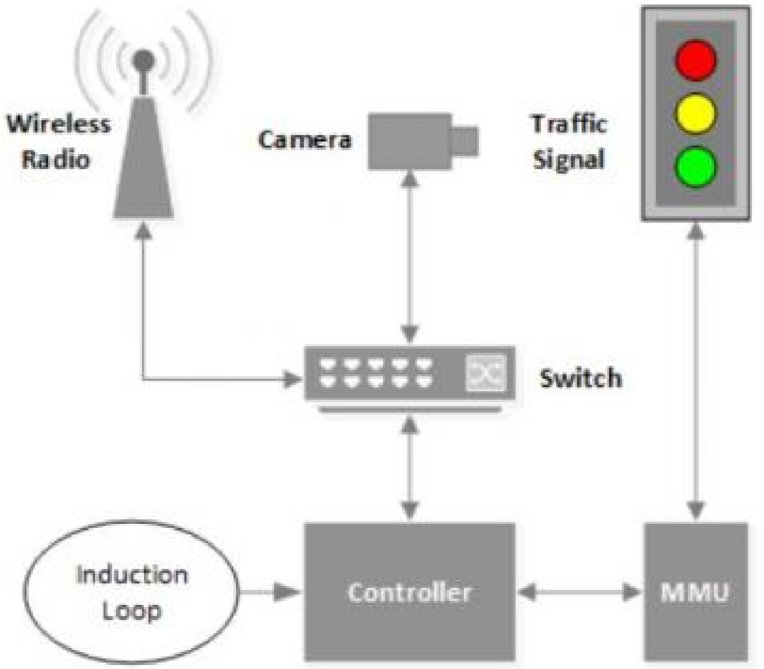
Michigan team finds security flaws in traffic lights

August 21 2014, by Nancy Owano



A typical traffic intersection. The radio connects to the switch and transmits controller diagnostics, live video feed, and other information back to the road agency. The malfunction management unit sits between the controller and lights and ensures that the lights are not put in an unsafe configuration. The controller adjusts light timings based on data from the induction loop. Credit: Branden Ghena, et al.

What if attackers could manipulate traffic lights so that accidents would happen with mayhem as the result? That is a question many would rather put off for another day but authorities feeling responsible for road safety are generally willing to consider all the what-ifs, assess their impact, and look for protective measures. According to a detailed report in Tuesday's MIT Technology Review, a road agency gave Michigan researchers permission to hack into almost 100 wirelessly networked traffic lights. The real news is what this electrical engineering and computer science team from the University of Michigan discovered. They saw three troubling weaknesses in the traffic light system they studied: unencrypted wireless connections, the use of default usernames and passwords that can be found online, and a debugging port easy to attack. Who is to blame? In their paper, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," which they will present at a computer security conference, they said no single device or design choice is at fault; the weaknesses instead "show a systemic lack of security consciousness.".

Overall, technology for traffic signals has delivered convenience and progress at a price. The authors noted that traffic signals were originally designed as standalone hardware, each running on fixed schedules, but they evolved into complex, networked systems. "Hardware systems that had previously been only physically accessible are now remotely accessible and software-controlled, opening a new door for attackers," they wrote.

How difficult would it be to break in? As MIT Technology Review said, "The Michigan researchers found that anyone with a computer that can communicate at the same frequency as the intersection radios—in this case, 5.8 gigahertz—could access the entire unencrypted network. It takes just one point of access to get into the whole system."

The team described types of scenarios possible, including a denial of service attack, where the normal functioning of lights would be stopped. More subtle manipulations could occur, as in manipulating the timings of an intersection relative to its neighbors. They said an attacker could also control lights for specific, personal gain. Lights could be changed to be green along the route the attacker was driving.

"Good approaches to improving security include enabling encryption on wireless networks, blocking non-essential traffic from being sent on the network, and regularly updating device firmware," they said. They believe the simplest solution with the greatest amount of impact would be changing the default credentials on all network devices.

Moving forward, there is good reason for further research. The authors believe what they discovered as security issues in traffic lights run across other systems. "An important area of research is the security of other critical infrastructure, such as the power grid and public water system. Much of this infrastructure has also undergone a phase change from independent nodes to a networked system and may have similar weaknesses."

Authors of the paper are Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. They said they were "extremely grateful to the personnel at the road agency who allowed us access to their network and hardware, but who, in the interest of protecting their infrastructure, wish to remain anonymous."

More information: Paper: Green Lights Forever: Analyzing the Security of Traffic Infrastructure (PDF): jhalderm.com/pub/papers/traffic-woot14.pdf

Citation: Michigan team finds security flaws in traffic lights (2014, August 21) retrieved 18 April 2024 from https://techxplore.com/news/2014-08-michigan-team-flaws-traffic.html