Green Lights Forever: Analyzing the Security of Traffic Infrastructure

RAJSHAKHAR PAUL

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Introduction

❑Earlier

- Traffic signals were designed as standalone hardware

❑Now

- It has become more complex, networked system
- Traffic controllers store multiple timing plans
- Integrate various sensor data
- Communicate with other intersections

❑So, traffic signal system has improved in terms of

- wasted time
- environmental impact
- public safety

Introduction

- Connection between intersection:
  - Physical connection is costly
  - Wireless networking helps to mitigate this cost

- Maximum traffic areas now use intelligent wireless traffic management system
  - Allows real-time monitoring
  - Allows coordination between adjacent intersections

Introduction

- The improvements introduce unintended side effect

  - As the systems are remotely accessible and software controlled,

It opens a new door for the attackers

Contribution

- ❑ Performs a security evaluation of a wireless traffic signal system deployed in the US
- ❑ Discovers several vulnerabilities in both the wireless network and the traffic light controller
- ❑ Demonstrates several attacks against the deployment
- ❑ Provides some recommendations

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Anatomy of a Traffic Intersection

- The modern traffic intersection is a combination of
  - various sensors
  - controllers
  - networking devices

Sensors

- ❑Used to detect vehicles
- ❑Buried in the roadway
- ❑Some sensors detect vehicles by measuring a change in inductance due to the metal body
- ❑Video detection is the mostly used technique
- ❑In US, 79% of all vehicle detection systems are based on video detection
- ❑Other less common sensors are microwave, radar, ultrasonic sensors, etc.

Controllers

❑Typically placed in a metal cabinet by the roadside along with relays

❑Read sensor inputs and control light states

❑Sensors are typically directly connected to the controller

❑Intersection can be configured to operate in several different mode:
- Pre-timed mode: lights are controlled solely on preset timings
- Semi-actuated mode: side street is activated based on sensors, main street runs continuously
- Fully-actuated mode: both streets are operated based on sensor data

❑Controllers can function as an isolated node or as a part of an interconnected system

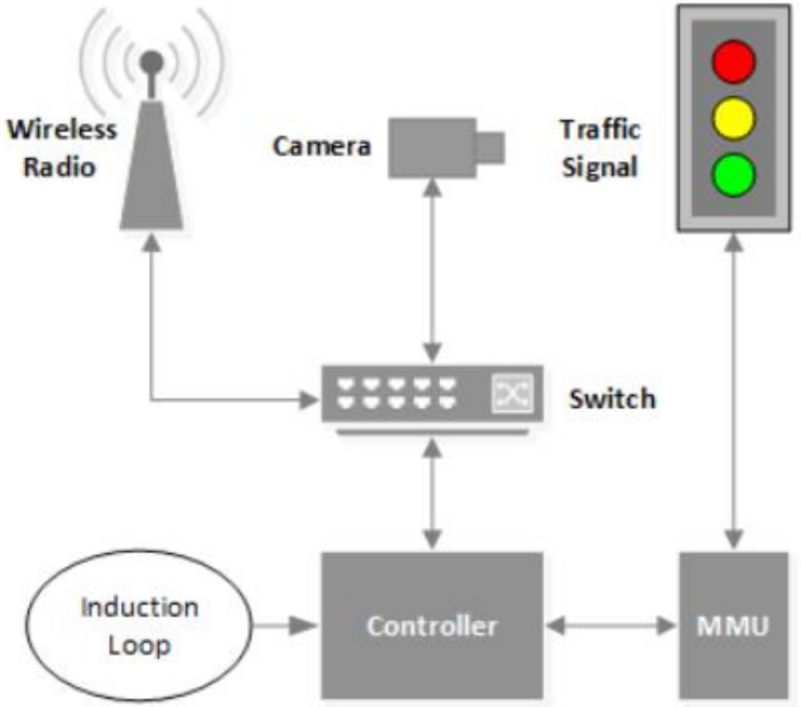
Communications

- Controllers can communicate with both each other and with a central server
- In dense urban areas, hard-wired communication through optical or electrical means is common
- When intersections are geographically distant, radios are used in point-to-point or point-to-multipoint configuration
- Radios commonly operate in the ISM band at 900 MHz or 5.8 GHz, or in the 4.9 GHz band

Malfunctioning Memory Unit (MMU)

- ❑Also known as Conflict Management Units
- ❑It is a hardware level safety mechanisms
- ❑Valid safe configurations are stored
- ❑If an unsafe configuration is detected, it overrides the controller and forces the light into a known safe configuration (like blinking reds)
- ❑Then the intersection enters a fault state and requires manual intervention to reset.

Typical Traffic Intersection



Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

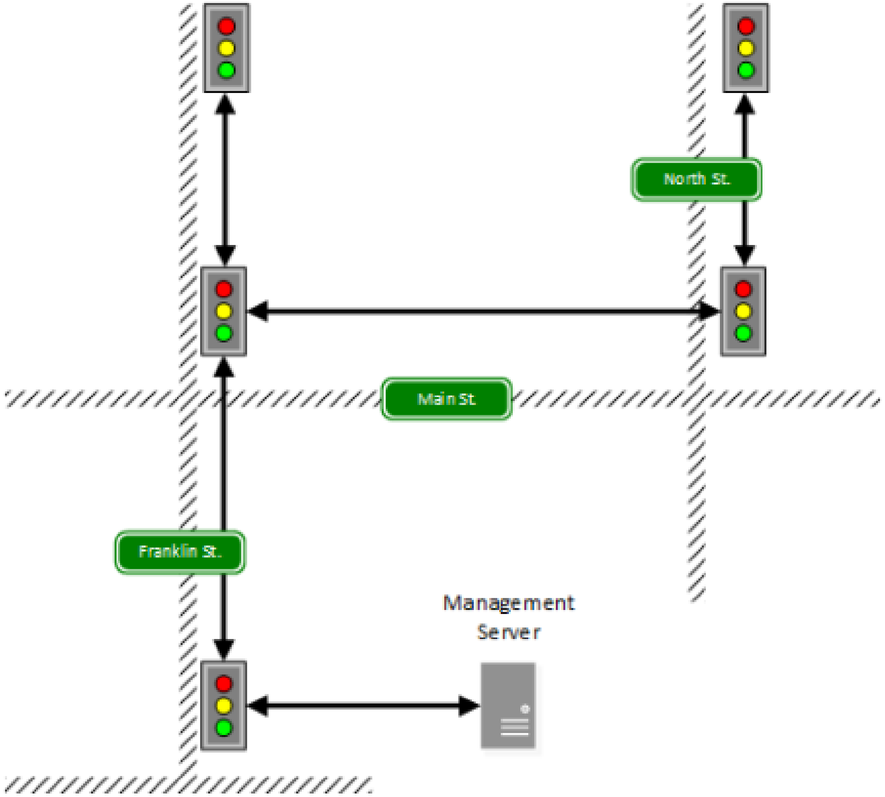
Broader Lesson

Conclusion

Case Study

- The study performed with cooperation from a road agency located in Michigan
- Report current traffic conditions to a central server
- This information can be used to make modifications in light timings of an intersection during traffic congestion
- Intersections operate in isolated mode and do not coordinate directly with one another

Example Traffic Signal Network



Existing Network Configuration

- One intersection act as a root node and connects back to management server under the control of road agency
- Intersections often have two radios
  - One slave radio to transmit to the next intersection towards the root
  - One master radio to receive from one or more child beyond it
- The system uses commercially available radios that operate on the ISM band at either 5.8 GHz or 900 MHz.
- 5.8 GHz radios are preferred as they provide higher data rates
- They communicate using a proprietary protocol (IEEE 802.11) to utilize point to point and point to multipoint connections
- They broadcast an SSID which is visible from standard laptops and smartphones
- The wireless connections are unencrypted and radios use factory default username and passwords

Existing Controller

❑All of the settings on the controller may be configured via physical interface on it

❑An FTP connection to the device allows access to a writable configuration database

❑This connection requires username and password which are fixed to default values that are published online by the manufacture

❑The controller runs the VxWorks 5.5 real-time operating system
- The default build settings leave a debug port open for testing purposes which has been marked as a vulnerability
-Connecting to the port requires no password and allows arbitrary reading and writing

Findings

❑Three major weakness have been discovered:

1. The network is accessible to attackers due to the lack of encryption
2. Devices on the network lack secure authentication due to the use of default usernames and passwords
3. The traffic controller is vulnerable to known exploits

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Threat Model

- Considering an attacker infiltrating the traffic network through its wireless infrastructure
- Assuming attacker has sufficient resources and motivation to monitor the network for extended period of time
- Assuming attacker does not have any physical access to any part of the traffic infrastructure
- With direct access to the traffic cabinet, the attacker can perform dangerous attacks

Accessing the Network

❑The attackers must first gain the access to the network. The process of gaining network access varies between radio types and configuration

❑5.8 GHz Radios:
- In the case of 5.8 GHz radios, any attacker with a wireless card capable of 5.8 GHz communication is able to identify the SSIDs of infrastructure networks
- Due to the lack of encryption, any radio that implements the proprietary protocol and has knowledge of the network's SSID can access the network

❑900 MHz Radios:
- Attackers requires the 16 bit slave ID value and network name.
- The authors haven't try to exploit this radio
- Brute force approach can be taken to determine the ID which could take several days

Accessing the Controller

❑Once in the network, there are two methods of accessing the controller
- The OS’s debug port
- The remote control capabilities of the controller

❑The authors use the open debug port of VxWorks OS
- It gives the attacker the ability to read and write arbitrary memory locations, kill tasks and even reboot the device
- The authors created a program to get access to the controller and also dump the entire contents of memory from the controller

Controlling the Lights

After gaining access to the controller there are number of methods to attack the device

The authors provide two primary attack vectors:
1. Malicious logic statements
- The logic processor on the controller allows an operator to plan actions that will be executed when conditions are met

2. Modified light timings
- Controller operation can also be modified by changing the timing values of light states
- MMU can prevent some attacks, but not all possible attacks (all way red lights, short duration of green lights, etc.)

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Types of Attacks

❑Denial of Service:
- Stopping normal light functionality (i.e. set all lights to red)
- The MMU may overcome the unsafe condition but the intersection will go under fault state which need manual intervention
- As remote attack possible, an attacker can disable traffic lights faster than technicians can be sent to repair that

❑Traffic Congestion:
- Attack can be possible to manipulate the timing of an intersection
- Could have real financial impacts on the society by wasting person-hours, safety, emissions and energy costs

Type of Attacks (contd)

❑Light Control:

- Attacker can control lights for personal gain
- Could create congestion

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Recommendations

Transportation department, traffic light operators, and equipment manufacturers can increase the security of their infrastructure in several practical ways

❑Wireless Security
- Many of the issues are because of wireless network configuration
- 5.8 GHz radios used in the deployment are more vulnerable to attack than 900 MHz radios
- SSID broadcasting should be disabled on the network
- 5.8 GHz radios supports WPA2 encryption which should be enabled in the field

❑Firewalls
- Radios and switch to put restrictions on network traffic whenever possible
- Only necessary communication should be allowed through
- Unused ports should be blocked to prevent attacks

Recommendations (contd)

❑ Firmware Updates

- Firmware of embedded devices should be kept up to date if the physical access of the device is possible
- Where physical access of the device is not possible (i.e. buried in the roadway), vendors should be clear with their customers about the weakness exist to take adequate measures.

❑ Changing Default Credentials

- Default credentials are often available on the internet thus provide no security whatsoever
- Device manufacturers should allow credentials to be changed

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Broader Lessons

The findings also carry some broader lessons

Network Trust
- Study shows lack of layered security in embedded systems
- Trusted network assumption would fail for a single vulnerability or misconfiguration

Hardware Failsafes
- Designer of embedded controller system should consider adding dedicated failsafe hardware when possible

Security Phase Change
- Devices that were purely electrical are now becoming computer controlled and even networked. So, exposing array of new security risk

Outline

Introduction

Anatomy of a Traffic Infrastructure

Case Study

Threat Model

Types of Attack

Recommendation

Broader Lesson

Conclusion

Conclusion

- Traffic control systems may have failsafe state. However, they are not safe from attackers
- With appropriate hardware and little effort, a traffic control system can be reconfigured
- Several types of attack including denial of services can be possible
- Practical solutions have been identified
- The discovered vulnerabilities in the infrastructure are not a fault of any one device or design choice, rather it is a systematic lack of security consciousness

Thank You