Auditing and Advancing the Cybersecurity of Traffic Signal Systems

Jacob Bednard, Dr. Fengwei Zhang

Computer and Systems Security Lab (COMPASS)

Computer Science

Opportunity and Significance

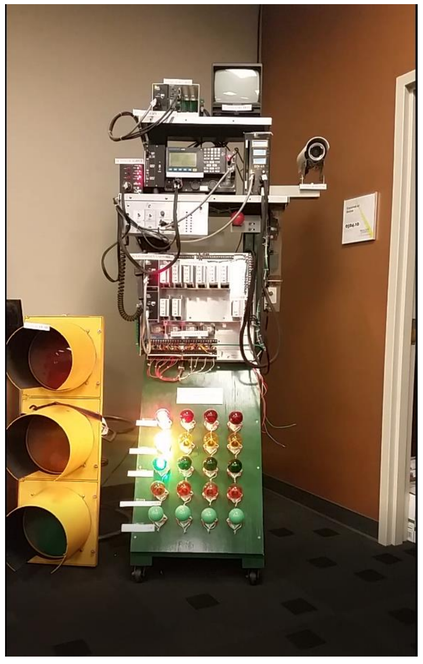
In recent years, traffic signal systems have welcomed numerous technological advancements that have been guided by the need for safe and efficient vehicle traffic flows in modern society. These advancements, accelerated by the introduction of affordable embedded computers, have given transportation officials the ability preform real-time remote modifications to traffic patterns in their search to accommodate ever-changing vehicle traffic flows. Unfortunately, improvements to traffic signal systems have not come without cost. In my research I looked to uncover cyber-security vulnerabilities that exist within traffic signals systems and specifically targeted the elusive “All-Directions Green Attack.” By exposing these vulnerabilities, it enables researchers to work with municipalities and manufactures to prevent cyberattacks before they happen.

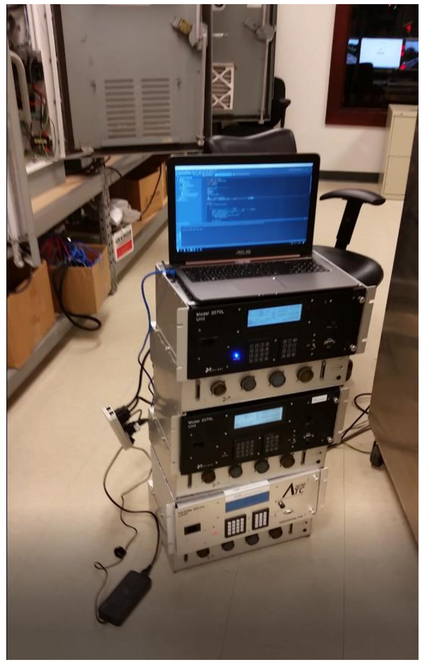
Technical Objectives

By utilizing existing municipal partnerships and access to Wayne State University’s Transportation Research Lab, researchers concluded an on-going exhaustive search for vulnerabilities and exploits contained within traffic signal systems. Specifically, researchers targeted devices contained within the NEMA TS-2 transportation standard. The NEMA TS-2 Standard [1] is commonly used across the United States as an architectural plan for implementing technology within traffic signal systems. Researchers will collect the results of the vulnerability analysis, inventory proof-of-concepts for exploits found, and provide thorough documentation regarding previous design decisions that have left traffic signal systems vulnerable.

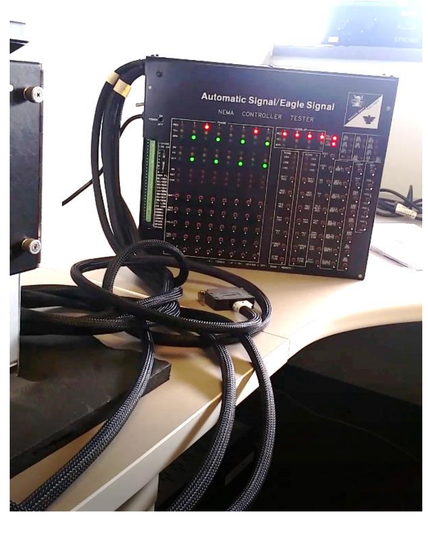
Partners

We would like to thank the Wayne State’s Transportation Research Group and the Research Opportunities for Undergraduates programs for support during our research. We would also like to thank the Macomb County Department of Roads and Oakland County Road Commission for their guidance during our research.





Research Partners of COMPASS



Approach, Accomplishments and Results

During our research we have uncovered that traffic signal systems face vulnerabilities due to key protocol flaws in the design of their standards. Due to these flaws we were able to reverse-engineer a Siemen’s Model 60 Traffic Controller and gain remote control of the system to control a traffic signal’s lights on-demand. Using this control, we showed that signal patterns were inherently safe. Ranging from simultaneously turning red-yellow-lights on, to all-directions flashing yellow, to flickering all-directions green lights, we found that these systems have the ability to put drivers at risk. Additionally, our attacks showed that we could effectively deploy ransomware to entire regions if precautions were not in place. This would leave a region with each intersection displaying all-directions red lights (or no lights at all). This attack would cost municipalities upwards of $2500 per intersection. We worked with Macomb County, Oakland County, and City of Detroit to remove this attack surface for their infrastructure.

Related Work and State of Practice

In 2014, research conducted by the University of Michigan[2] showed that traffic signal systems suffered from the risks of poor cybersecurity practice. In their findings, researchers showed that unsecured wireless networks supporting transportation systems could be exploited giving an attacker remote access to traffic control systems. With access, an attacker could manipulate traffic patterns at will. In addition, research performed by Cesar Cerrudo of IOActive showed that traffic signal systems could be exploited by utilizing a vulnerability found in common traffic signal vehicle detection peripherals[2]. This exploit effectively reduced the runtime length of specific traffic patterns causing significant vehicle traffic backups.

References

[1] NEMA TS 2-2003 (R2008) Traffic Controller Assemblies with NTCIP Requirements Version 02.06. https://www.nema.org/Standards/ComplimentaryDocuments/Contents%20and%20Scope%20TS%202-2003%20(R2008).pdf, 2012.

[2] Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. Green Lights Forever: Analyzing the Security of Traffic Infrastructure. In 8th USENIXWorkshop on Offensive Technologies (WOOT 14), San Diego, CA, 2014. USENIX Association.

[3] Cesar Cerrudo. Hacking US (and UK, Australia, France, etc.) Traffic Control Systems. IOActive Blog, 2014.