# Auditing and Advancing the Cyber Security of Traffic Signal Systems

Jacob Bednard and **Fengwei Zhang**

COMPuter And Systems Security (COMPASS) Lab
Department of Computer Science
College of Engineering, Wayne State University

# Who Am I

- Assistant Professor, joined Wayne State in 2015
- Research in the areas of systems security, with a focus on trustworthy execution, transparent malware analysis, etc.
- PhD from George Mason University
- Mentoring COMPASS lab students
  - Who sometimes listen to me…
- Father of two little ones
  - Anna, 3-year old daughter
  - Henry, 9-month baby son

Detroit Zoo on 02/18/2018

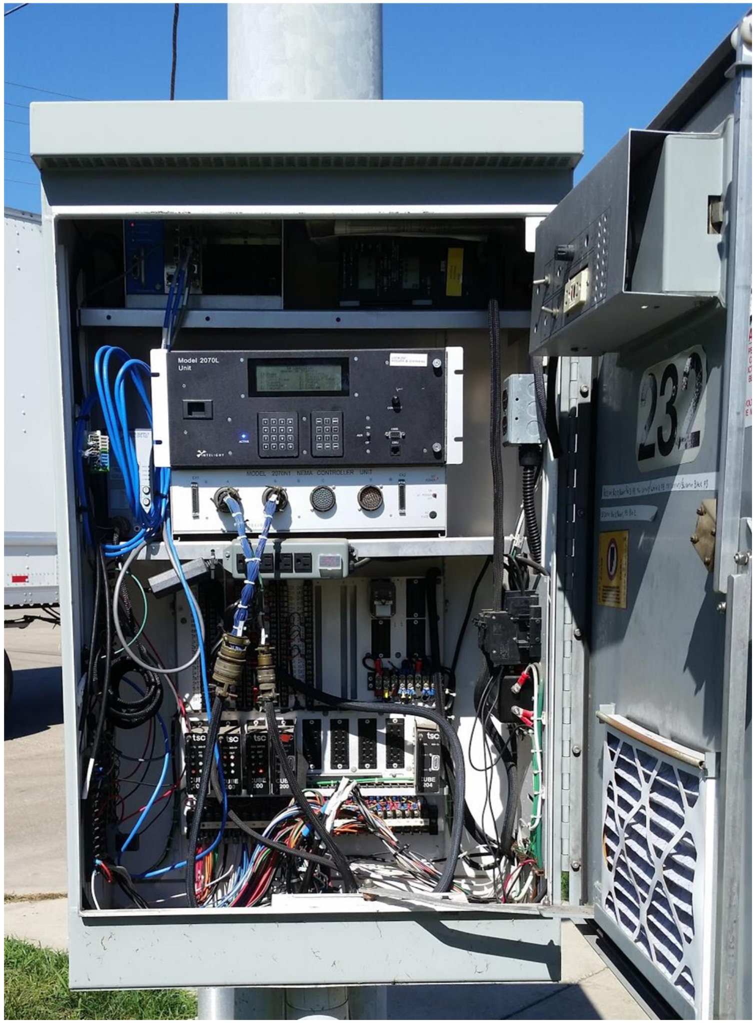
# Overview

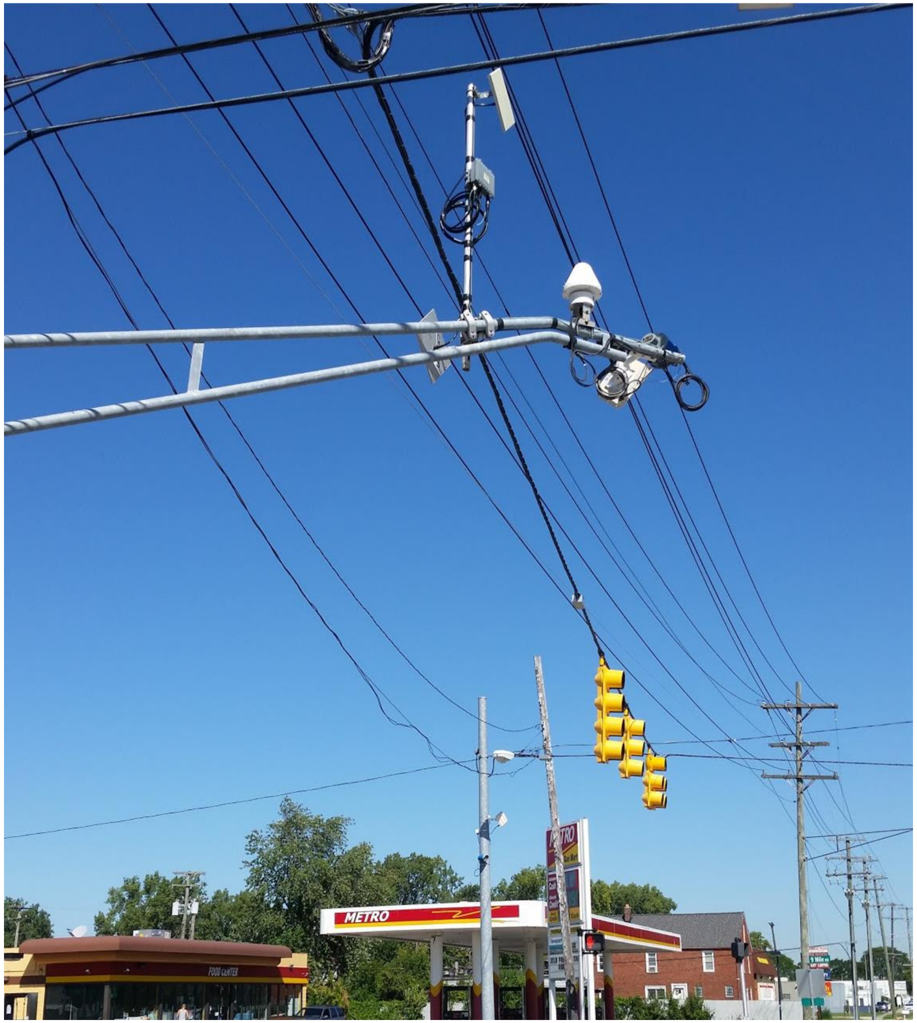
- Anatomy of a Traffic Intersection
- Attack Motivation & Considerations
- Attacks
- Defenses & Future Work

# Anatomy of a Traffic Intersection

What are traffic lights? *How do they work?*

# Traffic Intersection



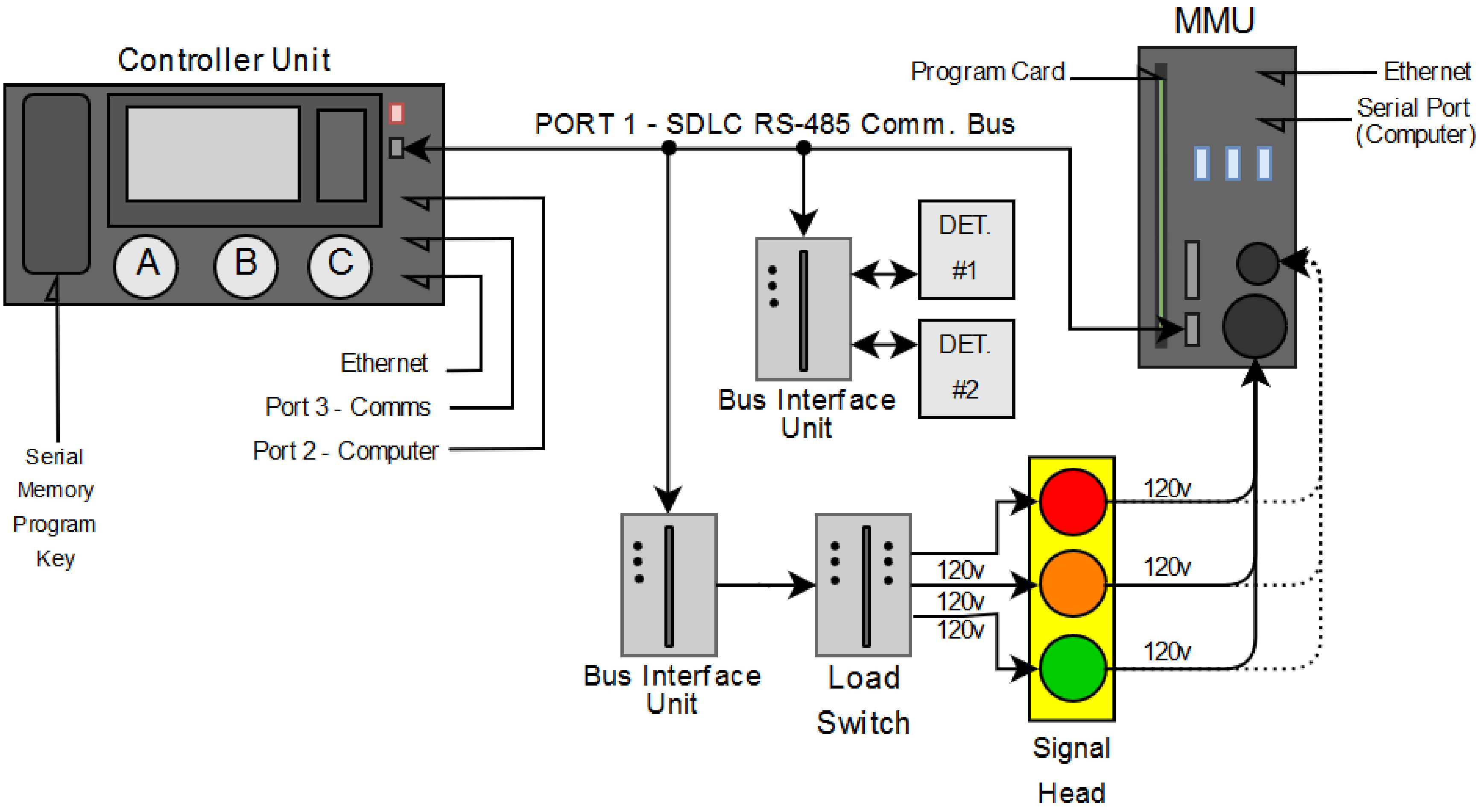


# Traffic Signal Cabinet

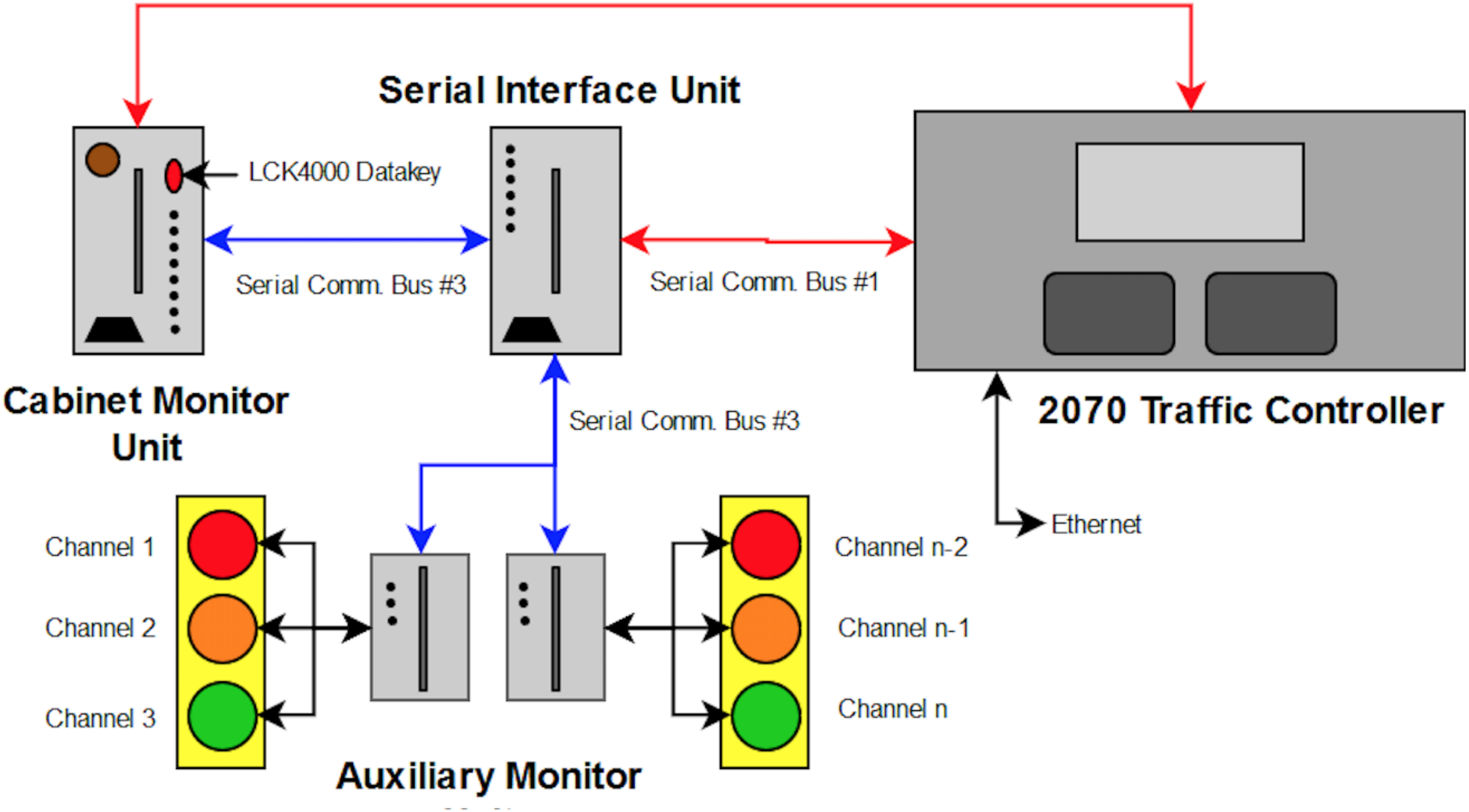
- Traffic controller unit
- Traffic signal fail-safe unit
- Multiple interface cards for communication
- Relays control electrical output to light bulbs

- Two traffic signal standards
  - NEMA TS 2 Cabinet standard
  - ITS Cabinet standard

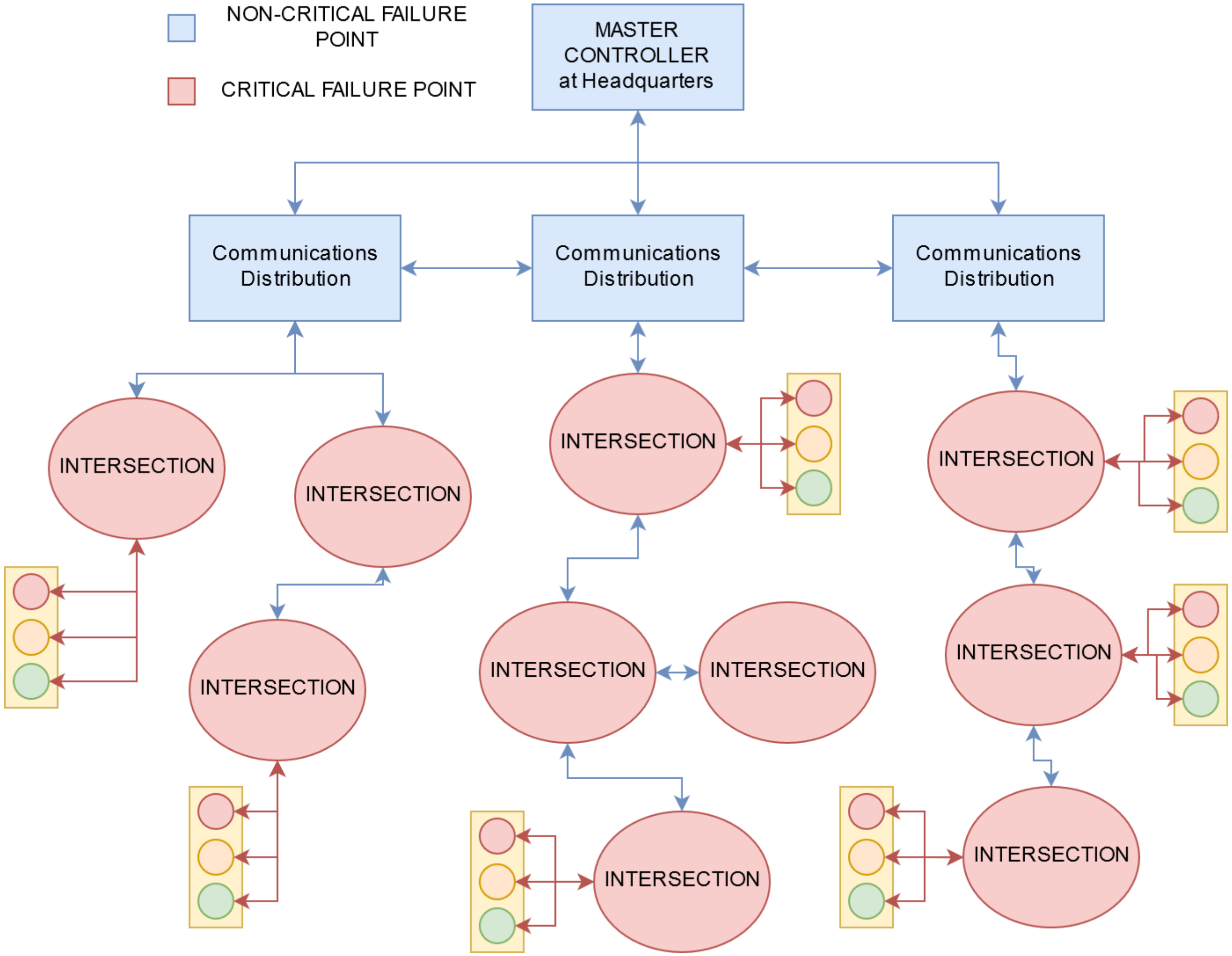
# NEMA TS 2 Cabinet Standard



# ITS Cabinet Standard



# Traffic Control Network



# Traffic Control Center

# Motivation & Considerations

Why hack traffic lights?

*I don’t see the financial gain...*

WIRELESS
PHONE
ENVIRONMENT
DRIVING
RESPONSIBILITY
FUTURE
HIGH-TECH
DREAMS
DRIVER
ROBOTIC
SERVICES
TOOLS
SELF-DRIVING
CONSUMPTION
AUTO
DRIVER LESS
HACKING
COMMERCIAL AVAILABILITY
TESTING PHASE
DILEMMAS
FEATURES
VEHICLES
WEEKNESSES
BENEFITS
AUTONOMOUS
USABILITY
ACCIDENTS
SAFETY
APPS
CONTROL SYSTEM
RESULTS
RISKS
OBSTACLES
QUESTIONS
PILOT
CARS
USABILITY
ROAD
CAR
REACTION TIME
www.shutterstock.com · 661074013

THIS LIGHT
NEVER TURNS
GREEN

# Attacks

Okay, how do I hack traffic lights?

# PHYSICAL ACCESS

NORTHSTAR
586-615-5186
POLICE
BOSCH

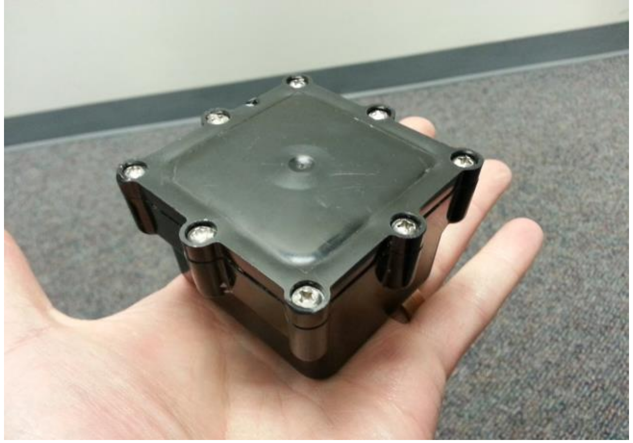
# Okay, those are all… non-stealthy

# REMOTE ACCESS

# Ceaser Cerrudo and Sensys Pucks

- Cerrudo hacked unsecure Sensys vehicle detection pucks through unencrypted WIFI

- Showed that he could manipulate the minimum and maximum green-durations at intersections

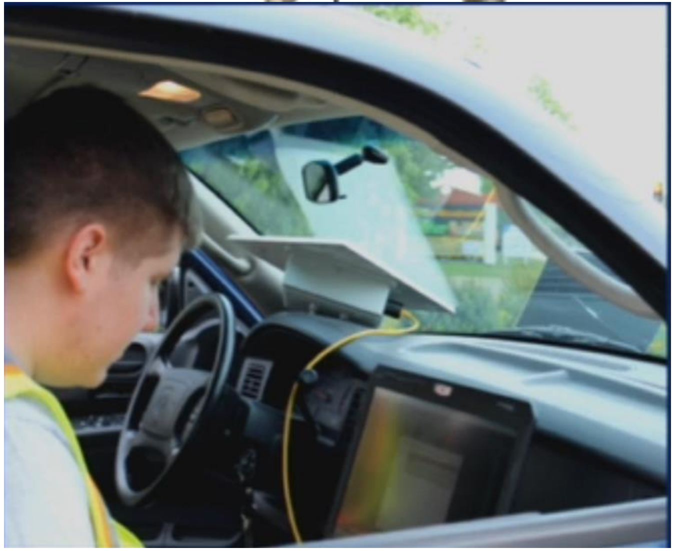


# Ghena and Unsecured 802.11

- Ghena found a municipality used unsecured wireless 802.11 WIFI networks to transmit data. (No Passwords)

- Found unsecured debug port on traffic controller VxWorks OS and unsecured NTCIP port.

- Proved basis for putting intersection into conflict flash on-demand (remotely)

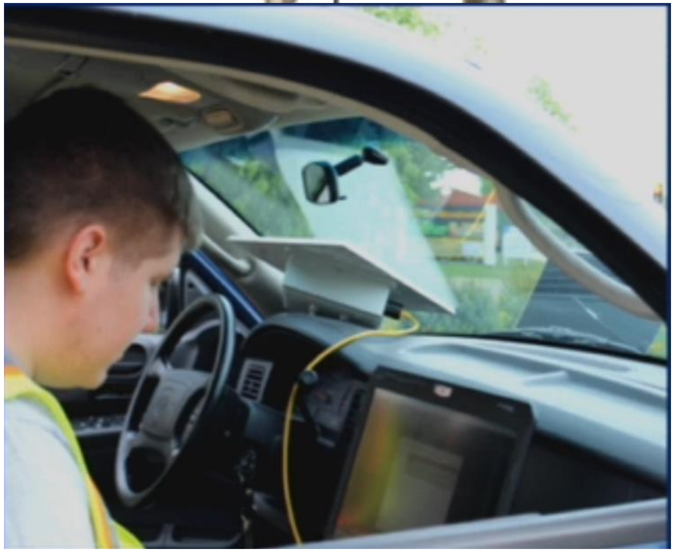


# Ghena and Unsecured 802.11

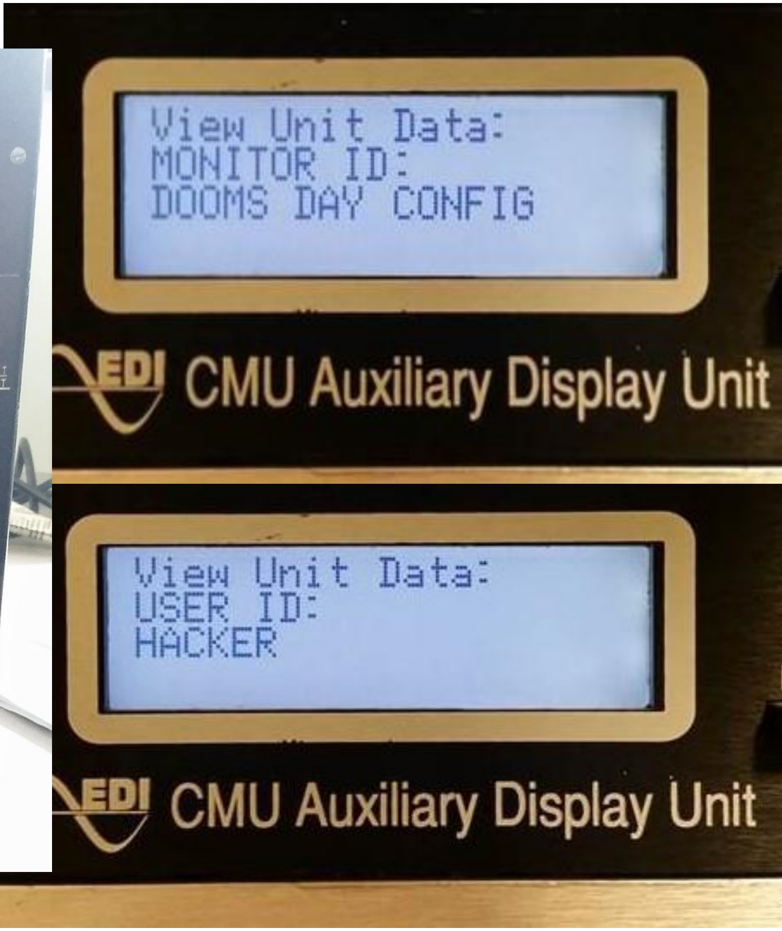
- Ghena found a municipality used unsecured wireless 802.11 WIFI networks to transmit data. (No Passwords)

- Found unsecured debug port on traffic controller VxWorks OS and unsecured NTCIP port.

- Proved basis for putting intersection into conflict flash on-demand (remotely)



# More Attacks



View Unit Data:
MONITOR ID:
DOOMS DAY CONFIG

View Unit Data:
USER ID:
HACKER

EDI CMU Auxiliary Display Unit
EDI CMU Auxiliary Display Unit

# Defense

Okay, now I’m terrified to drive...

*How do we prevent this?*

# Defense

DONT USE DEFAULT PASSWORDS

# Defense

DONT USE DEFAULT PASSWORDS

# Defense

DONT USE DEFAULT PASSWORDS

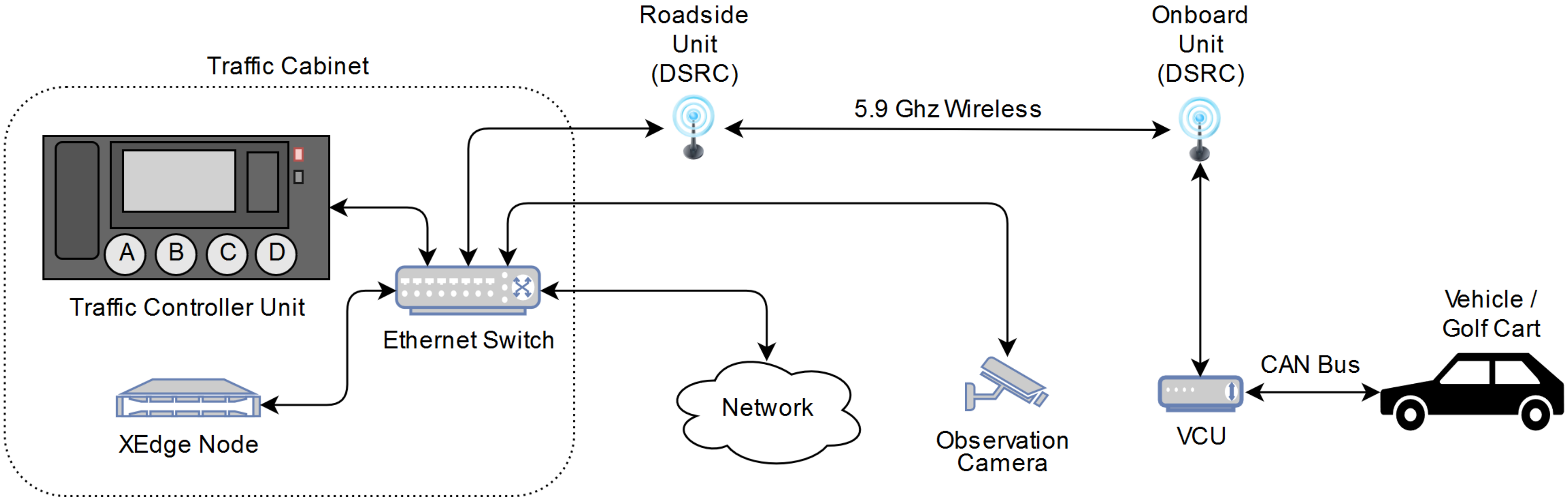
# Defense

DONT USE DEFAULT PASSWORDS

# Defense

- Use least privilege principle
- Update to the latest software
- Harden the monitoring and detecting mechanisms (CMU datakey firmware should not be modifiable)

# Future Work


Traffic Cabinet
A
B
C
D
Traffic Controller Unit
Ethernet Switch
XEdge Node
Roadside
Unit
(DSRC)
5.9 Ghz Wireless
Onboard
Unit
(DSRC)
Network
Observation
Camera
VCU
CAN Bus
Vehicle /
Golf Cart

# References

- 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.
- ITS Cabinet Standard: Intelligent Transportation System (ITS) Standard Specification for Road-side Cabinets, v01.02.17a.www.ite.org/standards/atc/ITS_Cabinet_v01.02.17a.doc, 2003.
- Cesar Cerrudo. Hacking US (and UK, Australia, France, etc.) Traffic Control Systems. IOActiveBlog, 2014.
- Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. GreenLights Forever: Analyzing the Security of Traffic Infrastructure. In8th USENIX Workshop on Offensive Technologies (WOOT 14), San Diego, CA, 2014. USENIX Association.

# Questions?

# THANK YOU!

Email: fengwei@wayne.edu

Homepage: http://fengwei.me