Connecting the Dots: An Assessment of Cyber-risks in Networked Building and Municipal Infrastructure Systems

Paul Francik, Travis Ashley, Michael Poplawski, Pacific Northwest National Laboratory
paul.francik@pnnl.gov; travis.ashley@pnnl.gov; michael.poplawski@pnnl.gov

Abstract

The buildings and city streets we walk down are changing. Driven by various data-driven use cases, there is increased interest in networking and integrating lighting and other building systems (e.g., heating, ventilation, and air conditioning (*HVAC), security, scheduling) that were previously not internet-facing, and equipping them with sensors that collect information about their environment and the people that inhabit it. These data-enabled systems can potentially deliver improved occupant and resident experiences and help meet the U.S. Department of Energy (DOE) national energy and carbon reduction goals. Deploying connected devices new to being networked, however, is not without its challenges. This paper explores tools available to system designers and integrators that facilitate a cybersecurity landscape assessment – or more specifically the identification of threats, vulnerabilities, and adversarial behaviors that could be used against these networked systems. These assessments can help stakeholders shift security prioritization proactively toward the beginning of the development process.*

Keywords: Networked building systems, Shodan, threat profile, vulnerability mapping, MITRE ATT&CK®

1. Introduction

Governments, cities, and even individual building owners are adopting networked technologies that can collect data about their surrounding environment so operators or building management systems can make decisions that lead to better use of resources and overall cost savings. The Barcelona Lighting Master Plan of 2012 capitalized on the city's fiber-optic infrastructure and transitioned traditional streetlights into telecommunication towers with a myriad of sensing capabilities that save an annual 37 million dollars (Adler, 2016). More recently, Chicago's Smart Lighting Program has replaced their High-Pressure Sodium Streetlights with more efficient light-emitting diode lights connected to a smart lighting management system that can automatically detect a streetlight outage, create a repair ticket, and assign a repair crew to fix it. This project is estimated to save $100 million over the next 10 years (City of Chicago, 2022). Other federal drivers include ambitious decarbonization goals spurred by climate change that aim to reduce greenhouse gasses by the year 2035 through efficiency upgrades to building systems through retrofit electrification modification in existing lighting and HVAC systems (Whitehouse, 2021).

However, deploying connected devices that are new to being networked, often referred to as Internet of Things (IoT) devices, is not without its challenges. Building systems that produce and consume data and interact with each other (and in some cases, with their occupants) introduce new attack vectors, and the threat landscape they represent grows with their integration and exposure to the internet. While these systems can enhance occupant and resident experiences and potentially reduce energy consumption, cost, and help meet carbon reduction goals, they can also be exploited if they are configured without the proper cybersecurity controls. Adversaries can shut down unprotected systems or leverage compromised access by pivoting into other valuable systems residing on the same network. For some system owners, this may prove to be only an inconvenience, but for others, it could result in damaging and even irrecoverable impacts.

Existing cybersecurity tools and frameworks enable system designers to identify potential threats and explore the impact of different technologies and system architectures. Further, they allow anyone – including system designers and adversaries – to perform reconnaissance on deployed systems by searching for targets, identifying weaknesses, and characterizing the most easily exploited vulnerabilities. Common and well-defined language about those behaviors and metrics for those weaknesses eases the identification and deployment of controls that could help avoid high exploits with high risk and impact. An understanding of the risks associated with the adoption of networked technology can make cybersecurity not feel so nebulous and can give stakeholders a baseline from which to discuss concerns with device vendors and third-party services so these technologies can be implemented safely and securely. The value of these tools and frameworks is often presented and evaluated in

URI: https://hdl.handle.net/10125/103374
978-0-9981331-6-4

isolation. This paper addresses how that value might be multiplied by the coordinated use of multiple tools and frameworks.

More specifically, we describe how a system designer might assemble intelligence that can be used to inform design choices by a) first creating a threat model and profile, b) using reconnaissance tools to identify known vulnerabilities in similar deployed systems, and c) identifying adversarial behavior that can be targeted by log scans and intrusion detection systems. This workflow can help manufacturers and adopters of networked systems characterize their threat landscape and shift security prioritization toward the beginning of the development process, while also giving them language to identify and talk about indicators of compromise.

2. Background

There are many ways by which an organization can assess their cybersecurity risk. Organizational choices are often based on or impacted by a number of factors such as the quality of available data, available tools, and prioritization in regard to the confidentiality, integrity, or availability of system assets, or services. Many organizations focus on identifying vulnerabilities in procured or installed software and systems via the use of vulnerability scanning or penetration testing.

Vulnerability scanning is an automated process that checks software for misconfigurations that could lead to a common vulnerability and exposure (CVE) where an adversary can use a known exploit to take advantage of that misconfiguration. Such scans can be performed at any point in the software development lifecycle as part of a secure coding practice, as well prior to deployment in a system. Notably, vulnerability scanning is typically software focused and does not generally consider hardware (e.g., gateways, mobile devices) or communication technologies.

Penetration testing is performed by a cybersecurity professional who acts as an adversary and attempts to examine the resilience and exploitability of agreed upon network services and assets. Caution must be taken when using this approach, as it can result in catastrophic damage to the system under test. While penetration testing is typically performed on systems that are already installed and configured, it can also be performed on mock or trial installations.

More holistic approaches to identifying cybersecurity risk that go beyond vulnerability scanning and penetration testing have been developed and are starting to see more adoption. The following sections describe some of these approaches.

2.1 Threat modeling

Threat modeling starts with the creation of a system abstraction that is suitable for analysis for potential threats. A threat profile is created by analyzing the model and identifying design-level security issues. Threat profiles reveal the types of threats that can exist and might be addressed during the design and build phases of a project, either by the vendor or the system integrator responsible for implementing cybersecurity controls. Threat profiles are a Recommended Minimum Standard for Vendor or Developer Verification of Code, as described by NIST in response to Executive Order 14028, Improving the Nations Cybersecurity. Threat profiles are particularly useful in instances where connected devices are bolted on to legacy systems already in service, and a complete overhaul of existing infrastructure and services is not financially viable or possible. In such instances, modeling can be used to understand the technology components and new data flows, and the subsequent determination of how to provide or limit access to systems and the information they contain.

2.2 Attack Surface Management

Anyone – adversary, researcher, building developer, or operator – can query one or more of the publicly available Attack Surface Management (ASM) tools that host repositories of publicly exposed devices, and target certain industries, manufacturers, and even technologies. For example, anyone that can perform a Google search can also use Shodan to perform similar searches looking for vulnerable devices. Shodan is a cyber-risk management tool that uses web spiders to crawl the internet and index exposed devices in a publicly accessible database (Matherly, 2022). Shodan was initially developed and demonstrated over 2012-2014 as part of the Shodan Intelligence Extraction project, also known as Project Shine. The tool was used to search for internet exposed supervisory control and data acquisition (SCADA) systems, and detailed reports were created for critical infrastructure networks that were directly connected to the internet (Radvanovsky, 2014). Two hundred and seven manufacturers were initially identified by applying over 900 search terms and using the results to categorized discovered devices. In the United States, over 600,000 instances of exposed SCADA and ICS devices were identified, representing approximately 34% of the worldwide attack surface. While the Project Shine scope was focused on SCADA and ICS network exposures, the vulnerabilities associated with these exposures were not identified, and the discovered systems were not classified by application (e.g., building management, lighting, security).

Adversaries that might utilize ASM tools can have a wide range of skills from very sophisticated to very juvenile. It is easier to look for known vulnerabilities that are unpatched and susceptible to exploit as opposed to discovering new ones known as zero-day exploits. It is for this reason that the United States released Binding Operational Directive 22-01, "Reducing the Significant Risk of Known Exploited Vulnerabilities," which establishes a catalogue of known vulnerabilities that attackers have exploited for years, and requires that federal civilian agencies identify and remediate them on their own systems (CISA, 2021). By controlling a catalogue of known vulnerabilities, the risk associated with these common attack vectors can be mitigated

2.3 Cyber adversarial behavior identification

Owners and operators may find it easier to relate to a vulnerability landscape that highlights behaviors associated with exploitations instead of the more technical details found in a CVE. One of the most commonly used behavioral framework is the MITRE ATT&CK® Matrix (ATT&CK) – which classifies cyber adversary behaviors as tactics and techniques (MITRE, 2022). Tactics represent behavior goals (i.e., the "why"), and techniques represent the actions taken by an adversary (i.e., the "how") to achieve that tactical goal. These classifications can be compared with defensive controls to identify where potential gaps exist within deployed systems. These comparisons provide offensive security professionals (e.g., red teams, penetration testers) and defensive security professionals (e.g., blue teams, network defenders) with a common language to talk about attack scenarios and how chaining multiple techniques together could achieve greater impacts than if they were just executed in isolation. They also enable defensive teams to document where existing controls are already in place and note if they are sufficient to withstand the identified techniques or if they can be retooled to provide additional controls and coverage. Often the ATT&CK matrix is used after an attack has occurred to identify the behaviors that were used and potentially assign attribution to groups that are notorious for their style or methods of infiltration – also known as Advanced Persistent Threats. Dragos performs an annual analysis of attacks on Operational Technology (OT) and industrial control systems that assigns attribution to groups that specifically target critical infrastructure (Dragos, 2021).

2.4 Mapping Known Vulnerabilities to Adversarial Behaviors

The Center for Threat Informed Defense (CTID) has mapped 839 CVEs to ATT&CK using well-described mapping methodologies, and posted the results to the GitHub project "ATT&CK to CVE for Impact" (Baker, 2021). Three mapping methods are defined, one by vulnerability type, a second by the functionality an attacker gains, and a third by the technique used by the attacker to execute the exploit. These methods are a valuable starting point for vulnerability reporters and researchers that desire to systematize the way they describe vulnerability data. However, manually wading through vulnerabilities and threat reports and mapping them to adversarial behaviors is an arduous and time-consuming process, even with a pre-defined methodology. A brief review of some past efforts at accelerating the mapping of CVEs to MITRE ATT&CK® follows, with a focus on their methods and effectiveness.

The CTID developed Threat Report ATT&CK™ Mapping (TRAM) as an open source platform that uses machine learning to speed up the mapping process and identify techniques that a human analyst may not have considered (CTID, 2021). However, manual review of the matches is still necessary to determine whether they are appropriate assignations.

A similar open-source GitHub project by Trustar uses Natural Language Processing (NLP) to automate the mapping of all NIST National Vulnerability database (NVD) CVEs to the MITRE ATT&CK framework (TruSTAR-daenerys, 2019). Notably, the tool's creator reports an accuracy of only 50%.

A threat modeling language called enterpriseLang was created to assess threats to the enterprise IT network (Xiong, Legrand, & al., 2021). EnterpriseLang maps network assets directly to ATT&CK. An additional level of abstraction could be applied to include vulnerability information to the meta-attack language so that CVEs could be used as an input to the simulation, but this approach has not yet been demonstrated in the literature.

A threat modeling tool called BRON links cyber-attack techniques to vulnerabilities based on commonly observed attack patterns (Hemberg & al., 2017). BRON is a unified mapping between ATT&CK, Common Weakness Enumeration (CWE), and CVE that enables bi-directional relational links to traverse between tactics and affected network assets. BRON uses corresponding nodes for attack patterns, and weaknesses as the intermediary steps between vulnerabilities and cyber-attack tactics. This requires the cyber-attack to be modeled based on a use case. A truncated approach could be designed such that it is agnostic to the threat actor by mapping directly between the vulnerability and the techniques based on the language used in the descriptions of these two nodes. This approach would encapsulate the threat information for the polar nodes of the BRON diagrams and enable a more generalized application.

Finally, the "CVE to ATT&CK" tool uses NLP techniques and Multi-Label Text Classification (MLTC) models to create a Multi-Head Joint Embedding Neural Network model that can automatically map CVEs disclosed over the past 10 years to ATT&CK techniques (Aditya, Lamine, & Nhien-An, 2021). This proprietary model is offered as a paid service by the company Tenable.

A simple comparison of the summarized mapping methods is provided in Table 1. "Language processing" refers to the use of machine learning to analyze the knowledgebase and enable automation. "Threat model language" denotes the use of an established threat modeling language to define the type of threat actors that would exploit a vulnerability. Methods that utilize "Threat labeling" automatically extract labels from the vulnerabilities and use them in the mapping process. "Regular expressions" refers to methods that use pattern matching in text of the knowledgebase descriptions. Finally, "Building automation" applies to methods that could be used for to OT in addition to Enterprise systems. Notably, none of the described methods is considered best-in-class or foolproof; all have significant room for improvement. Automated approaches, in general, produce false positives and require supervision to validate their results.

	ATT&CK to CVE	TRAM	TruSTAR daenerys	enterpriseLang	BRON	CVE to ATT&CK
Language processing		X	X	X		X
Threat model language	X			X		
Threat labeling			X			X
Regular expressions	X	X		X	X	
Building automation	X	X			X	X

Table 1. Comparison of ATT&CK mapping tools.

3. Methods and Impact

This research used industry-standard cybersecurity tools and frameworks; more specifically, the Microsoft Threat Modeling Tool (MTMT), the Shodan ASM tool, and MITRE ATT&CK® framework. These tools were used to develop a threat landscape for networked building systems in the United States. The paper is separated into three sections, each presenting the use of one of these tools or frameworks. All three analysis are performed for the same example use case: the design and deployment of a networked lighting system. While each analysis can be useful individually, the novel contribution of this paper is their integration into a workflow that delivers more value.

The first section describes the creation of a threat profile using the MTMT. The second section presents a means for identifying the presence of known but uncontrolled vulnerabilities in currently deployed building systems, including but not limited to lighting, by applying a set of custom fingerprinting techniques to a repository of publicly exposed devices created using Shodan. While many recent studies have used ASM tools to find exposed industrial control systems, the attack surface of building systems has not been as thoroughly characterized. The third section explains how the CVEs identified via the second analysis can be mapped to adversarial behaviors used to exploit them via the MITRE ATT&CK matrix.

Finally, the paper describes how these three analyses can be combined to create a cybersecurity landscape assessment that can be useful to system manufacturers, designers, and operators. This vulnerability landscapes is intended to be used proactively. Rather than looking at post-mortem data assigning attribution to a group or organization, we assume an adversarial posture by simply scanning for opportunities that exist within deployed systems and identifying what tactics and techniques could be employed to exploit the targeted products and protocols. This approach mimics the initial "reconnaissance" phase of a cyber-attack employed by many adversaries. Defining the threat landscape in the same way allows a system operator to see their assets from the perspective of their potential adversaries, rather than their own, often misleading perspective. A correlation of threats, uncontrolled vulnerabilities, and potential adversarial actions can enable system designers and operators to target potential gaps in coverage and provide their offensive and defensive cybersecurity teams with a common way of identifying the highest priority tactics, techniques, and vulnerabilities for mitigation. System designers and operators can directly incorporate the results of this work into their projects or adopt a similar method and workflow for assessing the cyber threat landscape for systems they plan to deploy, or already have deployed. Further, such threat landscapes can aid manufacturers in identifying opportunities to shore up cybersecurity controls in their products, These results and insights are timely as the U.S. DOE recently invested $61 million into 10 pilot projects that will deploy new technologies aimed to transform residential homes, commercial buildings, and federal facilities into state-of-the-art energy-efficient buildings contributing to a net-zero carbon economy (DOE, 2021). While new construction allows for the latest and greatest technologies, the reality is that many existing buildings will get retrofitted with networked systems to improve performance and capitalize on energy savings. Different buildings, however, can have unique characteristics and existing equipment that might make it challenging and risky to integrate new systems and technologies. The buildings industry has thus far not adopted leading edge approaches to the development and deployment of networked systems that perform core functions (e.g., lighting, heating, cooling), let alone those that utilize Internet-of-Things (IoT) devices. After witnessing the prevalence of malware targeting ICS, researchers at Forescout built malware whose final payload could persist at the automation level and executed their exploits on their constructed testbed to demonstrate how an adversary could do the same on real world deployed systems. Their study discovered previously unknown vulnerabilities in devices such as controllers and gateways and concluded that Building Automation Systems (BASs) may be as critical as ICS in terms of safety and security despite receiving a lot less attention from the security community (Dos Santos & al., 2020). Palo Alto's 2020 Unit 42 IoT Threat Report states that 57% of the devices they tested were vulnerable to medium or high severity attacks and 98% of device traffic was unencrypted (Unit 42, 2020). Current IoT systems are in general considered not to be secure. Rather, IoT devices are viewed to be the lowest hanging fruit by which adversaries can pivot into other valuable assets that reside on the same network.

4. Identifying Potential Threats

In a previous study (Francik, Ashley, & Poplawski, 2022) we used the Microsoft Threat Modeling Tool to create a threat profile for six conceptual connected lighting systems (CLS) with different system architectures. All threats were categorized using the STRIDE framework – a mnemonic for six separate threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges (Table 2).

	Threat	**Violation**	**Threat Definition**
S	**Spoofing Identity**	**Authentication**	**Impersonating something or someone else**
T	**Tampering with Data**	**Integrity**	**Modifying data or code**
R	**Repudiation**	**Non-repudiation**	**Claiming to have not performed an action**
I	**Information Disclosure**	**Confidentiality**	**Revealing information to someone not authorized to see it.**
D	**Denial of Service**	**Availability**	**Denying or degrading service to users**
E	**Elevation of Privileges**	**Authorization**	**Gaining access without proper authorization**

Table 2: the Microsoft STRIDE framework, a method for characterizing cybersecurity threats

We identified 57 unique threats spanning all six STRIDE categories, 77% of which applied to all six modeled lighting systems. The source of 65% of the applicable threats came from networking infrastructure (e.g., servers, routers, gateways,) that is needed to communicate with the lighting devices, whereas 35% of the remaining threats existed in the end-use devices themselves. The cumulative threats for each modeled CLS (A through F in Figure 1) by STRIDE category were added up to quantify the total attack surface. Hybrid systems utilizing both on-premise and cloud gateways (E and F) naturally created more opportunities to attempt infiltration as opposed to the homogenous systems that took advantage of only using either on-premise (A and C) or cloud (B and D) technologies. The impacts of two different approaches to authentication (A and B vs. C and D) were also assessed in the attack surface analysis.

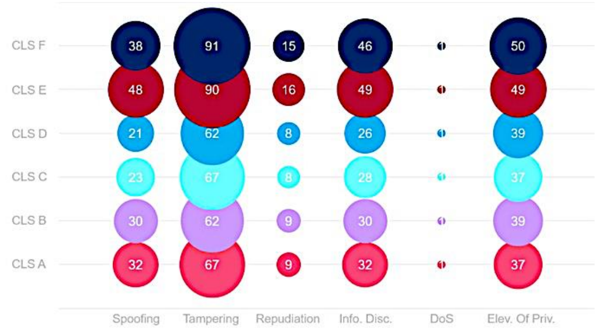
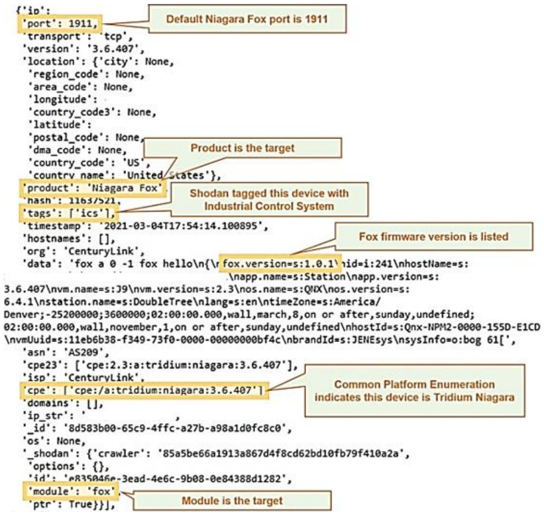


Figure 1: The cumulative attack surface for all six modeled streetlighting systems, mapped to the STRIDE framework.

A significant amount (63%) of the controls that would mitigate the identified threats was deemed to be the responsibility of manufacturers. The study documented opportunities where they could reasonably provide controls by implementing them on the devices or services themselves rather than applying a patch or secondary control after deployment at which point it may be too late. The remaining 37% were the responsibility of the system integrators and building operators to implement. Notably, in some cases, a manufacturer can provide the controls, but the user needs to turn them on or set them up properly; if they do not then that system potentially remains vulnerable.

5. Operating System Fingerprinting

In a forthcoming study (Ashley, Francik, & Poplawski, 2022), we used the ASM tool Shodan to take adversarial reconnaissance approach towards understanding commonly found vulnerabilities in lighting and other building systems. Shodan was used to target assets and communications protocols commonly found in OT systems. Figure 2 shows an example of a Shodan banner that is returned following the execution of a query. The highlighted banner properties were found to be useful in crafting signatures for operating system (OS) fingerprinting (Scarfone, Souppaya, Cody, & Orebaugh, 2008). OS fingerprinting was performed to identify device types based on the ports, services, and other information collected from the Shodan web scans.



```
{'ip':
 'port': 1911,
 'transport': 'tcp',
 'version': '3.6.407',
 'location': {'city': None,
  'region_code': None,
  'area_code': None,
  'longitude':
  'country_code3': None,
  'latitude':
  'postal_code': None,
  'dma_code': None,
  'country_code': 'US',
  'country name': 'United States'},
 'product': 'Niagara Fox',
 'hash': 11637521,
 'tags': ['ics'],
 'timestamp': '2021-03-04T17:54:14.100895',
 'hostnames': [],
 'org': 'CenturyLink',
 'data': 'fox a 0 -1 fox hello\n{\r fox.version=s:1.0.1\nid=i:241\nhostName=s:
                                        \napp.name=s:Station\napp.version=s:
3.6.407\nvm.name=s:J9\nvm.version=s:2.3\nos.name=s:QNX\nos.version=s:
6.4.1\nstation.name=s:DoubleTree\nlang=s:en\ntimeZone=s:America/
Denver;-25200000;3600000;02:00:00.000,wall,march,8,on or after,sunday,undefined;
02:00:00.000,wall,november,1,on or after,sunday,undefined\nhostId=s:Qnx-NPM2-0000-155D-E1CD
\nvmUuid=s:11eb6b38-f349-73f0-0000-00000000bf4c\nbrandId=s:JENEsys\nsysInfo=o:bog 61[',
 'asn': 'AS209',
 'cpe23': ['cpe:2.3:a:tridium:niagara:3.6.407'],
 'isp': 'CenturyLink',
 'cpe': ['cpe:/a:tridium:niagara:3.6.407']
 'domains': [],
 'ip_str': '            ',
 '_id': '8d583b00-65c9-4ffc-a27b-a98a1d0fc8c0',
 'os': None,
 '_shodan': {'crawler': '85a5be66a1913a867d4f8cd62bd10fb79f410a2a',
  'options': {},
  'id': 'e835046e-3ead-4e6c-9b08-0e84388d1282',
  'module': 'fox',
  'ptr': True}},
```

Default Niagara Fox port is 1911
Product is the target
Shodan tagged this device with Industrial Control System
Fox firmware version is listed
Common Platform Enumeration indicates this device is Tridium Niagara
Module is the target

Figure 2: Example Shodan banner for 'niagara fox'.

A Python script was developed to process the over one million banners that were returned by the targeted Shodan queries, each with a structure similar to but not necessarily identical to the example shown in Figure 2. The script automatically parsed these banners by iterating over pre-defined banner properties (e.g., Common Platform Enumeration, product, module, data) and generated a list of expressions for any string of alphanumeric characters separated by whitespace. These expressions were then validated in descending order by a count of occurrence, and banner signatures were crafted to target specific asset types or technologies, such as lighting devices or management servers, Building Automation and Control networks (BACnet) controllers or management devices, and programmable logic controllers. A total of 56,061 devices were identified using this technique and assigned to one of five asset classes (Figure 3).

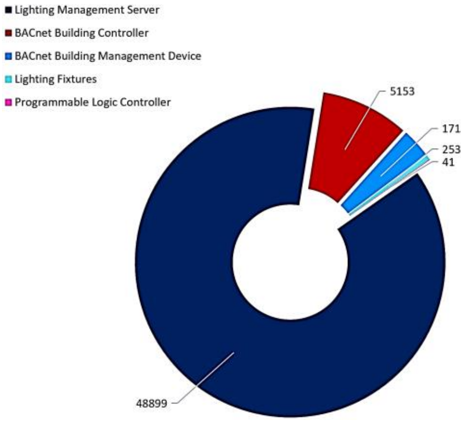


Figure 3: Devices and Asset Classes identified through Operating System fingerprinting of Shodan banners.

The databases that tools like Shodan query also contain information about vulnerabilities already known to exist within widely deployed devices and technologies (i.e., CVEs). The “vulns” property in banners returned by Shodan was parsed to identify 200+ CVE-IDs. Many of the same CVE-IDs were found across devices in one or more queries, so the total vulnerabilities found include repeated instances of these same 200+ CVE-IDs. Figure 4 shows the total number of vulnerabilities found, and a disaggregation by query type and vulnerabilities severity. Of these 16,672 CVE instances, 95% are medium- and high-severity, which means that exploiting these vulnerabilities could potentially have a high impact. Based on the location assigned to the Internet Protocol (IP) addresses, the exposed devices we identified with at least one CVE appeared to be located within 527 buildings globally, 74 of them residing in the United States. This set of known vulnerabilities found in exposed real-world systems associated with a specific industry can be used to prioritize the application of cybersecurity controls, perhaps in consideration of their ease of implementation and overall impact.

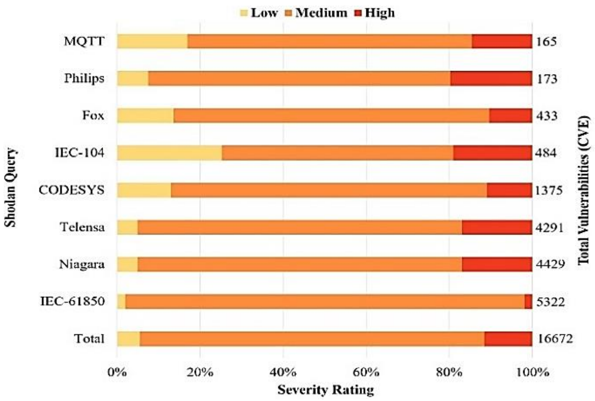


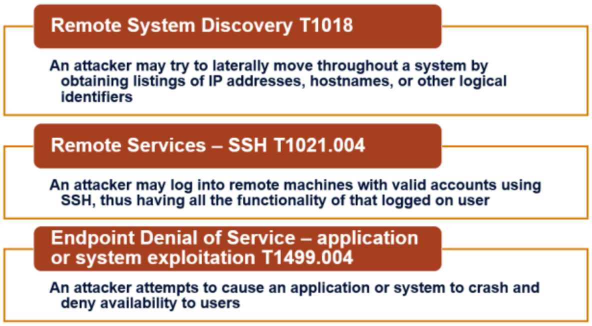
Figure 4: Number of vulnerabilities found binned by severity rating for each query.

6. Mapping Prioritized Vulnerabilities to Threat Actor Behavior

Following CISA’s Best Practices for MITRE ATT&CK® Mapping (CISA, 2021), the CVEs discovered using Shodan and the custom fingerprinting process were mapped to associated tactics and techniques. An attempt was made to identify existing mappings, and use tools that facilitate automated mapping. However, we decided to not use any tools reviewed in the Background, for one or more reasons. Only one of the CVEs mapped by the CTID matched the CVEs found by our Operating System Fingerprinting technique. At the time of our analysis, the TRAM tool required public URL inputs. In the time between analysis and the drafting of this paper, TRAM was updated such that it no longer requires public URLs, although training the ML model to recognize the associated tactics and techniques is something that would take time to achieve. TruSTAR was not used due to its low self-reported accuracy, enterpriseLang and BRON were not used due to the complexity of setting up their models, and funding constraints precluded the use of the Tenable tool.

As a result, most CVEs were mapped manually (i.e., by a human subject matter expert) by matching the keywords, phrases, intentions behind the attack – and the manner in which it could be carried out – to the matching descriptions and technical language of the CVE, including the impact severity rating. 12,806 exposed with CVEs were mapped to the Enterprise ATT&CK matrix, resulting in a threat landscape comprised of 12 tactics, 44 techniques, and 34 sub-techniques. Fifty-nine percent of these vulnerabilities were attributable to the three techniques shown in Figure 5.

A majority of techniques, 82%, were traceable to medium-severity impact vulnerabilities, 11% were traceable to high-severity impact vulnerabilities, and the remaining 7% were traceable to low-severity impact vulnerabilities (Figure 6). Thirteen techniques (29%) only affected two or fewer devices and therefore are an indication that those are weaknesses within individual configurations or patch management programs, and not of general concern. Eleven techniques could be used to exploit known vulnerabilities in all five communication protocols, suggesting that communication protocols are a systemic weakness in building systems. Further, a concerted effort to prevent the implementation of any one technique might improve the threat landscape for the entire building systems sector. Mapping details and results are provided in a forthcoming publication (Francik, Ashley, & Poplawski, MITRE ATT&CK, 2022).



Remote System Discovery T1018

An attacker may try to laterally move throughout a system by obtaining listings of IP addresses, hostnames, or other logical identifiers

Remote Services – SSH T1021.004

An attacker may log into remote machines with valid accounts using SSH, thus having all the functionality of that logged on user

Endpoint Denial of Service – application or system exploitation T1499.004

An attacker attempts to cause an application or system to crash and deny availability to users

Figure 5: The top three techniques that could lead to the exploitation of building and municipal infrastructure systems, based on the number of devices impacted and the methods described in this study.

7. Discussion and Recommendations

Internet-exposed systems will eventually be discovered. A majority of the CVEs discovered in this study had patches or software updates that could be applied to mitigate the vulnerability. It is possible that some of these systems were not patched because the risk of exploitation was accepted, or because the service interruption resulting from taking the assets offline would have a more severe impact than the risk of being compromised, or because they were forgotten or effectively invisible to the operator. Having a patch management policy whereby vulnerabilities are mitigated with software updates or preventive maintenance helps prevent compromises, data breaches, operational disruptions, and other adverse events (Souppaya & Scarfone, 2022).

However, we recommend taking a proactive approach from an adversarial perspective rather than a reactive approach from an inward-looking perspective. System designers and operators can characterize their potential exposure and risk before they become compromised by malicious actors by discovering the ways in which their systems can be entered and impacted.

For systems that are not yet deployed, we recommend, at a minimum, the development of threat profiles in the design phase to identify attack surfaces and threats that can be mitigated with strategically deployed controls. Further, as described in this study, we recommend scanning assets similar to those to be deployed that are already in operation, to get an idea of what vulnerabilities currently exist for that asset type, and what tactics and techniques adversaries might use to attack those assets.

For systems currently in operation, we recommend scanning all assets to identify publicly exposed and vulnerable devices, either by doing it yourself using one of the increasingly accessible and easy-to-use tools, or by hiring a trusted third-party service. Documented scan results can provide a baseline from which to discuss concerns with all stakeholders and be used to justify potential cybersecurity investments. Organizations can periodically run scans to get an updated snapshot of exposures and potential vulnerabilities on their network quarterly or as new devices and technologies are deployed. Once again, mapping existing known vulnerabilities to adversary tactics and techniques can enable one to take a more effective defensive posture.

While the methods presented here focused on connected building and municipal systems and were applied at a global scale, the same process could be performed on other asset types or applied at smaller scales to target a specific location, city, building, or range of IP addresses – and thereby tailored to an organization’s individual needs. Having some form of cyber threat intelligence to make informed decisions is crucial when setting out to design, build, configure, and operate new technologies in both retrofits and new construction scenarios.

Finally, we see an opportunity to save time and money in analysis resulting from the use of a common or standardized means for creating semantic models of buildings and building systems. The adoption of such an approach could reduce the time required to create a threat model by allowing for the ingestion of a design model and facilitating the integration of the described tools and techniques into a streamlined workflow. Such an integrated workflow might allow those without security teams in place to perform the work of an analyst and provide actionable insights that could be immediately incorporated to make the deployment or maintenance of their systems more resilient to outside attacks.

8. Conclusion

Networked systems offer great promise, but also pose significant risks. However, existing tools and frameworks can help define and manage those risks. These tools and frameworks offer analyses and common vocabulary that can be used throughout the design, specification, configuration, operation, and maintenance phases of deployment. This allows organizations more effective communication with their suppliers and subcontractors and takes a risk-based approach that prioritizes controls and budgets based on the biggest potential impacts of exploitation.

A regular review of the current threat landscape from an adversarial perspective can identify products or technologies that may be lacking a certain type of control. In many instances, it is likely that secondary controls will need to be incorporated to provide defense in depth, meaning that when one control fails or is never implemented, another mechanism is in place to mitigate impact. Product developers have the opportunity to make note of areas for improvement or growth in both the best interest of their brand, image, and reputation, as well as the clients who are purchasing their products and dependent on the available controls within the devices and connected technologies they are deploying.

Most importantly, the work and workflows presented here highlight the need for defining roles and responsibilities in controlling threats and vulnerabilities a) through manual processes that will require human maintenance and analysis, b) via technologies integrated or installed on the devices themselves, or c) through automated processes. This leads to better-understood security from the outset of a project, but also allows a way to document systems that have been in use and will be updated with new technologies. While security practitioners cannot predict the future with certain clarity, utilizing available open sources of data for the environment and industry being entered allow preliminary shielding and defenses to control the trending or most frequently exploited vulnerabilities that are already known.

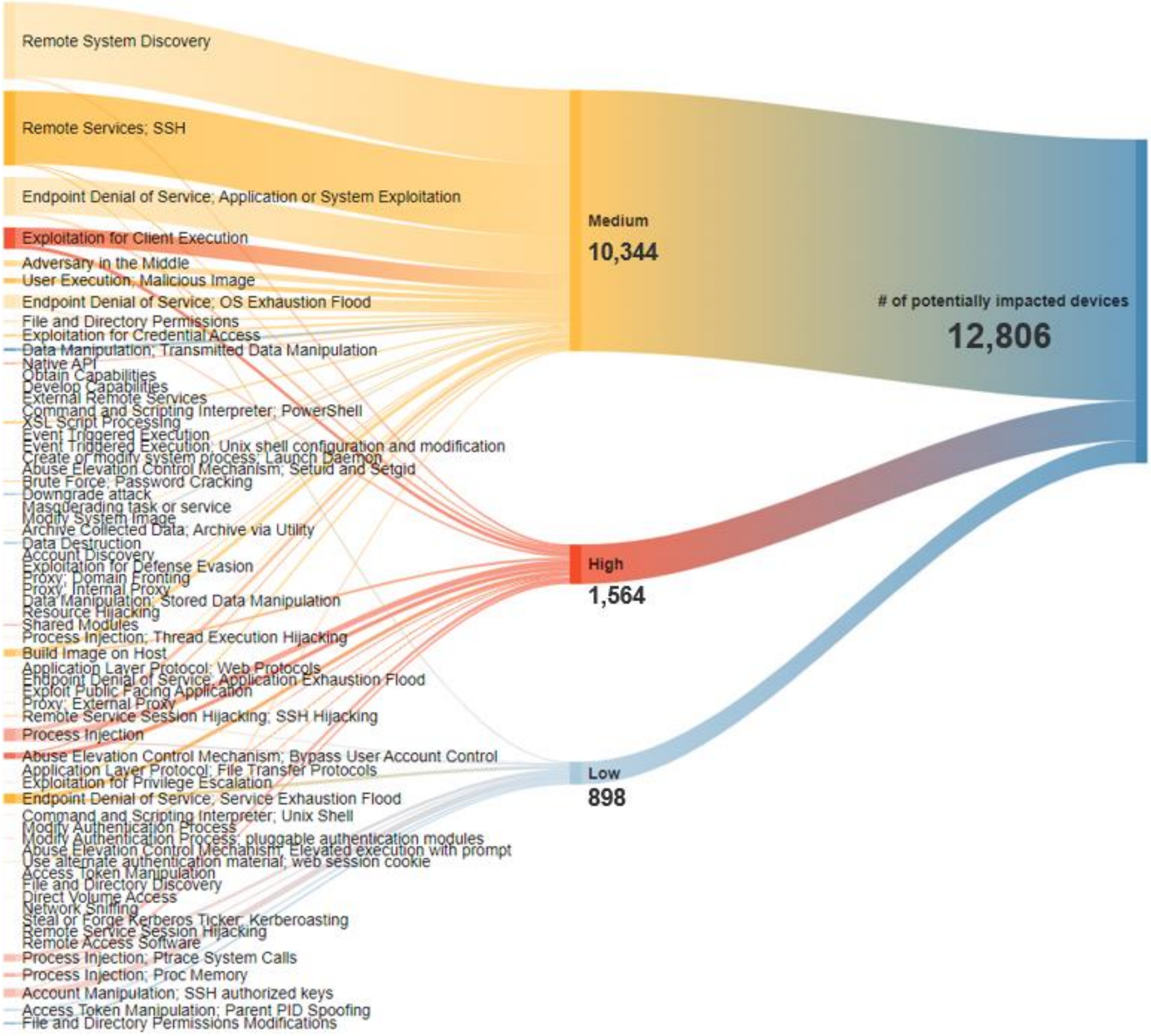


Figure 6: Distribution of techniques by impact severity level and the number of devices that could be affected

7. References

Aditya, K., Lamine, A., & Nhien-An, L.-K. (2021). Linking CVEs to MITRE ATT&CK Techniques. *The 16th International Conference on Availability, Reliability and security (ARES 2021)*, (p. 12). Vienna. doi:https://dl.acm.org/doi/10.1145/3465481.3465758

Adler, L. (2016, Feb 8th). *Data Smart City Solutions*. (Harvard) Retrieved from https://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789

Ashley, T., Francik, P., & Poplawski, M. (2022). *Fingerprinting and Vulnerability Assessment of Connected Lighting Systems through Shodan.* Richland: DOE.gov. Retrieved from Forthcoming

Baker, J. (2021, November 1). *Mapping MITRE ATT&CK® to CVEs for Impact*. Retrieved 2022, from https://github.com/center-for-threat-informed-defense/attack_to_cve/blob/master/methodology.md

Baker, J., & Davidson, M. (n.d.). ATT&CK to CVE. Retrieved from github.com/center-for-threat-informed-defense/attack_to_cve

CISA. (2021, June). *Best Practices for MITRE ATT&CK® Mapping*. Retrieved from CISA.gov: https://www.cisa.gov/uscert/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

CISA. (2021, November). *Binding Operational Directive 22-01*. Retrieved from https://www.cisa.gov/binding-operational-directive-22-01

City of Chicago. (2022, 02 09). *News Releases*. Retrieved from Chicago.gov: https://www.chicago.gov/city/en/depts/cdot/provdrs/future_projects_andconcepts/news/2022/february/mayor-lightfoot-announces-cdot-has-completed-chicago-smart-light.html

CTID, M. (2021). TRAM. CTID. Retrieved from https://github.com/center-for-threat-informed-defense/tram

DOE. (2021, October 13). *Articles*. Retrieved from Energy.gov: https://www.energy.gov/articles/doe-invests-61-million-smart-buildings-accelerate-renewable-energy-adoption-and-grid

Dos Santos, D., & al., e. (2020). *Cybersecurity in BAS.* Forescout. Retrieved from https://www.forescout.com/resources/bas-research-report-the-current-state-of-smart-building-cybersecurity-2/

Dragos. (2021). *2021 ICS Cybersecurity Year in Review*. Retrieved from dragos.com: https://www.dragos.com/year-in-review/

Francik, P., Ashley, T., & Poplawski, M. (2022). *A Cybersecurity Threat Profile for a Connected Lighting System*. Retrieved from OSTI.gov: https://www.energy.gov/eere/ssl/articles/cybersecurity-threat-profile-connected-lighting-system

Francik, P., Ashley, T., & Poplawski, M. (2022). *MITRE ATT&CK.* Richland: DOE.gov. Retrieved from Forthcoming

Hemberg, E., & al., e. (2017). *Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting.* MIT. Retrieved from arxiv.org/pdf/2010.00533.pdf

Lasky, J., & Yoder, S. (2019). MTIRE ATT&CKcon 2.0: ATT&CK Updates - TRAM. MITRE. Retrieved from https://www.youtube.com/watch?v=jVkMd9mAE-U

Matherly, J. (2022, May 13). *Shodan.* Retrieved from https://www.shodan.io/

MITRE. (2022). *Frequently Asked Questions*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/resources/faq/

MITRE. (n.d.). *Frequently Asked Question FAQ Mitre ATT&CK*. Retrieved from https://attack.mitre.org/resources/faq/

Radvanovsky, B. (2014, 10). *Project Shine Findings*. Retrieved from slideshare.net: https://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, September). *Technical Guide to Information Security Testing and Assessment.* Retrieved from NIST SP 800-115: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Souppaya, M., & Scarfone, K. (2022, April). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. Retrieved from NIST: https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

TruSTAR-daenerys. (2019, Mar 13). *Making Sense of Unstructured Intelligence Data Using NLP*. Retrieved from www.trustar.co/blog/making-sense-of-unstructured-data-using-nlp

Unit 42. (2020). *2020 Unit 42 IoT Threat Report.* Palo Alto Networks. Retrieved from https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Whitehouse. (2021, April 22). *The White House Briefing Room*. Retrieved from Whitehouse.gov: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/fact-sheet-president-biden-sets-2030-greenhouse-gas-pollution-reduction-target-aimed-at-creating-good-paying-union-jobs-and-securing-u-s-leadership-on-clean-energy-technologies/

Xiong, W., Legrand, E. Å., & al., e. (2021). *Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix.* Retrieved from https://doi.org/10.1007/s10270-021-00898-7