Light Security: Discovering Vulnerabilities in Theatrical Lighting Control Systems and Assessing Their Prevalence

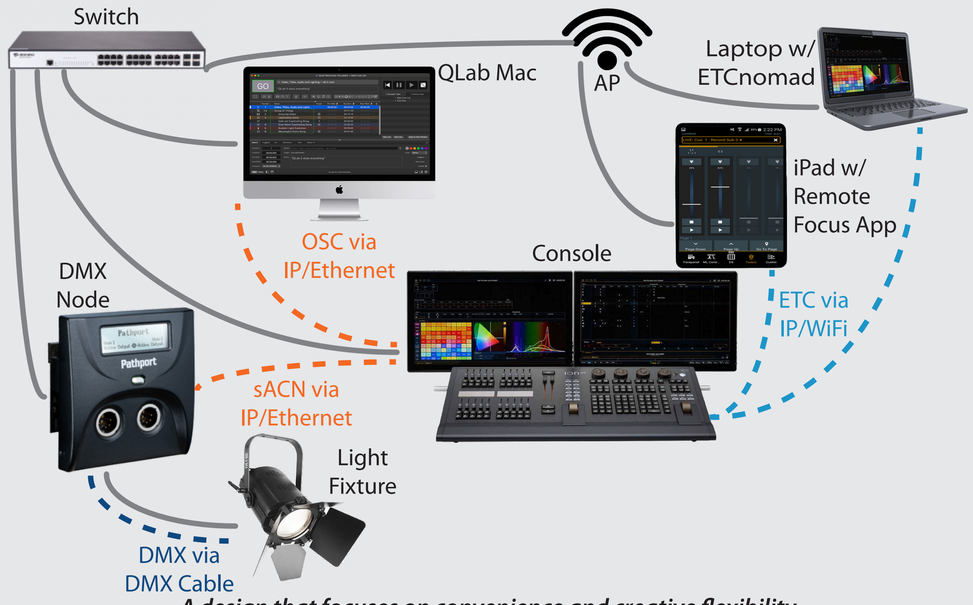
COLGATE

Brian Douglas, Jr. & Aaron Gember-Jacobson

Motivation

- Lighting control systems in theaters and concert venues increasingly rely on networked digital protocols, expanding their functionality—and their risk
- These systems often lack strong security protections, making them vulnerable to disruption, manipulation, or surveillance
- Motivated by the public safety and reputational stakes of compromised lighting systems, we conducted the first empirical study of lighting protocol vulnerabilities in the wild
- Our research aims to inform system administrators and support secure-by-design protocol development for entertainment infrastructure

Architecture of a System



A design that focuses on convenience and creative flexibility.

Protocols

sACN (Streaming Architecture for Control Networks)

- Sends fixture level data using multicast over Ethernet
- Prioritizes data with a numeric value per message

OSC (Open Sound Control)

- REST-like protocol for real-time cue triggering between devices
- Low-latency for cue synchronization

Proprietary Protocols (ETCnomad, iPad, etc.)

- Enables control of lighting consoles via desktop or mobile apps over WiFi
- Used for focus checks, cueing, and remote programming
- Widely accessible and officially supported by ETC across platforms

Vulnerabilities Identified

We identified vulnerabilities through a controlled experimental setup in Colgate University's new Experimental Exhibition and Performance Lab (EEP). The professionally installed system included an ETC EOS console, nodes, fixtures, sACN multicast traffic, and multiple remote control paths (OSC, WiFi apps).

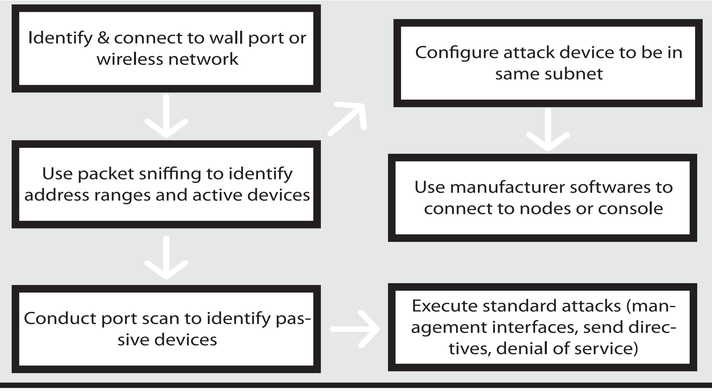
1.Console-Level Attacks

- ETC Eos software auto-discovers and connects to consoles on the same subnet, with no password required and allows changing cues, controlling fixtures, and deleting data
- Show Data Exfiltration of programmed cues, timing, and production data that is the property of the production and/or artist(s)
- OSC Command Injection (e.g., sending "/cs/playback/go") to trigger cues and adjust fixture levels remotely

2. Node-Level Attacks

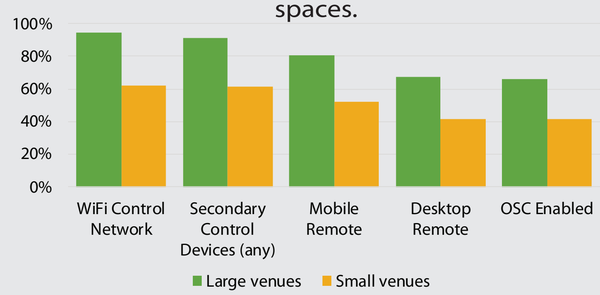
- Node Configuration Tampering using manufacturer software to modify settings (e.g. network configuration, universe mapping, etc.) or manipulate fixture levels
- Priority Message Spoofing to override legitimate sACN lighting control with higher-priority messages and prevent processing of legitimate control messages
- Flooding to overwhelm nodes with traffic on standard ports (e.g., 5568 for sACN)
- Exploiting default credentials or open services (SSH, Telnet) for operating system level control

Launching an Attack



Vulnerability Prevalence

We surveyed 333 lighting designers and theater technicians recruited via Facebook groups and forums. Responses spanned universities, public theaters, touring venues, and commercial spaces.



Among venues with 600+ capacity, 98% were vulnerable

We also performed a site visit to a small liberal arts college theater under show conditions.

- Confirmed the ability to connect using publicly accessible network jacks (such as in audience areas), capture traffic, and identify subnets and devices
- When the console was powered on, we could mirror its controls or override it using a virtual console
- Even powered-off, we controlled nodes using our own virtual console and injected sACN messages
- Accessed an ETC Paradigm house-light control system, via an unauthenticated web interface, to disable wall switches and force a hard restart using malformed code injection

Recommendations

- Networks need to be difficult to penetrate
  - Hiding SSID is not a method of security
  - Robust WiFi passwords
  - No enabled ports in public areas
- Networks need to be segmented properly
  - When multiple departments share a network (e.g. lighting and sound) they need to each be on a properly-firewalled VLAN to contain an attack's impact
  - Minimize the ability for any one device to connect to other devices it does not need to (e.g. WiFi devices to connect to nodes)
- Protocols need to authenticate and encrypt
  - Initial authentication should occur for OSC and sACN to only accept messages from authenticated senders
  - Messages should be encrypted to prevent data exfiltration and spoofing
- Robust user-management for consoles including authentication and encryption of iPad and remote traffic