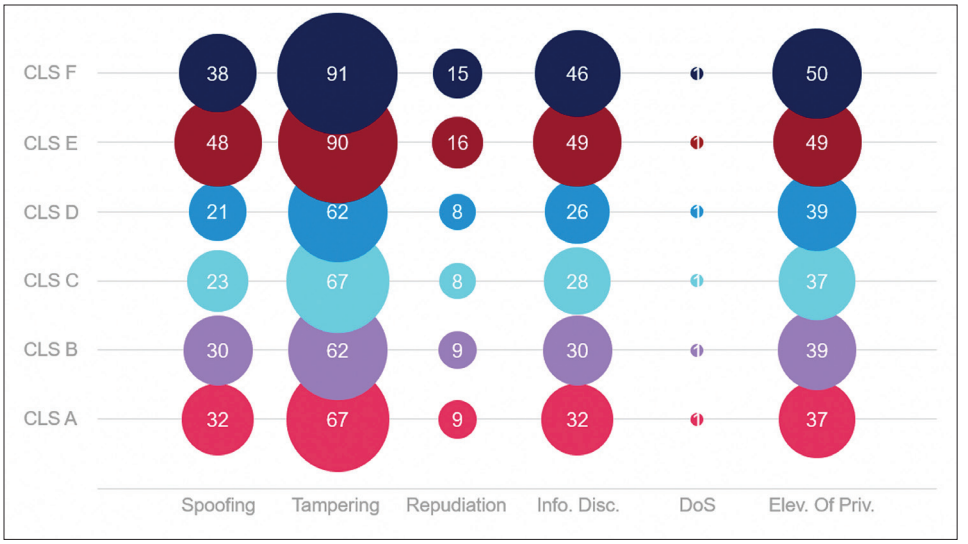

Figure 1. The cumulative attack surface for all six modeled street lighting systems, mapped to the threat categories from the STRIDE framework.

vulnerabilities"—especially systems or technologies that are widely deployed. With this knowledge in mind, specifiers, owners and operators might, in turn, prioritize the mitigation of threats that attackers are likely to target.

What is the current "threat landscape" for connected building systems—the number of known vulnerabilities that exist within deployed systems? In an initial attempt to characterize this landscape, we used Shodan—a repository of publicly exposed devices—together with a set of "fingerprinting" techniques that we developed to identify 74 buildings in the U.S. and 527 buildings globally that were exposed to the Internet and had at least one building system with a "known vulnerability" as defined by the MITRE Common Vulnerabilities and Exposures (CVE®) Program. There were 16,672 vulnerability instances discovered in these 527 buildings, spanning over 200 unique vulnerabilities (i.e., CVEs). A threat analysis determined the types of threats associated with the CVEs, some of which were high impact, such as denial of service, execution of arbitrary code and privilege escalation. Specifiers, owners and operators might want to consider prioritizing these threats or develop their own version of this prioritization process.

Viewing threats from an adversarial rather than a defensive viewpoint serves as an effective way to prioritize threats and flesh out risk sensitivity. The MITRE ATT&CK® Matrix for Enterprise was developed to characterize actions—categorized as tactics and techniques—that adversaries might take to achieve a specific goal. In recent years, many organizations have been integrating the MITRE ATT&CK® Matrix as a way to document where they have placed their defensive controls, against the most likely places an adversary might try to insert themselves within a network. We decided to map the CVEs discovered in the Shodan query to the tactics and techniques in the ATT&CK framework and explore how these vulnerabilities could be leveraged to launch a cyberattack against building control systems. Given that many sequences of tactics and techniques can be used to execute an attack, one useful metric for a given tactic or technique is how often it shows up in the mapping of a set of CVEs. Our analysis revealed that 61% of the vulnerabilities were

attributable to three techniques: Remote System Discovery; Remote Services SSH (Secure Shell); and Endpoint Denial of Service, Application or System Exploitation. Additional details about the described processes and the results they produced will be provided in forthcoming DOE reports.

Owners and operators may find that they can better identify their risk sensitivity to these tactics and techniques, as opposed to the threats identified by a threat profile or landscape analysis. In such instances, they might consider prioritizing the control of threats associated with the three techniques identified here, or the control of threats identified by their own execution of a similar process. More sophisticated owners and operators might use the results of an ATT&CK mapping to enable their internal offensive security professionals (red teams) and defensive security professionals (blue teams) to plan and execute cyberattack scenarios that would emulate the adversarial activity that they are most sensitive to, so that they can proactively test their cybersecurity resilience.

Building owners and operators that want to deploy networked systems to improve building performance and occupant experiences are right to be wary of their increased potential for cybersecurity attacks. However, that wariness need not harden into fear and paralysis. Cybersecurity professionals have developed and continue to refine frameworks and tools that can help identify threats and prioritize their control in a way that aligns with risk sensitivity. The workflows described here and presented in more detail in the referenced reports are examples of how these frameworks and tools can be put to practical use during system design and specification. We project that such workflows can support cybersecurity needs during system configuration and operation as well—by, for example, automatically setting baseline access permissions and thresholds that define suspicious behavior.

Finally, the definition of workflows also crystalizes the need to explicitly define roles and responsibilities for delivering good cyber hygiene—what threats will be controlled by: a) technologies integrated into devices and systems; b) automated processes implemented during system configuration; or c) manual processes (i.e., requiring human expertise) during system configuration.

More details are available in the recently published U.S. Department of Energy report, *A Cybersecurity Threat Profile for a Connected Lighting System*.

Paul Francik is a cybersecurity analyst at Pacific Northwest National Laboratory whose current research efforts are supported by the U.S. Department of Energy Solid-State Lighting program.

Michael Poplawski is a senior engineer at Pacific Northwest National Laboratory, where he supports the U.S. Department of Energy Building Technologies Office.

Travis Ashley is a cybersecurity engineer at Pacific Northwest National Laboratory in the cyber systems team in the electricity security group, where he supports the U.S. Department of Energy Solid-State Lighting program.