Understanding the Security of Traffic Signal Infrastructure

Zhenyu Ning, Fengwei Zhang, and Stephen Remias

COMPASS Lab
Wayne State University

WAYNE STATE
UNIVERSITY

DIMVA, June 19, 2019

Outline

WAYNE STATE UNIVERSITY

- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

Outline

WAYNE STATE UNIVERSITY

Introduction

WAYNE STATE UNIVERSITY

Traffic signal systems have introduced large regional networks and operation centers to help alleviate traffic congestion.

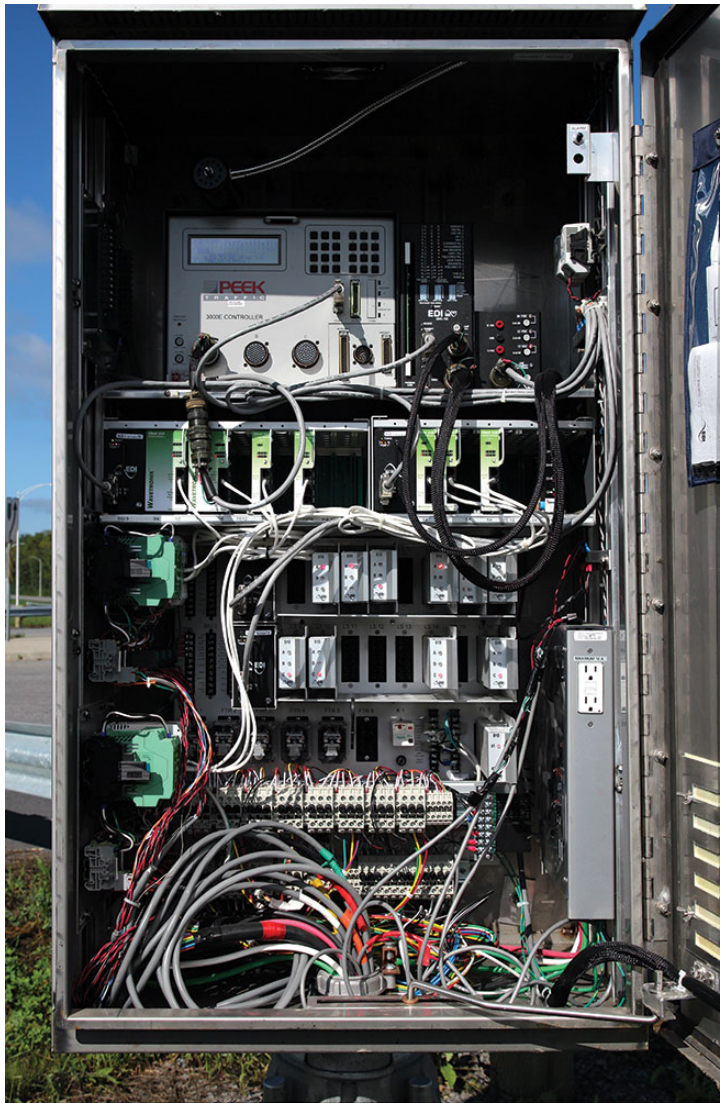
- Traditional traffic signal systems use rotating gears and wheels to control the traffic bulbs.
  - Simple, but lack of flexibility.

- Modern traffic signal systems have achieved a efficient control over the vehicle traffic via numerous technologies.

Modern Traffic Signal System

source: https://www.orangetraffic.com/product/mtq-traffic-light-distribution-and-control-cabinet/

Modern Traffic Signal System



source: https://www.orangetraffic.com/product/mtq-traffic-light-distribution-and-control-cabinet/

Introduction

WAYNE STATE UNIVERSITY

Is it secure?

WAYNE STATE UNIVERSITY

Is the traffic signal system secure?

- Previous research mainly focus on the traffic controller and network vulnerabilities.
  - [1, 2, 3]

- However, traffic signal systems are actually comprised of many components!
  - E.g., traffic controller, fail-safe systems, surveillance cameras, et, al.

Outline

WAYNE STATE UNIVERSITY

- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

Roadside Cabinets

WAYNE STATE UNIVERSITY

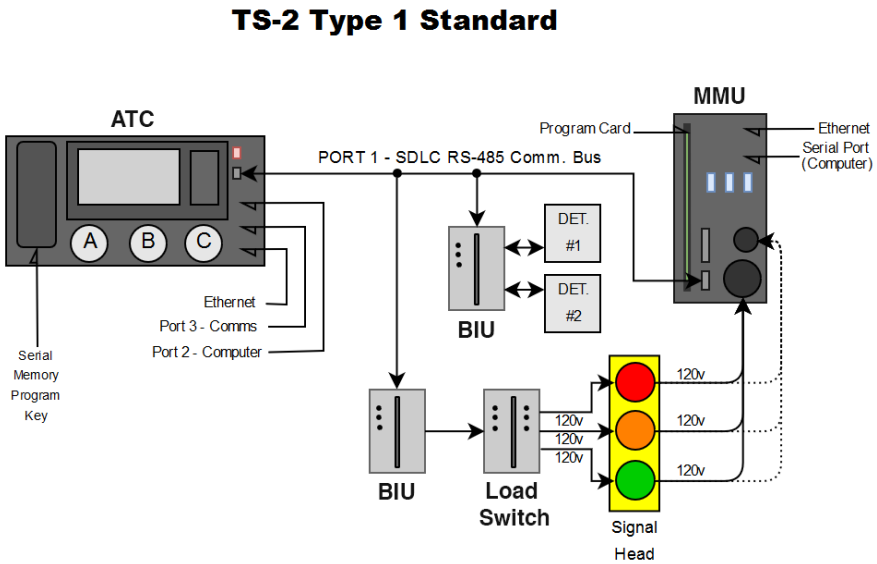
- A modern traffic signal systems is comprised of many hardware components.
- These components are normally placed in a roadside cabinet.
- Cabinet standards are applied to the components inside the cabinet.
  - TS-2 cabinet standard and ITS cabinet standard.

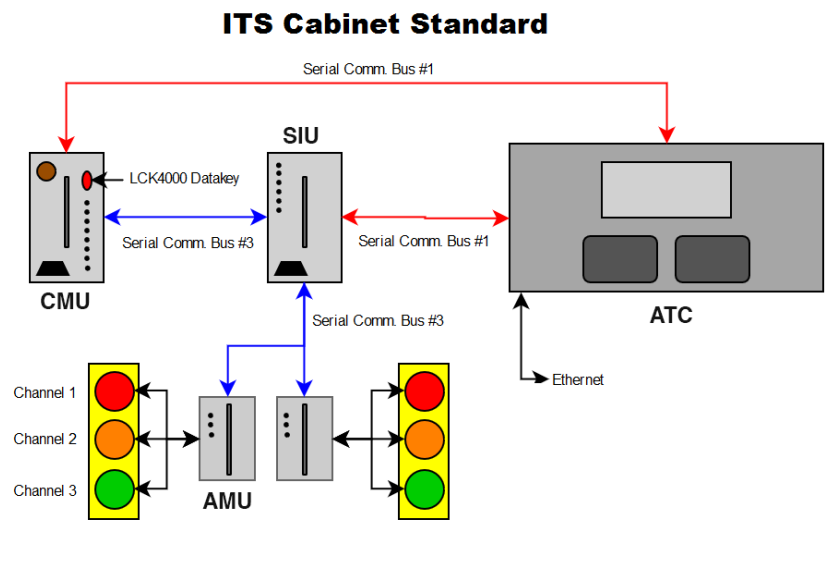
Cabinet Standards

WAYNE STATE UNIVERSITY

- The **TS-2 Cabinet Standard** was initially commissioned by National Electrical Manufacturers Association (NEMA) in 1998.
  - A replacement of NEMA TS-1 standard.
  - Using serial communication to replace hardwired I/O.
- The **ITS Cabinet Standard** is designed to supersede the NEMA TS-2 standard.
  - Published by American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), and NEMA.

Cabinet Standards





Advanced Transportation Controller

WAYNE STATE UNIVERSITY

The Advanced Transportation Controller (ATC) is the core part for a traffic signal control system.

- Build upon a Linux kernel with BusyBox.
- Directly controls the traffic signals with specific software.
- E.g., Intelight Model 2070 ATCs and Siemens Model 60 ATCs.

Fail-safe Components

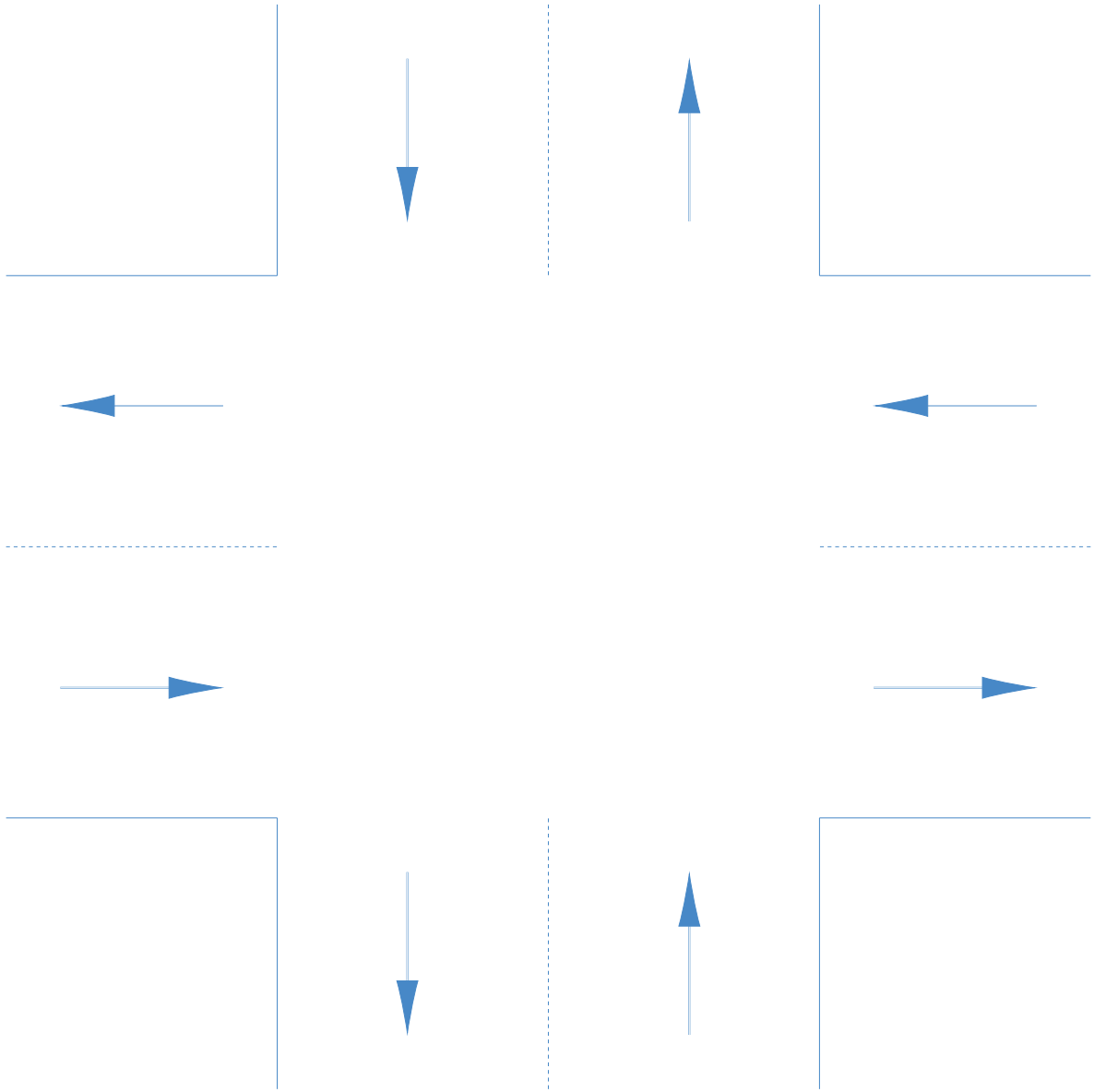
WAYNE STATE UNIVERSITY

The fail-safe components are used to guarantee that the traffic signals would not turn to a dangerous state even when the ATC is malfunctional.

- Malfunction Management Unit (MMU) in TS-2 Standard.
- Cabinet Monitor Unit (CMU) in ITS Standard.

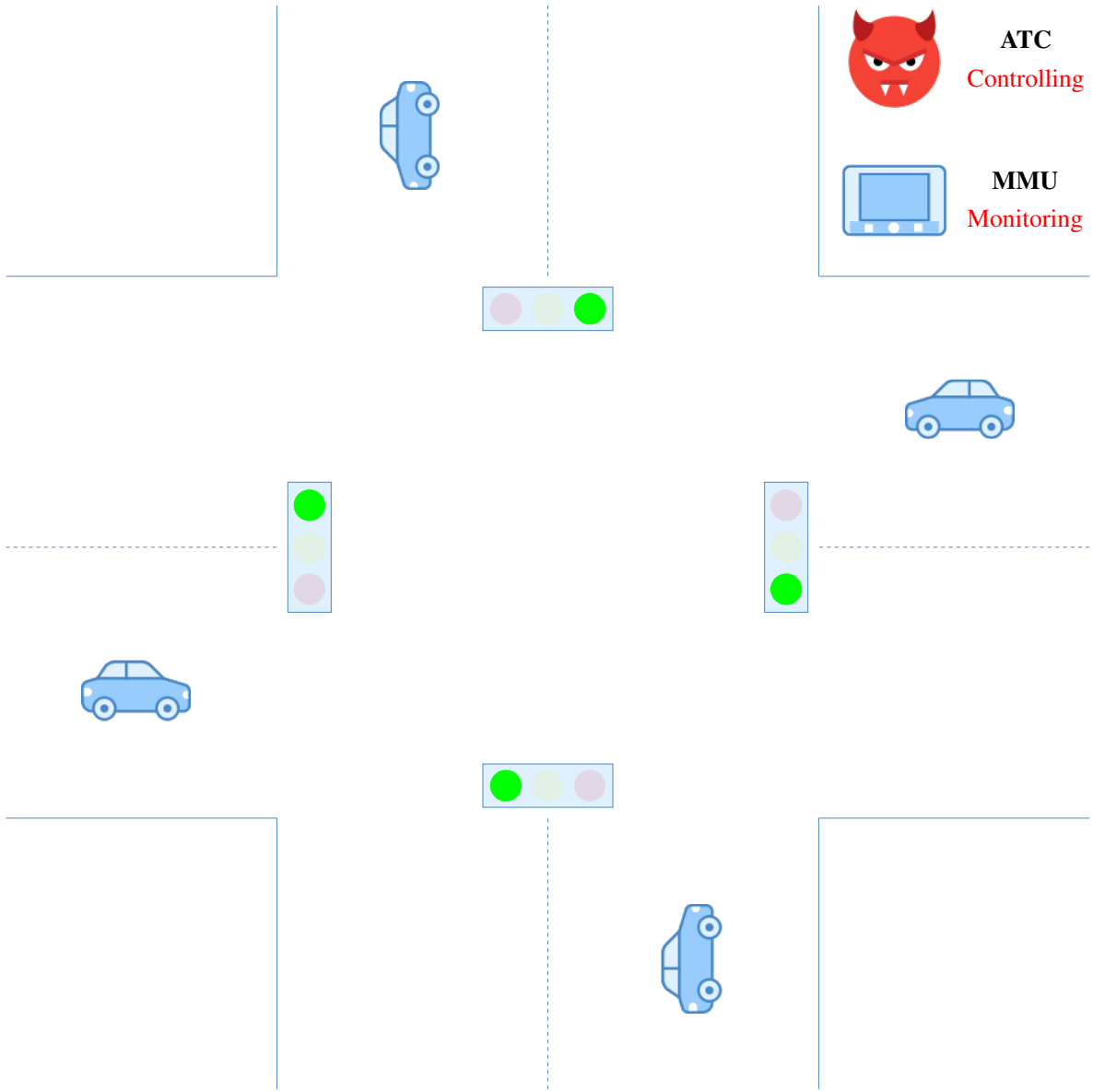
Fail-safe Components

WAYNE STATE UNIVERSITY



Fail-safe Components

Fail-safe Components



Fail-safe Components

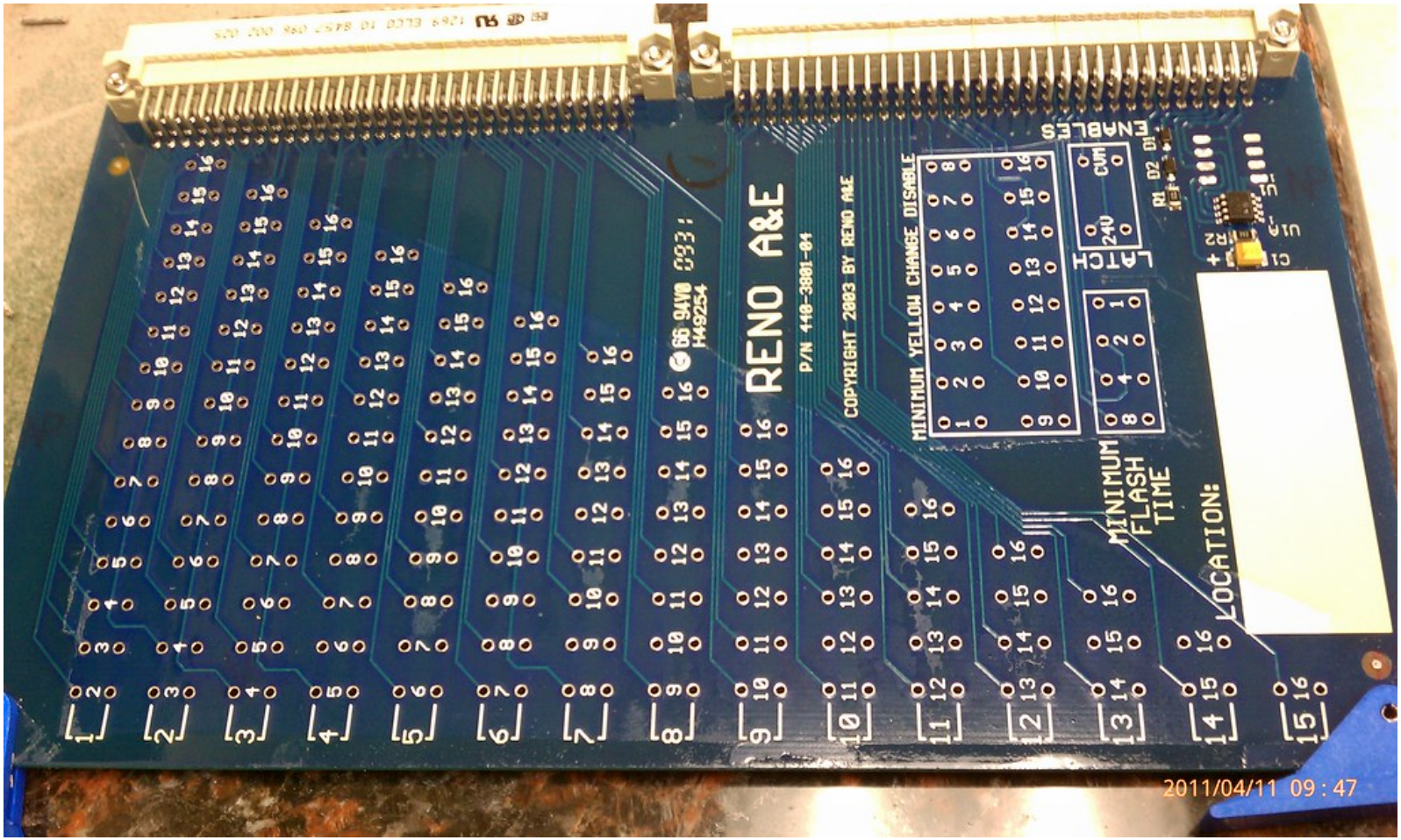
Fail-safe Components

WAYNE STATE UNIVERSITY

The conflict status is predefined by **Programming Card** in MMU and **Datakey** in CMU.

- In Programming Card, the conflict status is defined by soldered wire jumpers.
- Datakey is an EEPROM memory device.

MMU Programming Card



source: https://www.flickr.com/photos/robklug/5617557995/in/photostream/

CMU Datakey

WAYNE STATE UNIVERSITY

source: https://manualzz.com/doc/8353064/888-1212-001-monitorkey-operation-manual

Outline

WAYNE STATE UNIVERSITY

- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

Security Analysis

WAYNE STATE UNIVERSITY

- Methodology: Partnering with a municipality in USA.
- Analysis Environment:
  - A standard traffic signal system in our lab.
  - The traffic signal system lab in the municipality.
  - The deployed traffic signal system in the municipality.
- Devices:
  - TS-2 cabinets with Siemens Model 60 ATC and EDI MMU-16LE.
  - ITS cabinets with Intelight Model 2070 ATC and CMU-212.

Security Analysis

WAYNE STATE UNIVERSITY

How to attack the system?

Security Analysis

WAYNE STATE UNIVERSITY

How to attack the traffic signal system?

- Step 1 – Access the Traffic Signal System
- Step 2 – Control the Traffic Signals
- Step 3 – Bypass Fail-Safe Components
- Step 4 – Hide Yourself

Security Analysis

WAYNE STATE UNIVERSITY

How to attack the traffic signal system?

- Step 1 – Access the Traffic Signal System
- Step 2 – Control the Traffic Signals
- Step 3 – Bypass Fail-Safe Components
- Step 4 – Hide Yourself

Physical Access

WAYNE STATE UNIVERSITY

Obstacles for accessing the traffic signal system physically:

- Surveillance Camera
- Cabinet Lock
- Cabinet Door Status Monitoring

Surveillance Camera

WAYNE STATE UNIVERSITY

According to the municipality officials,

- There are 750 vehicle intersections in the municipality.
- 275 vehicle intersections are covered by traffic cameras.
- More than 60% of the intersections are out of surveillance.

Cabinet Lock

WAYNE STATE UNIVERSITY

According to the cabinet specifications, both TS-2 and ITS cabinets shall be provided with a Corbin #2 key.

- However, the Corbin #2 master key is sold online.
- The sold key is marked with the ability to open most traffic signal cabinets in the United States.
- With $5 USD, we are able to open all cabinets in the municipality lab.

Cabinet Door Status Monitoring

WAYNE STATE UNIVERSITY

In the ITS cabinets, the status of the door can be monitored by the CMU.

- ATC send query message to CMU to get the door status.
- In real-world deployment,
  - The door alarm message is saved to log file by ATC.
  - The log file is forwarded to the municipality every one-to-five minute.

Physical Access

WAYNE STATE UNIVERSITY

Obstacles for accessing the traffic signal system physically:

- ~~Surveillance Camera~~
  60% intersections are out of surveillance
- ~~Cabinet Lock~~
  $5 USD for the master key
- ~~Cabinet Door Status Monitoring~~
  Non-real-time alarm

Remote Access

WAYNE STATE UNIVERSITY

- Previous work [3] has shown that the wireless communication network is vulnerable.
- We find that the both type of ATCs use default credentials for the SSH and Telnet.
  - The municipality were not aware of the ability to login to the ATC over SSH.
- The public IP addresses of a number of ATCs can be identified on Shodan [4] website.

Security Analysis

WAYNE STATE UNIVERSITY

How to attack the traffic signal system?

- Step 1 – Access the Traffic Signal System
- Step 2 – Control the Traffic Signals
- Step 3 – Bypass Fail-Safe Components
- Step 4 – Hide Yourself

Control the Traffic Signals

WAYNE STATE UNIVERSITY

With physical access,

- The signal pattern can be configured by the control buttons on the front panel.
- No authentication is activated in analyzed ATCs.
  - Access code can be set to control the access, but the partnering municipality didn't do so.

Control the Traffic Signals

WAYNE STATE UNIVERSITY

Normally, the traffic signals are controlled by specific software running in the Linux kernel via several serial ports. With remote access,

- Directly write commands to the serial ports.
  - Command specification is publicly available.
  - Communication is unencrypted.
  - No authentication is required.
- Manipulate the driver of the front panel.

Security Analysis

WAYNE STATE UNIVERSITY

How to attack the traffic signal system?

- Step 1 – Access the Traffic Signal System
- Step 2 – Control the Traffic Signals
- Step 3 – Bypass Fail-Safe Components
- Step 4 – Hide Yourself

Bypass Fail-Safe Components

WAYNE STATE UNIVERSITY

With physical access,

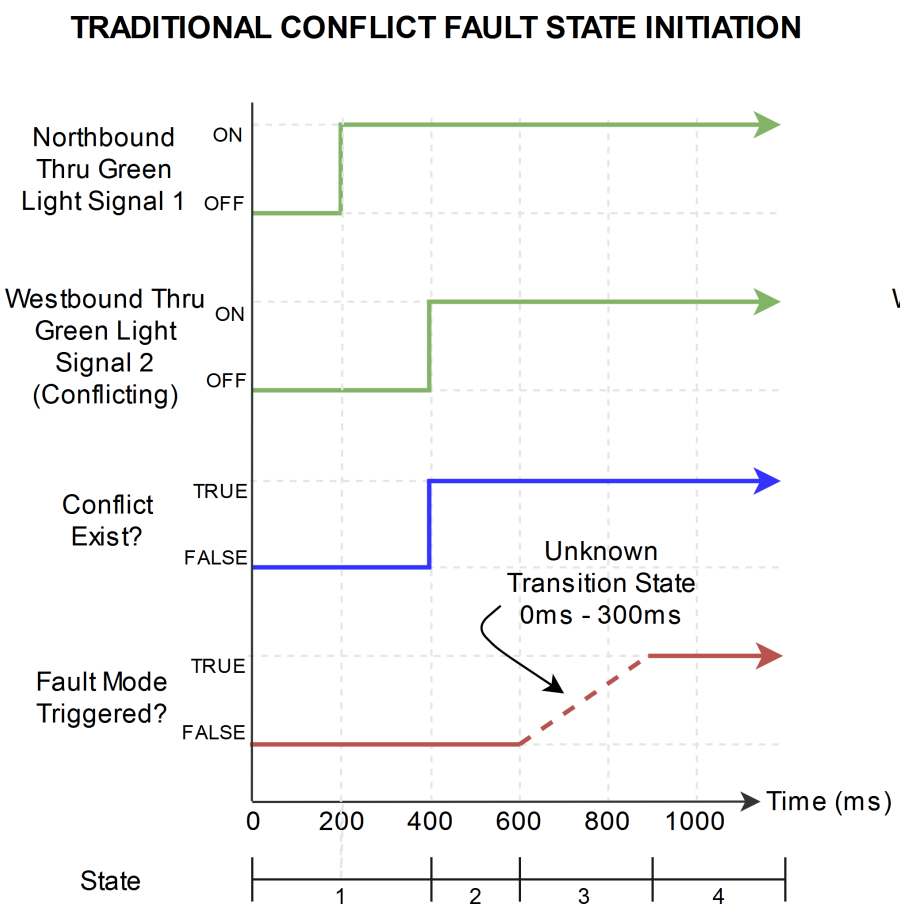
- For MMU, resolder the wire jumpers of the programming card.
- For CMU, reconfigure the parameters stored in the Datakey.
  - The configuration is unencrypted.
  - A customized Datakey access tool can be built by an Arduino Uno starter-kit.

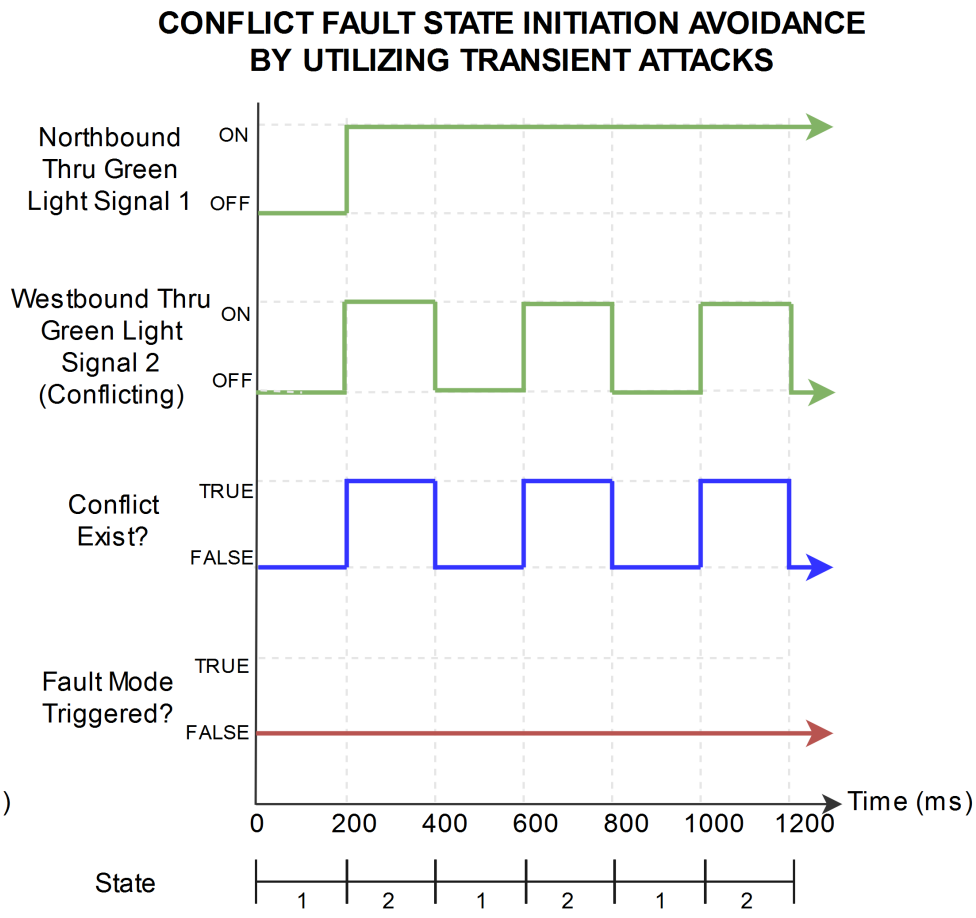
Bypass Fail-Safe Components

WAYNE STATE UNIVERSITY

- With remote only access, we are not able to bypass the fail-safe components completely.
- We design a transient avoidance tactic to fight the fail-safe components.

Transient Avoidance Tactic





Security Analysis

WAYNE STATE UNIVERSITY

How to attack the traffic signal system?

- Step 1 – Access the Traffic Signal System
- Step 2 – Control the Traffic Signals
- Step 3 – Bypass Fail-Safe Components
- Step 4 – Hide Yourself

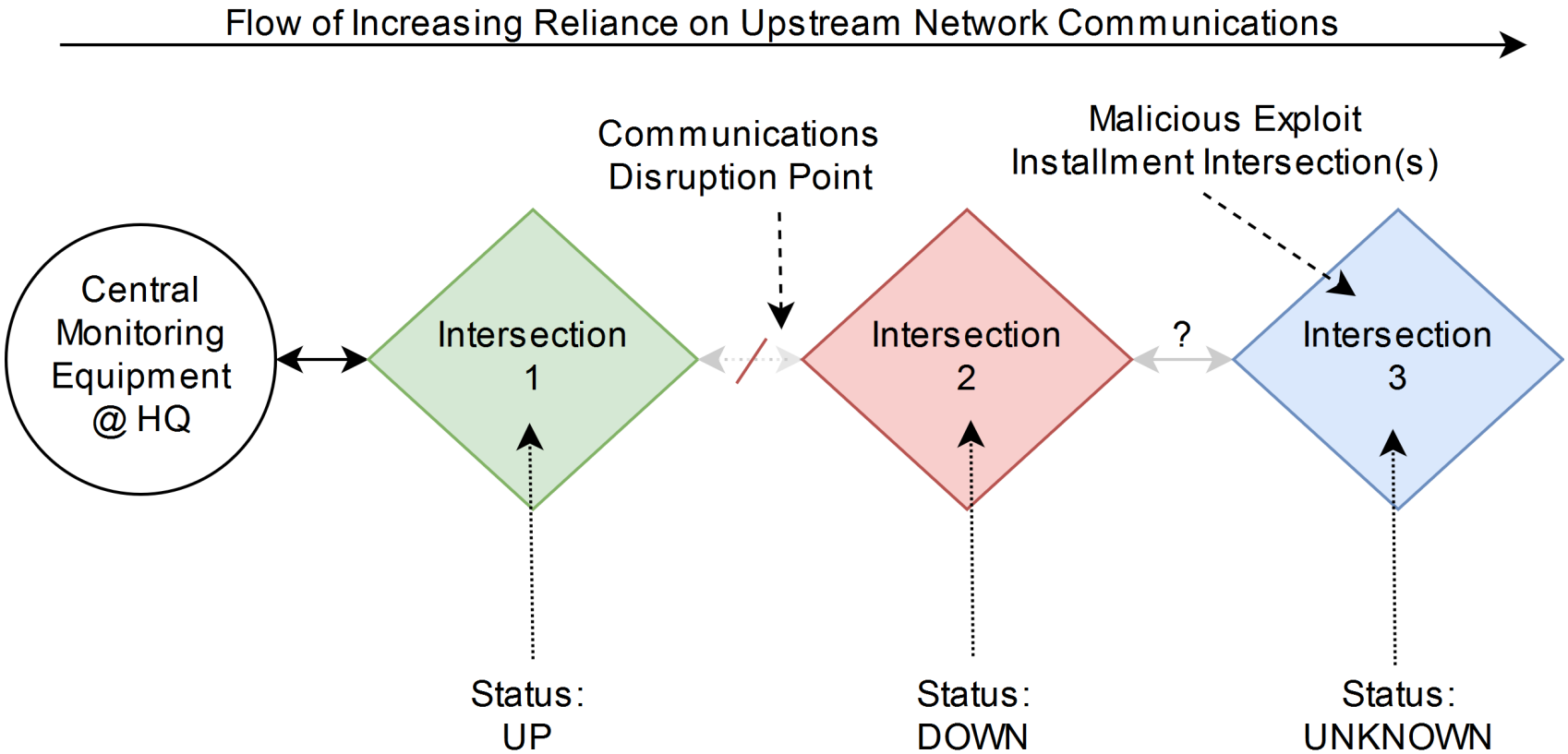
Traffic Network

WAYNE STATE UNIVERSITY

According to the municipality officials,

- Due to the geography that must be covered, the deployed traffic network are generally linear in communication flows.
- Redundant protocols are not used due to extra cost of additional equipment.
- Troubleshooting process of the traffic system mainly focus on the down point.

Diversionary Tactic

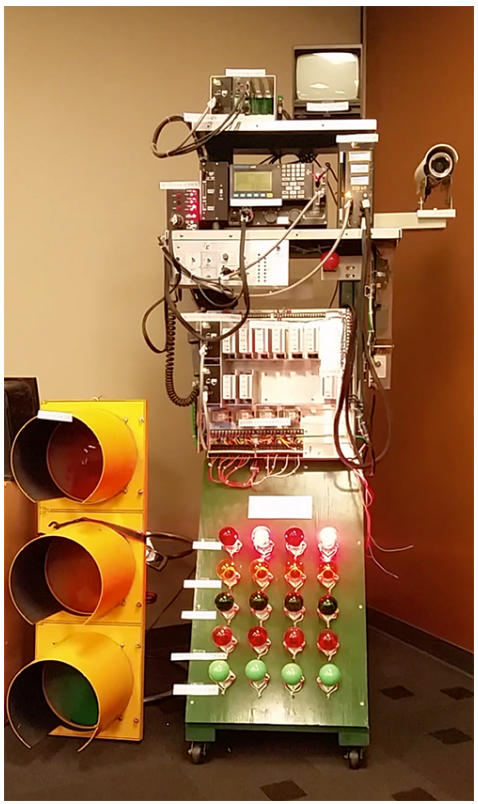


Outline

WAYNE STATE UNIVERSITY

- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

Attacks and Mitigations



Test environment in the municipality lab and our lab

Attack Scenarios

WAYNE STATE UNIVERSITY

- Stealthy Manipulation and Control
  - Stealthy control the traffic signal to introduce congestion.
- Ransomware Deployment
  - Change login credentials and lock ATC block startup process.
- All-Direction Green Lights
  - Transient avoidance tactic helps to make green light flashing.
  - Increase the flicker frequency to introduce optical illusion.

Recurrent Pulse Detection

WAYNE STATE UNIVERSITY

The Recurrent Pulse Detection (RPD) looks for voltage leaks lasting 1ms to 200ms and triggers a conflict state if a certain criteria level is met.

- In a certain time window, the duration of green light is cumulative.
- In practice, 24ms green light on-time with 17ms off-time will bypass the RPD.

Mitigations

WAYNE STATE UNIVERSITY

- Avoid default password and master key.
- The design should put security in mind.
  - Secure communication
  - Encrypted configuration
- Open access to the related software and specification with strict verification.

Outline

WAYNE STATE UNIVERSITY

- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

Conclusion

WAYNE STATE UNIVERSITY

- We present a comprehensive vulnerability analysis of the traffic signal system and identify a number of vulnerabilities.
- Attackers can conduct a variety of attacks including all-direction green lights to the traffic system.
- More attention should be paid to the security threats in the transportation community.

References I

[1] C. Cerrudo, "Hacking US (and UK, Australia, France, etc.) traffic control systems," 2014.

[2] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in Proceedings of 25th Network and Distributed System Security Symposium (NDSS'18), 2018.

[3] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT'14), 2014.

[4] Shodan, "Search engine for Internet-connected devices," https://www.shodan.io/.

Thank you!

WAYNE STATE UNIVERSITY

Questions?

{zhenyu.ning}@wayne.edu

http://compass.cs.wayne.edu