MICHIGAN ENGINEERING
UNIVERSITY OF MICHIGAN

COMPUTER SCIENCE
& ENGINEERING

Green Lights Forever

Analyzing the Security of Traffic Infrastructure

Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek,
and J. Alex Halderman

8th USENIX Workshop on Offensive Technologies (WOOT'14) – August 19, 2014

Motivating our investigation

Traffic Lights

Ubiquitous critical infrastructure





High-level overview of our findings

We evaluated an existing anonymous traffic infrastructure deployment

We discovered numerous issues with the system

- Both the road agency and vendors at fault

The real issue:

- An absence of security consciousness in the field

Outline

Anatomy of a traffic intersection

Security evaluation

Recommendations

How vehicles are detected

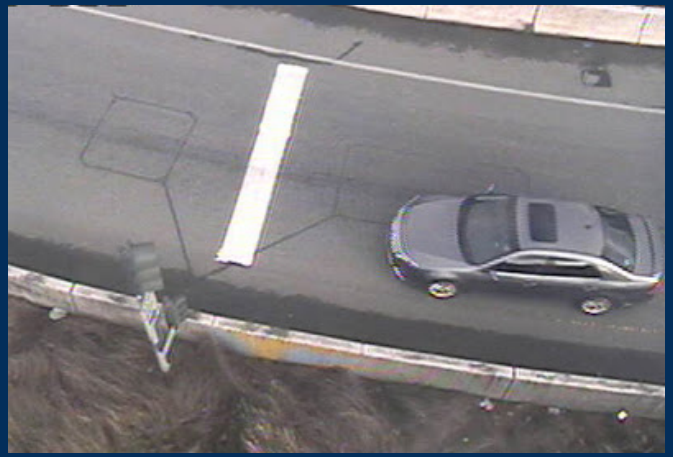
> 80% of intersections detect vehicles

Inductive sensors

- Wired and wireless

Video detection

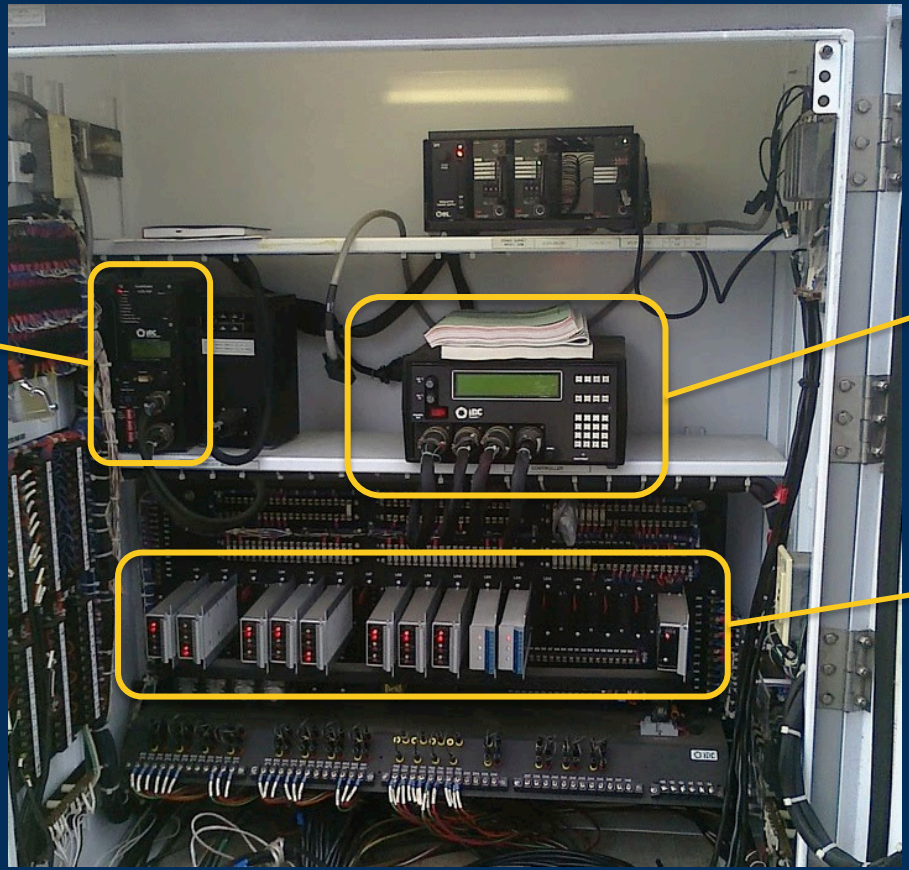
Microwave, Radar, Ultrasonic, etc.





Inside the traffic cabinet

Malfunction Management Unit (MMU)



Traffic Controller

Light Relays

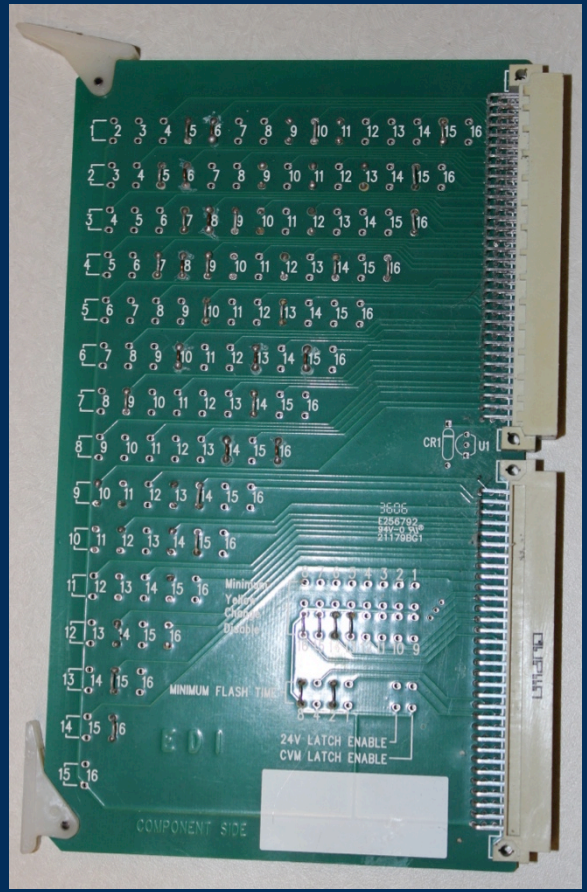
Malfunction Management Unit

Electrical failsafe

Hand-soldered configuration card
- Physical connections
- Whitelist of valid states

Invalid states trigger an override
- Goes to blinking red lights
- Requires manual reset

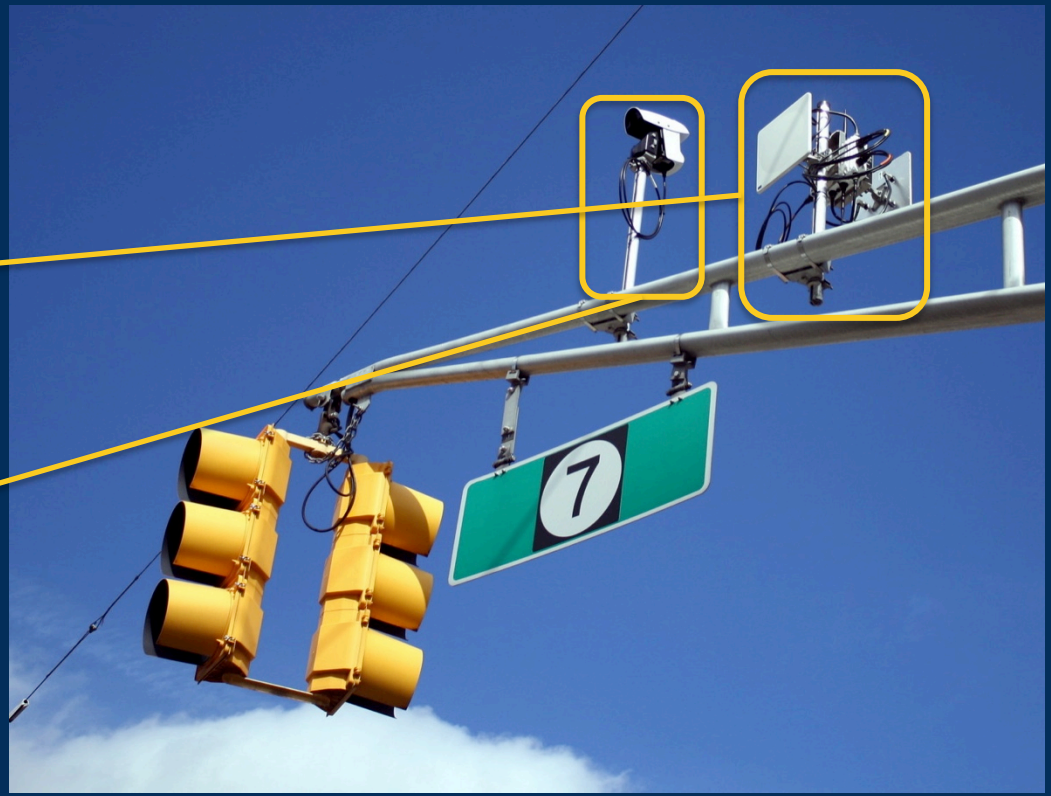
Stops 4-way green lights



Other intersection hardware

Radio communication
- Between controllers
- Back to main server

Video cameras
- Remote inspection



Overview of deployment

Collaborated with a road agency

- Urban area
- Approximately 100 lights total

Provided hardware for testing and access to deployment

- Initial testing all performed under a laboratory setting

As a condition of their involvement:

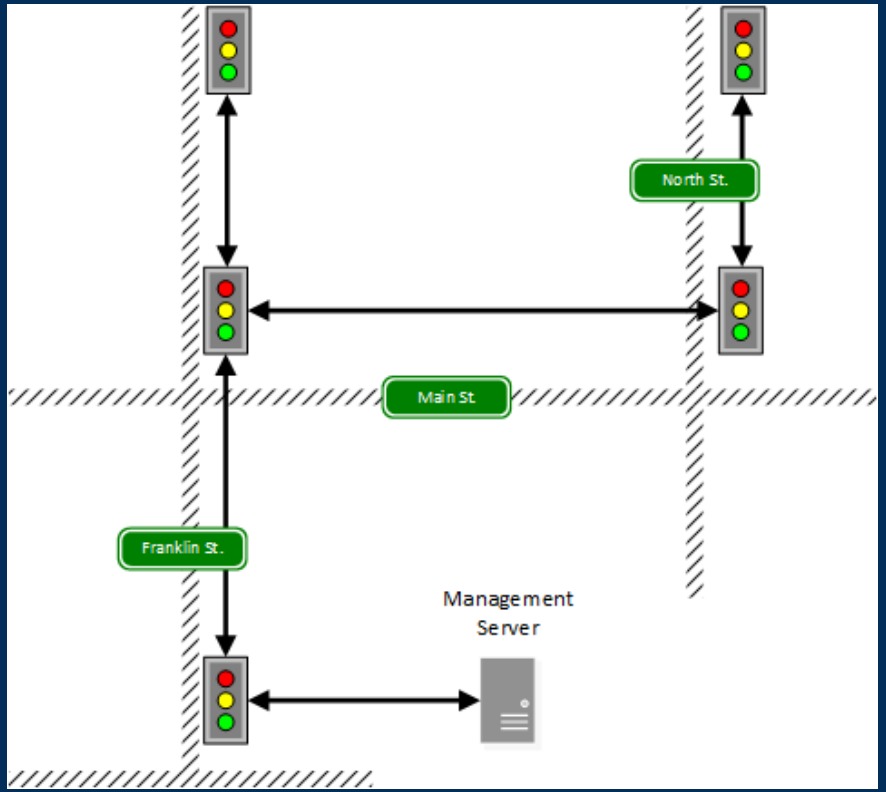
- Wish to remain anonymous and keep vendors anonymous

Deployment wireless network

Lights networked in a tree
- Single private network
- Data reporting only

Two communication bands
- 900 MHz
- 5.8 GHz

20 dBm with directional antennas



Findings – 900 MHz radios

No encryption enabled on connections

- Relies on proprietary protocol and frequency hopping
- WPA is possible

Default username and password in use

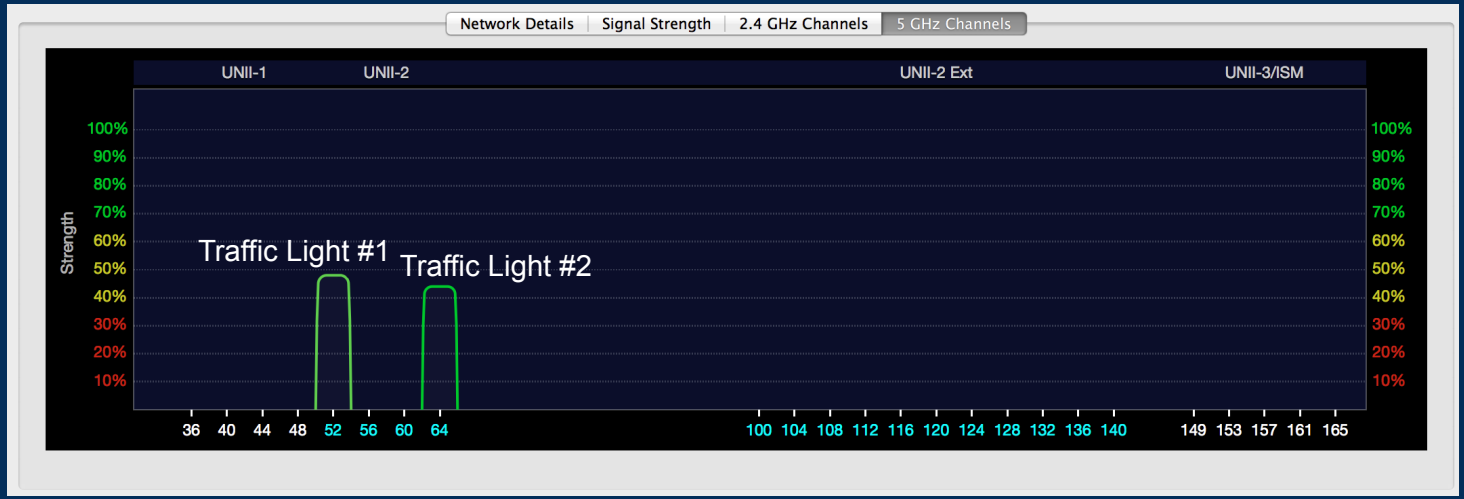
Vendor configuration software

- Requires default username and password to function

Findings - 5.8 GHz radios

Proprietary protocol

- Similar to 802.11 – still broadcasts an SSID
- Network name can be found on a standard laptop



Findings - 5.8 GHz radios

No encryption enabled on connections

- Relies on proprietary protocol
- WPA2 is possible

Default username and password in use

Vendor configuration software

- Allows password to be changed
- Assumes single password in use throughout deployment

Connecting to the network

How difficult is it?

1. Purchase 5.8 GHz radio from same vendor
2. Open laptop and find network SSID
3. Enter SSID into radio configuration as roaming slave

Network access at any point allows communication with all traffic light controllers in the deployment

Findings – Traffic controller

Usually controlled physically from the front panel

- No username or password by default
- Access control can be enabled, but is not simple

FTP server with database file for settings

- Unchangeable default username and password

Findings – Traffic controller

Runs VxWorks real-time operating system

- Default build leaves a debug port open
- Controller we tested was vulnerable
- Arbitrary access to read and write memory

- Actually, the vendor had already fixed this issue
  - The patch report didn’t mention it
  - Road agency hadn’t gotten around to updating controllers

Findings – Traffic controller

NTCIP 1202

- National Transportation Communications for ITS Protocol
- Standard defining communications for traffic controllers
- SNMP can be used to manage devices
- Does not provide protection from unauthorized access

Vendor program for remote controller interaction

- Uses NTCIP 1202 to emulate front panel interactions
- Easy to sniff with Wireshark

Controlling the controller

We created a library of commands based on vendor program
- Arrow keys, Number keys, Main Menu button

We then created a C program to act as a “traffic controller shell”
- Can manually change settings on the controller
- Can also run scripts to automatically perform actions
  - Advance lights
  - Freeze lights
  - Trigger MMU

Putting it all together

We can now:

- Access the network
- Connect to the controller
- Change light states

Next, we wanted to try it out at a real light

Demonstration on Deployment

T-intersection

MMU defaults to blinking yellows on main road

Required supplies

5.8 GHz radio

Laptop

AC power



Demonstration on Deployment

Connected to network
Ran controller shell
Changed light on command

Also accidentally triggered MMU twice



What can an attacker really do?

Denial of service

- It’s easy to trigger the MMU to take over
- Requires a technician to manually reset the device

Traffic congestion

- Possible to change timings such that a road becomes backed up

Individual light control

- Speedy getaways just like the movies

Recommendations for road agencies

Follow basic security best practices

Need to enable encryption

- Proprietary protocols do not cut it

Hiding SSIDs is a good idea

Add firewalls to block access to ports you aren’t using

Keep firmware up to date

Change default usernames and passwords

Recommendations for vendors

Enforce security

Require strong wireless security options

Allow and expect usernames and passwords to be changed

Somebody needs to be thinking about security

Vendor Response

Traffic controller vendor responded:

The company “has followed the accepted industry standard and it is that standard which does not include security”

Worrying for future Vehicle-to-Vehicle/Infrastructure technologies

Concluding Remarks

The real problem here is a lack of security consciousness

Traffic lights underwent a phase change

- Timing electronics to computerized systems
- Standalone devices to wireless networks
- Security did not keep up

Ensuring security of critical infrastructure should be a top priority

Acknowledgements

Many thanks to the anonymous road agency personnel who allowed us access to their network and hardware

Questions?

Green Lights Forever: Analyzing the Security of Traffic Infrastructure

Branden Ghena	brghena@umich.edu
William Beyer	wbeyer@umich.edu
Allen Hillaker	hillaker@umich.edu
Jonathan Pevarnek	jpevarne@umich.edu
J. Alex Halderman	jhalderm@eecs.umich.edu

MICHIGAN ENGINEERING
UNIVERSITY OF MICHIGAN