THE CONVERSATION
Academic rigour, journalistic flair

Traffic light hacking shows the Internet of Things must come with better security

August 22, 2014 6.12am BST

Confused? You will be if someone's making mischief with them. Julen Parra

Author

Bill Buchanan
Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University

The growing extent to which our day-to-day infrastructure is computer-controlled and internet-connected leaves it open to the possibility that malicious hackers could intercept data or take control of devices.

Often this sort of critical infrastructure is obvious, for example in electricity generation or supply, in large datacentres where hundreds or thousands of web-based companies are based, or in financial services. But often it is the least obvious elements that are most open to attack. For example, attacking the air conditioning system at a datacentre could cause catastrophic overheating of the computers there. Or affecting the control of traffic around a city or region, reducing roads to gridlock.

As we move towards a situation where computers control and optimise our lives using the data they record about us, our dependence on them grows, as does their vulnerability to failure. Protecting the

technology we rely on for our day-to-day lives from attack or failure must be a priority.

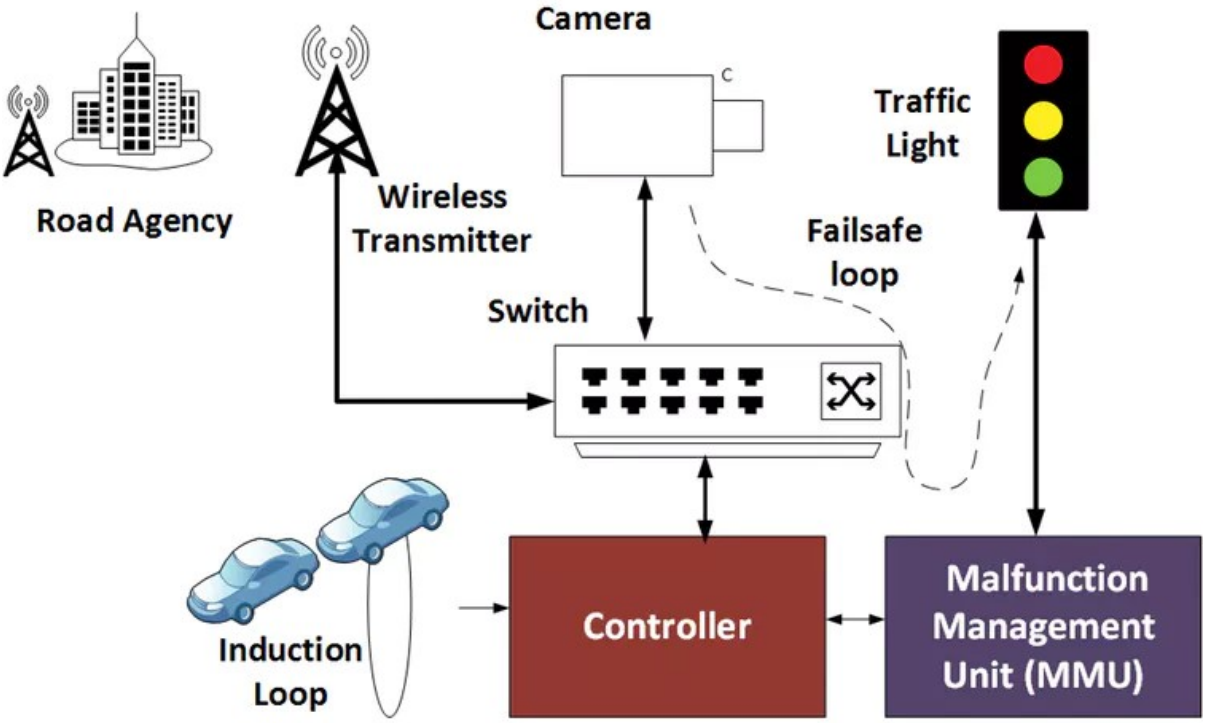
Traffic light hacking

To prove this point, a group of security researchers led by Alex Halderman at the University of Michigan published a report of how they managed to use a laptop and an off-the-shelf radio transmitter to break into and control more than 100 traffic light signals in Michigan City.

In order to be ethical in their approach they gained full permission from the road agency, and ensured there was no danger to drivers. The experiment was a test to see just how easily the traffic control infrastructure could be compromised.

In the US, the radio frequency used by traffic light controllers is typically in the industrial, scientific and medical (ISM) band at 900MHz or 5.8GHz. This means that the researchers were able to buy widely available wireless equipment to communicate with the devices.

What they found was weak wireless security with the use of open and unencrypted radio signals. This allows would-be intruders to eavesdrop on network traffic travelling over wireless radio signals to and from the traffic light controllers. In this way it's possible to see the usernames and passwords being used – and they found that the usernames and passwords used were in any case set to factory defaults, and could be easily found on the internet. The controllers also had a physical port for debugging at street level that was physically accessible and easily compromised.



How traffic lights are controlled. Bill Buchanan

Traffic light controllers are linked to an induction loop buried in the ground that monitors traffic passing through the junction, and to cameras that provide the colour of lights to the controller and, via radio transmitters, a live visual feed to road agency staff.

A malfunction management unit (MMU) ensures that the lights are not put into an unsafe state, such as showing red and green at the same time. The lights change colour according to the information the controller receives from the induction loop and camera, so that, if there is a good deal of traffic at the lights, the flow will be adjusted accordingly.

If malicious attackers can gain control of the MMU the lights can be forced into unsafe states or to steady red or steady green, which could cause traffic chaos citywide. The researchers found that just making a single connection between two wires would provide full control of the traffic lights.

Two many open doors

A typical security problem with many control systems is that there is often a physical connector known as a debugging port, used for troubleshooting, that is unsecured and provides easy access or information to attackers. A debugging port typically outputs status or error messages to devices connected to it, and from this information attackers can work out what electronic devices are being used and what software is being run. This provides vital information that helps an attacker find flaws or vulnerabilities that can be used to take control. It can also allow commands to be sent to the controller.

The researchers also found that the controller and MMU don't take any steps to verify that the messages they receive are from where they claim to be, and not from some other source. As the messages were not encrypted in any way, it was possible to analyse them and work out how to reproduce the correct commands, hijacking the channel and sending commands to operate the lights (a man in the middle attack). It was even possible to access the controller remotely, and ultimately the team was able to operate all the lights in the neighourhood.

They also found that you could attack the malfunction unit with incorrect signals to make it put the lights in a failure state, so for example all red - using a Denial of Service (DoS) method.

A metaphorical red light

Messing about with traffic lights may seem foolish, but this shows the system has several weaknesses, of design and implementation, that make it easy to attack. It's clear that security was not a major concern in how it was designed and built – and therein lies the problem. This is not a small issue; this type of system is used in more than 60% of the traffic junctions in the US.

If a malicious hacker wanted to bring a city to a standstill, this is how they could do it, fairly easily.

And this isn't just about traffic – there are many other types of critical systems infrastructure – telecommunications, power transmission, and others – that have been designed and installed over many decades with the same lax approach to security. Engineers need to start designing infrastructure that is secure by design, or it will be more than just traffic jams to worry about.

Hacking **Computer security** **Infrastructure** **Traffic light system**